Cyber Incident Threat Response Intelligence Report

Prepared for AR Billing Company LLC

By

Anthony Sullivan

5/13/2018

FOR OFFICIAL USE ONLY

This page intentionally blank

Executive Summary

Imagine an underwater mine field, your ship must transit the choke point; you know Advanced Persistent Threats (APT) exist, but you cannot see them. Modern software, particularly health information processing software use 80% to 90% third party Code Libraries, Open Source Databases, Dynamic Link Libraries and Open Source Web Services. The application specific code written is between 10% – 20% of the total software payload stack. The payload stack will usually include platform specific server software of which you have little to no code control or visibility. Without visibility the ability to remediate or protect against flaws both known and unknown using commercially available scanning and compliance tools is next to impossible. So just how pervasive is the problem? *Black Duck*, a major testing vendor published a report in April 2017 reinforcing just how pervasive the use of open source code has become in modern software architecture. Consider that 96% of the more than 1,000 commercial applications scanned contained open source components. 67 % of applications have known open source code vulnerabilities. On an average of 27 flaws per application found, slightly more than half of those flaws, 52% had a "High Severity" CVSS score.

On March 12tht 2018, AR Billing called to ask for help with their health information technology system. End-users were complaining that the servers were running very slow, endpoint work stations were experiencing dramatic application response latency. VoIP system experienced drop outs, requiring multiple system initializations throughout the day. The decision was mad to conduct an immediate Cyber Security Health checkup utilizing the *FortiGuard* Security Solution. Deployment of FortiGuard *Advance Threat Intelligence* client, revealed vulnerability, on the \\INTERGYSERVER that other products such as Malwarebytes, ESET and Symantec Endpoint Protection did not detect. The Greenway Health Intergy EMR software was flagged as non-compliant by the FortiClient Telemetry and Compliance client on *\\INTERGYSERVER*. Analysis of FortiGate traffic and Windows Event 4625 Audit Failures provided the initial insight into a suspected XTunnel on Port Zero that might be performing "Reconnaissance" and establishing a persistent Command and Control (C2) capability. It is verified that the APT has had a persistent presence since September 13th 2016, initial entry gained by exploiting a level 10 elevated privileges security flaw in the exceptionally vulnerable PostgreSQL 8.3.2 database. Without the FortiClient Telemetry and Compliance agent, we would of never known that Intergy used the PostgreSQL 8.3.2 database.

Greenway Health Intergy EMR uses the Postgres Database version 8.3.2. for imaging. This version has multiple vulnerabilities, the level 10 vulnerability allows an attacker to elevate privileges and when installed on a domain control gives the Postgres user Domain Admin rights by default. This automatically allows the user "Postgres" remote desktop access with Domain Admin rights. After figuring out that the user *Postgres@INTERGY.LOCAL* had admin right on remote desktop server *\\APOLLO.INTERGY.LOCAL* , the profile was scrutinized for anomalies and suspicious activity. Hidden folders and files of a malicious nature located at C:\users\postgres\desktop were found. The ability to install Intergy EMR on a domain controller should be disabled via an installation script immediately, so as to prevent innocent customers from installing the Intergy EMR software on a domain controller. *Greenway Health* has known about this CRITICAL SECURITY issue *CVE-2013-1903*since April 4th 2013..

Confidence is HIGH that malware is being used to create super massive global Mobile Ad-hoc Networks (MANET), networks with 500,000 BOTs or more. It is exceptionally difficult to track MANET infrastructure that can be used by various OP Net Campaigns conducted by "Advanced Persistent Threats". Infected MANET nodes can be owned by legitimate businesses or individuals, making it easy to incorrectly attribute malicious activity to a particular device. There is no real way for the public commercial user to tell the difference between victims and an APT.

Confidence is HIGH that a specialized packet sniffer C2 communication plugins allows the malware to communicate over Tor with C2 servers. There appears to be special capabilities built into the sniffer plugins of this malware possibly enabling the APT to take advantage of phones, routers, and devices from anywhere anytime. We are noticing very suspicious Android/Apple reconnaissance for Apple key values in the FortiGuard logged blocked events

Confidence is HIGH that BUSYBOX and AppleScript Encrypted C2 communications are taking place on Port Zero through an XTunnel. Tor module may be linked to lateral exploits designed to enhance a persistent presence on the network. The Tor module may also be linked to hijacking web publishing services. IIS wwwroot configuration changed to enable FTP and FAKE Site Certificate services.

Confidence is HIGH that the SLINGSHOT malware infected the Mikrotik VoIP router, the device was then used to conduct reconnaissance and detect devices on the Spectrum.net Enterprise Biz Network for straightforward data-collection purposes. Reconnaissance of the discovered network devices provides the APT insight into the value of the network and the devices it serves.

Confidence is HIGH that the APT deemed the AR Billing network a high value target containing ePHI, and chose to continue collecting content that passes through the device exploiting the Intergy database with SQL-Injection.

Confidence is HIGH that this APT has used BUSYBOX to implement a KILL COMMAND that can be used for a Cyber Armageddon. Imagine millions of routers smoke checked remotely from a Tor C2 Server..

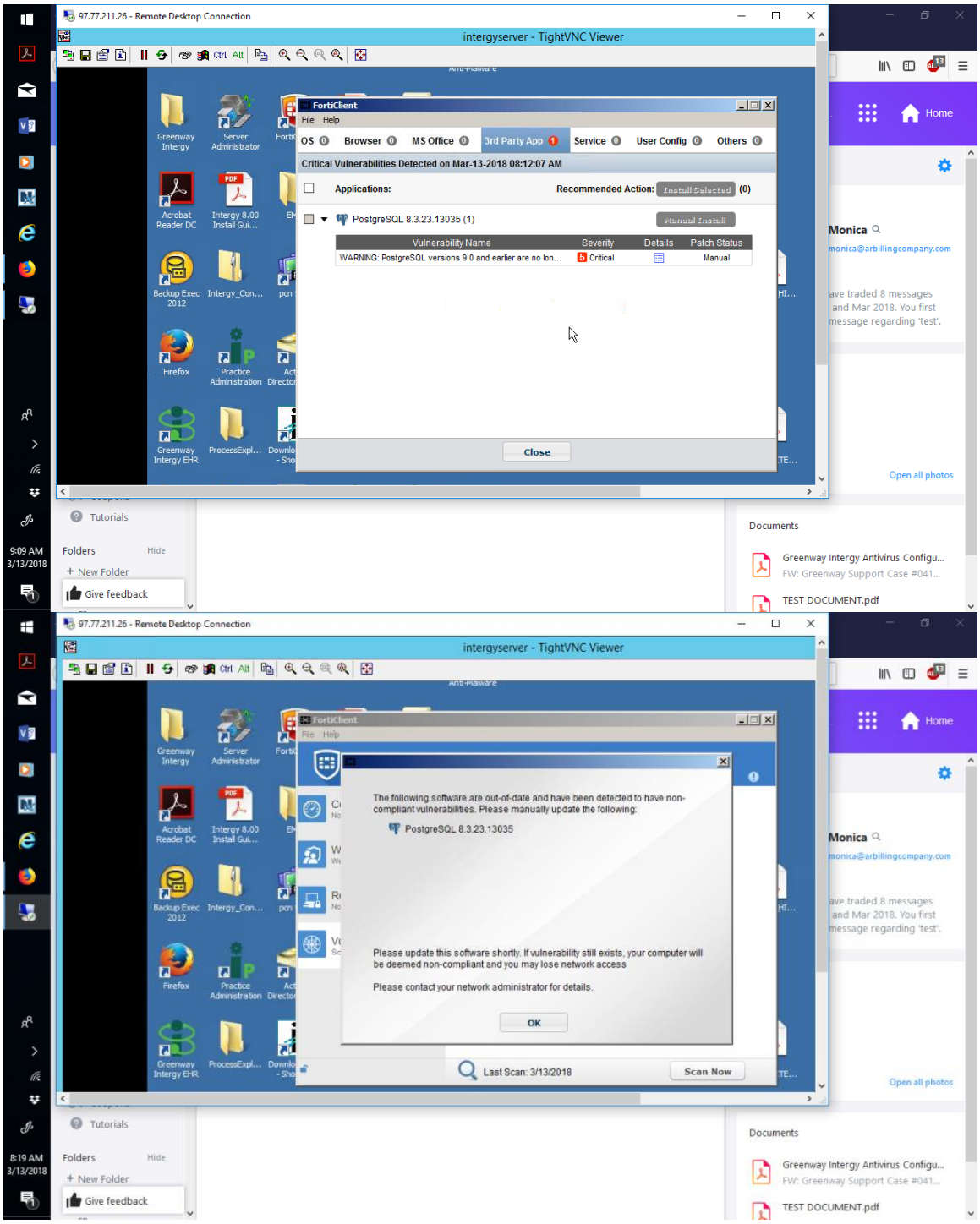
Confidence is HIGH that the APT has penetrated the new server already, found the DIAL Server service installed on the 16th of May, permanently blocked port zero and removed DIAL Server, we are going to need to deploy a HONEY Pot.

The Combatant's Actions and Tactics

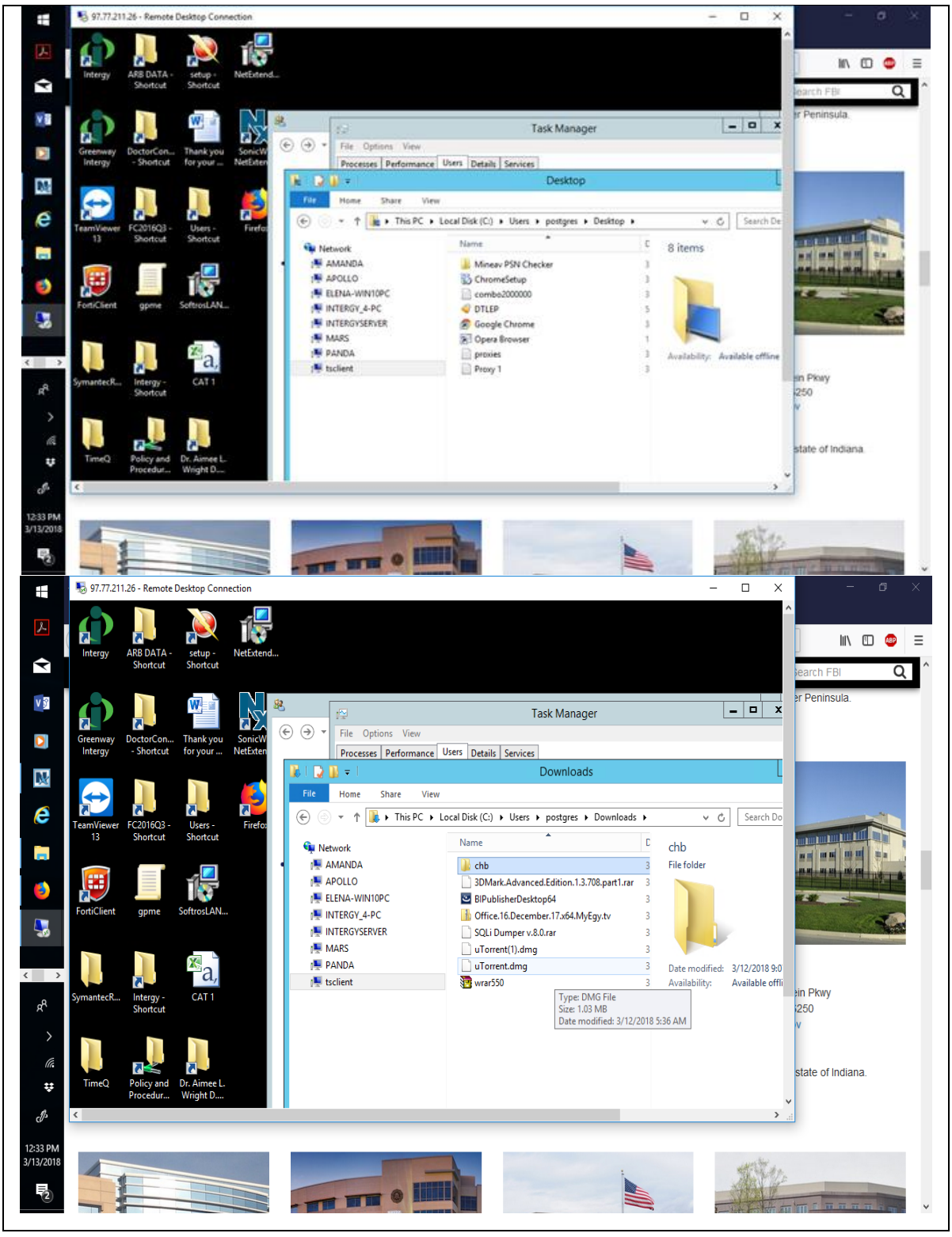
Analysis of Fortclient Telemetry and Compliance data provided a starting point into the unusual remote desktop activities of user *postres@Intergy.local*. The Forticlient blocked access to various pornographic sites and provided the location of suspicious folders and files. The FortiGuard flagged a new domain as suspicious; the server is located in Kazakhstan. The suspicious domain *Horux.kz* was interacting with Sexdumps.net, logs show an association with *CVV Dumps* at *Sexdumps*. *(CVV dump sites used for buying, selling or trading of credit card and identity information.)* Drilled down on Terminal Server *\\APOLLO.INTERGY.LOCAL* C:\User\Postgres\ with –h (Hidden) folder attribute removed, this allowed me to view, capture and analyze a rogue

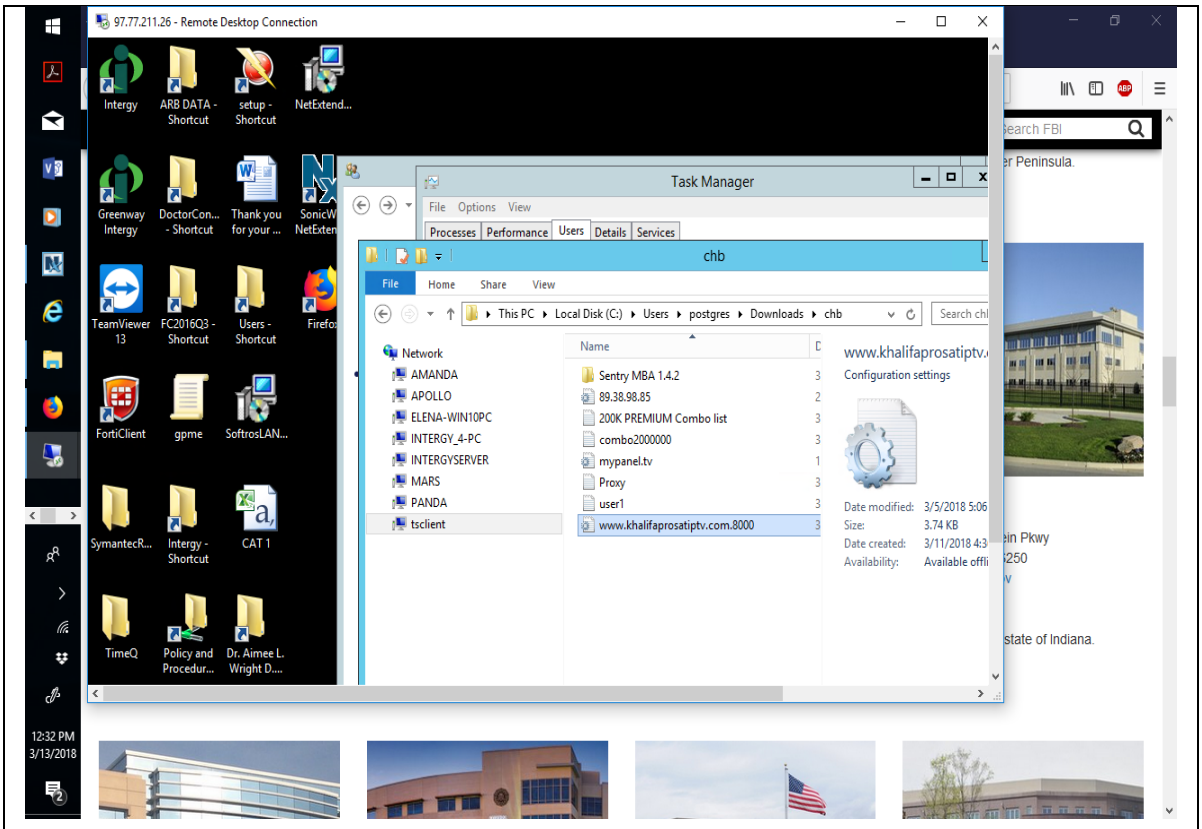
generic improved Trojan named Sentry_MBA.exe 1.4.2, developed by *Cracking Core*, provided by *Sentry MBA*, and exploited via Crackwebsite BlogSpot. Upon seeing the "Combo2000000" and PSN Checker bundled with the Desk Top Lock Express, immediately knew that something was up.

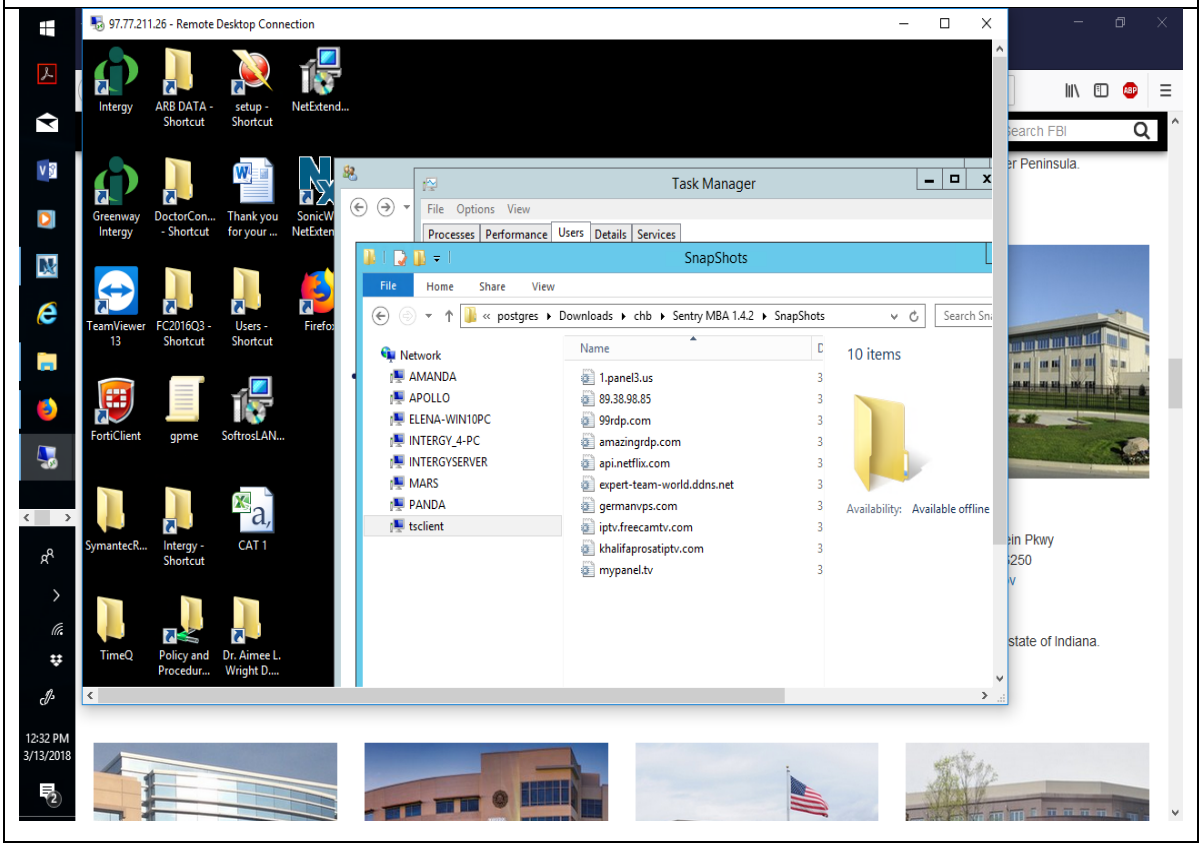
Upon further investigation and reverse engineering *Sentry_MBA.exe*, *DCMTK.dll*, *ISISLibrary.DLL*, and *DTLEP.exe*, it was discovered that the DCMTK Dynamic Link Library and Sentry_MBA.exe are customized and modified "Portable Executables" for process injection. .(The Portable Executable (PE) format is a file format for executables, object code, DLLs, FON Font files, and others used in 32-bit and 64-bit versions of Windows operating systems. The PE format is a data structure that encapsulates the information necessary for the Windows OS loader to manage the wrapped executable code.)


97.77.211.26 - Remote Desktop Connection
intergyserver - TightVNC Viewer
FortiClient
File Help
OS 0 Browser 0 MS Office 0 3rd Party App 1 Service 0 User Config 0 Others 0
Critical Vulnerabilities Detected on Mar-13-2018 08:12:07 AM
Applications:
Recommended Action:
Install Selected (0)
PostgreSQL 8.3.23.13035 (1)
Manual Install
Vulnerability Name
Severity
Details
Patch Status
WARNING: PostgreSQL versions 9.0 and earlier are no lon...
Critical
Manual
Close
Greenway Intergy
Server Administrator
Acrobat Reader DC
Intergy 8.00 Install Gui...
Backup Exec 2012
Intergy_Con...
Firefox
Practice Administration
Greenway Intergy EHR
ProcessExpl...
Tutorials
Folders
Hide
New Folder
Give feedback
9:09 AM
3/13/2018
Home
Monica
Open all photos
Documents
Greenway Intergy Antivirus Configu...
FW: Greenway Support Case #041...
TEST DOCUMENT.pdf
97.77.211.26 - Remote Desktop Connection
intergyserver - TightVNC Viewer
The following software are out-of-date and have been detected to have non-compliant vulnerabilities. Please manually update the following:
PostgreSQL 8.3.23.13035
Please update this software shortly. If vulnerability still exists, your computer will be deemed non-compliant and you may lose network access
Please contact your network administrator for details.
OK
Last Scan: 3/13/2018
Scan Now
8:19 AM
3/13/2018

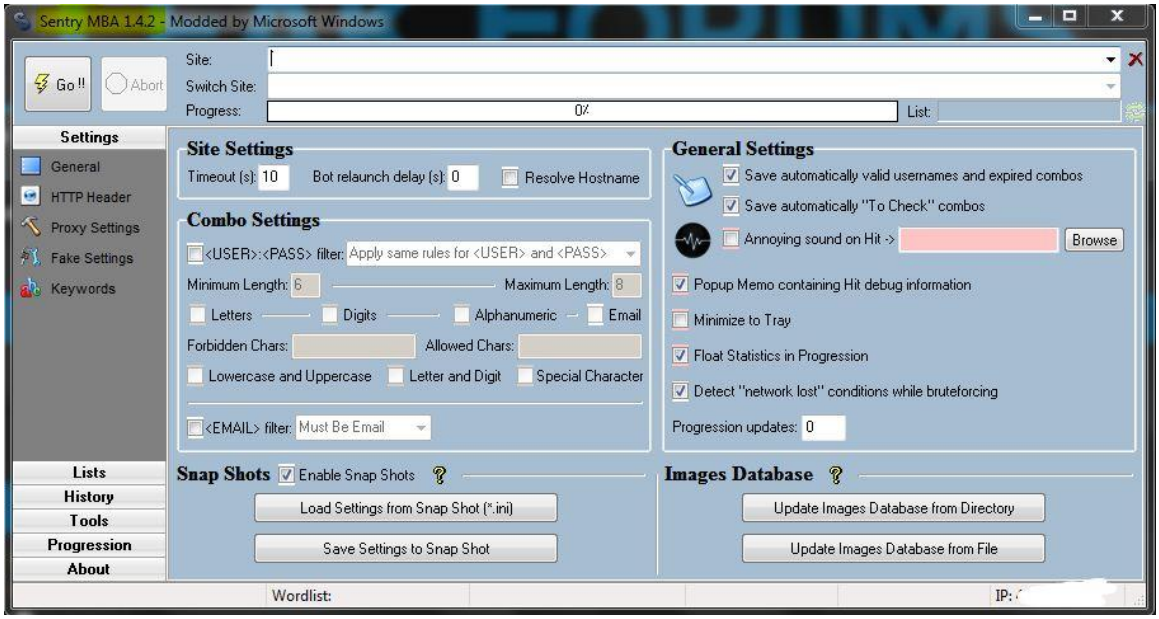
Postgres user file and folder analysis




97.77.211.26 - Remote Desktop Connection
Task Manager
File Options View
Processes Performance Users Details Services
chb
File Home Share View
This PC ▸ Local Disk (C:) ▸ Users ▸ postgres ▸ Downloads ▸ chb
Network
AMANDA
APOLLO
ELENA-WIN10PC
INTERGY_4-PC
INTERGYSERVER
MARS
PANDA
tsclient
Name
Sentry MBA 1.4.2
89.38.98.85
200K PREMIUM Combo list
combo2000000
mypanel.tv
Proxy
user1
www.khalifaprosatiptv.com.8000
Configuration settings
Date modified: 3/5/2018 5:06
Size: 3.74 KB
Date created: 3/11/2018 4:3
Availability: Available offli
Intergy
ARB DATA - Shortcut
setup - Shortcut
NetExtend...
Greenway Intergy
DoctorCon... - Shortcut
Thank you for your ...
SonicW NetExten
TeamViewer 13
FC2016Q3 - Shortcut
Users - Shortcut
Firefox
FortiClient
gpme
SoftrosLAN...
SymantecR...
Intergy - Shortcut
CAT 1
TimeQ
Policy and Procedur...
Dr. Aimee L. Wright D....
12:32 PM
3/13/2018


97.77.211.26 - Remote Desktop Connection
Task Manager
File Options View
Processes Performance Users Details Services
SnapShots
File Home Share View
« postgres ▸ Downloads ▸ chb ▸ Sentry MBA 1.4.2 ▸ SnapShots
Network
AMANDA
APOLLO
ELENA-WIN10PC
INTERGY_4-PC
INTERGYSERVER
MARS
PANDA
tsclient
Name
1.panel3.us
89.38.98.85
99rdp.com
amazingrdp.com
api.netflix.com
expert-team-world.ddns.net
germanvps.com
iptv.freecamtv.com
khalifaprosatiptv.com
mypanel.tv
10 items
Availability: Available offline
Intergy
ARB DATA - Shortcut
setup - Shortcut
NetExtend...
Greenway Intergy
DoctorCon... - Shortcut
Thank you for your ...
SonicW NetExten
TeamViewer 13
FC2016Q3 - Shortcut
Users - Shortcut
Firefox
FortiClient
gpme
SoftrosLAN...
SymantecR...
Intergy - Shortcut
CAT 1
TimeQ
Policy and Procedur...
Dr. Aimee L. Wright D....
12:32 PM
3/13/2018

Sentry MBA 1.4.2



The Sentry MBA 1.4.2 tool works by exploiting proxies to conduct attacks utilizing a combination list of credentials with a configuration file that relates to the target of interest.

The tool is very easy to use and draws information from three data sources to mount a devastating attack: a configuration file to align the attack to a specific target of interest; a "combo list" (list of valid usernames and passwords) and a list of proxies from which to relay the attack. The configuration files tells the tool how to attack a specific website; combo and config lists, which contain user credentials for websites that are traded and sold on hacker forums for Bitcoins. For a brute force attack to take place, a large combo list (500,000+ credentials), a config file and proxy configured for multiple tries so as to not get blocked. Since attacker is not brute forcing the same user account, there will never be a locked account. Combo list credentials will be valid somewhere while the config file will tell the tool how a website handles login requests, understand what captcha is running and know how many requests per proxy should be attempted. When a good config file is used it can be almost impossible to distinguish the attacks from legitimate login requests which make Sentry MBA very hard to detect, and defend against.

The most popular config files are login details for Netflix, Instagram and 'Universal Email Access Checker', with hundreds of downloads of each. The tool was substantiated by *SecureWorks* researcher Rafe Pilling, who told *Infosecurity* that by using Sentry MBA attackers will not target specific websites, but will select a list of targets opportunistically. He explained that credentials are collected from Pastebin and credential dumps, and the config file is needed to know where to put credentials on a website and let you know if you've logged in successfully or not. He said that the config file will show the tool where the username and password fields are, but he doubted that an average user could use or write a config file. "SentryMBA is like having a missile, but without the targeting information (the config) it wouldn't be as useful,"

Infosecurity suggested that Sentry MBA can be used two ways: with or without configs. It suggested that as Sentry MBA is a very robust tool, it can crack a handful of different authentication types and it is pretty powerful at determining fakes or hits. This requires a lot of information to get started on a site. "Sentry MBA if configured correctly, can determine when there is a fake response from the server - saving you time when cracking", *Infosecurity* said. Looking at the guides presented online, Pilling said that it was fairly obvious that those involved in distributing it "were not well versed in OPSEC and give away too much", and SecureWorks were able to identify one user easily. He said: "We are not talking super skilled individuals, but tool which if you configure it and get data and [you have] got a process that works. It does not require a deep understanding of it as proxy IPs will tell you if it is working or not."

Small sample of key captures on APOLLO.INTERGY.LOCAL

http://derin:derin@1.panel3.us|51.15.51.90:80|Success Source Keyword Match -> Found Key [LOGOUT] - Source Length: 56505||6q6FFt5coPabbVur6nxo|152223|0|||||1520704066|0||3||||0||||||

http://gence:gence@1.panel3.us|54.152.76.89:80|Success Source Keyword Match -> Found Key [Logout] - Source Length: 12527||UEdZd9ExDor6cep7NWO9|152223|0||PHPSESSID=f8jaad639lcoho5i8fepnauto0|||1520704067|0||3|||0||||||

http://dilim:dilim@1.panel3.us|52.71.88.214:80|Success Source Keyword Match -> Found Key [LOGOUT] - Source Length: 60359||gfWG6insmKmeabelsf1A|152223|0|||||1520704067|0||3||||0||||||

http://borte:borte@1.panel3.us|80.211.12.76:80|Success Source Keyword Match -> Found Key [LOGOUT] - Source Length: 56064||5MKusx7YI4DvZB04KtH7|152223|0|||||1520704073|0||3||||0||||||

http://tarlig:tarlig@1.panel3.us|82.146.38.42:80|Success Source Keyword Match -> Found Key [LOGOUT] - Source Length: 56184||1AMKmsv8vbSgRU8WhMhD|152223|0|||||1520704076|0||3||||0||||||

http://enis:enis@1.panel3.us|85.143.221.104:80|Success Source Keyword Match -> Found Key [LOGOUT] - Source Length: 69359||UzhgVh7xcgCoxuNxPUyi|152223|0|||||1520704077|0||3||||0||||||

http://tavli:tavli@1.panel3.us|91.121.110.111:80|Success Source Keyword Match -> Found Key [LOGOUT] - Source Length: 62333||5pwkHdXFZT89EJc37JUt|152223|0|||||1520704079|0||3||||0||||||

http://amir:amir@89.38.98.85|45.77.95.91:8080|After Form Redirect -> Success Source Keyword Match -> Found Key [>Expire Date:<] - Source Length: 1853567 - Found data to capture: Lupoto Expire Date: 27/02/2019 17:23||t2AJ4Ozc23kXRtlzkt5j|152223|0|Lupoto Expire Date: 27/02/2019 17:23|PHPSESSID=nkdsuq7rl7u4lqslh9pc8vl8jl|||1520706082|0||3||||0||||||

http://kader:kader@89.38.98.85|27.111.43.178:8080|After Form Redirect -> Success Source Keyword Match -> Found Key [>Expire Date:<] - Source Length: 1858064 - Found data to capture: Lupoto Expire Date: 08/06/2018 16:05||Q2exUwCBsbQeNnYxxKxl|152223|0|Lupoto Expire Date: 08/06/2018 16:05|PHPSESSID=lqkbp71nfnmvkqq1s5fjdi1r88|||1520706566|0||3||||0||||||

http://designer:designer@89.38.98.85|80.211.231.39:3128|After Form Redirect -> Success Source Keyword Match -> Found Key [>Expire Date:<] - Source Length: 1035360 - Found data to capture: Lupoto Expire

Date: 03/11/2018 23:26||J5UkDyPtApWMfU4Zf2tT|combo2000000|0|Lupoto Expire Date: 03/11/2018 23:26|PHPSESSID=k3t1jb2uskgv21eu68mgmdvc38|||1520767942|0||3||||0||||||

http://Sham1:Sham1@89.38.98.85|205.204.85.19:3128|After Form Redirect -> Success Source Keyword Match -> Found Key [>Expire Date:<] - Source Length: 941700 - Found data to capture: Lupoto Expire Date: 25/02/2019 16:56||Qnq5Ynws3S1tQBjxAEfg|combo2000000|0|Lupoto Expire Date: 25/02/2019 16:56|PHPSESSID=smdub2hqtc6ssdjhla803c39qi|||1520768374|0||3||||0||||||

http://sham1:sham1@89.38.98.85|80.211.5.160:8888|After Form Redirect -> Success Source Keyword Match -> Found Key [>Expire Date:<] - Source Length: 5556 - Found data to capture: Lupoto Expire Date: 25/02/2019 16:56||V77zakT02Hfx3UBjZQjj|combo2000000|0|Lupoto Expire Date: 25/02/2019 16:56|PHPSESSID=pg23m8q3hutemugse6i2gcsv1r|||1520769064|0||3||||0||||||

http://Aran1:Aran1@89.38.98.85|54.36.163.157:3128|After Form Redirect -> Success Source Keyword Match -> Found Key [>Expire Date:<] - Source Length: 758632 - Found data to capture: Lupoto Expire Date: 04/11/2018 00:13||neu4dqq8nAGP2xfCxsBC|combo2000000|0|Lupoto Expire Date: 04/11/2018 00:13|PHPSESSID=7q777ahm35jujmaa59148p1h20|||1520769871|0||3||||0||||||

http://arab1:arab1@89.38.98.85|212.237.61.210:8888|After Form Redirect -> Success Source Keyword Match -> Found Key [>Expire Date:<] - Source Length: 689528 - Found data to capture: Lupoto Expire Date: 15/12/2018 20:30||2ZfdRA5tuOkrKZsDVr72|combo2000000|0|Lupoto Expire Date: 15/12/2018 20:30|PHPSESSID=usum3v3kianf4rh3pi6k90rdnb|||1520770521|0||3||||0||||||

http://azmir:azmir@89.38.98.85|94.23.2.157:3128|After Form Redirect -> Success Source Keyword Match -> Found Key [>Expire Date:<] - Source Length: 814884 - Found data to capture: Lupoto Expire Date: 08/01/2019 18:23||mOGD9KRw30mbVbA42NEU|combo2000000|0|Lupoto Expire Date: 08/01/2019 18:23|PHPSESSID=ged5vcocltb244hrgud51v7k4b|||1520771430|0||3||||0||||||

SQLiDumper v.8.0

This tool is more powerful than the famous *Havij SQL injection*, an automatic SQL Injection tool, distributed by *ITSecTeam*, an Iranian security company. A grand jury in the Southern District of New York indicted seven Iranian individuals who were employed by two Iran-based computer companies, ITSecTeam (ITSEC) and Mersad Company (MERSAD), that performed work on behalf of the Iranian Government, including the Islamic Revolutionary Guard Corps, on computer hacking charges related to their involvement in an extensive campaign of over 176 days of distributed denial of service (DDoS) attacks.

Ahmad Fathi, 37; Hamid Firoozi, 34; Amin Shokohi, 25; Sadegh Ahmadzadegan, aka Nitrojen26, 23; Omid Ghaffarinia, aka PLuS, 25; Sina Keissar, 25; and Nader Saedi, aka Turk Server, 26, launched DDoS attacks against 46 victims, primarily in the U.S financial sector, between late 2011 and mid-2013. The attacks disabled victim bank websites, prevented customers from accessing their accounts online and collectively cost the victims tens of millions of dollars in remediation costs as they worked to neutralize and mitigate the attacks on their servers. In addition, Firoozi is charged with obtaining unauthorized access into the Supervisory Control and Data Acquisition (SCADA) systems of the Bowman Dam, located in Rye, New York, in August and September of 2013.

The name Havij means “carrot”, which is the tool’s icon. The tool is designed with a user-friendly GUI that makes it easy for an operator to retrieve the desired data. Such ease of use may be the reason behind the transition from attacks deployed by code-writing hackers to those by non-technical users.

Havij was published during 2010, and since its, release several other automatic SQL Injection tools (such as sqlmap) were introduced. However, Havij is still active and commonly used by both penetration testers and low level hackers.

SQLiDumper v.8.0 has many features including:

Supports Multi. Online search engine (to find the trajects);

-Automated exploiting and analyzing from a URL list;

-Automated search for data in a bulk URL list;

-Automated analyzer for injections points using URL, POST, Cookies, UserLogin or UserPassword;

-Dumper supports dumping data with multi-threading (databases/tables/columns/fetching data);

-Exploiter supports up to 100x threads;

-Analyzer and Dumper supports up to 50x threads;

-Advanced WAF bypass methods;

-Advanced custom query box;

-Dumper can dump large amounts of data, with greats control of delay each request (multi-threading);

-Easy switch vulnerabilities to vulnerabilities;

-Supports proxies list;

-GeoIP database;

-Internal database;

-Trash System;

-Admin login finder;

-Hash online cracker;

-Reverse IP;

-Standalone .exe (no install).

The SQL Injection Methods that are supported include:

MySQL

Union (Integer / String)

Error (Integer / String)

** Error Methods:

GET_HOST_ADDRESS

DRITHSX.SN

GET;APPINGXPATH.

Double Query

XPATH – ExtractValue

XPATH – UpdateXML

Brute Forcing

Blind

Load File

Load File Scanner

** Illegal Mix Of Collations:

UnHexHex()

Binary()

Cast As Char

Compress(Uncompress())

Convert Using utf8

Convert Using latin1

Aes_decrypt(aes_encrypt())

MS SQL

Union (Integer / String)

Error (Integer / String)

SQL_Latin1;

Cast As Char.

Oracle

Union (Integer / String)

Error (Integer / String)

Cast As Char.

** Supports TOP N Types:

ROWUM

RANK()

DESE_RANK()

** Analyzer detects also:

MS Access

PostgredSQL

Sybase

Use this dork in a dork scanner:

To use its dork scanner feature for a specific website, not a random search.

.aspx? & site:samplesite.com

.php? & site:samplesite.com

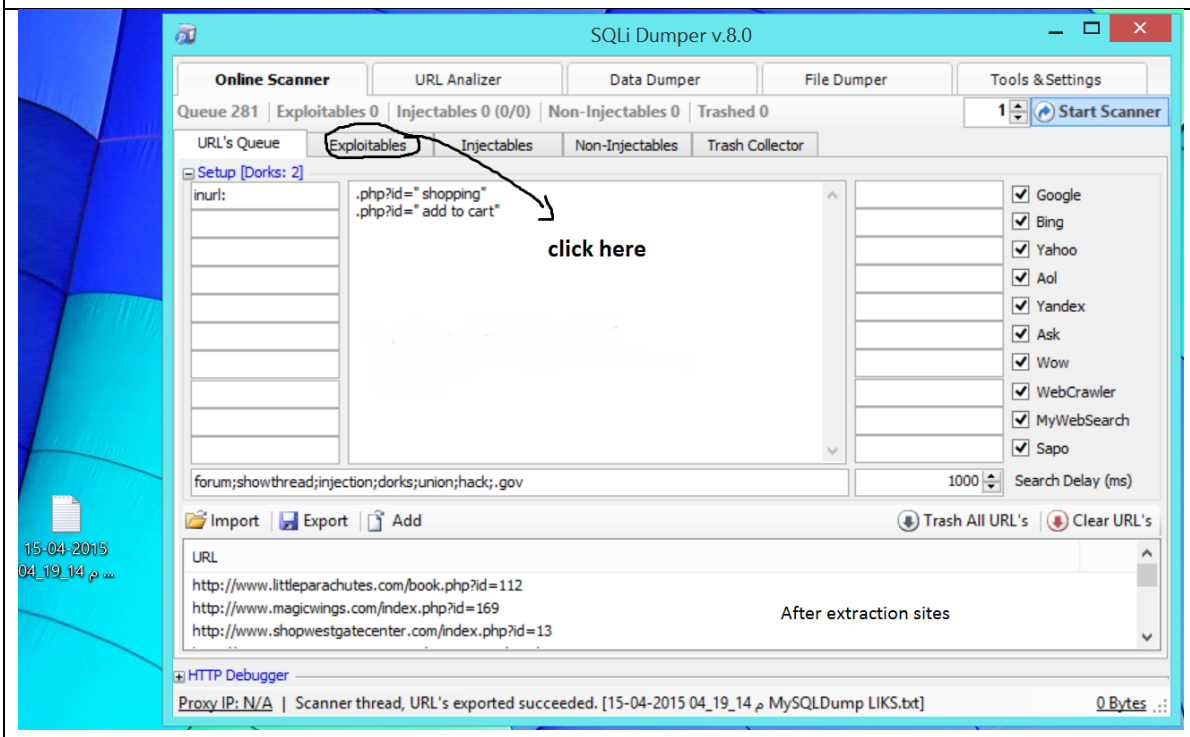
.asp? & site:samplesite.com

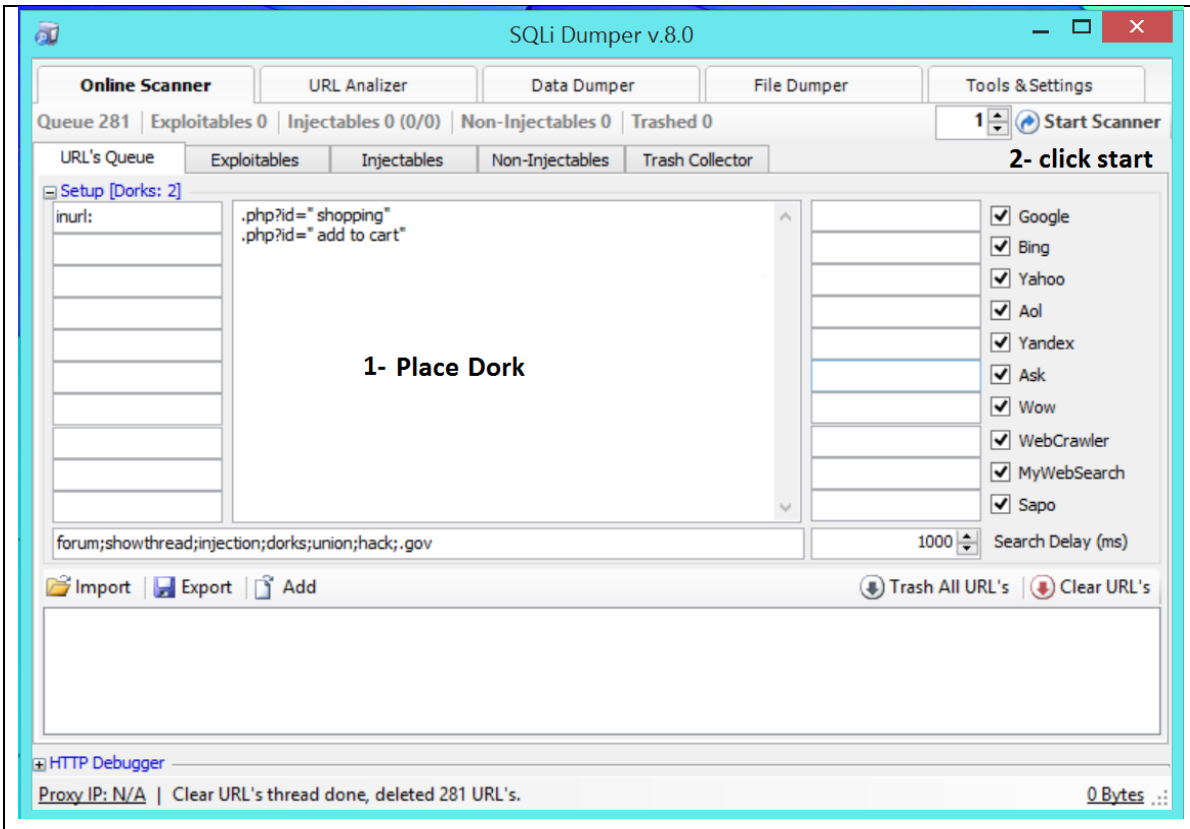
.pl?   & site:samplesite.com

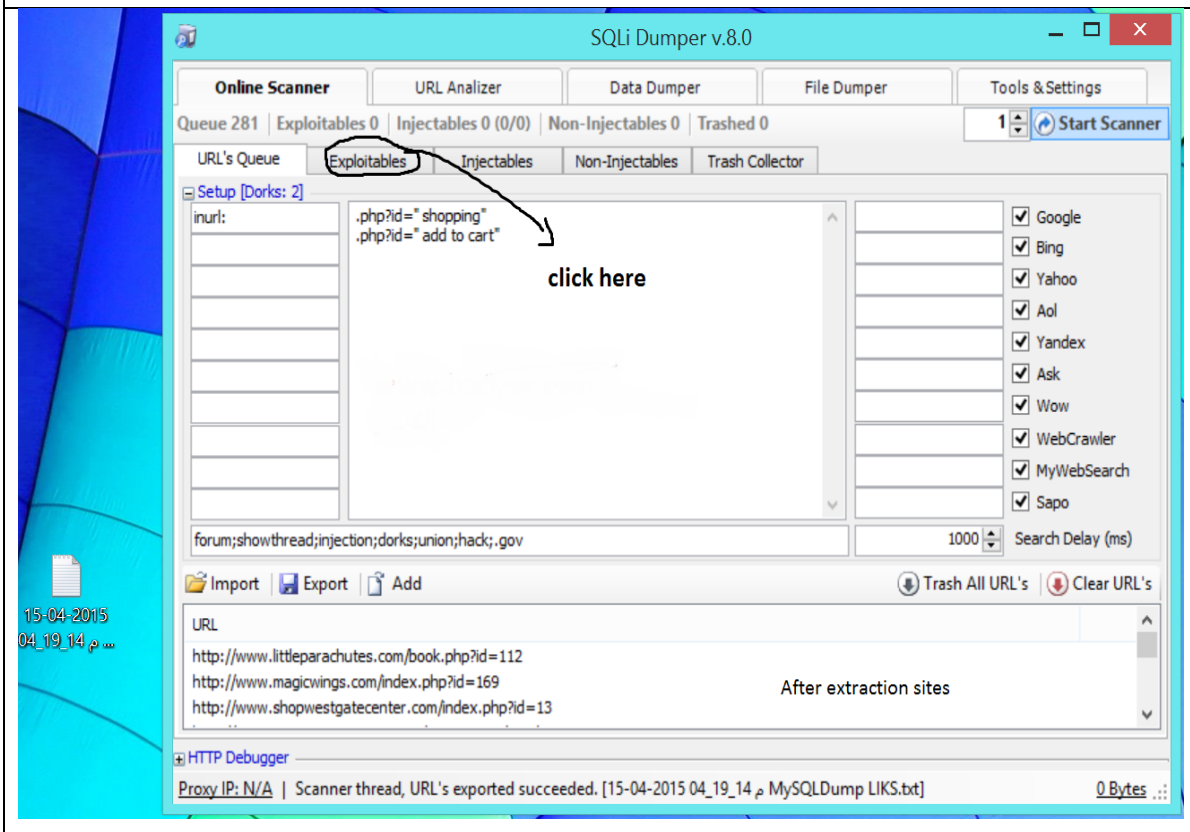
.jsp? & site:samplesite.com

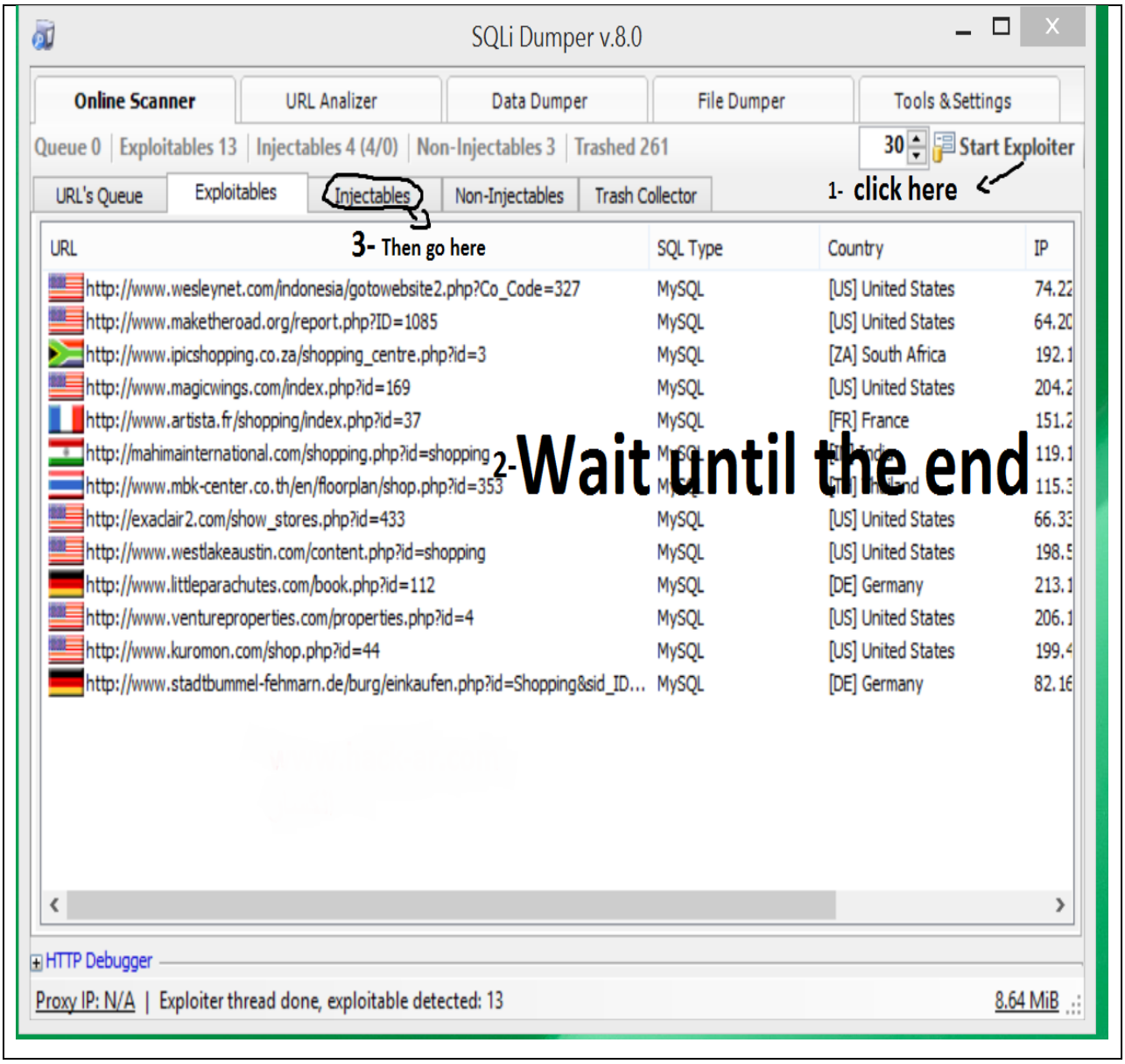
And, it simply fetches the links and automatically scans for SQL injection in those links.

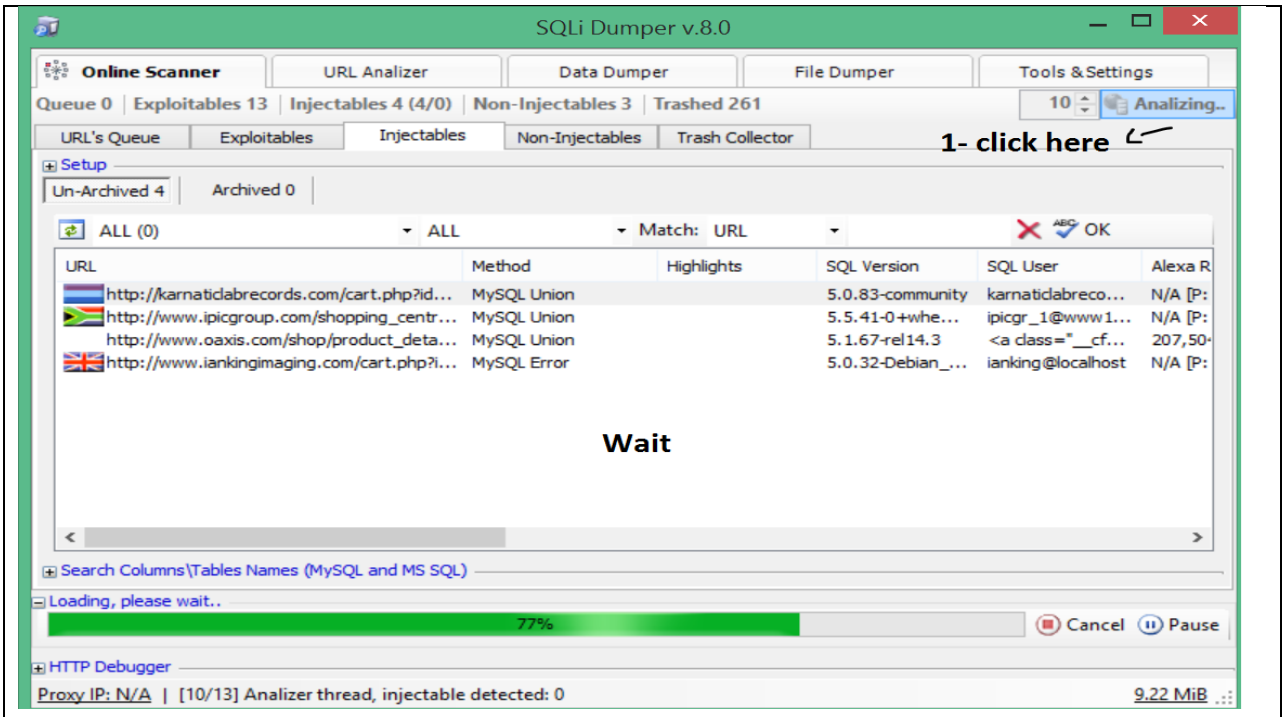
How to screenshots SQLiDumper V.8.0

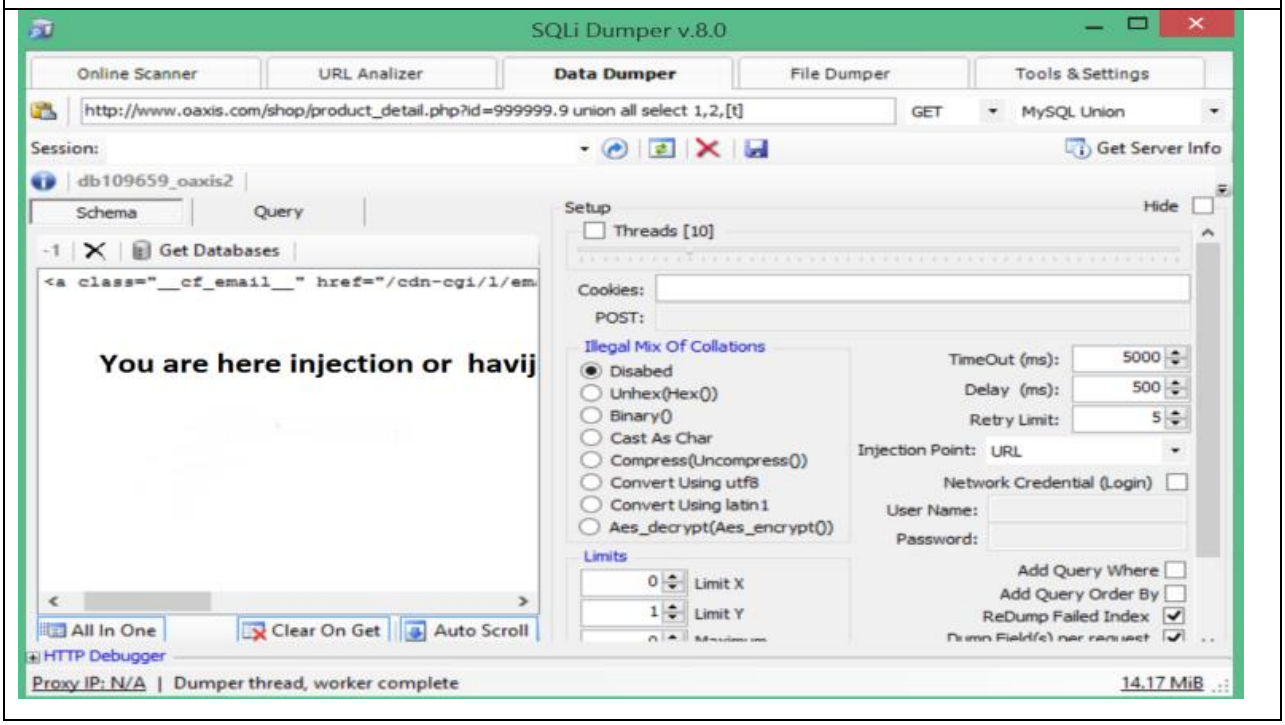


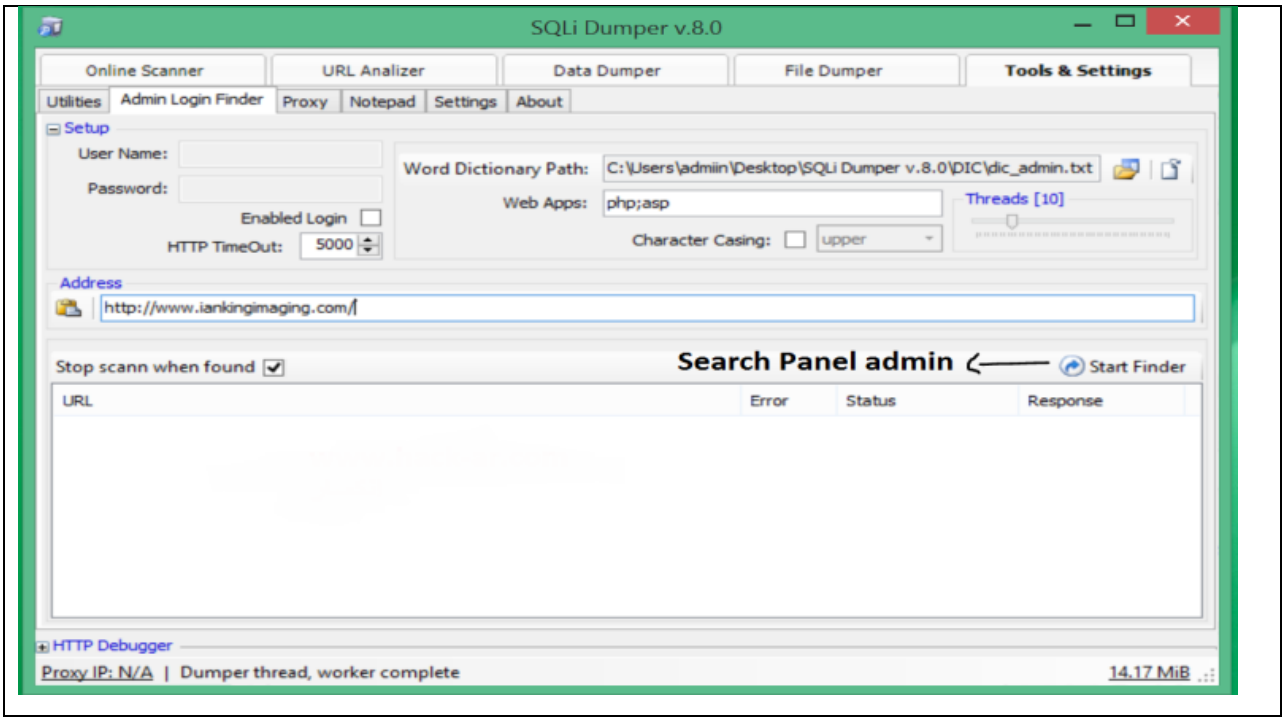

SQLi Dumper v.8.0
Online Scanner
URL Analizer
Data Dumper
File Dumper
Tools & Settings
Queue 281 | Exploitables 0 | Injectables 0 (0/0) | Non-Injectables 0 | Trashed 0
Start Scanner
URL's Queue
Exploitables
Injectables
Non-Injectables
Trash Collector
2- click start
Setup [Dorks: 2]
inurl:
.php?id=" shopping"
.php?id=" add to cart"
1- Place Dork
Google
Bing
Yahoo
Aol
Yandex
Ask
Wow
WebCrawler
MyWebSearch
Sapo
forum;showthread;injection;dorks;union;hack;.gov
1000
Search Delay (ms)
Import
Export
Add
Trash All URL's
Clear URL's
HTTP Debugger
Proxy IP: N/A | Clear URL's thread done, deleted 281 URL's.
0 Bytes


SQLi Dumper v.8.0
Online Scanner
URL Analizer
Data Dumper
File Dumper
Tools & Settings
Queue 281 | Exploitables 0 | Injectables 0 (0/0) | Non-Injectables 0 | Trashed 0
Start Scanner
URL's Queue
Exploitables
Injectables
Non-Injectables
Trash Collector
Setup [Dorks: 2]
inurl:
.php?id=" shopping"
.php?id=" add to cart"
click here
Google
Bing
Yahoo
Aol
Yandex
Ask
Wow
WebCrawler
MyWebSearch
Sapo
forum;showthread;injection;dorks;union;hack;.gov
1000
Search Delay (ms)
Import
Export
Add
Trash All URL's
Clear URL's
URL
http://www.littleparachutes.com/book.php?id=112
http://www.magicwings.com/index.php?id=169
http://www.shopwestgatecenter.com/index.php?id=13
After extraction sites
HTTP Debugger
Proxy IP: N/A | Scanner thread, URL's exported succeeded. [15-04-2015 04_19_14 MySQLDump LIKS.txt]
0 Bytes
15-04-2015
04_19_14


SQLi Dumper v.8.0
Online Scanner
URL Analizer
Data Dumper
File Dumper
Tools &Settings
Queue 0 | Exploitables 13 | Injectables 4 (4/0) | Non-Injectables 3 | Trashed 261
30
Start Exploiter
URL's Queue
Exploitables
Injectables
Non-Injectables
Trash Collector
1- click here
3- Then go here
URL
SQL Type
Country
IP
http://www.wesleynet.com/indonesia/gotowebsite2.php?Co_Code=327 MySQL [US] United States 74.22
http://www.maketheroad.org/report.php?ID=1085 MySQL [US] United States 64.20
http://www.ipicshopping.co.za/shopping_centre.php?id=3 MySQL [ZA] South Africa 192.1
http://www.magicwings.com/index.php?id=169 MySQL [US] United States 204.2
http://www.artista.fr/shopping/index.php?id=37 MySQL [FR] France 151.2
http://mahimainternational.com/shopping.php?id=shopping MySQL [IN] India 119.1
http://www.mbk-center.co.th/en/floorplan/shop.php?id=353 MySQL [TH] Thailand 115.3
http://exaclair2.com/show_stores.php?id=433 MySQL [US] United States 66.33
http://www.westlakeaustin.com/content.php?id=shopping MySQL [US] United States 198.5
http://www.littleparachutes.com/book.php?id=112 MySQL [DE] Germany 213.1
http://www.ventureproperties.com/properties.php?id=4 MySQL [US] United States 206.1
http://www.kuromon.com/shop.php?id=44 MySQL [US] United States 199.4
http://www.stadtbummel-fehmarn.de/burg/einkaufen.php?id=Shopping&sid_ID... MySQL [DE] Germany 82.16
2-Wait until the end
HTTP Debugger
Proxy IP: N/A | Exploiter thread done, exploitable detected: 13
8.64 MiB


SQLi Dumper v.8.0
Online Scanner
URL Analizer
Data Dumper
File Dumper
Tools & Settings
Queue 0 | Exploitables 13 | Injectables 4 (4/0) | Non-Injectables 3 | Trashed 261
10
Analizing..
URL's Queue
Exploitables
Injectables
Non-Injectables
Trash Collector
1- click here
Setup
Un-Archived 4
Archived 0
ALL (0)
ALL
Match: URL
OK
URL
Method
Highlights
SQL Version
SQL User
Alexa R
http://karnaticlabrecords.com/cart.php?id... MySQL Union 5.0.83-community karnaticlabreco... N/A [P:
http://www.ipicgroup.com/shopping_centr... MySQL Union 5.5.41-0+whe... ipicgr_1@www1... N/A [P:
http://www.oaxis.com/shop/product_deta... MySQL Union 5.1.67-rel14.3 <a class="__cf... 207,50
http://www.iankingimaging.com/cart.php?i... MySQL Error 5.0.32-Debian_... ianking@localhost N/A [P:
Wait
Search Columns\Tables Names (MySQL and MS SQL)
Loading, please wait..
77%
Cancel
Pause
HTTP Debugger
Proxy IP: N/A | [10/13] Analizer thread, injectable detected: 0
9.22 MiB

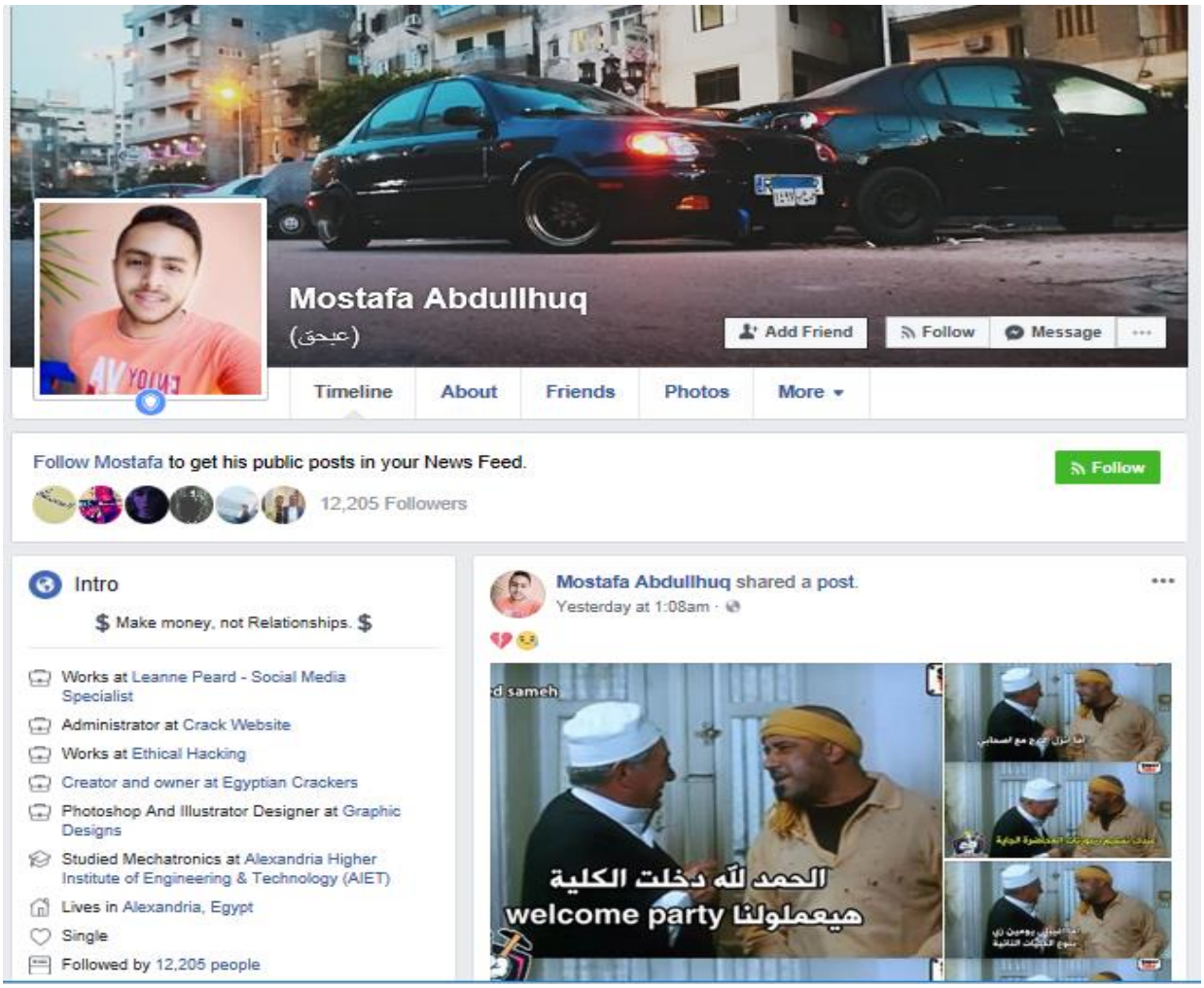

SQLi Dumper v.8.0
Online Scanner
URL Analizer
Data Dumper
File Dumper
Tools & Settings
http://www.oaxis.com/shop/product_detail.php?id=999999.9 union all select 1,2,[t]
GET
MySQL Union
Session:
Get Server Info
db109659_oaxis2
Schema
Query
Get Databases
<a class="__cf_email__" href="/cdn-cgi/l/em
You are here injection or havij
Setup
Hide
Threads [10]
Cookies:
POST:
Illegal Mix Of Collations
Disabed
Unhex(Hex())
Binary()
Cast As Char
Compress(Uncompress())
Convert Using utf8
Convert Using latin1
Aes_decrypt(Aes_encrypt())
TimeOut (ms): 5000
Delay (ms): 500
Retry Limit: 5
Injection Point: URL
Network Credential (Login)
User Name:
Password:
Limits
Limit X
Limit Y
Add Query Where
Add Query Order By
ReDump Failed Index
All In One
Clear On Get
Auto Scroll
HTTP Debugger
Proxy IP: N/A | Dumper thread, worker complete
14.17 MiB



Exceptionally suspicious content in the C:\Windows\font directory, so suspicious it leads me to believe that a newer; more improved ZERO DAY TTF Blend Vulnerability or other TTF Font Parsing exploit is taking place via cross linking of libraries. There is a possibility that that the Intergy 11 EMR software may be compromised with a built in ability to attack a machine and elevate privileges. There are many hidden DLL files in the font's directory. Dll files that are associated with Sentry_MBA.exe exploit.. Malwarebytes is detecting that DCMTK.dll is infected with "*Spyware On-Line Games*". Inspected proxy11 and proxies, analysis revealed that the proxy servers were being used to hide activity and bypass security. Drilling down on the C:\users\postgres\downloads Mineav PSN Checker found configuration files and applications to execute brute force, ransomeware and distributed denial of service attacks. The PSN Webkit, along with what appeared to be IPTV software, a Combo List with stolen username/passwords and Dynamic DNS software were found in hidden folders on the desktop of user Postgres.INTERGY.LOCAL. The PSN Webkit provides the ability for the attacker to create a LINUX Partition and run the Apache Webserver. Decided to check server backups and shadow copy for user profile "Postgres". Found a PDF GECU account statement for Jose M Barrios for the purchase of a domain. Conducted a search for additional information on Jose M Barrios aka Jose Hernandez, it is an outside possibility that Jose Hernandez may be a fugitive from the DEA in California. HIPAA Security rule requires that the FBI be notified in the event of a breach. The FBI was notified at this point a decision was made to disable the Postgres user, capture as much data as possible for FBI Cyber and prepare AR Billing Company for a forklift upgrade. Complete rebuild of servers and workstations will be required with the implementation of offensive security technical implementation protocols for network infrastructure, server operating systems, Win 10 Pro workstations, Win 7 Pro to Win 10 Pro upgrades and deployment of FortiClient Telemetry / Compliance agents on all remote workstation

Targets of Interest (TOI's)

Mostafa Abdullhuq

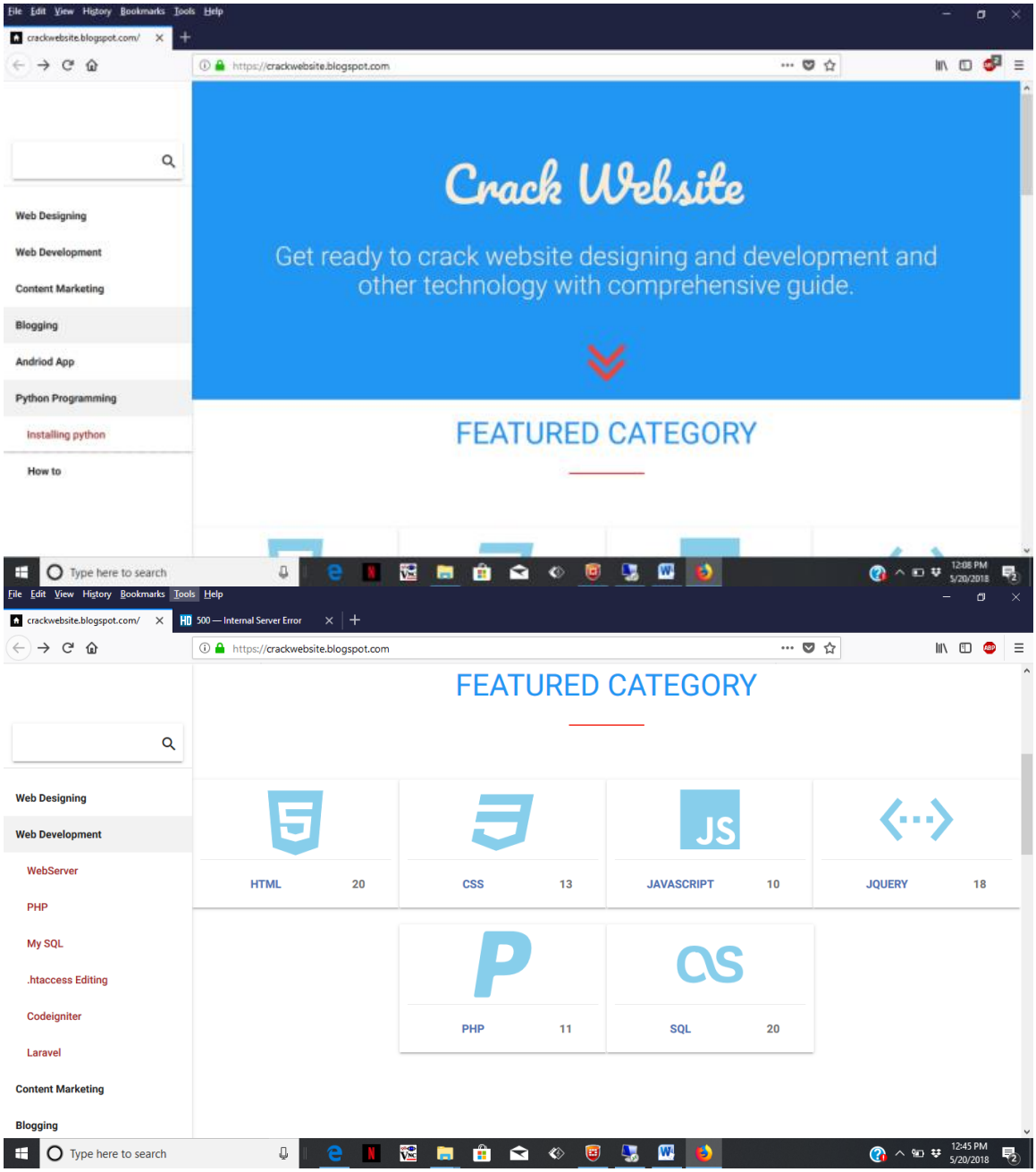


Screenshot

{"login_success":{"message":"Login Successful","userId":"100000764586624","userProperties": {"First Name":"mostafaabdullhuq","Email":"mostafaabdullhuq@gmail.com","Created":"2016-12-13T14:51:41-06:00","Account Type":"Basic","Registration Type":"Email","School":"3311","Student Status":"Student","Tutor Status":"Not a tutor","Knowledge Drive Status":"Not knowledge drive","Questions Deposited":"0"}}}

[WPFiles]E:\Users\MostafaAbdullhuq\Desktop\SPAM\Programmes\Sentry MBA 1.4.2\SnapShots\coursehero.com.ini||108369A699A060FAE62D5B87AE77CDF9=2

[WPTime]Time=35386861 https://mostafaabdullhuq.sarahah.com

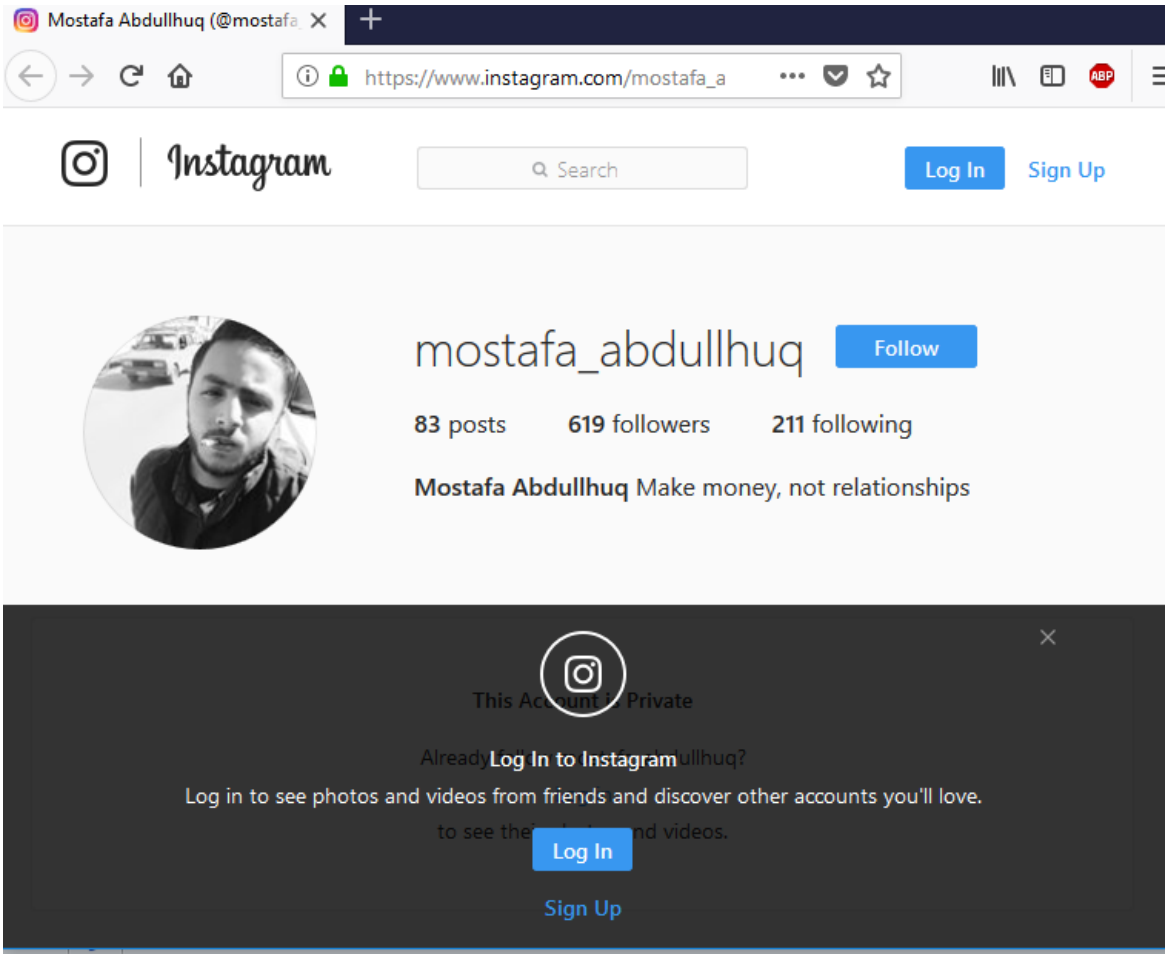


http://89.38.98.85 , https://99rdp.com/billings/dologin.php , https://amazingrdp.com/whmcs/clientarea.php , http://expert-team-world.ddns.net http://iptv.freecamtv.com https://www.germanvps.com/dologin.php http://www.khalifaprosatiptv.com , http://mypanel.tv , https://api.netflix.com/PaparazziTeam , http://1.panel3.us , mostafaabdullhuq@gmail.com https://mostafaabdullhuq.sarahah.com/ https://www.instagram.com/mostafa_abdullhuq/ https://www.facebook.com/mostafaabdullhuq

Administrator at CrackWebsite https://crackwebsite.blogspot.com/

CrackWebsite on Facebook *https://crackwebsite.blogspot.com/*

Instagram



https://www.instagram.com/mostafa_abdullhuq/

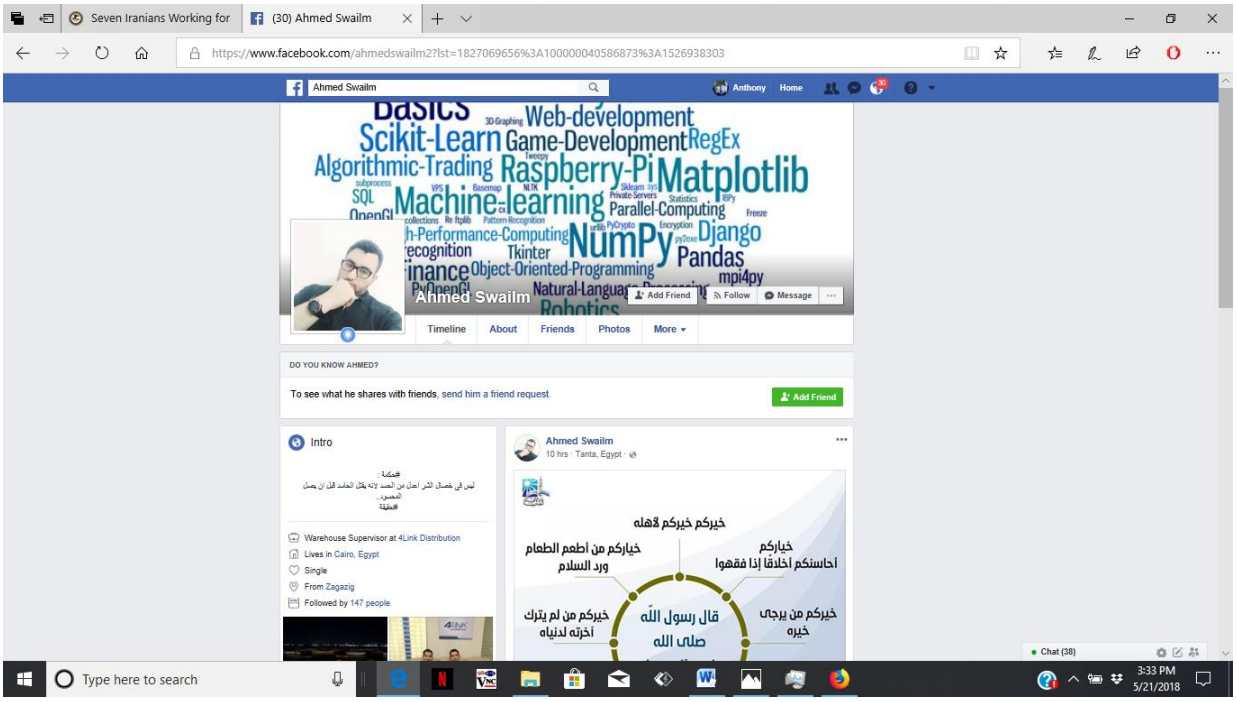
Video of Mostafa Abdullhuq

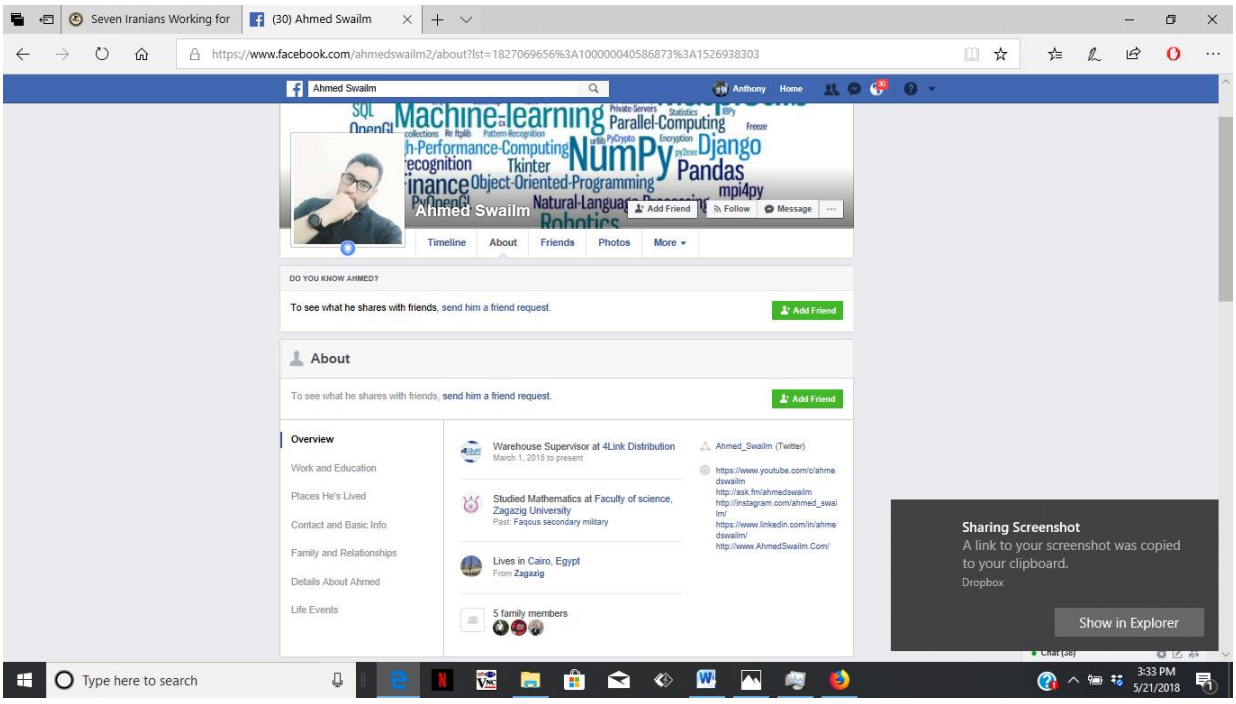
https://www.facebook.com/magdy.mohamed.3762/videos/t.100001831100799/1559360927454930/?type=2&video_source=user_video_tab

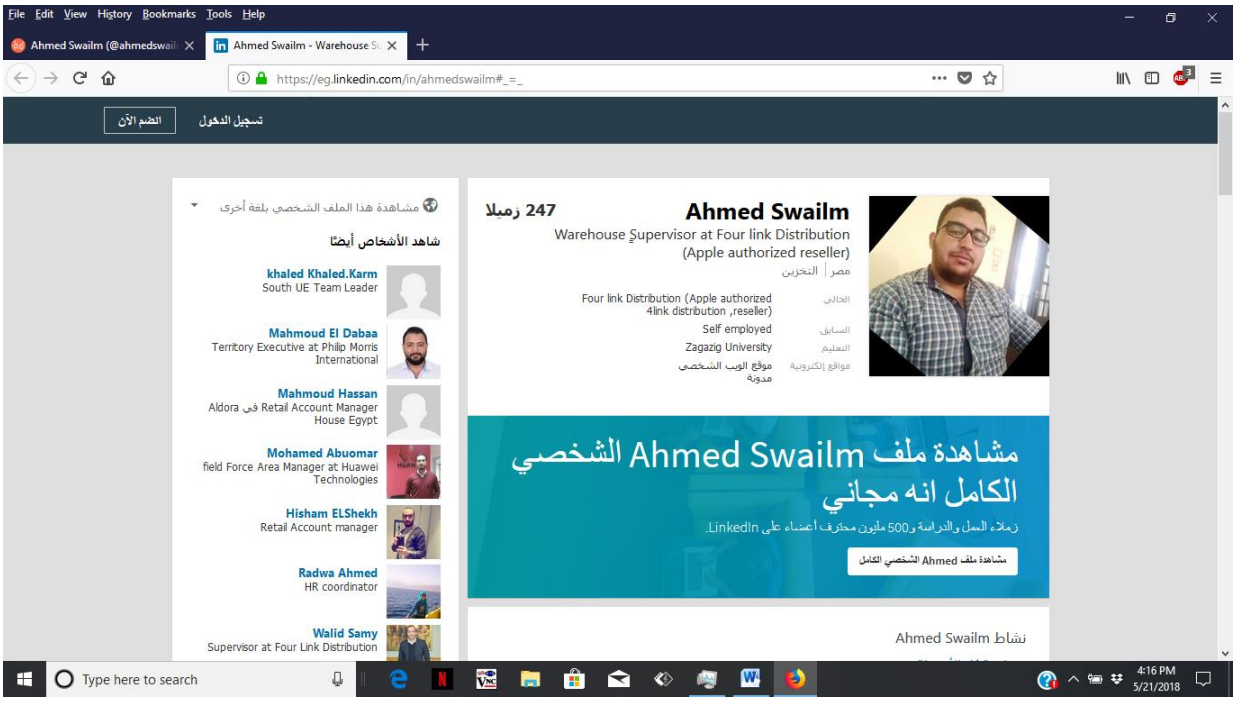
Maddy Mohamed friend of MostafaAbdullhuq

https://www.facebook.com/magdy.mohamed.3762?hc_ref=ARRWW_xGjVGvdbjrGgZTOGcoV50XEkNm-24_kBELtaOcPWqLmyqVeP6v9avbhasIRfA

Ahmed Swailm



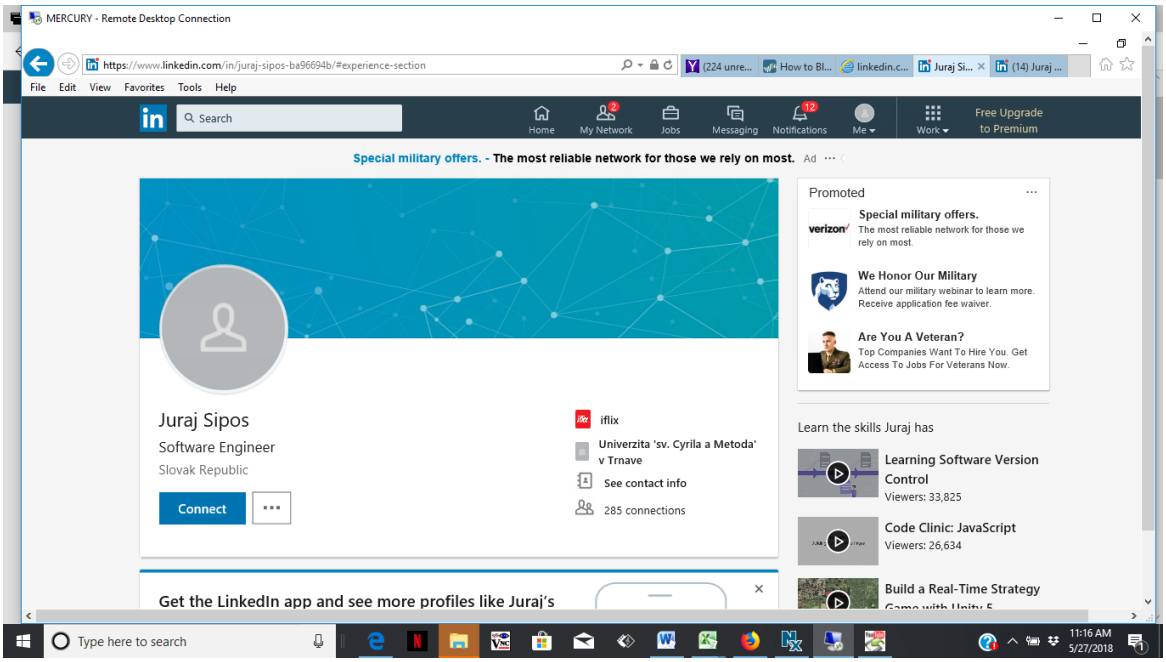


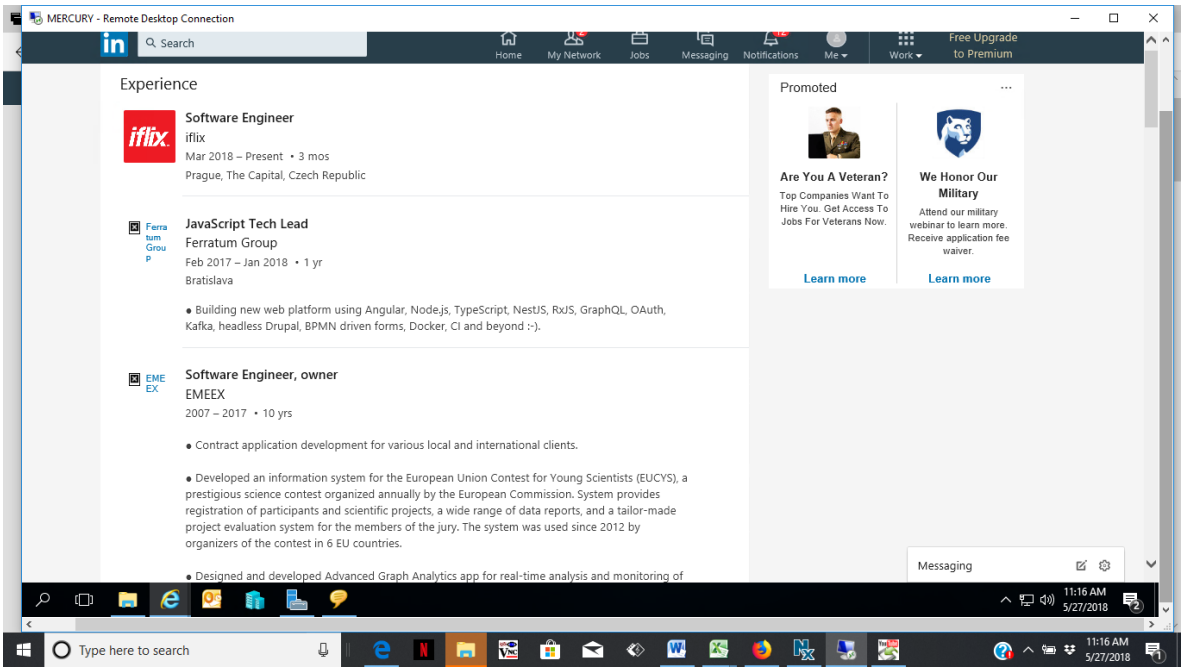


Social Links

Ahmed_Swailm(Twitter) http://instagram.com/ahmed_swailm/
https://www.linkedin.com/in/ahmedswailm/

Juraj Sipos





date=2018-03-12 time=05:57:45 logver=2 type=traffic level=info sessionid=57452524 hostname=APOLLO pcdomain=intergy.local uid=8331A2218F7042CC8915BD7A467A56A6 devid=FCT800116072253 5 fgtserial=N/A emsserial=N/A regip=N/A srcname=N/A srcproduct=N/A srcip=N/A srcport=N/A direction=outbound dstip=N/A remotename=" include \"lib.event.tis\" include \"lib.GUIDebugger.tis\"; include \"lib.tooltip.tis\" include \"lib.animations.tis\" include \"li" dstport=N/A user=postgres@INTERGY.LOCAL proto=6 rcvdbyte=N/A sentbyte=N/A utmaction=userbrowsed utmevent=webfilter threat=N/A vd=N/A fctver=5.6.5.1150 os="Microsoft Windows Server 2012 R2 Standard Edition, 64-bit (build 9600)" usingpolicy="" service=http url="/2/2013 * @author \\n * @author Copyright (c) 2013 ESET, spol. s r. o. * @note current owner: Juraj Sipos (sipos@eset.sk) * @note IMPORTANT: Before doing any significant change to this file check your plan with the current owner to avoid unexpected behavior. */ <div class=\"label\">{{label}} <widget type=\"select-dropdown\" novalue=\"{{novalue}}\"> {{#items}} <option value=\"{{value}}\" depth=\"{{depth}}\" >{{text}}</option> {{/items}} </widgetpostgres@INTERGY.LOCAL userinitiated=1 browsetime=9

Jose M Barrios

Found a PDF GECU account statement for Jose M Barrios for the purchase of a domain.

GECU
WE'RE WITH YOU

Account Number 5368 2101 0091 2864

SUMMARY OF ACCOUNT ACTIVITY	
Previous Balance	$0.00
- Payments	$2,518.52
- Other Credits	$113.84
+ Purchases	$69.94
+ Other Debits	$2,518.52
+ Cash Advances	$0.00
Past Due Amount	$0.00
Fees Charged	**$25.00**
Interest Charged	**$0.00**
New Balance	**$18.90-**
Account Number Ending In	2864
Credit Limit	$2,500.00
Available Credit	$2,500.00
Statement Closing Date	02/05/2018
Days this Billing Cycle	31

PAYMENT INFORMATION	
New Balance	$18.90-
Minimum Payment Due (MPD)	**$0.00**
Payment Due Date	**3/2/2018**

Late Payment Warning: If we do not receive your minimum payment by the date listed above, you may have to pay up to a $25.00 late fee.

If you would like information about credit counseling services, call 1-866-248-3453.

TO CONTACT US

For Member Service, please call: 800-810-2252
To report a lost or stolen card, please call: 800-810-2252
Website: www.gecu.com

Send notice of billing errors to:
PO Box 10409
Des Moines, IA 50306-0409

New Balance	Payment Due Date	Amount Past Due	Minimum Payment Due
$18.90-	3/2/2018	$0.00	$0.00

TRANSACTIONS

Trans Date	Post Date	Description	Reference Number	Amount
01/18	01/18	PAYMENT - ONLINE EL PASO TX	8536821D3F5P96MEZ	-2,518.52
01/20	01/22	WWW.LHSPAY.COM BURNHAM-ON-CR GB	9520914D50000RESY	49.95
01/22	01/22	ADJUSTMENT-PURCHASES	F197800DF000CR245	-49.95

See Reverse Side for Important Information and Billing Rights Summary

5617 YQG 002 7 5 180205 0 N PAGE 1 of 3 1 0 1978 0100 GEP4 O1AB5617

Please detach this portion and return with your payment to ensure proper credit. Retain upper portion for your records.

GECU
PO Box 10409
Des Moines, IA 50306-0409

Account Number 5368 2101 0091 2864

New Balance	$18.90-
Payment Due Date	**3/2/2018**
Minimum Payment Due	**$0.00**

Amount Enclosed $

Please check the box and make address/phone changes on the back. ☐

* *Do not fold, staple, clip, send cash or non-US funds*
* *Please detach and enclose bottom portion with payment*
* *Make checks or money orders payable to:*

Payments received as instructed will be posted to your account on the day of receipt.
Non-conforming payments may be subject to a 5 day delay in posting.

JOSE M BARRIOS
1770 PICO ALTO DR APT D
EL PASO TX 79935-3349

GECU
PO Box 37035
Boone IA 50037-0035

*536821010091286400000000000000001890

Conducted a search for additional information on Jose M Barrios alias Jose Hernandez, it is an outside possibility that Jose Hernandez may be a fugitive from the DEA in California. HIPAA Security rule requires that the FBI be notified in the event of a breach. The FBI was notified at this point a decision was made to disable the Postgres user, capture as much data as possible for FBI Cyber and prepare AR Billing Company for a forklift upgrade. Complete rebuild of servers and workstations is required along with implementation of offensive security technical implementation protocols for network infrastructure, server operating systems, Win 10 Pro workstations version 1803, upgrade Win 7 Pro to Win 10 Pro version 1803, deployment of FortiClient Telemetry and Compliance agents on all remote workstations.

The Combatant's Tactics

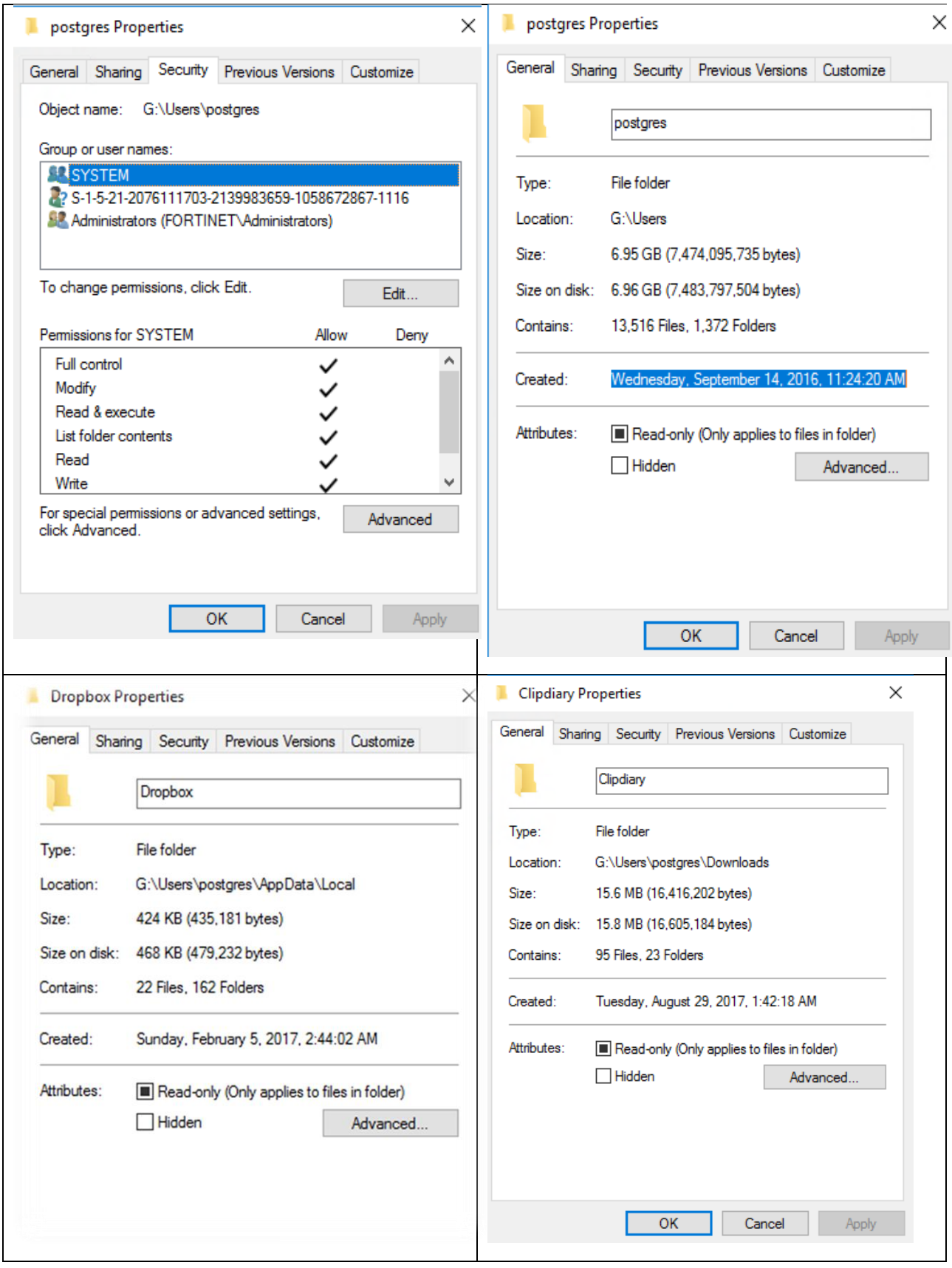
Summarize in one paragraph the combatant's actions and tactics, as well as the effects that the intrusion had on the victims. This section of the report overlays the intrusion kill chain's phases over the diamond model vertices to capture the core characteristics of the malicious activities.

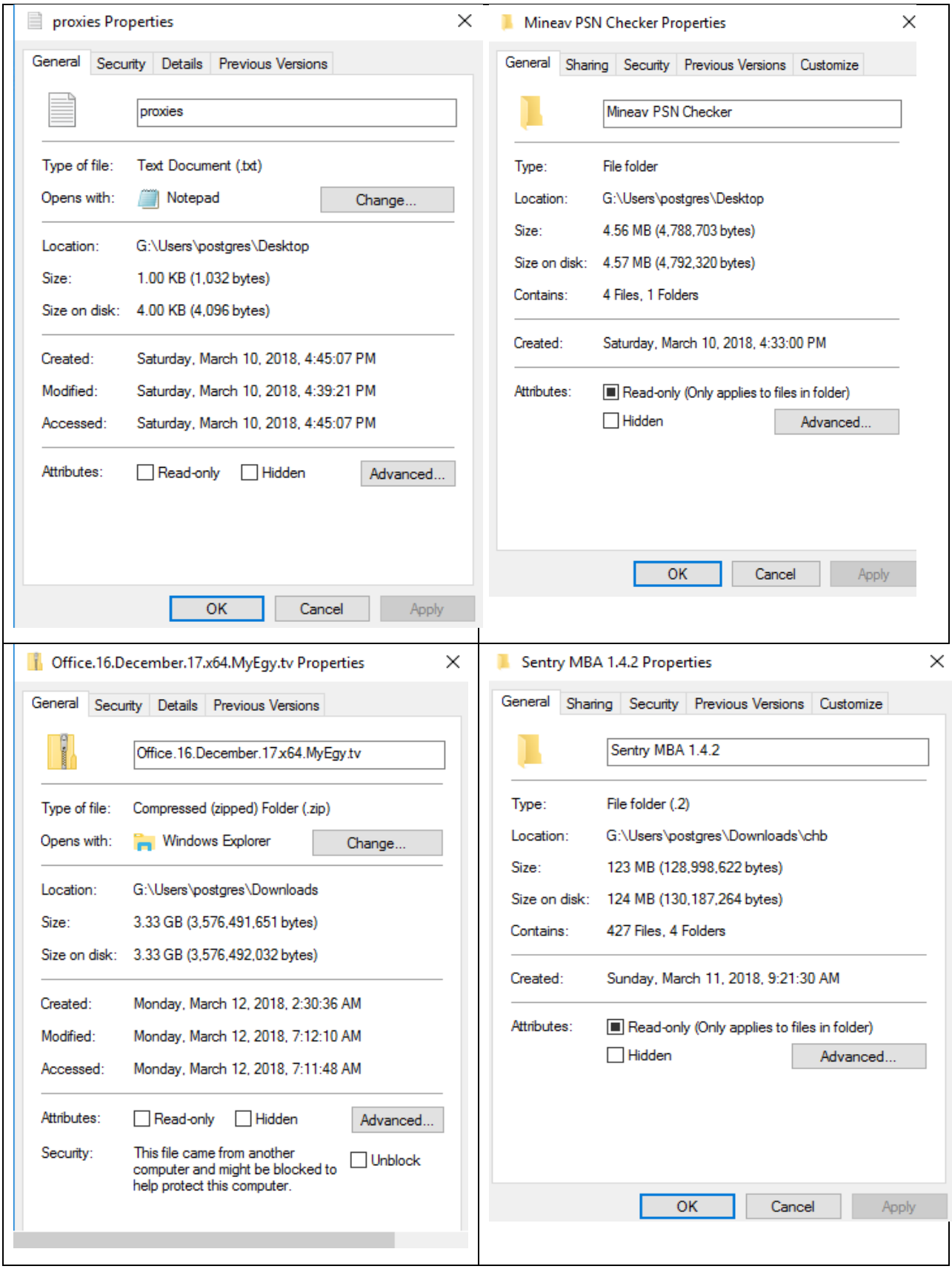
After establishing a persistent foothold on the network, attacker moved laterally conducting reconnaissance and intelligence gathering of systems. With Sentry_MBA.Exe, armed with server configuration files, Combo List, Proxy Servers, the combatant created BOTS that interrogated, engaged and exploited hundreds of thousands of servers. The combatant successfully exploited usernames and password logins at sites such as NetFlix, Amazon, Teamviewer and GECU. Combatant hijacked Internet Information Server and appears to be trying to spoof login pages for nefarious purposes. All of this activity leaves a distinctive signature on a firewall security log and Windows security logs. Attacker used XTunnel Port Zero to establish a SSH connection to the server

Initial Access

AR Billing is the target of an Advanced Persistent Threat. (APT; is a network attack in which an unauthorized person gains access to a network and stays there undetected for a long period of time in order to steal data, rather than cause damage to the organization.).

1st occurrence of user RDP user Intergy\Postgres, September 14th 2016 3 weeks after a fresh build of Intergy Terminal Server Apollo. User Postgres is the point of entry undetected for several years. User did not become active until February of 2017, when Dropbox was loaded and a payload of 162 folders and 22 files transferred.


postgres Properties
General
Sharing
Security
Previous Versions
Customize
Object name: G:\Users\postgres
Group or user names:
SYSTEM
S-1-5-21-2076111703-2139983659-1058672867-1116
Administrators (FORTINET\Administrators)
To change permissions, click Edit.
Edit...
Permissions for SYSTEM
Allow
Deny
Full control
Modify
Read & execute
List folder contents
Read
Write
For special permissions or advanced settings, click Advanced.
Advanced
OK
Cancel
Apply
postgres Properties
General
Sharing
Security
Previous Versions
Customize
postgres
Type: File folder
Location: G:\Users
Size: 6.95 GB (7,474,095,735 bytes)
Size on disk: 6.96 GB (7,483,797,504 bytes)
Contains: 13,516 Files, 1,372 Folders
Created: Wednesday, September 14, 2016, 11:24:20 AM
Attributes:
Read-only (Only applies to files in folder)
Hidden
Advanced...
OK
Cancel
Apply
Dropbox Properties
General
Sharing
Security
Previous Versions
Customize
Dropbox
Type: File folder
Location: G:\Users\postgres\AppData\Local
Size: 424 KB (435,181 bytes)
Size on disk: 468 KB (479,232 bytes)
Contains: 22 Files, 162 Folders
Created: Sunday, February 5, 2017, 2:44:02 AM
Attributes:
Read-only (Only applies to files in folder)
Hidden
Advanced...
Clipdiary Properties
General
Sharing
Security
Previous Versions
Customize
Clipdiary
Type: File folder
Location: G:\Users\postgres\Downloads
Size: 15.6 MB (16,416,202 bytes)
Size on disk: 15.8 MB (16,605,184 bytes)
Contains: 95 Files, 23 Folders
Created: Tuesday, August 29, 2017, 1:42:18 AM
Attributes:
Read-only (Only applies to files in folder)
Hidden
Advanced...
OK
Cancel
Apply


proxies Properties
General
Security
Details
Previous Versions
proxies
Type of file: Text Document (.txt)
Opens with: Notepad
Change...
Location: G:\Users\postgres\Desktop
Size: 1.00 KB (1,032 bytes)
Size on disk: 4.00 KB (4,096 bytes)
Created: Saturday, March 10, 2018, 4:45:07 PM
Modified: Saturday, March 10, 2018, 4:39:21 PM
Accessed: Saturday, March 10, 2018, 4:45:07 PM
Attributes: Read-only Hidden
Advanced...
OK
Cancel
Apply
Mineav PSN Checker Properties
General
Sharing
Security
Previous Versions
Customize
Mineav PSN Checker
Type: File folder
Location: G:\Users\postgres\Desktop
Size: 4.56 MB (4,788,703 bytes)
Size on disk: 4.57 MB (4,792,320 bytes)
Contains: 4 Files, 1 Folders
Created: Saturday, March 10, 2018, 4:33:00 PM
Attributes: Read-only (Only applies to files in folder)
Hidden
Advanced...
OK
Cancel
Apply
Office.16.December.17.x64.MyEgy.tv Properties
General
Security
Details
Previous Versions
Office.16.December.17.x64.MyEgy.tv
Type of file: Compressed (zipped) Folder (.zip)
Opens with: Windows Explorer
Change...
Location: G:\Users\postgres\Downloads
Size: 3.33 GB (3,576,491,651 bytes)
Size on disk: 3.33 GB (3,576,492,032 bytes)
Created: Monday, March 12, 2018, 2:30:36 AM
Modified: Monday, March 12, 2018, 7:12:10 AM
Accessed: Monday, March 12, 2018, 7:11:48 AM
Attributes: Read-only Hidden
Advanced...
Security: This file came from another computer and might be blocked to help protect this computer.
Unblock
Sentry MBA 1.4.2 Properties
General
Sharing
Security
Previous Versions
Customize
Sentry MBA 1.4.2
Type: File folder (.2)
Location: G:\Users\postgres\Downloads\chb
Size: 123 MB (128,998,622 bytes)
Size on disk: 124 MB (130,187,264 bytes)
Contains: 427 Files, 4 Folders
Created: Sunday, March 11, 2018, 9:21:30 AM
Attributes: Read-only (Only applies to files in folder)
Hidden
Advanced...
OK
Cancel
Apply

Exploit Public-Facing Application Hardware Trusted Relationship Valid Accounts

The use of software, data, or commands to take advantage of a weakness in an Internet-facing computer system or program in order to cause unintended or unanticipated behavior. The weakness in the system can be a bug, a glitch, or a design vulnerability. These applications are often websites, but can include databases (like SQL), standard services (like SMB2 or SSH), and any other applications with Internet accessible open sockets, such as web servers and related services. Depending on the flaw being exploited this may include Exploitation for Defense Evasion. PosgreSQL 8.3.2 provided the trusted relationship entry point.

Exploitation for Defense Evasion Technique

Platform Linux, Windows, macOS

Permissions Required User

Data Sources Windows Error Reporting, Process Monitoring, File monitoring

Defense Bypassed Anti-virus, System access controls

Exploitation of a software vulnerability occurs when a combatant takes advantage of a programming error in a program, service, or within the operating system software or kernel itself to execute combatant-controlled code. Vulnerabilities may exist in defensive security software that can be used to disable or circumvent them.

Targets of Interest (TOI's) may have prior knowledge through reconnaissance that security software exists within an environment or they may perform checks during or shortly after the system is compromised for Security Software Discovery. The security software will likely be targeted directly for exploitation. There are examples of antivirus software being targeted by persistent threat groups to avoid detection.

Mitigation

Update software regularly by employing patch management for internal enterprise endpoints and servers. Develop a robust cyber threat intelligence capability to determine what types and levels of threat may use software exploits and o-days against a particular organization. Make it difficult for TOI's to advance their operation through exploitation of undiscovered or unpatched vulnerabilities by using sandboxing, if available. Other types of virtualization and application microsegmentation may also mitigate the impact of some types of exploitation. The risks of additional exploits and weaknesses in implementation may still exist.3

Detection

Security applications that look for behavior used during exploitation such as Windows Defender Exploit Guard (WDEG) and the Enhanced Mitigation Experience Toolkit (EMET) can be used to mitigate some exploitation behavior. Control flow integrity checking is another way to potentially identify and stop a

software exploit from occurring. Many of these protections depend on the architecture and target application binary for compatibility and may not work for software targeted for defense evasion.

Software: XTunnel, X-Tunnel, XAPS

XTunnel, X-Tunnel, XAPS

Software

ID	S0117
Aliases	XTunnel, X-Tunnel, XAPS
Type	Malware
Platform	Windows

XTunnel a VPN-like network proxy tool that can relay traffic between a C2 server and a victim. It was first seen in May 2013 and reportedly used by APT28 during the compromise of the Democratic National Committee.

Techniques Used

Standard Cryptographic Protocol

XTunnel uses SSL/TLS and RC4 to encrypt traffic.

TOI's use command and control over an encrypted channel using a known encryption protocol like HTTPS or SSL/TLS. The use of strong encryption makes it difficult for defenders to detect signatures within combatant command and control traffic.

Use of a standard non-application layer protocol for communication between host and C2 server or among infected hosts within a network. The list of possible protocols is extensive. Specific examples include use of network layer protocols, such as the Internet Control Message Protocol (ICMP), and transport layer protocols, such as the User Datagram Protocol (UDP).

ICMP communication between hosts is one example. Because ICMP is part of the Internet Protocol Suite, it is required to be implemented by all IP-compatible hosts; however, it is not as commonly monitored as other Internet Protocols such as TCP or UDP and may be used by TOI's to hide communications.

Some TOI's may use other encryption protocols and algorithms with symmetric keys, such as RC4, that rely on encryption keys encoded into malware configuration files and not public key cryptography. Such keys may be obtained through malware reverse engineering.

Mitigation

Network intrusion detection and prevention systems that use network signatures to identify traffic for specific combatant malware can be used to mitigate activity at the network level. Use of encryption protocols may make typical network-based C2 detection more difficult due to a reduced ability to signature the traffic. Prior knowledge of combatant C2 infrastructure may be useful for domain and IP address blocking, but will likely not be an effective long-term solution because TOI's can change infrastructure often.41

Detection

SSL/TLS inspection is one way of detecting command and control traffic within some encrypted communication channels.42 SSL/TLS inspection does come with certain risks that should be considered before implementing to avoid potential security issues such as incomplete certificate validation.

If malware uses encryption with symmetric keys, it may be possible to obtain the algorithm and key from samples and use them to decode network traffic to detect malware communications signatures.

In general, analyze network data for uncommon data flows (e.g., a client sending significantly more data than it receives from a server). Processes utilizing the network that do not normally have network communication or have never been seen before are suspicious. Analyze packet contents to detect communications that do not follow the expected protocol behavior for the port that is being used.

Credentials in Files –

XTunnel is capable of accessing locally stored passwords on victims.

TOI's may search local file systems and remote file shares for files containing passwords. These can be files created by users to store their own credentials, shared credential stores for a group of individuals, configuration files containing passwords for a system or service, or source code/binary files containing embedded passwords.

It is possible to extract passwords from backups or saved virtual machines through Credential Dumping.1 Passwords may also be obtained from Group Policy Preferences stored on the Windows Domain Controller.

Mitigation

Establish an organizational policy that prohibits password storage in files. Ensure that developers and system administrators are aware of the risk associated with having plaintext passwords in software configuration files that may be left on endpoint systems or servers. Preemptively search for files containing passwords and remove when found. Restrict file shares to specific directories with access only to necessary users. Remove vulnerable Group Policy Preferences.

Detection

While detecting TOI's accessing these files may be difficult without knowing they exist in the first place, it may be possible to detect combatant use of credentials they have obtained. Monitor the command-line arguments of executing processes for suspicious words or regular expressions that may indicate searching for a password (for example: password, pwd, login, secure, or credentials). See Valid Accounts for more information.

Remote File Copy –

XTunnel is capable of downloading additional files.

Files may be copied from one system to another to stage combatant tools or other files over the course of an operation. Files may be copied from an external combatant-controlled system through the Command and Control channel to bring tools into the victim network or through alternate protocols with another tool such as FTP. Files can also be copied over on Mac and Linux with native tools like scp, rsync, and sftp.

TOI's may also copy files laterally between internal victim systems to support Lateral Movement with remote Execution using inherent file sharing protocols such as file sharing over SMB to connected network shares or with authenticated connections with Windows Admin Shares or Remote Desktop Protocol.

Mitigation

Network intrusion detection and prevention systems that use network signatures to identify traffic for specific combatant malware or unusual data transfer over known tools and protocols like FTP can be used to mitigate activity at the network level. Signatures are often for unique indicators within protocols and may be based on the specific obfuscation technique used by a particular combatant or tool, and will likely be different across various malware families and versions. TOI's will likely change tool C2 signatures over time or construct protocols in such a way as to avoid detection by common defensive tools.

Detection

Monitor for file creation and files transferred within a network over SMB. Unusual processes with external network connections creating files on-system may be suspicious. Use of utilities, such as FTP, that does not normally occur may also be suspicious.

Analyze network data for uncommon data flows (e.g., a client sending significantly more data than it receives from a server). Processes utilizing the network that do not normally have network communication

or have never been seen before are suspicious. Analyze packet contents to detect communications that do not follow the expected protocol behavior for the port that is being used.

Network Service Scanning –

XTunnel is capable of probing the network for open ports.

TOI's may attempt to get a listing of services running on remote hosts, including those that may be vulnerable to remote software exploitation. Methods to acquire this information include port scans and vulnerability scans using tools that are brought onto a system.

Mitigation

Use network intrusion detection/prevention systems to detect and prevent remote service scans. Ensure that unnecessary ports and services are closed and proper network segmentation is followed to protect critical servers and devices.

Identify unnecessary system utilities or potentially malicious software that may be used to acquire information about services running on remote systems, and audit and/or block them by using whitelisting13 tools, like AppLocker, or Software Restriction Policies16 where appropriate.

Detection

System and network discovery techniques normally occur throughout an operation as a combatant learns the environment. Data and events should not be viewed in isolation, but as part of a chain of behavior that could lead to other activities, such as Lateral Movement, based on the information obtained.

Normal, benign system and network events from legitimate remote service scanning may be uncommon, depending on the environment and how they are used. Legitimate open port and vulnerability scanning may be conducted within the environment and will need to be deconflicted with any detection capabilities developed. Network intrusion detection systems can also be used to identify scanning activity. Monitor for process use of the networks and inspect intra-network flows to detect port scans.

Command-Line Interface

XTunnel has been used to execute remote commands.1

Command-line interfaces provide a way of interacting with computer systems and is a common feature across many types of operating system platforms.1 One example command-line interface on Windows systems is cmd, which can be used to perform a number of tasks including execution of other software. Command-line interfaces can be interacted with locally or remotely via a remote desktop application, reverse shell session, etc. Commands that are executed run with the current permission level of the command-line interface process unless the command includes process invocation that changes permissions context for that execution (e.g. Scheduled Task).

TOI's may use command-line interfaces to interact with systems and execute other software during the course of an operation.

Mitigation

Audit and/or block command-line interpreters by using whitelisting tools, like AppLocker, or Software Restriction Policies where appropriate.

Detection

Command-line interface activities can be captured through proper logging of process execution with command-line arguments. This information can be useful in gaining additional insight to TOI's' actions through how they use native processes or custom tools.

Connection Proxy

XTunnel relays traffic between a C2 server and a victim.

Command-line interfaces provide a way of interacting with computer systems and is a common feature across many types of operating system platforms.1 One example command-line interface on Windows systems is cmd, which can be used to perform a number of tasks including execution of other software. Command-line interfaces can be interacted with locally or remotely via a remote desktop application, reverse shell session, etc. Commands that are executed run with the current permission level of the command-line interface process unless the command includes process invocation that changes permissions context for that execution (e.g. Scheduled Task).

TOI's may use command-line interfaces to interact with systems and execute other software during the course of an operation.

Mitigation

Network intrusion detection and prevention systems that use network signatures to identify traffic for specific combatant malware can be used to mitigate activity at the network level. Signatures are often for unique indicators within protocols and may be based on the specific C2 protocol used by a particular combatant or tool, and will likely be different across various malware families and versions. TOI's will likely change tool C2 signatures over time or construct protocols in such a way as to avoid detection by common defensive tools.20

Detection

Processes utilizing the network that do not normally have network communication or have never been seen before are suspicious. Network activities disassociated from user-driven actions from processes that normally require user direction are suspicious.

Analyze network data for uncommon data flows (e.g., a client sending significantly more data than it receives from a server or between clients that should not or often do not communicate with one another).

Processes utilizing the network that do not normally have network communication or have never been seen before are suspicious. Analyze packet contents to detect communications that do not follow the expected protocol behavior for the port that is being used.20

Fallback Channels - The C2 server used by **XTunnel** provides a port number to the victim to use as a fallback in case the connection closes on the currently used port.

Binary Padding - A version of **XTunnel** introduced in July 2015 inserted junk code into the binary in a likely attempt to obfuscate it and bypass security products.

Obfuscated Files or Information - A version of **XTunnel** introduced in July 2015 obfuscated the binary using opaque predicates and other techniques in a likely attempt to obfuscate it and bypass security products.

FortiNet Security Log excerpts

To view entire log click on this link

Sentry_MBA.exe traffic snapshots

 Novosibirskaya	date=2018-03-11 time=16:23:59 logver=2 type=traffic level=warning sessionid=57452524 hostname=APOLLO pcdomain=intergy.local uid=8331A2218F7042CC8915BD7A467A56A6 devid=FCT8001160722535 fgtserial=FWF30D3X16002938 emsserial=N/A regip=N/A srcname=Sentry_MBA.exe srcproduct=N/A srcip=192.168.2.12 srcport=59756 direction=outbound dstip=109.111.180.145 remotename=iptv.freecamtv.com dstport=3128 user=postgres@INTERGY.LOCAL proto=6 rcvdbyte=N/A sentbyte=N/A utmaction=blocked utmevent=antivirus threat="Adult/Mature Content:Pornography" vd=root fctver=5.6.5.1150 os="Microsoft Windows Server 2012 R2 Standard Edition, 64-bit (build 9600)" usingpolicy="" service=http url=:8000/get.php?username=Zr2eXH9M&password=071CyXf6&type=m3u userinitiated=0 browsetime=N/A	109.111.180.145 - IP Address Lookup The IP address location of 109.111.180.145 is Novosibirsk 630007, Novosibirskaya Oblast' (NVS), Russia (RU). 109.111.180.145 is a public IP address that belongs to ASN 34757 which is under the control of Sibirskie Seti Ltd.. The address resides in the IP address range 109.111.176.0 - 109.111.183.255 (CIDR notation: 109.111.176.0/21), and the whole subnet spans a total number of 2,048 individual IP addresses. The prefix 109/8 (109.0.0.0/8) was allocated to RIPE NCC by the Internet Assigned Numbers Authority (IANA) in January 2009.
 Taipei City Taiwan	date=2018-03-11 time=16:23:59 logver=2 type=traffic level=warning sessionid=57452524 hostname=APOLLO pcdomain=intergy.local uid=8331A2218F7042CC8915BD7A467A56A6 devid=FCT8001160722535 fgtserial=FWF30D3X16002938 emsserial=N/A regip=N/A srcname=Sentry_MBA.exe srcproduct=N/A srcip=192.168.2.12 srcport=59761 direction=outbound dstip=124.12.48.82 remotename=iptv.freecamtv.com dstport=8088 user=postgres@INTERGY.LOCAL proto=6 rcvdbyte=N/A sentbyte=N/A utmaction=blocked utmevent=antivirus threat="Adult/Mature Content:Pornography" vd=root fctver=5.6.5.1150 os="Microsoft Windows Server 2012 R2 Standard Edition, 64-bit (build 9600)" usingpolicy="" service=http url=:8000/get.php?username=w4zZlt1K&password=qIPOEGYl&type=m3u userinitiated=0 browsetime=N/A	124.12.48.82 - IP Address Lookup The IP address location of 124.12.48.82 is Taipei, Taipei City (TPE), Taiwan (TW). 124.12.48.82 is a public IP address that belongs to ASN 9924 which is under the control of Taiwan Fixed Network, Telco and Network Service Provider.. The address resides in the IP address range 124.8.0.0 - 124.12.255.255 (CIDR notation: 124.8.0.0/14, 124.12.0.0/16), and the whole subnet spans a total number of 327,680 individual IP addresses. The prefix 124/8 (124.0.0.0/8) was allocated to APNIC by the Internet Assigned Numbers Authority (IANA) in January 2005.
	date=2018-03-11 time=16:23:59 logver=2 type=traffic level=warning sessionid=57452524 hostname=APOLLO pcdomain=intergy.local uid=8331A2218F7042CC8915BD7A467A56A6 devid=FCT8001160722535 fgtserial=FWF30D3X16002938 emsserial=N/A regip=N/A srcname=Sentry_MBA.exe srcproduct=N/A srcip=192.168.2.12 srcport=59760 direction=outbound dstip=122.72.18.35 remotename=iptv.freecamtv.com dstport=80 user=postgres@INTERGY.LOCAL proto=6 rcvdbyte=N/A sentbyte=N/A utmaction=blocked utmevent=antivirus threat="Adult/Mature Content:Pornography" vd=root fctver=5.6.5.1150 os="Microsoft Windows Server 2012 R2 Standard Edition, 64-bit (build 9600)" usingpolicy="" service=http url=:8000/get.php?username=SEFTpril&password=tRXm9BBw&type=m3u userinitiated=0 browsetime=N/A	122.72.18.35 - IP Address Lookup The IP address location of 122.72.18.35 is Beijing, Beijing (BJ), China (CN). 122.72.18.35 is a public IP address that belongs to ASN 9394 which is under the control of China TieTong Telecommunications Corporation. The address resides in the IP address range 122.64.0.0 - 122.95.255.255 (CIDR notation: 122.64.0.0/11), and the whole subnet spans a total number of 2,097,152 individual IP addresses. The prefix 122/8 (122.0.0.0/8) was allocated to APNIC by the Internet Assigned Numbers Authority (IANA) in January 2006.

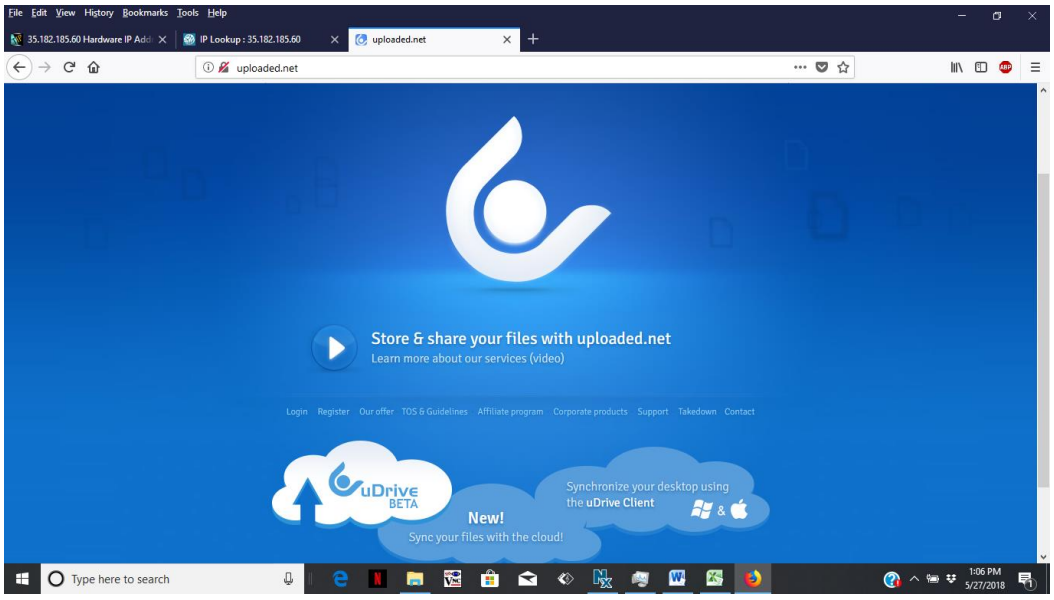
Etihad Airways Dubai date=2018-03-02 time=18:09:55 logver=2 type=traffic level=info sessionid=57844268 hostname=APOLLO pcdomain=intergy.local uid=8331A2218F7042CC8915BD7A467A56A6 devid=FCT8001160722535 fgtserial=FWF30D3X16002938 emsserial=N/A regip=N/A srcname=N/A srcproduct=N/A srcip=N/A srcport=N/A direction=outbound dstip=N/A remotename=agents.etihad.com dstport=80 user=postgres@INTERGY.LOCAL proto=6 rcvdbyte=N/A sentbyte=N/A utmaction=userbrowsed utmevent=webfilter threat=N/A vd=root fctver=5.6.5.1150 os="Microsoft Windows Server 2012 R2 Standard Edition, 64-bit (build 9600)" usingpolicy="" service=http url=/en/ userinitiated=1 browsetime=2

Vacation to Dubai

date=2018-03-02 time=17:21:04 logver=2 type=traffic level=info sessionid=57844268 hostname=APOLLO pcdomain=intergy.local uid=8331A2218F7042CC8915BD7A467A56A6 devid=FCT8001160722535 fgtserial=FWF30D3X16002938 emsserial=N/A regip=N/A srcname=N/A srcproduct=N/A srcip=N/A srcport=N/A direction=outbound dstip=N/A remotename=res.www.vaxvacationaccessintl.com dstport=443 user=postgres@INTERGY.LOCAL proto=6 rcvdbyte=N/A sentbyte=N/A utmaction=userbrowsed utmevent=webfilter threat=N/A vd=root fctver=5.6.5.1150 os="Microsoft Windows Server 2012 R2 Standard Edition, 64-bit (build 9600)" usingpolicy="" service=https url=/Booking/travelerspaymentinfo/default.aspx?itin=2&shoppingid=AAEAAAD/////AQAAAAAAAAAGAQAAABMxNjU5ODI1MDg1NDY1MTE1NzU5Cw== userinitiated=1 browsetime=20

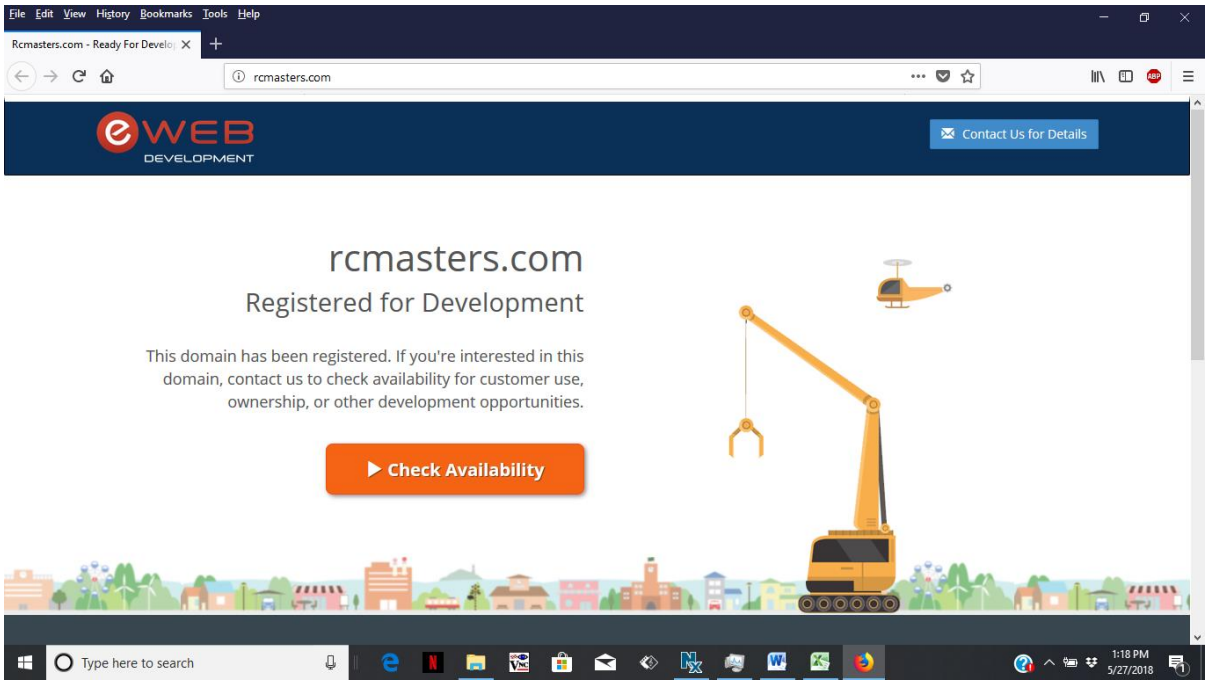
date=2018-03-12 time=15:34:27 logver=2 type=traffic level=info sessionid=57452524 hostname=APOLLO pcdomain=intergy.local uid=8331A2218F7042CC8915BD7A467A56A6 devid=FCT8001160722535 fgtserial=N/A emsserial=N/A regip=N/A srcname=N/A srcproduct=N/A srcip=N/A srcport=N/A direction=outbound dstip=N/A remotename=uploaded.net dstport=80 user=postgres@INTERGY.LOCAL proto=6 rcvdbyte=N/A sentbyte=N/A utmaction=userbrowsed utmevent=webfilter threat=N/A vd=N/A fctver=5.6.5.1150 os="Microsoft Windows Server 2012 R2 Standard Edition, 64-bit (build 9600)" usingpolicy="" service=http url=/file/xs3xx6gc userinitiated=1 browsetime=1

Exfiltration of data



date=2018-03-12 time=05:57:45 logver=2 type=traffic level=info sessionid=57452524 hostname=APOLLO pcdomain=intergy.local uid=8331A2218F7042CC8915BD7A467A56A6 devid=FCT8001160722535 fgtserial=N/A emsserial=N/A regip=N/A srcname=N/A srcproduct=N/A srcip=N/A srcport=N/A direction=outbound dstip=N/A remotename=" include \"lib.event.tis\" include \"lib.GUIDebugger.tis\"; include \"lib.tooltip.tis\" include \"lib.animations.tis\" include \"li" dstport=N/A user=postgres@INTERGY.LOCAL proto=6 rcvdbyte=N/A sentbyte=N/A utmaction=userbrowsed utmevent=webfilter threat=N/A vd=N/A fctver=5.6.5.1150 os="Microsoft Windows Server 2012 R2 Standard Edition, 64-bit (build 9600)" usingpolicy="" service=http url="/2/2013 * @author \\n * @author Copyright (c) 2013 ESET, spol. s r. o. * @note current owner: Juraj Sipos (sipos@eset.sk) * @note IMPORTANT: Before doing any significant change to this file check your plan with the current owner to avoid unexpected behavior. */ <div class=\"label\">{{label}} <widget type=\"select-dropdown\" novalue=\"{{novalue}}\"> {{#items}} <option value=\"{{value}}\" depth=\"{{depth}}\" >{{text}}</option> {{/items}} </widgetpostgres@INTERGY.LOCAL userinitiated=1 browsetime=9

Manipulation of Fortinet Firewall by software engineer in Juraj Sipos in the Slovak Republic



Exfiltration of data to Web Development Tor C2 data center

date=2018-03-12 time=00:56:22 logver=2 type=traffic level=warning sessionid=57452524 hostname=APOLLO pcdomain=intergy.local uid=8331A2218F7042CC8915BD7A467A56A6 devid=FCT8001160722535 fgtserial=FWF30D3X16002938 emsserial=N/A regip=N/A srcname=firefox.exe srcproduct=Firefox srcip=192.168.2.12 srcport=55357 direction=outbound dstip=35.182.185.60 remotename=upload-file.com dstport=80 user=postgres@INTERGY.LOCAL proto=6 rcvdbyte=N/A sentbyte=N/A utmaction=blocked utmevent=antivirus threat="Security Risk:Newly Observed Domain" vd=root fctver=5.6.5.1150 os="Microsoft Windows Server 2012 R2 Standard Edition, 64-bit (build 9600)" usingpolicy="" service=http url=/ userinitiated=0 browsetime=N/A	The IP address location of 35.182.185.60 is "Montreal H3G, Quebec (QC), Canada (CA)". 35.182.185.60 is a public IP address that belongs to ASN 16509 which is under the control of "Amazon.com, Inc.". The prefix 035/8 (35.0.0.0/8) was delegated for administration to "ARIN" by the Internet Assigned Numbers Authority (IANA) in April 1994.

Reverse IP address lookup is the process of mapping an IP address to its corresponding hostnames. Below you will find a list of hostnames that resolve to IP address 35.182.185.60.

www.eicat.com www.globusconsulting.com www.rcmasters.com pastein.com tonation.com **www.projectlaw.com** saimiri.com **www.doofmann.com www.pressworker.com** allyindustries.com server.starkad.com link88.com **www.stand-together.com www.tupina.com www.synspire.com www.ittranslation.com** report-covers.com **www.mtstyle.com www.mixbase.com www.hard-power.com www.hh-cc.com www.target-market.com** ns2.servercities.com **www.tlicious.com** paleda.com

Video references

What is QUIC?

https://www.youtube.com/watch?v=WNsxD-D4Zak

QUIC and WebRTC DataChannels - Ian Swett https://www.youtube.com/watch?v=mIvyOFu1c1Q

QUIC Next generation multiplexed transport over UDP

https://www.youtube.com/watch?v=cSNT88_gedw

Iliyan Peychev: HTTP 2.0 and QUIC - protocols of the (near) future | JSConf EU 2014

https://www.youtube.com/watch?v=qyexqwG6fGI

How Secure and Quick is QUIC? Provable Security and Performance Analyses

https://www.youtube.com/watch?v=vXgbPZ-1-us

How To Hide a Virus Payload in JPG Image -Undetectable Backdoor

https://www.youtube.com/watch?v=KTkm33xmnFY

Veil-Evasion - How To Generate Undetectable Payloads | Antivirus Bypass

https://www.youtube.com/watch?v=iz1twCSJZyo

Ochko123 - How the Feds Caught Russian Mega-Carder Roman Seleznev

https://www.youtube.com/watch?v=6Chp12sEnWk

Internet Hackers in 2017 Documentary

https://www.youtube.com/watch?v=fX3JReuIMyo

Anonymous Down The Deep Dark Web Documentary

https://www.youtube.com/watch?v=oslnoIWh__Q

APT28' A Window into Russia's Cyber Espionage Operations - FireEye Part 2

https://www.youtube.com/watch?v=Q4qn1HQOt6s

Anatomy of an Advanced Persistent Threat (APT) Group

https://www.youtube.com/watch?v=SZCE677ijMU

One Team: Team FireEye

https://www.youtube.com/watch?v=dhogvQKRvpA

Cloud-based Threat Detection and Investigation – FireEye Threat Analytics Platform Demo

https://www.youtube.com/watch?v=1yCGzRzry4Q

Intro to Darknets Tor and I2P

https://www.youtube.com/watch?v=tjJYC2LuJlo

DEF CON 22 Touring the Darkside of the Internet An Introduction to Tor & Darknets and Bitcoin

https://www.youtube.com/watch?v=60X7Rd60VIk

Introduction to TOR

https://www.youtube.com/watch?v=pyq4vwxqvSI

How to access the Deep Web using Tor

https://www.youtube.com/watch?v=NQrUZdsw2hA

TOR Hidden Services – Computerphile

https://www.youtube.com/watch?v=lVcbq_a5N9I

Onion Routing – Computerphile

https://www.youtube.com/watch?v=QRYzre4bf7I

Finding Tor hidden services

https://www.youtube.com/watch?v=1SitlwcKEHs

How TOR (The Onion Router) Works

https://www.youtube.com/watch?v=C_-sG1P-q8E

Injecting Metasploit Payload To Android Apps [Hacking Android with Persistance

https://www.youtube.com/watch?v=I2bZbf4DjHM

Hacking Android Smartphone With Metasploit [Explained / Tutorial]

https://www.youtube.com/watch?v=gfAE1xVBNdo

"60 Minutes" shows how easily your phone can be hacked

https://www.youtube.com/watch?v=zGUR6ka09ys

Find Out Who's Tracking You Through Your Phone

https://www.youtube.com/watch?v=OYKPvPbm2jA

What is multipath TCP?

https://www.youtube.com/watch?v=r0SNmm3FOU4

Multipath TCP Tutorial

https://www.youtube.com/watch?v=WpoKr3B64tA

Multipath TCP

https://www.youtube.com/watch?v=02nBaaIoFWU

Anonymous Down The Deep Dark Web Documentary

https://www.youtube.com/watch?v=oslnoIWh__Q

Sentry Mba Netflix Config Tutorial Hack/Crack

https://www.youtube.com/watch?v=ok9er3OTEiY

How to hack Fb Accounts Using Sentry Mba 100 % Working Guarantee

https://www.youtube.com/watch?v=DfiUyhPGuiE

Sentry MBA V1.4.2 MODED

(مـ بـ تدىء مـ سـ توى)الـ كوذ فج عمل كـ يـ فـ يه-الـ رابـ ع الـ درس-الـ مواق ع تـ كريـ ك دوره

https://www.youtube.com/watch?v=l1CcicQRNOI

Crack Netflix with Sentry MBA+being sport config 2017

https://www.youtube.com/watch?v=3T66LQNTRIM

Alpha Crack™

https://www.youtube.com/channel/UCmtnLpMvres_04Ezsza_2GA

Today Show[29]|Cracking Fitbit.com| Sentry MBA Proxyless|Variable config

https://www.youtube.com/watch?v=YPCrsrOyaWo

Cracking Home by Ahmed Swailm

http://www.crackinghome.tk/

https://www.youtube.com/channel/UCawaKAtNztgT3HPZCzJyJbw

https://www.facebook.com/ahmedswailm2

https://www.youtube.com/user/egy2u/videos

3D Mark Advanced Edition 1.3.708

https://www.picktorrent.com/torrents/3dmark-advanced-edition-1-3-708/

https://www.cybrary.it/op3n/pentesting-sqli-dumper-v8-tool/

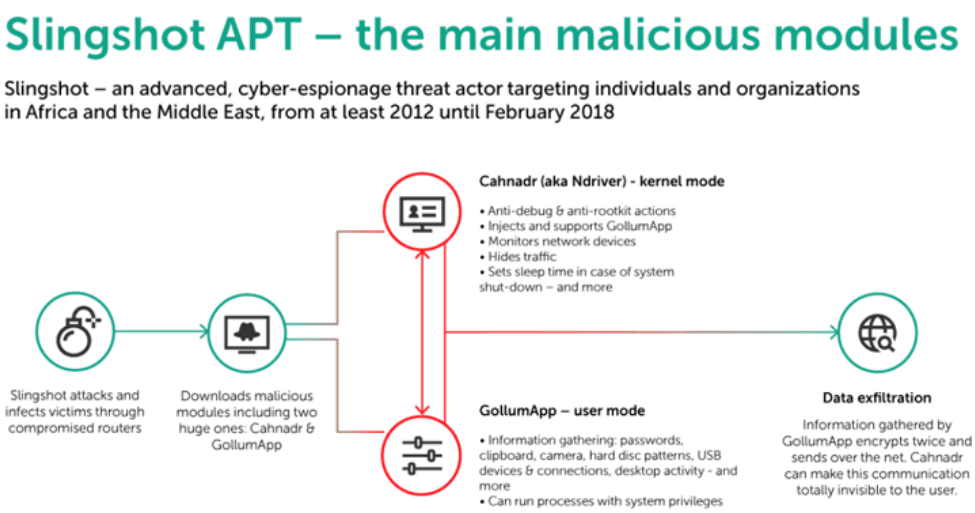
SLINGSHOT Stage 2 attack

Begins 2018-03-25 23:31:02 Ends 2018-04-11 16:58:36 when Mikrotik VoIP router was reset and firmware updated. Port 0 Linux ***SLINGSHOT*** exploit uses, ***BusyBox***, a software that provides several stripped-down Unix tools in a single executable file. It runs in a variety of POSIX environments such as Linux, Android, and FreeBSD, although many of the tools it provides are designed to work with interfaces provided by the Linux kernel. It was specifically created for embedded operating systems with very limited resources. The authors dubbed it "The Swiss Army knife of Embedded Linux", as the single executable replaces basic functions of more than 300 common commands. It is released as free software under the terms of the GNU General Public License v2.

Once the router is compromised, the attackers replace one of its DDL (dynamic link libraries) file with a malicious one from the file-system, which loads directly into the victim's computer memory when the user runs Winbox Loader software.

Defending against this threat

Defense against this threat is incredibly difficult due to the embedded nature of the OS on the affected devices. The majority of SOHO devices are connected directly to the internet, with no managed security device or firewall between device and combatants. This challenge is augmented by the fact that most of the affected devices have publicly known vulnerabilities which are not convenient for the average user to patch. Additionally, these devices have no built-in anti-malware capabilities. These three facts together make this threat extremely hard to counter, resulting in extremely limited opportunities to employ any type of defensive security. A list of various tactics used to exploit systems by class has been compiled to aid in the defense of systems from an APT.

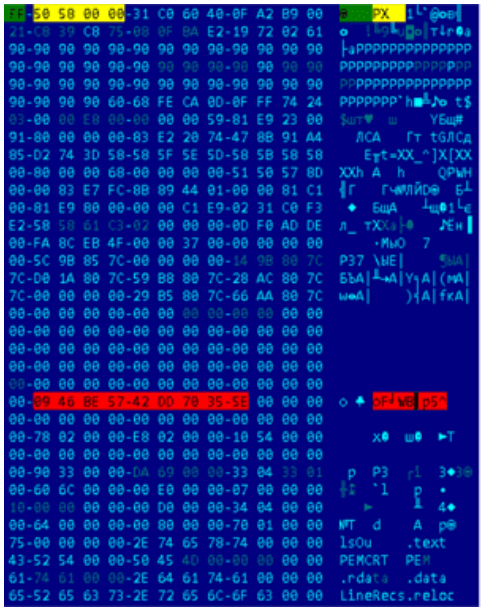


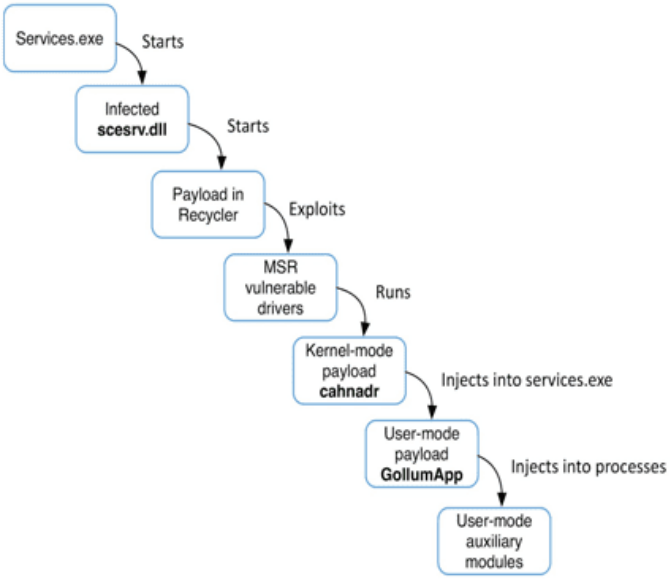
Winbox Loader is a legitimate management tool designed by Mikrotik for Windows users to easily configure their routers that downloads some DLL files from the router and execute them on a system. This way the malicious DLL file runs on the targeted computer and connects to a remote server to download the final payload, i.e., Slingshot malware.

Slingshot malware includes two modules—**Cahnadr** (a kernel mode module) and **GollumApp** (a user mode module), designed for information gathering, persistence and data exfiltration. Cahnadr module, aka NDriver, takes care of anti-debugging, rootkit and sniffing functionality, injecting other modules, network communications—basically all the capabilities required by user-mode modules. "[Cahnadr is a] kernel-mode program is able to execute malicious code without crashing the whole file system or causing Blue Screen.

Written in pure C language, Canhadr/Ndriver provides full access to the hard drive and operating memory despite device security restrictions, and carries out integrity control of various system components to avoid debugging and security detection.

Whereas GollumApp is the most sophisticated module which has a wide range of spying functionalities that allow attackers to capture screenshots, collect network-related information, passwords saved in web browsers, all pressed keys, and maintains communication with remote command-and-control servers.





Since GollumApp runs in kernel mode and can also run new processes with SYSTEM privileges, the malware gives attackers full control of the infected systems.

Although Kaspersky has not attributed this group to any country but based on clever techniques it used and limited targets, the security firm concluded that it is definitely a highly skilled and English-speaking state-sponsored hacking group.

"Slingshot is very complex, and the developers behind it have clearly spent a great deal of time and money on its creation. Its infection vector is remarkable—and, to the best of our knowledge, unique," researchers say.

SLINGSHOT attack log data

Load More (53 incidents left)

The first incident:

2018-03-25 23:31:02

{

"PORT HIT": "97.77.211.30:58479->89.#.#.4:23",

"MESSAGES": "Array

(

[08:30:24] => enable

system

shell

sh

[08:30:24+1] => cat /proc/mounts; /bin/busybox SJCLS

)

TOI Tactics

Adversarial Tactics, Techniques & Common Knowledge

For in-depth technical descriptions, discussions, references, details and intelligence on the methods used, click on the links below for Adversarial Tactics Techniques and Common Knowledge Wiki links below. MITRE's Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK™) is a curated knowledge base and model for cyber adversary behavior, reflecting the various phases of an adversary's lifecycle and the platforms they are known to target. ATT&CK is useful for understanding security risk against known adversary behavior, for planning security improvements, and verifying defenses work as expected.

Execution

AppleScript CMSTP Command-Line Interface Control Panel Items Dynamic Data Exchange Execution through API Execution through Module Load Exploitation for Client Execution Graphical User Interface InstallUtil LSASS Driver Launchctl Local Job Scheduling Mshta PowerShell Regsvcs/Regasm Regsvr32 Rundll32 Scheduled Task Scripting Service Execution Signed Binary Proxy Execution Signed Script Proxy Execution Source Space after Filename Third-party Software Trap Trusted Developer Utilities User Execution Windows Management Instrumentation Windows Remote Management

Persistence

.bash_profile and .bashrc Accessibility Features AppCert DLLs AppInit DLLs Application Shimming Authentication Package BITS Jobs Bootkit Browser Extensions Change Default File Association Component Firmware Component Object Model Hijacking Create Account DLL Search Order Hijacking Dylib Hijacking External Remote Services File System

Permissions Weakness Hidden Files and Directories Hooking Hypervisor Image File Execution Options Injection Kernel Modules and Extensions LC_LOAD_DYLIB Addition LSASS Driver Launch Agent Launch Daemon Launchctl Local Job Scheduling Login Item Logon Scripts Modify Existing Service Netsh Helper DLL New Service Office Application Startup Path Interception Plist Modification Port Knocking Port Monitors Rc.common Re-opened Applications Redundant Access Registry Run Keys / Start Folder SIP and Trust Provider Hijacking Scheduled Task Screensaver Security Support Provider Service Registry Permissions Weakness Shortcut Modification Startup Items System Firmware

Privilege Escalation

Access Token Manipulation Accessibility Features AppCert DLLs AppInit DLLs Application Shimming Bypass User Account Control DLL Search Order Hijacking Dylib Hijacking Exploitation for Privilege Escalation Extra Window Memory Injection File System Permissions Weakness Hooking Image File Execution Options Injection Launch Daemon New Service Path Interception Plist Modification Port Monitors Process Injection SID-History Injection Scheduled Task Service Registry Permissions Weakness Setuid and Setgid Startup Items Sudo Sudo Caching Valid Accounts Web Shell

Discovery

Account Discovery Application Window Discovery Browser Bookmark Discovery File and Directory Discovery Network Service Scanning Network Share Discovery Password Policy Discovery Peripheral Device Discovery Permission Groups Discovery Process Discovery Query Registry Remote System Discovery Security Software Discovery System Information Discovery System Network Configuration Discovery System Network Connections Discovery System Owner/User Discovery System Time Discovery

Defense Evasion

Access Token Manipulation BITS Jobs Binary Padding Bypass User Account Control CMSTP Clear Command History Code Signing Component Firmware Component Object Model Hijacking Control Panel Items DCShadow DLL Search Order Hijacking DLL Side-Loading Deobfuscate/Decode Files or Information Disabling Security Tools Exploitation for Defense Evasion Extra Window Memory Injection File Deletion File System Logical Offsets Gatekeeper Bypass HISTCONTROL Hidden Files and Directories Hidden Users Hidden Window Image File Execution Options Injection Indicator Blocking Indicator Removal from Tools Indicator Removal on Host Indirect Command Execution Install Root Certificate InstallUtil LC_MAIN Hijacking Launchctl Masquerading Modify Registry Mshta NTFS File Attributes Network Share Connection Removal Obfuscated Files or Information Plist Modification Port Knocking Process Doppelgänging Process Hollowing Process Injection

Redundant Access Regsvcs/Regasm Regsvr32 Rootkit Rundll32 SIP and Trust Provider Hijacking

Lateral Movement

AppleScript Application Deployment Software Distributed Component Object Model Exploitation of Remote Services Logon Scripts Pass the Hash Pass the Ticket Remote Desktop Protocol Remote File Copy Remote Services Replication Through Removable Media SSH Hijacking Shared Webroot Taint Shared Content Third-party Software Windows Admin Shares Windows Remote Management

Collection

Audio Capture Automated Collection Clipboard Data Data Staged Data from Information Repositories Data from Local System Data from Network Shared Drive Data from Removable Media Email Collection Input Capture Man in the Browser Screen Capture Video Capture

Exfiltration

Automated Exfiltration Data Compressed Data Encrypted Data Transfer Size Limits Exfiltration Over Alternative Protocol Exfiltration Over Command and Control Channel Exfiltration Over Other Network Medium Exfiltration Over Physical Medium Scheduled Transfer

Command and Control

Commonly Used Port Communication Through Removable Media Connection Proxy Custom Command and Control Protocol Custom Cryptographic Protocol Data Encoding Data Obfuscation Domain Fronting Fallback Channels Multi-Stage Channels Multi-hop Proxy Multiband Communication Multilayer Encryption Port Knocking Remote Access Tools Remote File Copy Standard Application Layer Protocol Standard Cryptographic Protocol Standard Non-Application Layer Protocol Uncommonly Used Port Web Service

Credential Access

Account Manipulation Bash History Brute Force Credential Dumping Credentials in Files Credentials in Registry Exploitation for Credential Access Forced Authentication Hooking Input Capture Input Prompt Kerberoasting Keychain LLMNR/NBT-NS Poisoning Network

Sniffing Password Filter DLL Private Keys Replication Through Removable Media Securityd Memory Two-Factor Authentication Interception

The Combatant's Capabilities

Lateral movement consists of techniques that enable a combatant to access and control remote systems on a network and could, but does not necessarily; include execution of tools on remote systems. The lateral movement techniques could allow a combatant to gather information from a system without needing additional tools, such as a remote access tool.

A combatant can use lateral movement for many purposes, including remote execution of tools, pivoting to additional systems, access to specific information or files, access to additional credentials, or to cause an effect. The ability to remotely execute scripts or code can be a feature of combatant remote access tools, but TOI's may also reduce their tool footprint on the network by using legitimate credentials alongside inherent network and operating system functionality to remotely connect to systems.

Movement across a network from one system to another may be necessary to achieve a combatant's goals. Thus lateral movement, and the techniques that lateral movement relies on, are often very important to a combatant's set of capabilities and part of a broader set of information and access dependencies that the combatant takes advantage of within a network. To understand intrinsic security dependencies, it is important to know the relationships between accounts and access privileges across all systems on a network.1 Lateral movement may not always be a requirement for a combatant. If a combatant can reach the goal with access to the initial system, then additional movement throughout a network may be unnecessary

Tactics

AppleScript

MacOS and OS X applications send AppleEvent messages to each other for interprocess communications (IPC). These messages can be easily scripted with AppleScript for local or remote IPC. Osascript executes AppleScript and any other Open Scripting Architecture (OSA) language scripts. A list of OSA languages installed on a system can be found by using the osalang program.

AppleEvent messages can be sent independently or as part of a script. These events can locate open windows, send keystrokes, and interact with almost any open application locally or remotely.

TOI's can use this to interact with open SSH connection, move to remote machines, and even present users with fake dialog boxes. These events cannot start applications remotely (they can start them locally though), but can interact with applications if they're already running remotely. Since this is a scripting language, it can be used to launch more common techniques as well such

as a reverse shell via python [2]. Scripts can be run from the command lie via osascript /path/to/script or osascript -e "script here".

Application Deployment Software

TOI's may deploy malicious software to systems within a network using application deployment systems employed by enterprise administrators. The permissions required for this action vary by system configuration; local credentials may be sufficient with direct access to the deployment server, or specific domain credentials may be required. However, the system may require an administrative account to log in or to perform software deployment. Access to a network-wide or enterprise-wide software deployment system enables a combatant to have remote code execution on all systems that are connected to such a system. The access may be used to laterally move to systems, gather information, or cause a specific effect, such as wiping the hard drives on all endpoints.

Distributed Component Object Model

Windows Distributed Component Object Model (DCOM) is transparent middleware that extends the functionality of Component Object Model (COM)3 beyond a local computer using remote procedure call (RPC) technology. COM is a component of the Windows application programming interface (API) that enables interaction between software objects. Through COM, a client object can call methods of server objects, which are typically Dynamic Link Libraries (DLL) or executables (EXE).

Permissions to interact with local and remote server COM objects are specified by access control lists (ACL) in the Registry.456 By default, only Administrators may remotely activate and launch COM objects through DCOM.

TOI's may use DCOM for lateral movement. Through DCOM, TOI's operating in the context of an appropriately privileged user can remotely obtain arbitrary and even direct shellcode execution through Office applications7 as well as other Windows objects that contain insecure methods.89 DCOM can also execute macros in existing documents10 and may also invoke Dynamic Data Exchange (DDE) execution directly through a COM created instance of a Microsoft Office application11, bypassing the need for a malicious document.

Exploitation of Remote Services

Exploitation of a software vulnerability occurs when a combatant takes advantage of a programming error in a program, service, or within the operating system software or kernel itself to execute combatant-controlled code. A common goal for post-compromise exploitation of remote services is for lateral movement to enable access to a remote system.

An combatant may need to determine if the remote system is in a vulnerable state, which may be done through Network Service Scanning or other Discovery methods looking for common, vulnerable software that may be deployed in the network, the lack of certain patches that may

indicate vulnerabilities, or security software that may be used to detect or contain remote exploitation. Servers are likely a high value target for lateral movement exploitation, but endpoint systems may also be at risk if they provide an advantage or access to additional resources.

There are several well-known vulnerabilities that exist in common services such as SMB12 and RDP13 as well as applications that may be used within internal networks such as MySQL14 and web server services.15

Depending on the permissions level of the vulnerable remote service and combatant may achieve Exploitation for Privilege Escalation as a result of lateral movement exploitation as well.

Logon Scripts

Windows allows logon scripts to be run whenever a specific user or group of users log into a system.16 The scripts can be used to perform administrative functions, which may often execute other programs or send information to an internal logging server.

If TOI's can access these scripts, they may insert additional code into the logon script to execute their tools when a user logs in. This code can allow them to maintain persistence on a single system, if it is a local script, or to move laterally within a network, if the script is stored on a central server and pushed to many systems. Depending on the access configuration of the logon scripts, either local credentials or an administrator account may be necessary.

Mac allows login and logoff hooks to be run as root whenever a specific user logs into or out of a system. A login hook tells Mac OS X to execute a certain script when a user logs in, but unlike startup items, a login hook executes as root17. There can only be one login hook at a time though. If TOI's can access these scripts, they can insert additional code to the script to execute their tools when a user logs in.

Pass the Hash

Pass the hash (PtH) is a method of authenticating as a user without having access to the user's cleartext password. This method bypasses standard authentication steps that require a cleartext password, moving directly into the portion of the authentication that uses the password hash. In this technique, valid password hashes for the account being used are captured using a Credential Access technique. Captured hashes are used with PtH to authenticate as that user. Once authenticated, PtH may be used to perform actions on local or remote systems. Windows 7 and higher with KB2871997 require valid domain user credentials or RID 500 administrator hashes.

Pass the Ticket

Pass the ticket (PtT) is a method of authenticating to a system using Kerberos tickets without having access to an account's password. Kerberos authentication can be used as the first step to lateral movement to a remote system.

In this technique, valid Kerberos tickets for Valid Accounts are captured by Credential Dumping. A user's service tickets or ticket granting ticket (TGT) may be obtained, depending on the level of access. A service ticket allows for access to a particular resource, whereas a TGT can be used to request service tickets from the Ticket Granting Service (TGS) to access any resource the user has privileges to access.1920

Silver Tickets can be obtained for services that use Kerberos as an authentication mechanism and are used to generate tickets to access that particular resource and the system that hosts the resource (e.g., SharePoint).19

Golden Tickets can be obtained for the domain using the Key Distribution Service account KRBTGT account NTLM hash, which enables generation of TGTs for any account in Active Directory

Remote Desktop Protocol

Remote desktop is a common feature in operating systems. It allows a user to log into an interactive session with a system desktop graphical user interface on a remote system. Microsoft refers to its implementation of the Remote Desktop Protocol (RDP) as Remote Desktop Services (RDS). There are other implementations and third-party tools that provide graphical access Remote Services similar to RDS.

TOI's may connect to a remote system over RDP/RDS to expand access if the service is enabled and allows access to accounts with known credentials. TOI's will likely use Credential Access techniques to acquire credentials to use with RDP. TOI's may also use RDP in conjunction with the Accessibility Features technique for Persistence.

TOI's may also perform RDP session hijacking which involves stealing a legitimate user's remote session. Typically, a user is notified when someone else is trying to steal their session and prompted with a question. With System permissions and using Terminal Services Console, c:\windows\system32\tscon.exe [session number to be stolen], and a combatant can hijack a session without the need for credentials or prompts to the user. This can be done remotely or locally and with active or disconnected sessions. It can also lead to Remote System Discovery and Privilege Escalation by stealing a Domain Admin or higher privileged account session. All of this can be done by using native Windows commands, but it has also been added as a feature in RedSnarf

Remote File Copy

Files may be copied from one system to another to stage combatant tools or other files over the course of an operation. Files may be copied from an external combatant-controlled system through the Command and Control channel to bring tools into the victim network or through alternate protocols with another tool such as FTP. Files can also be copied over on Mac and Linux with native tools like scp, rsync, and sftp. TOI's may also copy files laterally between internal victim systems to support Lateral Movement with remote Execution using inherent file sharing

protocols such as file sharing over SMB to connected network shares or with authenticated connections with Windows Admin Shares or Remote Desktop Protocol.

Remote Services

A combatant may use Valid Accounts to log into a service specifically designed to accept remote connections, such as telnet, SSH, and VNC. The combatant may then perform actions as the logged-on user

Replication Through Removable Media

TOI's may move onto systems, possibly those on disconnected or air-gapped networks, by copying malware to removable media and taking advantage of Autorun features when the media is inserted into a system and executes. In the case of Lateral Movement, this may occur through modification of executable files stored on removable media or by copying malware and renaming it to look like a legitimate file to trick users into executing it on a separate system. In the case of Initial Access, this may occur through manual manipulation of the media, modification of systems used to initially format the media, or modification to the media's firmware itself.

SSH Hijacking

Secure Shell (SSH) is a standard means of remote access on Linux and Mac systems. It allows a user to connect to another system via an encrypted tunnel, commonly authenticating through a password, certificate or the use of an asymmetric encryption key pair.

In order to move laterally from a compromised host, TOI's may take advantage of trust relationships established with other systems via public key authentication in active SSH sessions by hijacking an existing connection to another system. This may occur through compromising the SSH agent itself or by having access to the agent's socket. If an combatant is able to obtain root access, then hijacking SSH sessions is likely trivial.272829 Compromising the SSH agent also provides access to intercept SSH credentials.30

SSH Hijacking differs from use of Remote Services because it injects into an existing SSH session rather than creating a new session using Valid Accounts

Shared Webroot

TOI's may add malicious content to an internally accessible website through an open network file share that contains the website's webroot or Web content directory and then browse to that content with a Web browser to cause the server to execute the malicious content. The malicious content will typically run under the context and permissions of the Web server process, often resulting in local system or administrative privileges, depending on how the Web server is configured. This mechanism of shared access and remote execution could be used for lateral movement to the system running the Web server. For example, a Web server running PHP with

an open network share could allow a combatant to upload a remote access tool and PHP script to execute the RAT on the system running the Web server when a specific page is visited.

Taint Shared Content

Content stored on network drives or in other shared locations may be tainted by adding malicious programs, scripts, or exploit code to otherwise valid files. Once a user opens the shared tainted content, the malicious portion can be executed to run the combatant's code on a remote system. TOI's may use tainted shared content to move laterally. A directory share pivot is a variation on this technique that uses several other techniques to propagate malware when users access a shared network directory. It uses Shortcut Modification of directory .LNK files that use Masquerading to look like the real directories, which are hidden through Hidden Files and Directories. The malicious .LNK-based directories have an embedded command that executes the hidden malware file in the directory and then opens the real intended directory so that the user's expected action still occurs. When used with frequently used network directories, the technique may result in frequent reinfections and broad access to systems and potentially to new and higher privileged accounts

Third-party Software

Third-party applications and software deployment systems may be in use in the network environment for administration purposes (e.g., SCCM, VNC, HBSS, Altiris, etc.). If a combatant gains access to these systems, then they may be able to execute code.

TOI's may gain access to and use third-party application deployment systems installed within an enterprise network. Access to a network-wide or enterprise-wide software deployment system enables a combatant to have remote code execution on all systems that are connected to such a system. The access may be used to laterally move to systems, gather information, or cause a specific effect, such as wiping the hard drives on all endpoints.

The permissions required for this action vary by system configuration; local credentials may be sufficient with direct access to the deployment server, or specific domain credentials may be required. However, the system may require an administrative account to log in or to perform software deployment.

Windows Admin Shares

Windows systems have hidden network shares that are accessible only to administrators and provide the ability for remote file copy and other administrative functions. Example network shares include C$, ADMIN$, and IPC$.

TOI's may use this technique in conjunction with administrator-level Valid Accounts to remotely access a networked system over server message block (SMB) to interact with systems using remote procedure calls (RPCs), transfer files, and run transferred binaries through remote Execution. Example execution techniques that rely on authenticated sessions over SMB/RPC are

Scheduled Task, Service Execution, and Windows Management Instrumentation. TOI's can also use NTLM hashes to access administrator shares on systems with Pass the Hash and certain configuration and patch levels.

The *Net* utility can be used to connect to Windows admin shares on remote systems using net use commands with valid credentials.

Windows Remote Management

Windows Remote Management (WinRM) is the name of both a Windows service and a protocol that allows a user to interact with a remote system (e.g., run an executable, modify the Registry, and modify services). It may be called with the winrm command or by any number of programs such as PowerShell

Reconnaissance

Russian state-sponsored cyber combatants have conducted both broad-scale and targeted scanning of Internet address spaces. Such scanning allows these combatants to identify enabled Internet-facing ports and services, conduct device fingerprinting, and discover vulnerable network infrastructure devices. Protocols targeted in this scanning include

Telnet (typically Transmission Control Protocol (TCP) port 23, but traffic can be directed to a wide range of TCP ports such as 80, 8080, etc.),

Hypertext Transport Protocol (HTTP, port 80),

Simple Network Management Protocol (SNMP, ports 161/162), and

Cisco Smart Install (SMI port 4786).

Login banners and other data collected from enabled services can reveal the make and model of the device and information about the organization for future engagement.

Device configuration files extracted in previous operations can enhance the reconnaissance effort and allow these combatants to refine their methodology.

Cookies to Russian domains January 20th 2018,

yandexuid	yp	i	
2460840315116434163	1831794163.yrts.1516434163	U2mxsT1p2VkZSsy+NLXBxIabtBaWMdRcx390pMV970SGfQIVk5rpMw1jot12doTsg5hO7Q072CQuJaoqHwG63Xw2h3U=	
yandex.ru/	yandex.ru/	yandex.ru/	
2147484672	2147484672	2147492864	
4179483520	4179483520	4179483520	
31376880	31376880	31376880	

1097903192 30642626 * *	1098058940 30642626	1098058940 30642626 *	

Weaponization

Commercial and government security organizations have identified specially crafted SNMP and SMI packets that trigger the scanned device to send its configuration file to a cyber-actor-controlled host via Trivial File Transfer Protocol (TFTP), User Datagram Protocol (UDP) port 69. The configuration file contains a significant amount of information about the scanned device, including password hash values. These values allow cyber combatants to derive legitimate credentials. The configuration file also contains SNMP community strings and other network information that allows the cyber combatants to build network maps and facilitate future targeted exploitation.

Delivery

If the targeted network is blocking external SNMP at the network boundary, cyber combatants spoof the source address of the SNMP UDP datagram as coming from inside the targeted network. The design of SMI (directors and clients) requires the director and clients to be on the same network. However, since SMI is an unauthenticated protocol, the source address for SMI is also susceptible to spoofing.

Exploitation

Legitimate user masquerade is the primary method by which these cyber combatants exploit targeted network devices. In some cases, the combatants use brute-force attacks to obtain Telnet and SSH login credentials. However, for the most part, cyber combatants are able to easily obtain legitimate credentials, which they then use to access routers. Organizations that permit default or commonly used passwords, have weak password policies, or permit passwords that can be derived from credential-harvesting activities, allow cyber combatants to easily guess or access legitimate user credentials. Cyber combatants can also access legitimate credentials by extracting password hash values from configurations sent by owners and operators across the Internet or by SNMP and SMI scanning.

Armed with the legitimate credentials, cyber combatants can authenticate into the device as a privileged user via remote management services such as Telnet, SSH, or the web management interface.

Installation

SMI is an unauthenticated management protocol developed by Cisco. This protocol supports a feature that allows network administrators to download or overwrite any file on any Cisco router or switch that supports this feature. This feature is designed to enable network administrators to remotely install and configure new devices and install new OS files.

On November 18, 2016, a Smart Install Exploitation Tool (SIET) was posted to the Internet. The SIET takes advantage of the unauthenticated SMI design. Commercial and government security organizations have noted that Russian state-sponsored cyber combatants have leveraged the SIET to abuse SMI to download current configuration files. Of concern, any actor may leverage this capability to overwrite files to modify the device configurations, or upload maliciously modified OS or firmware to enable persistence. Additionally, these network devices have writeable file structures where malware for other platforms may be stored to support lateral movement throughout the targeted network.

Command and Control

Cyber combatants masquerade as legitimate users to log into a device or establish a connection via a previously uploaded OS image with a backdoor. Once successfully logged into the device, cyber combatants execute privileged commands. These cyber combatants create a man-in-the-middle scenario that allows them to

- extract additional configuration information,
- export the OS image file to an externally located cyber actor-controlled FTP server,
- modify device configurations,
- create Generic Routing Encapsulation (GRE) tunnels, or
- mirror or redirect network traffic through other network infrastructure they control.

At this stage, cyber combatants are not restricted from modifying or denying traffic to and from the victim. Although there are no reports of this activity, it is technically possible.

Tactical Communications Behavior

The command and control tactic represents how TOI's communicate with systems under their control within a target network. There are many ways a combatant can establish command and control with various levels of covertness, depending on system configuration and network topology. Due to the wide degree of variation available to the combatant at the network level, only the most common combatants were used to describe the differences in command and control. There are still a great many specific techniques within the documented methods, largely due to how easy it is to define new protocols and use existing, legitimate protocols and network services for communication.

The resulting breakdown should help convey the concept that detecting intrusion through command and control protocols without prior knowledge is a difficult proposition over the long term. TOI's' main constraints in network-level defense avoidance are testing and deployment of tools to rapidly change their protocols, awareness of existing defensive technologies, and access to legitimate Web services that, when used appropriately, make their tools difficult to distinguish from benign traffic.

Commonly Used Port

TOI's may communicate over a commonly used port to bypass firewalls or network detection systems and to blend with normal network activity to avoid more detailed inspection. They may use commonly open ports such as

TCP:80 (HTTP)

TCP:443 (HTTPS)

TCP:25 (SMTP)

TCP/UDP:53 (DNS)

They may use the protocol associated with the port or a completely different protocol.

For connections that occur internally within an enclave (such as those between a proxy or pivot node and other nodes), examples of common ports are

TCP/UDP:135 (RPC)

TCP/UDP:22 (SSH)

TCP/UDP:3389 (RDP)

Communication Through Removable Media

TOI's can perform command and control between compromised hosts on potentially disconnected networks using removable media to transfer commands from system to system. Both systems would need to be compromised, with the likelihood that an Internet-connected system was compromised first and the second through lateral movement by Replication Through Removable Media. Commands and files would be relayed from the disconnected system to the Internet-connected system to which the combatant has direct access.

Connection Proxy

A connection proxy is used to direct network traffic between systems or act as an intermediary for network communications. Many tools exist that enable traffic redirection through proxies or port redirection, including HTRAN, ZXProxy, and ZXPortMap.

The definition of a proxy can also be expanded out to encompass trust relationships between networks in peer-to-peer, mesh, or trusted connections between networks consisting of hosts or systems that regularly communicate with each other.

The network may be within a single organization or across organizations with trust relationships. TOI's could use these types of relationships to manage command and control communications, to reduce the number of simultaneous outbound network connections, to provide resiliency in the face of connection loss, or to ride over existing trusted communications paths between victims to avoid suspicion.

Custom Command and Control Protocol

TOI's may communicate using a custom command and control protocol instead of using existing Standard Application Layer Protocol to encapsulate commands. Implementations could mimic well-known protocols.

Custom Cryptographic Protocol

TOI's may use a custom cryptographic protocol or algorithm to hide command and control traffic. A simple scheme, such as XOR-ing the plaintext with a fixed key, will produce a very weak ciphertext.

Custom encryption schemes may vary in sophistication. Analysis and reverse engineering of malware samples may be enough to discover the algorithm and encryption key used.

Some TOI's may also attempt to implement their own version of a well-known cryptographic algorithm instead of using a known implementation library, which may lead to unintentional errors.

Data Encoding

Command and control (C2) information is encoded using a standard data encoding system. Use of data encoding may be to adhere to existing protocol specifications and includes use of ASCII, Unicode, Base64, MIME, UTF-8, or other binary-to-text and character encoding systems. Some data encoding systems may also result in data compression, such as gzip.

Data Obfuscation

Command and control (C2) communications are hidden (but not necessarily encrypted) in an attempt to make the content more difficult to discover or decipher and to make the communication less conspicuous and hide commands from being seen. This encompasses many methods, such as adding junk data to protocol traffic, using steganography, commingling legitimate traffic with C2 communications traffic, or using a non-standard data encoding system, such as a modified Base64 encoding for the message body of an HTTP request.

Domain Fronting

Domain fronting takes advantage of routing schemes in Content Delivery Networks (CDNs) and other services which host multiple domains to obfuscate the intended destination of HTTPS traffic or traffic tunneled through HTTPS.5 The technique involves using different domain names in the SNI field of the TLS header and the Host field of the HTTP header. If both domains are served from the same CDN, then the CDN may route to the address specified in the HTTP header after unwrapping the TLS header. A variation of the technique, "domainless" fronting, utilizes a SNI field that is left blank; this may allow the fronting to work even when the CDN attempts to validate that the SNI and HTTP Host fields match (if the blank SNI fields are ignored). For example, if domain-x and domain-y are customers of the same CDN, it is possible to place domain-x in the TLS header and domain-y in the HTTP header. Traffic will appear to be going to domain-x, however the CDN may route it to domain-y.

Fallback Channels

TOI's may use fallback or alternate communication channels if the primary channel is compromised or inaccessible in order to maintain reliable command and control and to avoid data transfer thresholds.

Multi-Stage Channels

TOI's may create multiple stages for command and control that are employed under different conditions or for certain functions. Use of multiple stages may obfuscate the command and control channel to make detection more difficult.

Remote access tools will call back to the first-stage command and control server for instructions. The first stage may have automated capabilities to collect basic host information, update tools, and upload additional files. A second remote access tool (RAT) could be uploaded at that point to redirect the host to the second-stage command and control server. The second stage will likely be more fully featured and allow the combatant to interact with the system through a reverse shell and additional RAT features.

The different stages will likely be hosted separately with no overlapping infrastructure. The loader may also have backup first-stage callbacks or Fallback Channels in case the original first-stage communication path is discovered and blocked.

Multi-hop Proxy

To disguise the source of malicious traffic, TOI's may chain together multiple proxies. Typically, a defender will be able to identify the last proxy traffic traversed before it enters their network; the defender may or may not be able to identify any previous proxies before the last-hop proxy. This technique makes identifying the original source of the malicious traffic even more difficult by requiring the defender to trace malicious traffic through several proxies to identify its source.

Multiband Communication

Some TOI's may split communications between different protocols. There could be one protocol for inbound command and control and another for outbound data, allowing it to bypass certain firewall restrictions. The split could also be random to simply avoid data threshold alerts on any one communication.

Multilayer Encryption

A combatant performs C2 communications using multiple layers of encryption, typically (but not exclusively) tunneling a custom encryption scheme within a protocol encryption scheme such as HTTPS or SMTPS.

Port Knocking

Port Knocking is a well-established method used by both defenders and TOI's to hide open ports from access. To enable the port, the system expects a series of packets with certain characteristics before the port will be opened. This is often accomplished by the host based firewall, but could also be implemented by custom software.

This technique has been observed to both for the dynamic opening of a listening port as well as the initiating of a connection to a listening server on a different system.

The observation of the signal packets to trigger the communication can be conducted through different methods. One means, originally implemented by Cdoor, is to use the libpcap libraries to sniff for the packets in question. Another method leverages raw sockets, which enables the malware to use ports that are already open for use by other programs.

Remote Access Tools

TOI's may use legitimate desktop support and remote access software, such as Team Viewer, Go2Assist, LogMein, etc, to establish an interactive command and control channel to target systems within networks. These services are commonly used as legitimate technical support software, and may be whitelisted within a target environment. Remote access tools like VNC, , and Teamviewer are used frequently when compared with other legitimate software commonly used by TOI's.

Remote access tools may be established and used post-compromise as alternate communications channel for Redundant Access or as a way to establish an interactive remote desktop session with the target system. They may also be used as a component of malware to establish a reverse connection or back-connect to a service or combatant controlled system.

Admin tools such as TeamViewer have been used by several groups targeting institutions in countries of interest to the Russian state and criminal campaigns.

Remote File Copy

Files may be copied from one system to another to stage combatant tools or other files over the course of an operation. Files may be copied from an external combatant-controlled system through the **Command and Control** channel to bring tools into the victim network or through alternate protocols with another tool such as **FTP**. Files can also be copied over on Mac and Linux with native tools like scp, rsync, and sftp. TOI's may also copy files laterally between internal victim systems to support **Lateral Movement** with remote **Execution** using inherent file sharing protocols such as file sharing over SMB to connected network shares or with authenticated connections with **Windows Admin Shares** *or* **Remote Desktop Protocol**.

Standard Application Layer Protocol

TOI's may communicate using a common, standardized application layer protocol such as HTTP, HTTPS, SMTP, or DNS to avoid detection by blending in with existing traffic. Commands to the remote system, and often the results of those commands, will be embedded within the protocol traffic between the client and server. For connections that occur internally within an enclave (such as those between a proxy or pivot node and other nodes), commonly used protocols are RPC, SSH, or RDP

Standard Cryptographic Protocol

TOI's use command and control over an encrypted channel using a known encryption protocol like HTTPS or SSL/TLS. The use of strong encryption makes it difficult for defenders to detect signatures within combatant command and control traffic. Some TOI's may use other encryption protocols and algorithms with symmetric keys, such as RC4, that rely on encryption keys encoded into malware configuration files and not public key cryptography. Such keys may be obtained through malware reverse engineering.

Standard Non-Application Layer Protocol

Use of a standard non-application layer protocol for communication between host and C2 server or among infected hosts within a network. The list of possible protocols is extensive.9 Specific examples include use of network layer protocols, such as the Internet Control Message Protocol (ICMP), and transport layer protocols, such as the User Datagram Protocol (UDP). ICMP communication between hosts is one example. Because ICMP is part of the Internet Protocol Suite, it is required to be implemented by all IP-compatible hosts;10 however, it is not as commonly monitored as other Internet Protocols such as TCP or UDP and may be used by TOI's to hide communications.

Uncommonly Used Port

TOI's, conduct C2 communications over a non-standard port to bypass proxies and firewalls that have been improperly configured.

Web Service

TOI's may use an existing, legitimate external Web service as a means for relaying commands to a compromised system.

These commands may also include pointers to command and control (C2) infrastructure. TOI's may post content, known as a dead drop resolver, on Web services with embedded (and often obfuscated/encoded) domains or IP addresses. Once infected, victims will reach out to and be redirected by these resolvers.

Popular websites and social media acting as a mechanism for C2 may give a significant amount of cover due to the likelihood that hosts within a network are already communicating with them prior to a compromise. Using common services, such as those offered by Google or Twitter, makes it easier for TOI's to hide in expected noise. Web service providers commonly use SSL/TLS encryption; giving TOI's an added level of protection.

Use of Web services may also protect back-end C2 infrastructure from discovery through malware binary analysis while also enabling operational resiliency (since this infrastructure may be dynamically changed).

The Surface, Deep, and Dark Webs

With the Tor network being such a big player in the dark web, the Invisible Internet Project (I2P) is an overlay network and darknet that allows applications to send messages to each other pseudonymously and securely. Uses include anonymous Web surfing, chatting, blogging and file transfers. The software that implements this layer is called an I2P router and a computer running I2P is called an I2P node.

The Tor network is a group of volunteer-operated servers that allows people to improve their privacy and security on the Internet. Tor's users employ this network by connecting through a series of virtual tunnels rather than making a direct connection, thus allowing both organizations and individuals to share information over public networks without compromising their privacy. Along the same line, Tor is an effective censorship circumvention tool, allowing its users to reach otherwise blocked destinations or content. Tor can also be used as a building block for software developers to create new communication tools with built-in privacy features.

Individuals use Tor to keep websites from tracking them and their family members, or to connect to news sites, instant messaging services, or the like when these are blocked by their local Internet providers. Tor's onion services let users publish web sites and other services without needing to reveal the location of the site. Individuals also use Tor for socially sensitive communication: chat rooms and web forums for rape and abuse survivors, or people with illnesses.

Journalists use Tor to communicate more safely with whistleblowers and dissidents. Non-governmental organizations (NGOs) use Tor to allow their workers to connect to their home website while they're in a foreign country, without notifying everybody nearby that they're working with that organization.

Groups such as Indymedia recommend Tor for safeguarding their members' online privacy and security. Activist groups like the Electronic Frontier Foundation (EFF) recommend Tor as a mechanism for maintaining civil liberties online. Corporations use Tor as a safe way to conduct competitive analysis, and to protect sensitive procurement patterns from eavesdroppers. They also use it to replace traditional VPNs, which reveal the exact amount and timing of communication. Which locations have employees working late? Which locations have employees consulting job-hunting websites? Which research divisions are communicating with the company's patent lawyers?

A branch of the U.S. Navy uses Tor for open source intelligence gathering, and one of its teams used Tor while deployed in the Middle East recently. Law enforcement uses Tor for visiting or surveilling web sites without leaving government IP addresses in their web logs, and for security during sting operations.

The first module in the afternoon examines how we scrape content from paste sites. These websites sometimes contain content such as user names and passwords of compromised user accounts, detailed network information about our target's systems, or just data that our customers need to know. We then turn our focus to international issues by performing OSINT activities on websites outside of the United States. Considering that a big barrier to using non-English websites can be the language, students learn how to use techniques to translate content and search locally for relevant information. We also will examine how to discover popular websites and applications used in foreign countries. Since we talk about international data and traveling around the world, our courseware finishes up with an examination of how we track transportation (planes, boats, cars, etc.).

Using translation sites to practice transforming languages into other languages

Discovering the popular websites and mobile apps used in several countries

The Dark Web

Risks in using the dark web

Overview of top three dark web networks

Freenet

Modes of Freenet

Accessing Freenet

Services and resources in the Freenet

I2P - Invisible Internet Project

What data is in I2P?

I2P tunnels

Using I2P

Eepsites

Tor

- **Who uses Tor and why**?
- **How Tor works**
- **Dangers of using Tor**
- **Accessing Tor**
- **Tor hidden services**
- **Sharing files in Tor**
- **Searching Data Dump Sites**
- **What do people use paste sites for?**
- **Harvesting content from paste sites**

Hidden embeded persistant Cryptocurrency Miners

Cryptocurrency Miners hidden in websites now run even after users close the browser

https://news.bitcoin.com/hackers-target-400000-computers-with-mining-malware/

Putting It All Together

Kill Chain phase					Defensible actions						
					Control	Detect	Deny	Disrupt	Degrade	Deceive	Contain
Pre-Compromise	①	Reconnaissance		Attacker performs research on target	Prevent	D Threat intelligence D Network and web log monitoring	D Border firewall D Information sharing policy	D	D	D Honeypot	D N/A
	②	Phishing		Attacker sends low volume targeted email, etc.		D General awareness training D Self-phishing training	D Self-phishing training D Email filters	D	D Phishing Response Process Improvements	D	D N/A
Compromise	③	Infiltration		User opens attachment – installs malware	Detect	D Endpoint malware protection D Secured (patched) endpoint	D Proxy/URL filter D Network threat protection D Limit user privileges	D DEP	D	D	D N/A
	④	Backdoor		Attacker accesses user's machine		D HIDS D NIDS D Log monitoring D Endpoint malware protection	D HIPS D NIPS D Secured (patched) endpoint	D	D	D	D Limit administrator rights D Internal host based firew
	⑤	Lateral Movement		Attacker elevates rights, accesses systems	Investigate (Respond)	D Log monitoring and alerting D Endpoint malware protection	D Secure password D Patch management D Vulnerability scanning D 2-factor authentication D Privilege separation	D DEP	D	D	D Host based firewalls D Strong access controls D Network segmentation
Post-Compromise	⑥	Data Collection		Attacker acquires data		D Log Monitoring and alerting	D User access control D Network segmentation D Encryption	D DLP	D	D DNS redirect	D Trust zones D Incident response D Strong access controls D Network segmentation D Robust backups
	⑦	Exfiltration		Attacker takes data out of target's environment and harvests the data	Recover	D Audit logs D Log monitoring and alerting	D Egress filtering D Whitelisting D Encryption	D DLP	D	D	D Incident response D Strong access controls D Network segmentation D Robust backups

Information Security Kill Chain

"Cyber Kill Chain" has been widely used by the security community to describe the different stages of cyberattacks

KEY:

Indicate the status of the security control in your environment according to the key below. Add security controls to the matrix if needed. Based on this overall assessment, determine whether or not there are obvious gaps in your security controls for the various phases of the kill chain. Also, this assessment would identify if your security efforts are concentrated too much on a single phase of the kill chain, e.g. lots of preventive controls, but not enough detective controls.

Green: Security control in place
Yellow: Security control mostly in place; needs improvement
Orange: Project underway to implement the security control
Blue: Considering the control, but implementation not yet underway or approved
Black: Unlikely to be implemented; not cost effective

Appendix A

Framework for Improving Critical Infrastructure Cybersecurity (based on NIST 800-53), with guidance from Executive Order 13636 issued February 12, 2013: **https://goo.gl/BjwLBa**

A high level outline of the framework recommends these broad areas be addressed:

- Identify (assets and risks)
- Protect (assets from risks)
- Detect (attacks)
- Respond (disaster response, harden defenses)
- Recover (resume service, review security posture)

NIST Special Publication 800-53 Recommended Security Controls for Federal Information Systems: **https://goo.gl/nMEbno**

We've also made available as a separate handout, a one page overview of NIST 800-53 courtesy of BAI Information Security Consulting and Training from their Risk Management Framework Resource Center: https://rmf.org/

Acronyms:

- ACL – Access Control List
- DEP – Data Execution Prevention
- DLP – Data Loss Prevention
- DNS – Domain Name System
- HIDS – Host Intrusion Detection System
- NIDS – Network Intrusion Detection Syste
- HIPS – Host Intrusion Detection System
- NIPS – Network Intrusion Prevention Sys

The Combatant's Infrastructure

Describe the infrastructure, such as IP addresses, domain names, program names, etc. used by the combatant. Categorize your insights according to the corresponding phase of the intrusion kill chain, as structured in the following table.

Reconnaissance

Weaponization

Delivery

Exploitation

Installation

Command and Control

Actions on Objectives

The Victims and Affected Assets

Describe the victims affected by the combatant's actions. Address applicable victim identifiers such as people and organization names. Also outline the affected victim assets, such as networks, systems and applications. Categorize your insights according to the corresponding phase of the intrusion kill chain, as structured in the following table.

Reconnaissance

Weaponization

Delivery

Exploitation remotename=upload-file.com

35.182.185.60 IP address report

https://tools.tracemyip.org/lookup/35.182.185.60

Installation

Command and Control

Actions on Objectives

Course of Action During Incident Response

Summarize in one paragraph the steps you've taken when responding to the various phases of the intrusion chain. The section below should describe your actions in greater detail.

Discovery consists of techniques that allow the combatant to gain knowledge about the system and internal network. When TOI's gain access to a new system, they must orient themselves to what they now have control of and what benefits operating from that system give to their current objective or overall goals during the intrusion. The operating system provides many native tools that aid in this post-compromise information-gathering phase.

Tactic Description

Describe in the following table the steps you've taken to determine what the combatant has done so far as part of the intrusion, as determined based on the analysis of logs, network packer captures, forensic data and other sources.

Reconnaissance

Weaponization

Delivery

Exploitation

Installation

Command and Control

Actions on Objectives

Detect

Describe in the following table the measures you've put in place to identify the combatant's future activities related to the applicable intrusion phase. Explain how you defined and deployed indicators and signatures, additional sensors or instrumentation, security event data monitors, etc.

https://tools.verifyemailaddress.io/

http://botscout.com/

https://namechk.com/

https://github.com/SharadKumar97/OSINT-SPY

https://thatsthem.com/

Reconnaissance

Weaponization

Delivery

Exploitation

Installation

Command and Control

Actions on Objectives

Deny

Describe in the following table the measures you've implemented to block the combatant from taking the malicious actions, staying within the context of the intrusion phase described in this report. For instance, did you block specific IPs at the perimeter firewall, patch targeted vulnerabilities, block emails that matched specific patterns, etc.?

Reconnaissance

Weaponization

Delivery

Exploitation

Installation

Command and Control

Actions on Objectives

Disrupt

Describe in the following table the measures you've established to interfere with the combatant's attack in progress to cause it to fail. For instance, did you use an intrusion prevention system or firewall to terminate the combatant's active network connections, quarantined suspicious files, distributed updated antivirus signatures, etc.?

Reconnaissance

Weaponization

Delivery

Exploitation

Installation

Command and Control

Actions on Objectives

Degrade

Describe in the following table the actions you've taken to slow down or otherwise degrade the attack in progress. One example of such measures might be to configure the network equipment to rate-limit the connections attributed to the combatant.

Reconnaissance

Weaponization

Delivery

Exploitation

Installation

Command and Control

Actions on Objectives

Deceive

Describe in the following table the steps you've taken to misinform the combatant in the context of the applicable intrusion phase. Deception might involve planting fake assets that might interest the intruder, redirecting the combatant's network connections, fooling malware into believing the targeted system is already infected, employing honey tokens, etc.

http://www.projecthoneypot.org/

Reconnaissance

Weaponization

Delivery

Exploitation

Installation

Command and Control

Actions on Objectives

Destroy

Describe in the following table the offensive actions you've taken against the combatant to reduce their ability to carry out the intrusion. Such steps are generally unavailable to private individuals or firms outside of specific law enforcement or military organizations, although coordination and intelligence sharing with these organizations is within scope of this section.

Reconnaissance

Weaponization

Delivery

Exploitation

Installation

Command and Control

Actions on Objectives

Intrusion Campaign Analysis

https://www.theepochtimes.com/exclusive-russian-hackers-attacking-85-major-companies-including-steam-amazon-and-apple-pay_2160168.html

A group of Russian hackers is launching cyberattacks to steal user credentials from at least 85 companies. Targets include Amazon, American Airlines, AT&T, Best Buy, Wells Fargo, DropBox, Dunking Donuts, Ebay, GoDaddy, Uber, Match.com, McDonald's, Office Depot, PayPal, Pizza Hut, Steam, Apple Pay, and others.

Configuration files being used in the attacks were intercepted by a private darknet security group, and copies were provided to Epoch Times. Data is still thin on who the individuals behind the attacks are, although they appear to be common cybercriminals and not tied to any government operations. They were speaking Russian in their online chats, and were using Russian servers.

Ed Alexander, a darknet investigator who provided the information, said with the attacks on Apple Pay, in particular, he saw the hackers "capturing card numbers and full identities," which even included answers to personal questions users are asked when they seek to recover lost passwords.

"When I saw this file earlier this week, I took my iPhones off Apple Pay," he said.

With the attacks targeting Steam, one of the most popular video game platforms, with an estimated 125 million active users, the Russian hackers were seen stealing user emails and passwords. By gaining access to the accounts, the hackers gain access to virtual items in each user's account, which they can sell for virtual currencies or through online auction websites for real money.

The hackers had cyberattack files customized for each company they were targeting, and Alexander was able to provide copies of the attack files. The files were individual configurations for a black market cracking tool known as Sentry MBA.

Sentry MBA, enables hackers to automatically test stolen usernames and passwords across a large number of sites. It uses machine learning to do optical character recognition, similar to DeathByCAPTCHA. It can then masquerade as Safari, Firefox or another web browser to make a set of login requests look like they are coming from many different users instead of from a single

attacker's computer, said Shuman Ghosemajumder, chief technology officer at Shape Security. The practice could give criminals control of millions of accounts each day.

Sentry MBA uses what's known as "credential stuffing," which takes advantage of users who use the same usernames and passwords across multiple websites. If a website gets breached somewhere and, for example, 10,000 user credentials from the hacked site get sold on hacker websites, hackers can buy these accounts and use them with Sentry MBA to test whether any of the logins work on another site or service.

The Sentry MBA tool has largely replaced the older methods for "brute forcing" that randomly-generates passwords on a massive scale until it's able to find the correct password for an account.

The customized Sentry MBA configuration files used by the Russian hackers are designed to bypass security protocols unique to each website—such as CAPTCHA to ensure logins are from humans and not bots, and systems that block multiple login attempts.

Sentry MBA is extremely effective, since it's common for people to use the same usernames and passwords on multiple services. For example, in 2010, close to 1.5 million users had their data released online after Gawker was breached; and in 2011, more than 93,000 users had their information hacked on Sony's PlayStation Network. According to software security community OWASP, about two-thirds of users from the Sony attack used the same credentials on Gawker.

https://www.dowjones.com/insight/artificial-intelligence-transforms-hacker-arsenal/

Artificial intelligence, growing more potent and easier to use, threatens to compound the already considerable challenges companies face as they deal with cyberattacks, researchers warn. While rare, they say early signs of such advanced forms of attacks have already been detected.

Earlier this year, cybersecurity firm Darktrace Inc. spotted a never-before-seen attack at a client company in India that used rudimentary machine learning to observe and learn patterns of normal user behavior inside a network, Chief Executive Nicole Eagan said. The software then began to mimic that normal behavior, effectively blending into the background and becoming harder for security tools to spot. Darktrace declined to discuss the case in greater detail.

It wasn't exactly clear what the goal of the attack was, but Ms. Eagan said the use of AI and machine learning in cyber breaches opens up a range of dangerous scenarios, from the ability of intruders to more easily scan networks for unpatched ports to the automated composition of emails that match the tone and writing style of someone that the intended target knows.

"We do imagine that there will be a time when attackers use machine learning and artificial intelligence as part of the attack. We have seen early signs of that," she said.

Early manifestations of machine learning in cyberattacks already can be found.F or years, a service called Death by Captcha has used machine learning models to quickly defeat the familiar CAPTCHA system, in which people verify their identity by entering a string of squiggly letters. Using a process called optical character recognition,the software identifies and learns from millions of different images of those blurry figures until it's trained to recognize them and solve the CAPTCHA.

Data scientists at ZeroFOX Inc. in 2016 built a neural network that parsed Twitter data to write phishing posts that targeted specific users. Phishing is a common attack method in which hackers use fake emails or other tools to trick employees into giving them access to a target system or victim. The research project established that algorithms could analyze a person's social media feeds to craft highly-targeted social engineering attacks.

"Attackers try to match the phishing attack to users by extracting data on them. You can scale a lot of the crime economy by utilizing a form of basic machine learning," said Tomer Weingarten, founder and CEO of SentinelOne, a company that deploys machine learning and artificial intelligence to defend against attacks at the endpoints of a network. "It happens with every phishing campaign you see. I would call it statistical analysis, a form of machine learning."

The growing sophistication of fast-moving, modern cyberattacks is forcing companies to employ similar technologies to defend themselves. By turning to artificial intelligence companies also can help plug the gaps left by a shortage of cybersecurity talent and the growing scale of attacks.

Mastercard Inc. is experimenting with software to automate the response to phishing attacks. Every incoming email is sent through a platform that uses machine learning to analyze each email and produce a risk score. High-risk emails are quarantined and reviewed by a security analyst before delivery who determines the appropriate action.

On a good day, human security analysts are alerted to a potential phishing attack and fix the problem in an hour, says Ron Green, Mastercard's chief security officer. The new software, built as part of a security automation initiative led by the U.S. National Security Agency and Johns Hopkins University, can identify and fix the problem within minutes.

Security experts are quick to point out that technologies such as machine learning can be put to legal and illegal use, and that it's only a matter of time before the most advanced forms of AI are used by attackers.

"It's inevitable that we see the other side start to use the same set of tools," said Joe Levy, CTO of cybersecurity firm Sophos.

Is Kaspersky a FSB Secret Backdoor?

https://www.dhs.gov/news/2017/09/13/dhs-statement-issuance-binding-operational-directive-17-01

Release Date: September 13, 2017

For Immediate Release Office of the Press Secretary

Contact: 202-282-8010

WASHINGTON – After careful consideration of available information and consultation with interagency partners, Acting Secretary of Homeland Security Elaine Duke today issued a Binding Operational Directive (BOD) directing Federal Executive Branch departments and agencies to take actions related to the use or presence of information security products, solutions, and services supplied directly or indirectly by AO Kaspersky Lab or related entities.

The BOD calls on departments and agencies to identify any use or presence of Kaspersky products on their information systems in the next 30 days, to develop detailed plans to remove and discontinue present and future use of the products in the next 60 days, and at 90 days from the date of this directive, unless directed otherwise by DHS based on new information, to begin to implement the agency plans to discontinue use and remove the products from information systems.

This action is based on the information security risks presented by the use of Kaspersky products on federal information systems. Kaspersky anti-virus products and solutions provide broad access to files and elevated privileges on the computers on which the software is installed, which can be exploited by malicious cyber combatants to compromise those information systems. The Department is concerned about the ties between certain Kaspersky officials and Russian intelligence and other government agencies, and requirements under Russian law that allow Russian intelligence agencies to request or compel assistance from Kaspersky and to intercept communications transiting Russian networks. The risk that the Russian government, whether acting on its own or in collaboration with Kaspersky, could capitalize on access provided by Kaspersky products to compromise federal information and information systems directly implicates U.S. national security.

The Department's priority is to ensure the integrity and security of federal information systems. Safeguarding federal government systems requires reducing potential vulnerabilities, protecting against cyber intrusions, and anticipating future threats. While this action involves products of a Russian-owned and operated company, the Department will take appropriate action related to the products of any company that present a security risk based on DHS's internal risk management and assessment process.

DHS is providing an opportunity for Kaspersky to submit a written response addressing the Department's concerns or to mitigate those concerns. The Department wants to ensure that the company has a full opportunity to inform the Acting Secretary of any evidence, materials, or data that may be relevant. This opportunity is also available to any other entity that claims its commercial interests will be directly impacted by the directive. Further information about this process will be available in a Federal Register Notice.

https://jamestown.org/program/fsb-formidable-player-russias-information-security-domain/

https://www.wired.com/story/router-hacking-slingshot-spy-operation-compromised-more-than-100-targets/

Routers, both the big corporate kind and the small one gathering dust in the corner of your home, have long made an attractive target for hackers. They're always on and connected, often full of unpatched security vulnerabilities, and offer a convenient chokepoint for eavesdropping on all the data you pipe out to the internet. Now security researchers have found a broad, apparently state-sponsored hacking operation that goes a step further, using hacked routers as a foothold to drop highly sophisticated spyware even deeper inside a network, onto the computers that connect to those compromised internet access points.

Researchers at security firm Kaspersky on Friday revealed a long-running hacking campaign, which they call "Slingshot," that they believe planted spyware on more than a hundred targets in

11 countries, mostly in Kenya and Yemen. The hackers gained access to the deepest level of victim computers' operating system, known as the kernel, taking full control of target machines. And while Kaspersky's researchers haven't yet determined how the spyware initially infected the majority of those targets, in some cases the malicious code had been installed via small-business-grade routers sold by the Latvian firm MikroTik, which the Slingshot hackers had compromised.

Unlike previous router-hacking campaigns that have used routers themselves as eavesdropping points—or the far more common home router hacks that use them as fodder for distributed-denial-of-service attacks aimed at taking down websites—the Slingshot hackers appear to have instead exploited routers' position as a little-scrutinized foothold that can spread infections to sensitive computers within a network, allowing deeper access to spies. Infecting a router at a business or coffee shop, for instance, would then potentially give access to a broad range of users.

"It's quite an overlooked place," says Kaspersky researcher Vicente Diaz. "If someone is performing a security check of an important person, the router is probably the last thing they'll check… It's quite easy for an attacker to infect hundreds of these routers, and then you have an infection inside their internal network without much suspicion."

Infiltrating Internet Cafes?

Kaspersky research director Costin Raiu offered one theory as to Slingshot's targets: Internet cafes. MikroTik routers are particularly popular in the developing world, where internet cafes remain common. And while Kaspersky detected the campaign's spyware on machines using consumer-grade Kaspersky software, the routers it targeted were designed for networks of dozens of machines. "They're using home user licenses, but who has 30 computers at home?" Raiu says. "Maybe not all are internet cafes, but some are."

The Slingshot campaign, which Kaspersky believes persisted undetected for the last six years, exploits MikroTik's "Winbox" software, which is designed to run on the user's computer to allow them to connect to and configure the router, and in the process downloads a collection of dynamic link library, or .dll, files from the router to the user's machine. When infected with Slingshot's malware, a router includes a rogue .dll in that download that transfers to the victim's machine when they connect to the network device.

'It's quite easy for an attacker to infect hundreds of these routers.' Vicente Diaz, Kaspersky

That .dll serves as the foothold on the target computer, and then itself downloads a collection of spyware modules onto the target PC. Several of those modules function, like most programs, in normal "user" mode. But another, known as Cahnadr, runs with deeper kernel access. Kaspersky describes that kernel spyware as the "main orchestrator" of Slingshot's multiple PC infections. Together, the spyware modules have the ability to collect screenshots, read information from open windows, read the contents of the computer's hard drive and any peripherals, monitor the local network, and log keystrokes and passwords.

Kaspersky's Raiu speculates that perhaps Slingshot would use the router attack to infect an internet cafe administrator's machine and then use that access to spread to the PCs it offered to customers. "It's quite elegant, I think," he added.

An Unknown Infection Point

Slingshot still presents plenty of unanswered questions. Kaspersky doesn't actually know if routers served as the initial point of infection for many of the Slingshot attacks. It also concedes that it's not exactly sure how the initial infection of the MikroTik routers took place in the cases where they were used, though it points to one MikroTik router hacking technique mentioned last March in WikiLeaks' Vault7 collection of CIA hacking tools known as ChimayRed.

MikroTik responded to that leak in a statement at the time by pointing out that the technique didn't work in more recent versions of its software. When WIRED asked MikroTik about Kaspersky's research, the company pointed out that the ChimayRed attack also required the router's firewall to be disabled, which would otherwise be on by default. "This did not affect many devices," a MikroTik spokesperson wrote in an email to WIRED. "Only in rare cases would somebody misconfigure their device."

Kaspersky, for its part, emphasized in its blog post on Slingshot that it hasn't confirmed whether it was the ChimayRed exploit or some other vulnerability that hackers used to target MikroTik's routers. But they do note that the latest version of MikroTik routers don't install any software on the user's PC, removing Slingshot's path to infect its target computers.

Five-Eye Fingerprints

As murky as Slingshot's penetration technique may be, the geopolitics behind it may be even thornier. Kaspersky says it's not able to determine who ran the cyberespionage campaign. But they note that its sophistication suggests that it's the work of a government, and that textual clues in the malware's code suggest English-speaking developers. Aside from Yemen and Kenya, Kaspersky also found targets in Iraq, Afghanistan, Somalia, Libya, Congo, Turkey, Jordan and Tanzania.

All of that—particularly just how many of those countries have seen active US military operations—suggests that Kaspersky, a Russian firm often accused of ties to Kremlin intelligence agencies whose software is now banned from US government networks, might be outing a secret hacking campaign carried out by the US government, or one of its "Five-Eyes" allies of English-speaking intelligence partners.

But Slingshot could also be the work of French, Israeli, or even Russian intelligence services seeking to keep tabs on terrorism hotspots. Jake Williams, a former NSA staffer and now the founder of Rendition Infosec, argues that nothing in Kaspersky's findings strongly indicate the nationality of the Slingshot hackers, noting that some of their techniques resemble those used by the Russian state-sponsored hacker group Turla and Russian crime networks. "Without more research, the attribution on this is really weak," Williams says. "If it was Five-Eyes and Kaspersky outed the group, I don't really see an issue there. They are doing what they do: exposing [state-sponsored hacking] groups."1

Kaspersky, for its part, insists that it doesn't know who's responsible for the Slingshot campaign, and seeks to protect its customers. "Our golden rule is we detect malware and it doesn't matter where it comes from," says Kaspersky researcher Alexei Shulmin.

Regardless of who's behind the attack, the hackers may have already been forced to develop new intrusion techniques, now that MikroTik has removed the feature they had exploited. But

Kaspersky warns that the spyware campaign nonetheless serves as a warning that sophisticated state-sponsored hackers aren't just aiming at traditional infection points like PCs and servers as they look for any machine that can let them bypass the armor of their targets. "Our visibility is too partial. We don't look at networking devices," says Diaz. "It's a convenient place to slide under the radar."

If applicable, summarize in one paragraph the relationship between the intrusion discussed earlier in the report and other related intrusions that, when taken together, form a campaign. Mention the indicators and behaviors shared across the intrusions within the campaign. Outline the commercial, geopolitical or other combatants that might have motivated the combatant's activities.

Other Intrusions in the Campaign

https://www.reuters.com/article/us-usa-russia-sanctions-energygrid/in-a-first-u-s-blames-russia-for-cyber-attacks-on-energy-grid-idUSKCN1GR2G3

Beginning in March 2016, or possibly earlier, Russian government hackers sought to penetrate multiple U.S. critical infrastructure sectors, including energy, nuclear, commercial facilities, water, aviation and manufacturing, according to a U.S. security alert published Thursday.

The Department of Homeland Security and FBI said in the alert that a "multi-stage intrusion campaign by Russian government cyber combatants " had targeted the networks of small commercial facilities "where they staged malware, conducted spear phishing, and gained remote access into energy sector networks." The alert did not name facilities or companies targeted.

The direct condemnation of Moscow represented an escalation in the Trump administration's attempts to deter Russia's aggression in cyberspace, after senior U.S. intelligence officials said in recent weeks the Kremlin believes it can launch hacking operations against the West with impunity.

It coincided with a decision Thursday by the U.S. Treasury Department to impose sanctions on 19 Russian people and five groups, including Moscow's intelligence services, for meddling in the 2016 U.S. presidential election and other malicious cyber-attacks.

Russia in the past has denied it has tried to hack into other countries' infrastructure, and vowed on Thursday to retaliate for the new sanctions.

'UNPRECEDENTED AND EXTRAORDINARY'

U.S. security officials have long warned that the United States may be vulnerable to debilitating cyber-attacks from hostile TOI's. It was not clear what impact the attacks had on the firms that were targeted.

But Thursday's alert provided a link to an analysis by the U.S. cyber security firm Symantec last fall that said a group it had dubbed Dragonfly had targeted energy companies in the United States and Europe and in some cases broke into the core systems that control the companies' operations.

Malicious email campaigns dating back to late 2015 were used to gain entry into organizations in the United States, Turkey and Switzerland, and likely other countries, Symantec said at the time, though it did not name Russia as the culprit.

The decision by the United States to publicly attribute hacking attempts of American critical infrastructure was "unprecedented and extraordinary," said Amit Yoran, a former U.S. official who founded DHS's Computer Emergency Response Team.

"I have never seen anything like this," said Yoran, now chief executive of the cyber firm Tenable, said.

A White House National Security Council spokesman did not respond when asked what specifically prompted the public blaming of Russia. U.S. officials have historically been reluctant to call out such activity in part because the United States also spies on infrastructure in other parts of the world.

News of the hacking campaign targeting U.S. power companies first surfaced in June in a confidential alert to industry that described attacks on industrial firms, including nuclear plants, but did not attribute blame.

"People sort of suspected Russia was behind it, but today's statement from the U.S. government carries a lot of weight," said Ben Read, manager for cyber espionage analysis with cyber security company FireEye Inc.

ENGINEERS TARGETED

The campaign targeted engineers and technical staff with access to industrial controls, suggesting the hackers were interested in disrupting operations, though FireEye has seen no evidence that they actually took that step, Read said.

A former senior DHS official familiar with the government response to the campaign said that Russia's targeting of infrastructure networks dropped off after the publication in the fall of Symantec's research and an October government alert, which detailed technical forensics about the hacking attempts but did not name Russia.

The official declined to say whether the campaign was still ongoing or provide specifics on which targets were breached, or how close hackers may have gotten to operational control systems.

An electrical line technician works on restoring power in Vilonia, Arkansas April 29, 2014. REUTERS/Carlo Allegri

"We did not see them cross into the control networks," DHS cyber security official Rick Driggers told reporters at a dinner on Thursday evening.

Driggers said he was unaware of any cases of control networks being compromised in the United States and that the breaches were limited to business networks. But, he added, "We know that there is intent there."

It was not clear what Russia's motive was. Many cyber security experts and former U.S. officials say such behavior is generally espionage-oriented with the potential, if needed, for sabotage.

Russia has shown a willingness to leverage access into energy networks for damaging effect in the past. Kremlin-linked hackers were widely blamed for two attacks on the Ukrainian energy grid in 2015 and 2016, which caused temporary blackouts for hundreds of thousands of customers and were considered first-of-their-kind assaults.

Senator Maria Cantwell, the top Democrat on the Senate Energy and Natural Resources Committee, asked the Trump administration earlier this month to provide a threat assessment gauging Russian capabilities to breach the U.S. electric grid.

It was the third time Cantwell and other senators had asked for such a review. The administration has not yet responded, a spokesman for Cantwell's office said on Thursday.

Last July, there were news reports that the Wolf Creek Nuclear Operating Corp, which operates a nuclear plant in Kansas, had been targeted by hackers from an unknown origin.

Spokeswoman Jenny Hageman declined to say at the time if the plant had been hacked but said that there had been no operational impact to the plant because operational computer systems were separate from the corporate network. Hageman on Thursday said the company does not comment on security matters.

John Keeley, a spokesman for the industry group the Nuclear Energy Institute, said: "There has been no successful cyber-attack against any U.S. nuclear facility, including Wolf Creek."

Reporting by Dustin Volz and Timothy Gardner, additional reporting by Jim Finkle; Editing by Tom Brown, Alistair Bell and Cynthia Osterman

Major Cyber incidents since January 2017

April 2018. Israeli cyber researchers revealed that Hamas had planted spyware in mobile phones owned by members of Fatah, a rival Palestinian faction

April 2018. Reports from cyber security researchers indicate that Chinese state-sponsored hacking groups have targeted Japanese defense companies in an attempt to gain information on Tokyo's policies towards North Korea

April 2018. Cyber security researchers warn that North Korean hacking groups are expanding their range of targets, attacking industries in Japan, Vietnam, and the Middle East

April 2018. US and UK officials issued a joint warning that Russia was deliberately targeting western critical infrastructure by compromising home and business routers

April 2018. The director of the UK's Government Communications Headquarters (GCHQ) announced that the organization had been conducting offensive cyber operations against ISIS to suppress their propaganda, disrupt their coordination, and protect deployed military personnel

April 2018. The chief of Germany's domestic intelligence services accused Russia of being behind the December 2017 attack on the government's computer networks

April 2018. The UK's National Cyber Security Centre released an advisory note warning that Russian state combatants were targeting UK critical infrastructure by infiltrating supply chains

April 2018. All government services of Sint. Maarten, a Caribbean island and constitute country of the Netherlands, were taken offline for a week after a cyber-attack. According to local authorities, this is the third cyber-attack the country has faced in just over a year.

April 2018. The North Korean hacking group responsible for the SWIFT attacks was found to have targeted a Central American online casino in an attempt to siphon funds

March 2018. Online services for the city of Atlanta were disrupted after a ransomware attack struck the city's networks, demanding $55,000 worth of bitcoin in payment. The city would eventually spend approximately $2.6 million recovering from the attack.

March 2018. Baltimore's 911 dispatch system was taken down for 17 hours after a ransomware attack, forcing the city to revert to manual dispatching of emergency services

March 2018. The US Departments of Justice and Treasury accused Iran in an indictment of stealing intellectual property from more than 300 universities, as well as government agencies and financial services companies.

March 2018. The FBI and Department of Homeland Security issued a joint technical alert to warn of Russian cyber-attacks against US critical infrastructure. Targets included energy, nuclear, water, aviation, and manufacturing facilities.

March 2018. A data breach of the company Under Armor compromised the information of 150 million users of its fitness and nutrition tracking app MyFitnessPal

March 2018. Cybersecurity researchers reveal that a Chinese hacking group used malware to attack the service provider for the UK government in an attempt to gain access to combatants at various UK government departments and military organizations

March 2018. Cybersecurity researchers announce evidence that the same North Korean hacking group linked to the SWIFT financial network attacks has been targeting several major Turkish banks and government finance agencies.

March 2018. A UN report details attempts by North Korean hackers to compromise email accounts of the members of a UN panel enforcing trade sanctions against North Korea.

February 2018. German news reported that a Russian hacking group had breached the online networks of Germany's foreign and interior ministries, exfiltrating at least 17 gigabytes of data in an intrusion that went undetected for a year.

February 2018. The Justice Department indicted 13 Russians and three companies for their online efforts to interfere in the 2016 US presidential elections.

February 2018. The US and UK formally blame Russia for the June 2017 NotPetya ransomware attack that caused billions of dollars in damages across the world.

February 2018. A cyberattack on the Pyeongchang Olympic Games attributed to Russia took the official Olympic website offline for 12 hours and disrupted wifi and televisions at the Pyeongchang Olympic stadium.

February 2018. Officials at the Department of Homeland Security confirmed that Russian hackers successfully penetrated the voter registration rolls of several US states prior to the 2016 election.

January 2018. China denied that the computer network it supplied to the African Union allowed it access the AU's confidential information and transfer it to China, or that it had bugged offices in the AU headquarters that it had built.

January 2018. A Japan-based cryptocurrency exchange reveals that it lost $530 million worth of the cryptocurrency NEM in a hack, in what amounts to possibly the largest cryptocurrency heist of all time.

January 2018. Norwegian officials discover a "very professional" attempt to steal patient data from a Norwegian hospital system, in an attack they speculate was connected to the upcoming NATO Trident Juncture 18 military exercise.

January 2018. A hacking group with ties to the Lebanese General Directorate of General Security was revealed to have been involved in a six-year campaign to steal text messages, call logs, and files from journalists, military officers, corporations, and other targets in 21 countries worldwide.

January 2018. The Unique Identification Authority of India and its Aadhaar system are hacked by unknown combatants , resulting in the personal data of more than 1 billion people being available for purchase.

December 2017. French company Schneider Electric was forced to shut down operations of a power plant in the Middle East after malware compromised its industrial control systems. Analysis by security researchers indicated that the attack was sponsored by a nation-state.

November 2017. Three Chinese nationals employed at a China-based Internet security firm are indicted by a US grand jury for computer hacking, theft of trade secrets, conspiracy, and identity theft against employees of Siemens, Moody's Analytics, and Trimble.

November 2017. Uber discloses that it paid hackers $100,000 to delete the stolen data of 57 million of its customers and drivers, including names, phone numbers, email addresses, and license plate numbers.

November 2017. Cybersecurity researchers report a cyberespionage campaign targeting government organizations in South America and Southeast Asia. The group, deemed to have nation-state capabilities, aimed to acquire foreign policy information from diplomatic and government entities.

November 2017. Cybersecurity researchers report a sophisticated Vietnamese hacking group responsible for cyber espionage campaigns targeting the ASEAN organization, foreign corporations with an interest in Vietnamese industries, and media, human rights, and civil society organizations.

October 2017. A major wave of ransomware infections hits media organizations, train stations, airports, and government agencies in Russia and Eastern Europe. Security researchers found strong evidence linking the attack to the creators of NotPetya, and noted that the malware used leaked NSA-linked exploits to move through networks. Ukrainian police later reported that the

ransomware was a cover for a quiet phishing campaign undertaken by the same actor to gain remote access to financial and other confidential data.

October 2017. Yahoo updates the previous projections of 1 billion account affected in its massive 2013 breach, acknowledging that all 3 billion accounts were compromised.

October 2017. Russian hackers reported to be targeting potential attendees of CyCon, a cybersecurity conference organized by the US Army and the NATO CCD COE

October 2017. DHS and FBI reports warn of Russia-linked hackers targeting industrial control systems at US energy companies and other critical infrastructure organizations

October 2017. Poland's Defense Minister reports that the country repelled a third Russian hacking attempt against companies in Poland, reportedly part of a larger campaign against Eastern European corporations.

October 2017. North Korean hackers were found to have targeted US electric companies in a spear-phishing campaign meant to probe utilities' defenses.

October 2017. North Korean hackers allegedly broke into South Korea's defense data center in 2016 and stole a large trove of sensitive documents over the course of a year, including joint U.S.-South Korean blueprints for war on the peninsula.

October 2017. China allegedly carried out a cyberattack against a U.S. think tank and law firm, both involved with fugitive Chinese tycoon Guo Wengui.

October 2017. The Australian Government revealed that hackers compromised an Australian national security contractor in 2016 and stole large amounts of data, including information related to the development of the F-35 Joint Strike Fighter.

October 2017. Reports surface that Russian government-backed hackers stole NSA hacking secrets from a contractor in 2015 by exploiting the Kaspersky antivirus software on the contractor's home computer

September 2017. Russia compromised the personal smartphones of NATO soldiers deployed to Poland and the Baltic states.

September 2017. Press reports say that the US Cyber Command targeted North Korea's the Reconnaissance General Bureau for denial of service attacks.

September 2017. China allegedly inserted malware into widely used PC Cleaner management tool. The malware targeted at least 20 major international technology firms.

September 2017. The SEC reported that cybercriminals accessed the agency's files in 2016 and used the information gathered for illicit trading

September 2017. Credit monitoring firm Equifax disclosed a July data breach that revealed 143 million people's full names, social security numbers, birth dates, home addresses and driver's license numbers, as well as 209,000 credit card numbers.

September 2017. Researchers report malware infections in Cambodia designed to surveil dissidents and disrupt domestic political activity.

August 2017 . Researchers inform the Estonian Information System Authority of a vulnerability potentially affecting the use of 750,000 Estonian e-ID cards. The government replaced the compromised cards in late 2017, but claims that no cards were ever hacked.

August 2017. South Korea's Cyber Warfare Research Center reports that North Korea has been targeting South Korean Bitcoin exchanges.

August 2017. A state-sponsored spyware campaign targeted Indian and Pakistani government security and military organizations.

August 2017. The Scottish Parliament suffered from a brute force cyberattack similar to the one that compromised the British Parliament in June.

July 2017 . The Swedish Transport Agency's outsourced data is hacked, potentially compromising confidential information and classified information on military plans.

July 2017. Security researchers revealed details of a wide-ranging malware campaign linked to China which used over 600 strains of malware to conduct espionage operations on Southeast Asian military and government organizations

July 2017. GCHQ issued a warning saying that state-sponsored hackers had likely broken into the Industrial Control Systems of UK energy companies

July 2017. Security researchers revealed an Iran-linked cyber espionage group active since 2013 that had used spear phishing and watering hole attacks to target government institutions, defense companies, IT firms and more in Israel, Saudi Arabia, the US, Germany, Jordan, and Turkey.

July 2017. The FBI and DHS announced that hackers had been targeting US energy facilities including the Wolf Creek Nuclear Operating Corporation in a campaign bearing resemblance to the operations of a known Russian hacking group

July 2017. Cyber research firms reported a new malware campaign launched the day after North Korea's July missile tests. The identified family of malware featured a command and control infrastructure with links to South Korea, and had previously been used in three other campaigns linked to North Korea.

July 2017. Hackers attacked a partner of UniCredit, Italy's largest bank, gaining access to loan and biographical data from 400,000 client accounts

July 2017 . Russian hackers used leaked NSA tools to compromise Wi-Fi servers in European and Middle Eastern hotels in a campaign targeting top diplomats and industrial leaders.

July 2017. The Qatari government accused hackers in the United Arab Emirates of posting fake news and attacking Qatari state-run media websites in a campaign designed to widen a rift between Gulf states.

June 2017. The New York Times revealed that spyware sold to the Mexican government was being used to target human rights lawyers, journalists, and anti-corruption activists

June 2017. US-CERT identified the North Korean government as being behind a DDoS botnet infrastructure used to target media, financial, aerospace, and critical infrastructure organizations worldwide. Hidden Cobra

June 2017. A Russia-linked hacking group was found to have launched a spear-phishing campaign against Montenegro after the country announced its decision to join NATO. Fancy Bear

June 2017. A NotPetya ransomware attack shut down the port terminals of Danish shipping giant Maersk for two days, causing an estimated $300 million in associated costs

June 2017. Russian hackers used an updated ransomware program to target Ukrainian infrastructure, including power companies, airports, and public transit.

June 2017. A brute-force attack alleged to have been carried out by Iranian state combatants compromised nearly 90 British members of parliament, whose email accounts were hacked.

May 2017. A ransomware campaign spread to 99 countries using a vulnerability revealed in the Shadow Brokers' April 2017 dump of NSA tools.

May 2017. Lebanon accused Israel of hacking the Lebanese telecoms network and sending audio and WhatsApp messages to 10,000 people claiming that Hezbollah's leader was behind the death of the group's top commander.

May 2017. Thousands of emails and other documents from the campaign of French president-elect Emmanuel Macron, totaling 9 gigabytes, were released shortly before the election, in an effort linked to Russia.

April 2017. Irish state-owned utility EirGrid suffered a security breach at the hands of state-sponsored hackers involving a virtual wiretap allowing access to the company's unencrypted communications.

April 2017. The Lazarus Group, thought to be associated with North Korea, was found to be involved in a spear phishing campaign against US defense contrcombatants

April 2017. Cybersecurity researchers revealed a growing cyber-espionage campaign originating in China and targeting construction, engineering, aerospace and telecom companies, as well as government agencies, in the U.S., Europe, and Japan.

April 2017. The Danish Defense Intelligence Service reported that a "foreign player," alleged by the Danish press to be Russia espionage group, had accessed Defense Ministry email accounts in 2015 and in 2016, but was unable to retrieve classified information.

April 2017. The Shadow Brokers, the group that claimed to have hacked the NSA in August 2016, released yet another trove of purported NSA hacking tools, including one that allowed the NSA to break into the SWIFT interbank messaging and money transfer system.

April 2017. Chinese attempts to penetrate South Korean military, government and defense industry networks continued at an increasing rate since a February announcement that the THAAD missile defense system would be deployed in South Korea.

March 2017. An intelligence report revealed a Russian operation to send malicious spear-phishing messages to more than 10,000 Twitter users in the Department of Defense. The malicious payloads delivered through these messages gave Russian hackers access to the victim's device and Twitter account.

March 2017. The U.S. Department of Justice indicted two Russian intelligence agents and two criminal hackers over the September 2014 Yahoo hack, which compromised 500 million user accounts.

March 2017. Chinese police arrested 96 suspects charged with hacking into the servers of social media, gaming and video streaming sites, stealing personal information, and posting the information for sale on online forums.

March 2017. Wikileaks released a trove of sophisticated CIA hacking tools dated from 2013 to 2016, claiming that the release reflected several hundred million lines of CIA-developed code.

February 2017. A suspected Russian hacker breaches at least 60 universities and US government organizations using SQL injections, including HUD, NOAA, Cornell University, and NYU, among many others. This follows up a hack by the same actor against the U.S. Electoral Assistance Commission in December 2016.

February 2017. Indian Central Bureau of Investigation and Army officers were targeted by a phishing campaign purportedly mounted by Pakistan.

February 2017. Hackers compromised the Singaporean military's web access system and stole the personal information of 850 people. The Ministry of Defense said it was likely the attack was state sponsored.

February 2017. A sophisticated malware operation extracted over 600 gigabytes of data from 70 mostly Ukrainian targets in the fields of critical infrastructure, news media, and scientific research.

January 2017. A Swedish foreign policy institute accused Russia of conducting an information warfare campaign, using fake news, false documents, and disinformation intended to weaken public support for Swedish policies.

https://www.us-cert.gov/ncas/alerts/TA18-106A

Describe other incidents or intrusions that share commonalities with the intrusion discussed earlier in the report. Explain whether the shared attributes indicate a low/medium/high likelihood that the intrusions form a larger campaign. Provide internal and external intrusion names or other relevant identifiers. Include references to related internal and external documents. Clarify when the intrusions occurred.

Shared Intrusion Attributes

Specify the key indicators and behavioral characteristics that are consistent across intrusions within the campaign. Categorize the attributes according to the kill chain phase when they were exhibited and their relevance to the combatant description, attack

infrastructure, capabilities (tactics, techniques and procedures) and the affected victims. Wherever possible, account for Combatant, Infrastructure, Capabilities and Victim in each applicable phase of the kill chain.

	Combatant	*Infrastructure*	*Capabilities*	*Victim*
Reconnaissance				
Weaponization				
Delivery				
Exploitation				
Installation				
Command and Control				
Actions on Objectives				

Falcon Sandbox Hybrid Analysis

Sentry_MBA.exe
Analyzed on April 18th 2018 15:13:42 (CEST) running the Kernelmode monitor
Guest System: Windows 7 64 bit, Professional, 6.1 (build 7601), Service Pack 1
Report generated by Falcon Sandbox v8.00 © Hybrid Analysis
Incident Response
Risk Assessment
Remote Access
Reads terminal service related keys (often RDP related)
Tries to identify its external IP address
Fingerprint
Reads the active computer name
tries to identify its external IP address
Network Behavior
Contacts 1 domain and 3 hosts.
External Systems
Detected Suricata Alert
Details
Detected alert "ET POLICY External IP Lookup - checkip.dyndns.org" (SID: 2021378, Rev: 2, Severity: 1) categorized as "Potential Corporate Privacy Violation"
source
Suricata Alerts
relevance
10/10
Sample was identified as malicious by a large number of Antivirus engines
Details
31/65 Antivirus vendors marked sample as malicious (47% detection rate)
source
External System
relevance
10/10
Malicious artifacts seen in the context of a contacted host
Details
Found malicious artifacts related to "216.146.38.70": ...
URL: http://checkip.dyndns.org/?rnd1=33216.3278528643&rnd2=59231.6897187268 (AV positives: 1/67 scanned on 03/06/2018 13:06:32)
URL: http://checkip.dyndns.org/?rnd1=34041.1516621234&rnd2=57253.0789191814 (AV positives: 1/67 scanned on 03/05/2018 18:28:27)
URL: http://checkip.dyndns.org/?rnd1=33425.5490255882&rnd2=19394.4414407751 (AV positives: 1/67 scanned on 03/05/2018 08:31:59)
URL: http://checkip.dyndns.org/?rnd1=65133.2115752345&rnd2=9021.2377109474 (AV positives: 1/67 scanned on 03/05/2018 08:31:40)
URL: http://checkip.dyndns.org/ (AV positives: 1/67 scanned on 03/04/2018 15:39:17)

File SHA256: fod3ec1d36c3f58d60709db60672815b5d3bac6800b160ce5aef5bb1a7e22657 (AV positives: 38/66 scanned on 04/18/2018 12:24:23)
File SHA256: 256133752 1ecbf8330ecccf77065f94171ad7c333b1d12eddc5fed7f158e83af (AV positives: 22/65 scanned on 04/18/2018 11:12:29)
File SHA256: 392dea505d85adbb98e2bd3aaebf219dca245a3b9bfa19f9454fc2d915c64bee (AV positives: 58/67 scanned on 04/18/2018 10:44:02)
File SHA256: 634e96b9b9bf998de32711acc293c648ec5d1d963525778c4605f40f417d46ff (AV positives: 56/67 scanned on 04/18/2018 10:00:48)
File SHA256: 2456b7eb4c634c87c6d55423e87c02ceb082c11a8b05664aee48b0981036d5df (AV positives: 57/67 scanned on 04/18/2018 09:55:09)
File SHA256: 5c0f290b4134bb879982d52adbfc48bf735793f59ef209d5cdb60b0a340c6842 (Date: 04/18/2018 00:11:38)
File SHA256: aa58c750621d7078ac7fc7439d6ad1c5f8930ad9e4b8dc72bbbdb864171038dd (Date: 04/17/2018 11:39:58)
File SHA256: cb8dc0b182dde6b35ea8b8650e13441f50cdcef57d458a0e06ad29b29411dec6 (Date: 04/15/2018 19:29:19)
File SHA256: a3a7e11503d2b99931ad25e428bbc9c103b6bb34f5ad6d2d465f82def76ce8f7 (Date: 04/09/2018 23:02:19)
File SHA256: e9895a641f234ac4d82d42f8d12677c043f801bc047bc54cfba639fe5dfcd9ed (Date: 04/09/2018 14:45:46)
source
Network Traffic
relevance
10/10
Tries to identify its external IP address
Details
"checkip.dyndns.org"
source
Network Traffic
relevance
6/10
Suspicious Indicators
Cryptographic Related
Found a cryptographic related string
Details
"Blowfish" (Indicator: "blowfish"; File: "Sentry_MBA.exe.bin")
source
String
relevance
10/10
Environment Awareness
Reads the active computer name
Details
"<Input Sample>" (Path: "HKLM\SYSTEM\CONTROLSET001\CONTROL\COMPUTERNAME\ACTIVECOMPUTERNAME" ; Key: "COMPUTERNAME")
source

Registry Access
relevance
5/10
Details
Detected alert "ET POLICY DynDNS CheckIp External IP Address Server Response" (SID: 2014932, Rev: 2, Severity: 2) categorized as "Potentially Bad Traffic"
source
Suricata Alerts
relevance
10/10
Network Related
Found potential IP address in binary/memory
Details
Heuristic match: "1.2.840.10008.1.2.4.50"
Heuristic match: "1.2.840.10008.1.2.4.91"
Heuristic match: "1.2.840.10008.1.2.4.70"
Heuristic match: "1.2.840.10008.1.2.4.57"
Heuristic match: "1.2.840.10008.1.2.4.100"
Heuristic match: "POST /6b06490d-f9fd-424c-8b6d-83edc4369e89/ HTTP/1.1Cache-Control: no-cacheConnection: ClosePragma: no-cacheContent-Type: application/soap+xmlUser-Agent: WSDAPIContent-Length: 733Host: 192.168.56.153:5357"
Heuristic match: "Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.9.0.11) Gecko/2009060215 Firefox/3.0.11"
source
String
relevance
3/10
Uses a User Agent typical for browsers, although no browser was ever launched
Details
Found user agent(s): Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
source
Network Traffic
relevance
10/10
Remote Access Related
Reads terminal service related keys (often RDP related)
Details
"<Input Sample>" (Path: "HKLM\SYSTEM\CONTROLSET001\CONTROL\TERMINAL SERVER"; Key: "TSUSERENABLED")
source
Registry Access
relevance
10/10
Unusual Characteristics
Installs hooks/patches the running process
Details

"<Input Sample>" wrote bytes "b0956800" to virtual address "0x00795AEC" (part of module "SENTRY_MBA.EXE")
"<Input Sample>" wrote bytes "7d0790778 1ed8e77ae868d77c6e08c77effd8f772d168e7760149077478d8d77a8e28c7760898d7700000000ad379a758b2d9a75b6419a7500000000" to virtual address "0x74871000" (part of module "WSHTCPIP.DLL")
"<Input Sample>" wrote bytes "c0df8c771cf98b77ccf88b770d648d7700000000c0119f7500000000fc3e9f7500000000e0139f75000000009457f47525e08c77c6e08c7700000000bc6af3750000000cf319f7500000000 9319f4750000000002c329f7500000000" to virtual address "0x75891000" (part of module "NSI.DLL")
"<Input Sample>" wrote bytes "711107027a3b0602ab8b02007f950200fc8c0200729602006cc805001ecd03027d260302" to virtual address "0x758B07E4" (part of module "USER32.DLL")
"<Input Sample>" wrote bytes "9495 6800" to virtual address "0x00795AF0" (part of module "SENTRY_MBA.EXE")
"<Input Sample>" wrote bytes "8cd04900" to virtual address "0x0046B48E" (part of module "SENTRY_MBA.EXE")
source
Hook Detection
relevance
10/10
Informative
External Systems
Detected Suricata Alert
Details
Detected alert "ET INFO DYNAMIC_DNS Query to *.dyndns. Domain" (SID: 2012758, Rev: 5, Severity: 3) categorized as "Misc activity"
source
Suricata Alerts
relevance
10/10
General
Contacts domains
Details
"checkip.dyndns.org"
source
Network Traffic
relevance
1/10
Contacts server
Details
"2.21.242.213:80"
"172.227.102.35:80"
"216.146.38.70:80"
source
Network Traffic
relevance

1/10
Creates mutants
details
"\Sessions\1\BaseNamedObjects\MutexNPA_UnitVersioning_3356"
"MutexNPA_UnitVersioning_3356"
source
Created Mutant
relevance
3/10
GETs files from a webserver
Installation/Persistance
Touches files in the Windows directory
Details
"<Input Sample>" touched file "%WINDIR%\SysWOW64\en-US\msvfw32.dll.mui"
"<Input Sample>" touched file "%WINDIR%\Fonts\StaticCache.dat"
"<Input Sample>" touched file "%WINDIR%\SysWOW64\en-US\user32.dll.mui"
"<Input Sample>" touched file "%WINDIR%\winsxs\x86_microsoft.windows.c..-
controls.resources_6595b64144ccf1df_6.0.7600.16385_en-us_581cd2bf5825dde9\comctl32.dll.mui"
"<Input Sample>" touched file "%WINDIR%\Globalization\Sorting\SortDefault.nls"
"<Input Sample>" touched file "%WINDIR%\SysWOW64\en-US\shell32.dll.mui"
"<Input Sample>" touched file "%WINDIR%\SysWOW64\en-US\msctf.dll.mui"
"<Input Sample>" touched file "%WINDIR%\SysWOW64\en-US\KernelBase.dll.mui"
source
API Call
relevance
7/10
Network Related
Found potential URL in binary/memory
Details
Pattern match:
"https://jcl.svn.sourceforge.net:443/svnroot/jcl/trunk/jcl/source/common/JclResources.pas"
Pattern match:
"https://jcl.svn.sourceforge.net:443/svnroot/jcl/trunk/jcl/source/common/JclBase.pas"
Pattern match:
"https://jcl.svn.sourceforge.net:443/svnroot/jcl/trunk/jcl/source/windows/JclWin32.pas"
Pattern match:
"https://jcl.svn.sourceforge.net:443/svnroot/jcl/trunk/jcl/source/common/JclLogic.pas"
Pattern match:
"https://jcl.svn.sourceforge.net:443/svnroot/jcl/trunk/jcl/source/common/JclStringConversions.p
as"
Pattern match:
"https://jcl.svn.sourceforge.net:443/svnroot/jcl/trunk/jcl/source/common/JclCharsets.pas"
Pattern match:
"https://jcl.svn.sourceforge.net:443/svnroot/jcl/trunk/jcl/source/common/Jcl8087.pas"
Pattern match:
"https://jcl.svn.sourceforge.net:443/svnroot/jcl/trunk/jcl/source/common/JclIniFiles.pas"

Pattern match:
"https://jcl.svn.sourceforge.net:443/svnroot/jcl/trunk/jcl/source/common/JclSysInfo.pas"
Pattern match:
"https://jcl.svn.sourceforge.net:443/svnroot/jcl/trunk/jcl/source/common/JclUnicode.pas"
Pattern match:
"https://jcl.svn.sourceforge.net:443/svnroot/jcl/trunk/jcl/source/common/JclWideStrings.pas"
Pattern match:
"https://jcl.svn.sourceforge.net:443/svnroot/jcl/trunk/jcl/source/windows/JclRegistry.pas"
Pattern match:
"https://jcl.svn.sourceforge.net:443/svnroot/jcl/trunk/jcl/source/common/JclSynch.pas"
Pattern match:
"https://jcl.svn.sourceforge.net:443/svnroot/jcl/trunk/jcl/source/common/JclMath.pas"
Pattern match:
"https://jcl.svn.sourceforge.net:443/svnroot/jcl/trunk/jcl/source/common/JclStreams.pas"
Pattern match:
"https://jcl.svn.sourceforge.net:443/svnroot/jcl/trunk/jcl/source/common/JclAnsiStrings.pas"
Pattern match:
"https://jcl.svn.sourceforge.net:443/svnroot/jcl/trunk/jcl/source/common/JclStrings.pas"
Pattern match:
"https://jcl.svn.sourceforge.net:443/svnroot/jcl/trunk/jcl/source/windows/JclShell.pas"
Pattern match:
"https://jcl.svn.sourceforge.net:443/svnroot/jcl/trunk/jcl/source/windows/JclSecurity.pas"
Pattern match:
"https://jcl.svn.sourceforge.net:443/svnroot/jcl/trunk/jcl/source/common/JclDateTime.pas"
Pattern match:
"https://jcl.svn.sourceforge.net:443/svnroot/jcl/trunk/jcl/source/common/JclFileUtils.pas"
Pattern match:
"https://jcl.svn.sourceforge.net:443/svnroot/jcl/trunk/jcl/source/windows/JclConsole.pas"
Pattern match:
"https://jcl.svn.sourceforge.net:443/svnroot/jcl/trunk/jcl/source/common/JclUnitVersioning.pas"
Pattern match:
"https://jcl.svn.sourceforge.net:443/svnroot/jcl/trunk/jcl/source/common/JclSysUtils.pas"
Pattern match:
"https://jcl.svn.sourceforge.net:443/svnroot/jcl/trunk/jcl/source/common/JclRTTI.pas"
Pattern match:
"https://jcl.svn.sourceforge.net:443/svnroot/jcl/trunk/jcl/source/common/JclMime.pas"
Pattern match: "http://www.w3.org/2003/05/soap-envelope"
Pattern match: "http://www.microsoft.com"
Heuristic match: "checkip.dyndns.org"
Pattern match: "http://checkip.dyndns.org"
Pattern match: "http://csrc.nist.gov/publications/nistpubs/800-38a/sp800-38a.pdf|section"
Pattern match: "http://www.itl.nist.gov/fipspubs/fip180-1.htm"
source
String
relevance
10/10
System Security

Creates or modifies windows services
Details
"<Input Sample>" (Access type: "CREATE"; Path: "HKLM\SYSTEM\CURRENTCONTROLSET\SERVICES\TCPIP\PARAMETERS")
source
Registry Access
relevance
10/10
Opens the Kernel Security Device Driver (KsecDD) of Windows
Details
"<Input Sample>" opened "\Device\KsecDD"
source
API Call
relevance
10/10
All Details:
Sentry_MBA.exe
PID: 3356, Report UID: 00016469-00003356
MD5: 72098edfebfcc92f2e1e8d4bf30a7ae7
SHA256: 1760d2349d8001dd5c9639841cb9e814da94f8212922b56fed4b5d5f00dd49d2
Packers identified
PEiD BobSoft Mini Delphi -> BoB / BobSoft
PE header basic information
Target machine Intel 386 or later processors and compatible processors
Compilation timestamp 1992-06-19 22:22:17
Entry Point 0x00342F90
Number of sections 8

Campaign Motivations

Outline the likely motivation for the combatant's activities across the intrusion campaign, including the relevant commercial, geopolitical or other combatants. If practical, offer substantiated theories regarding the attribution of the campaign to specific individuals, groups or nation states.

Defending against this threat

Defending against this threat is extremely difficult due to the nature of the affected devices. The majority of them are connected directly to the internet, with no security devices or services between them and the potential attackers. This challenge is augmented by the fact that most of the affected devices have publicly known vulnerabilities which are not convenient for the average user to patch. Additionally, most have no built-in anti-malware capabilities. These three facts together make this threat extremely hard to counter, resulting in extremely limited opportunities to interdict malware, remove vulnerabilities, or block threats.

Despite these challenges, Talos has released protections for this threat from multiple angles, to try to take advantage of the limited options that exist. We developed and deployed more than 100 Snort signatures for the publicly known vulnerabilities for the devices that are associated with this threat. These rules have been deployed in the public Snort set, and can be used by anyone to help defend their devices. In addition, we have done the usual blacklisting of domains/IPs as appropriate and convicting of the hashes associated with this threat to cover those who are protected by the Cisco Security ecosystem. We have reached out to Linksys, Mikrotik, Netgear, TP-Link and QNAP regarding this issue. (Note: QNAP has been aware of certain aspects of VPNFilter and previously done work to counter the threat.) Finally, we have also shared these indicators and our research with international law enforcement and our fellow members of the Cyber Threat Alliance in advance of this publication so they could move quickly to help counter this threat more broadly.

Recommendations

We recommend that:

Users of SOHO routers and/or NAS devices reset them to factory defaults and reboot them in order to remove the potentially destructive, non-persistent stage 2 and stage 3 malware.

Internet service providers that provide SOHO routers to their users reboot the routers on their customers' behalf.

If you have any of the devices known or suspected to be affected by this threat, it is extremely important that you work with the manufacturer to ensure that your device is up to date with the latest patch versions. If not, you should apply the updated patches immediately.

ISPs work aggressively with their customers to ensure their devices are patched to the most recent firmware/software versions.

Due to the potential for destructive action by the threat actor, we recommend out of an abundance of caution that these actions be taken for all SOHO or NAS devices, whether or not they are known to be affected by this threat.

Exploitation

At the time of this publication, we do not have definitive proof on how the threat actor is exploiting the affected devices. However, all of the affected makes/models that we have uncovered had well-known, public vulnerabilities. Since advanced threat actors tend to only use the minimum resources necessary to accomplish their goals, we assess with high confidence that no zero day exploits were used.

SLINGSHOT attack log

2018-04-11 16:58:36

{

"PORT HIT": "97.77.211.30:52266->74.#.#.10:23",

"MESSAGES": "Array

(

[17:57:50] => enable

system

shell

sh

[17:57:50+1] => cat /proc/mounts; /bin/busybox CFRKS

)

"

}

2018-04-11 16:41:39

{

"PORT HIT": "97.77.211.30:55769->145.#.#.30:8022",

"MESSAGES": "Array

(

[00:41:11] => GET / HTTP/1.1

Host: 145.#.#.30:8080

User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/52.0.2743.116 Safari/537.36

Content-Length: 0

)

"

}

2018-04-11 16:41:39

{

"PORT HIT": "97.77.211.30:39174->145.#.#.30:8042",

"MESSAGES": "Array

(

[00:41:11] => GET / HTTP/1.1

Host: 145.#.#.30:8082

User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/52.0.2743.116 Safari/537.36

Content-Length: 0

)

"

}

2018-04-11 12:51:28

{

"PORT HIT": "97.77.211.30:47793->91.#.#.60:23",

"MESSAGES": "Array

(

[18:50:57] => enable

system

shell

sh

[18:50:57+1] => cat /proc/mounts; /bin/busybox WHIQL

)

"

}

2018-04-11 11:46:57

{

"PORT HIT": "97.77.211.30:55098->89.#.#.245:8080",

"MESSAGES": "Array

(

[20:46:28] => GET / HTTP/1.1

Host: 89.#.#.245:8080

User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_11_6) AppleWebKit/601.7.7 (KHTML, like Gecko) Version/9.1.2 Safari/601.7.7

Content-Length: 0

)

"

}

2018-04-11 08:26:28

{

"PORT HIT": "97.77.211.30:49978->107.#.#.122:23",

"MESSAGES": "Array

(

[14:25:58] => enable

system

shell

sh

[14:25:58+1] => cat /proc/mounts; /bin/busybox
ZZIOL

)

"

}

2018-04-11 05:52:47

{

"PORT HIT": "97.77.211.30:51371->103.#.#.85:8080",

"MESSAGES": "Array

(

[18:52:06] => GET / HTTP/1.1

Host: 103.#.#.85:8080

User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/51.0.2704.103 Safari/537.36

Content-Length: 0

)

"

}

2018-04-11 04:00:10

{

"PORT HIT": "97.77.211.30:51286->104.#.#.171:8080",

"MESSAGES": "Array

(

[07:00:01] => GET / HTTP/1.1

Host: 104.#.#.171:8080

User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/52.0.2743.116 Safari/537.36

Content-Length: 0

)

"

}

2018-04-11 02:22:27

{

"PORT HIT": "97.77.211.30:60446->31.#.#.64:23",

"MESSAGES": "Array

(

[08:21:44] => enable

system

shell

sh

[08:21:44+1] => cat /proc/mounts; /bin/busybox
ZFDGA

)

"

}

2018-04-10 18:40:20

{

"PORT HIT": "97.77.211.30:47187->185.#.#.65:23",

"MESSAGES": "Array

(

[00:39:58] => enable

system

shell

sh

[00:39:58+1] => cat /proc/mounts; /bin/busybox
MOBON

)

"

}

2018-04-10 09:47:29

{

"PORT HIT": "97.77.211.30:51185->89.#.#.187:8080",

"MESSAGES": "Array

(

[18:46:55] => GET / HTTP/1.1

Host: 89.#.#.187:8080

User-Agent: Mozilla/5.0 (Windows NT 10.0;
WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/52.0.2743.116 Safari/537.36

Content-Length: 0

)

"

}

2018-04-10 06:13:01

{

"PORT HIT": "97.77.211.30:58710->89.#.#.154:8080",

"MESSAGES": "Array

(

[15:12:25] => GET / HTTP/1.1

Host: 89.#.#.154:8080

User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/51.0.2704.103 Safari/537.36

Content-Length: 0

)

"

}

2018-04-10 03:12:25

{

"PORT HIT": "97.77.211.30:49794->5.#.#.189:23",

"MESSAGES": "Array

(

[10:11:50] => enable

system

shell

sh

[10:11:51] => cat /proc/mounts; /bin/busybox
GYWLU

)

"

}

2018-04-10 00:01:35

{

"PORT HIT": "97.77.211.30:52877->50.#.#.11:23",

"MESSAGES": "Array

(

[02:00:48] => enable

system

shell

sh

[02:00:48+1] => cat /proc/mounts; /bin/busybox
NSVGQ

)
"
}
2018-04-09 23:13:43

{
"PORT HIT": "97.77.211.30:55438->184.#.#.106:23",
"MESSAGES": "Array
(
[22:13:22] => enable
system
shell
sh

[22:13:22+1] => cat /proc/mounts; /bin/busybox
SNQIP

)
"
}
2018-04-09 21:13:38

{

"PORT HIT": "97.77.211.30:56646->209.#.#.23:23",

"MESSAGES": "Array

(

[23:13:08] => enable

system

shell

sh

[23:13:08+1] => cat /proc/mounts; /bin/busybox
GQCYR

)

"

}

2018-04-09 15:07:53

{

"PORT HIT": "97.77.211.30:51893->5.#.#.228:23",

"MESSAGES": "Array

(

[22:07:33] => enable

system

shell

sh

[22:07:33+1] => cat /proc/mounts; /bin/busybox WBHWD

)

"

}

2018-04-09 11:40:59

{

"PORT HIT": "97.77.211.30:45942->119.#.#.35:8080",

"MESSAGES": "Array

(

[03:40:32] => GET / HTTP/1.1

Host: 119.#.#.35:8080

User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/52.0.2743.116 Safari/537.36

Content-Length: 0

)

"

}

2018-04-09 09:53:17

{

"PORT HIT": "97.77.211.30:38919->156.#.#.106:23",

"MESSAGES": "Array

(

[15:52:34] => enable

system

shell

sh

[15:52:35] => cat /proc/mounts; /bin/busybox
GMEJR

)

"

}

2018-04-09 03:37:37

{

"PORT HIT": "97.77.211.30:38604->209.#.#.70:8080",

"MESSAGES": "Array

(

[05:37:19] => GET / HTTP/1.1

Host: 209.#.#.70:8080

User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/52.0.2743.116 Safari/537.36

Content-Length: 0

)

"

}

2018-04-09 03:37:37

{

"PORT HIT": "97.77.211.30:50611->209.#.#.66:82",

"MESSAGES": "Array

(

[05:37:19] => GET / HTTP/1.1

Host: 209.#.#.70:82

User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_11_6) AppleWebKit/601.7.7 (KHTML, like Gecko) Version/9.1.2 Safari/601.7.7

Content-Length: 0

)

"

}

2018-04-08 14:45:14

{

"PORT HIT": "97.77.211.30:43465->185.#.#.4:23",

"MESSAGES": "Array

(

[20:44:34] => enable

system

shell

sh

[20:44:34+1] => cat /proc/mounts; /bin/busybox
SMXKE

)

"

}

2018-04-08 13:03:57

{

"PORT HIT": "97.77.211.30:45521->185.#.#.7:23",

"MESSAGES": "Array

(

[19:03:10] => enable

system

shell

sh

[19:03:10+1] => cat /proc/mounts; /bin/busybox
WCAPG

)

"

}

2018-04-07 20:11:19

{

"PORT HIT": "97.77.211.30:34250->5.#.#.253:8080",

"MESSAGES": "Array

(

[05:11:09] => GET / HTTP/1.1

Host: 5.#.#.253:8080

User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/51.0.2704.103 Safari/537.36

Content-Length: 0

)

"

}

2018-04-07 20:11:19

{

"PORT HIT": "97.77.211.30:57938->178.#.#.160:82",

"MESSAGES": "Array

(

[05:11:09] => GET / HTTP/1.1

Host: 5.#.#.253:82

User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/51.0.2704.103 Safari/537.36

Content-Length: 0

)

"

}

2018-04-07 17:56:32

{

"PORT HIT": "97.77.211.30:43873->195.#.#.74:23",

"MESSAGES": "Array

(

[01:55:45] => enable

system

shell

sh

[01:55:45+1] => cat /proc/mounts; /bin/busybox
YALCG

)

"

}

2018-04-07 16:32:50

{

"PORT HIT": "97.77.211.30:35115->209.#.#.224:23",

"MESSAGES": "Array

(

[18:32:09] => enable

system

shell

sh

[18:32:09+1] => cat /proc/mounts; /bin/busybox FNYVF

)

"

}

2018-04-07 12:07:41

{

"PORT HIT": "97.77.211.30:59592->89.#.#.68:8080",

"MESSAGES": "Array

(

[21:07:12] => GET / HTTP/1.1

Host: 89.#.#.68:8080

User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/52.0.2743.116 Safari/537.36

Content-Length: 0

)

"

}

2018-04-03 18:32:33

{

"PORT HIT": "97.77.211.30:36588->63.#.#.194:23",

"MESSAGES": "Array

(

[20:32:06] => enable

system

shell

sh

[20:32:06+1] => cat /proc/mounts; /bin/busybox TFZCX

)

"

}

2018-04-03 09:30:25

{

"PORT HIT": "97.77.211.30:52234->192.#.#.199:23",

"MESSAGES": "Array

(

[12:29:48] => enable

system

shell

sh

[12:29:48+1] => cat /proc/mounts; /bin/busybox
LRSOR

)

"

}

2018-04-03 05:59:00

{

"PORT HIT": "97.77.211.30:51650->153.#.#.106:23",

"MESSAGES": "Array

(

[11:58:32] => enable

system

shell

sh

[11:58:32+1] => cat /proc/mounts; /bin/busybox LNMLQ

)

"

}

2018-04-03 05:32:37

{

"PORT HIT": "97.77.211.30:39994->72.#.#.50:23",

"MESSAGES": "Array

(

[08:32:06] => enable

system

shell

sh

[08:32:06+1] => cat /proc/mounts; /bin/busybox QWRJK

)

"

}

2018-04-03 03:06:24

{

"PORT HIT": "97.77.211.30:32813->89.#.#.252:8080",

"MESSAGES": "Array

(

[12:06:01] => GET / HTTP/1.1

Host: 89.#.#.252:8080

User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/51.0.2704.103 Safari/537.36

Content-Length: 0

)

"

}

2018-04-02 23:06:25

{

"PORT HIT": "97.77.211.30:34874->145.#.#.16:8080",

"MESSAGES": "Array

(

[07:05:56] => GET / HTTP/1.1

Host: 145.#.#.16:8080

User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/52.0.2743.116 Safari/537.36

Content-Length: 0

)

"

}

2018-04-02 19:10:34

{

"PORT HIT": "97.77.211.30:52858->209.#.#.23:23",

"MESSAGES": "Array

(

[21:09:54] => enable

system

shell

sh

[21:09:54+1] => cat /proc/mounts; /bin/busybox CJZGT

)

"

}

2018-04-02 18:07:57

{

"PORT HIT": "97.77.211.30:45211->89.#.#.12:7025",

"MESSAGES": "Array

(

[03:07:31] => GET / HTTP/1.1

Host: 89.#.#.12:8080

User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/52.0.2743.116 Safari/537.36

Content-Length: 0

)

"

}

2018-04-02 15:35:01

{

"PORT HIT": "97.77.211.30:35957->41.#.#.77:23",

"MESSAGES": "Array

(

[23:34:14] => enable

system

shell

sh

[23:34:14+1] => cat /proc/mounts; /bin/busybox
GQPZR

)

"

}

2018-04-02 09:55:15

{

"PORT HIT": "97.77.211.30:60448->217.#.#.160:23",

"MESSAGES": "Array

(

[17:54:37] => enable

system

shell

sh

[17:54:37+1] => cat /proc/mounts; /bin/busybox
JCZPG

)
"
}
2018-04-02 09:00:46

{
"PORT HIT": "97.77.211.30:36130->209.#.#.91:23",
"MESSAGES": "Array
(
[11:00:18] => enable
system
shell
sh

[11:00:18+1] => cat /proc/mounts; /bin/busybox
WGAGE

)
"
}
2018-04-02 08:06:09

{

"PORT HIT": "97.77.211.30:41977->104.#.#.175:8080",

"MESSAGES": "Array

(

[11:05:46] => GET / HTTP/1.1

Host: 104.#.#.175:8080

User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/51.0.2704.103 Safari/537.36

Content-Length: 0

)

"

}

2018-04-01 14:01:56

{

"PORT HIT": "97.77.211.30:55479->67.#.#.23:7003",

"MESSAGES": "Array

(

[16:01:36] => GET / HTTP/1.1

Host: 67.#.#.23:8080

User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_11_6) AppleWebKit/601.7.7 (KHTML, like Gecko) Version/9.1.2 Safari/601.7.7

Content-Length: 0

)

"

}

2018-04-01 06:37:58

{

"PORT HIT": "97.77.211.30:34096->63.#.#.194:23",

"MESSAGES": "Array

(

[08:37:14] => enable

system

shell

sh

[08:37:14+1] => cat /proc/mounts; /bin/busybox YYSHP

)

"

}

2018-04-01 05:34:09

{

"PORT HIT": "97.77.211.30:46946->185.#.#.69:8082",

"MESSAGES": "Array

(

[13:33:39] => GET / HTTP/1.1

Host: 185.#.#.69:8082

User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/51.0.2704.103 Safari/537.36

Content-Length: 0

)

"

}

2018-04-01 05:34:09

{

"PORT HIT": "97.77.211.30:52230->185.#.#.69:8080",

"MESSAGES": "Array

(

[13:33:39] => GET / HTTP/1.1

Host: 185.#.#.69:8080

User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/52.0.2743.116 Safari/537.36

Content-Length: 0

)

"

}

2018-04-01 05:26:06

{

"PORT HIT": "97.77.211.30:59392->198.178.116.238:23",

"MESSAGES": "Array

(

[07:25:44] => enable

system

shell

sh

[07:25:44+1] => cat /proc/mounts; /bin/busybox SWYQP

)

"

}

2018-03-30 20:39:51

{

"PORT HIT": "97.77.211.30:53523->151.#.#.229:23",

"MESSAGES": "Array

(

[04:39:16] => enable

system

shell

sh

[04:39:16+1] => cat /proc/mounts; /bin/busybox
QNXEL

)

"

}

2018-03-30 08:07:36

{

"PORT HIT": "97.77.211.30:45280->151.#.#.65:23",

"MESSAGES": "Array

(

[15:06:57] => enable

system

shell

sh

[15:06:57+1] => cat /proc/mounts; /bin/busybox
ZKKNT

)

"

}

2018-03-30 05:08:50

{

"PORT HIT": "97.77.211.30:60947->89.#.#.2:23",

"MESSAGES": "Array

(

[14:08:06] => enable

system

shell

sh

[14:08:06+1] => cat /proc/mounts; /bin/busybox
CUCCJ

)
"
}
2018-03-28 20:04:10

{
"PORT HIT": "97.77.211.30:52845->156.#.#.64:23",
"MESSAGES": "Array
(
[02:03:49] => enable
system
shell
sh

[02:03:50] => cat /proc/mounts; /bin/busybox
VVDCX

)
"
}
2018-03-27 21:33:39

{

"PORT HIT": "97.77.211.30:33872->158.#.#.127:23",

"MESSAGES": "Array

(

[22:33:11] => enable

system

shell

sh

[22:33:11+1] => cat /proc/mounts; /bin/busybox
NDPQS

)

"

}

2018-03-27 17:24:07

{

"PORT HIT": "97.77.211.30:36946->151.#.#.65:23",

"MESSAGES": "Array

(

[00:23:19] => enable

system

shell

sh

[00:23:19+1] => cat /proc/mounts; /bin/busybox
AXLRS

)

"

}

2018-03-27 01:47:30

{

"PORT HIT": "97.77.211.30:53809->63.#.#.194:23",

"MESSAGES": "Array

(

[03:46:57] => enable

system

shell

sh

[03:46:57+1] => cat /proc/mounts; /bin/busybox
BVBSC

)

"

}

2018-03-26 20:40:49

{

"PORT HIT": "97.77.211.30:42913->139.#.#.233:23",

"MESSAGES": "Array

(

[09:40:10] => enable

system

shell

sh

[09:40:10+1] => cat /proc/mounts; /bin/busybox
GCKHO

)

"

}

2018-03-26 08:28:35

{

"PORT HIT": "97.77.211.30:38782->184.#.#.82:23",

"MESSAGES": "Array

(

[09:27:54] => enable

system

shell

sh

[09:27:54+1] => cat /proc/mounts; /bin/busybox PHPPU

)

"

}

2018-03-26 00:05:27

{

"PORT HIT": "97.77.211.30:56301->89.#.#.2:23",

"MESSAGES": "Array

(

[09:04:48] => enable

system

shell

sh

[09:04:49] => cat /proc/mounts; /bin/busybox

SFQMI

)

"

}

2018-03-25 23:31:02

{

"PORT HIT": "97.77.211.30:58479->89.#.#.4:23",

"MESSAGES": "Array

(

[08:30:24] => enable

system

shell

sh

[08:30:24+1] => cat /proc/mounts; /bin/busybox
SJCLS

)

"

}

References

^ ↑ Lambert, J. (2015, April 26). Defenders think in lists. Attackers think in graphs. As long as this is true, attackers win.. Retrieved May 13, 2015.

^ ↑ Yerko Grbic. (2017, February 14). Macro Malware Targets Macs. Retrieved July 8, 2017.

^ ↑ Microsoft. (n.d.). Component Object Model (COM). Retrieved November 22, 2017.

^ ↑ Microsoft. (n.d.). DCOM Security Enhancements in Windows XP Service Pack 2 and Windows Server 2003 Service Pack 1. Retrieved November 22, 2017.

^ ↑ Microsoft. (n.d.). Setting Process-Wide Security Through the Registry. Retrieved November 21, 2017.

^ ↑ Microsoft. (n.d.). Registry Values for System-Wide Security. Retrieved November 21, 2017.

^ ↑ Nelson, M. (2017, November 16). Lateral Movement using Outlook's CreateObject Method and DotNetToJScript. Retrieved November 21, 2017.

^ ↑ Nelson, M. (2017, January 5). Lateral Movement using the MMC20 Application COM Object. Retrieved November 21, 2017.

^ ↑ Nelson, M. (2017, January 23). Lateral Movement via DCOM: Round 2. Retrieved November 21, 2017.

^ ↑ Nelson, M. (2017, September 11). Lateral Movement using Excel.Application and DCOM. Retrieved November 21, 2017.

^ ↑ Tsukerman, P. (2017, November 8). Leveraging Excel DDE for lateral movement via DCOM. Retrieved November 21, 2017.

^ ↑ CIS. (2017, May 15). Multiple Vulnerabilities in Microsoft Windows SMB Server Could Allow for Remote Code Execution. Retrieved April 3, 2018.

^ ↑ National Vulnerability Database. (2017, June 22). CVE-2017-0176 Detail. Retrieved April 3, 2018.

^ ↑ National Vulnerability Database. (2017, February 2). CVE-2016-6662 Detail. Retrieved April 3, 2018.

^ ↑ National Vulnerability Database. (2017, September 24). CVE-2014-7169 Detail. Retrieved April 3, 2018.

^ ↑ Microsoft. (2005, January 21). Creating logon scripts. Retrieved April 27, 2016.

^ ↑ Apple. (2011, June 1). Mac OS X: Creating a login hook. Retrieved July 17, 2017.

^ ↑ National Security Agency/Central Security Service Information Assurance Directorate. (2013, December 16). Spotting the Combatant with Windows Event Log Monitoring. Retrieved November 12, 2014.

a b ↑ Metcalf, S. (2014, November 22). Mimikatz and Active Directory Kerberos Attacks. Retrieved June 2, 2016.

^ ↑ Deply, B. (2014, January 13). Pass the ticket. Retrieved June 2, 2016.

^ ↑ Campbell, C. (2014). The Secret Life of Krbtgt. Retrieved December 4, 2014.

^ ↑ Microsoft. (n.d.). Remote Desktop Services. Retrieved June 1, 2016.

^ ↑ Alperovitch, D. (2014, October 31). Malware-Free Intrusions. Retrieved November 4, 2014.

^ ↑ Korznikov, A. (2017, March 17). Passwordless RDP Session Hijacking Feature All Windows versions. Retrieved December 11, 2017.

^ ↑ Beaumont, K. (2017, March 19). RDP hijacking—how to hijack RDS and RemoteApp sessions transparently to move through an organisation. Retrieved December 11, 2017.

^ ↑ NCC Group PLC. (2016, November 1). Kali Redsnarf. Retrieved December 11, 2017.

^ ↑ Duarte, H., Morrison, B. (2012). (Mis)trusting and (ab)using ssh. Retrieved January 8, 2018.

^ ↑ Adam Boileau. (2005, August 5). Trust Transience: Post Intrusion SSH Hijacking. Retrieved December 19, 2017.

^ ↑ Beuchler, B. (2012, September 28). SSH Agent Hijacking. Retrieved December 20, 2017.

^ ↑ M.Léveillé, M. (2014, February 21). An In-depth Analysis of Linux/Ebury. Retrieved January 8, 2018.

^ ↑ Routin, D. (2017, November 13). Abusing network shares for efficient lateral movements and privesc (DirSharePivot). Retrieved April 12, 2018.

^ ↑ Wikipedia. (2016, June 12). Server Message Block. Retrieved June 12, 2016.

^ ↑ Microsoft. (2003, March 28). What Is RPC?. Retrieved June 12, 2016.

^ ↑ Microsoft. (n.d.). How to create and delete hidden or administrative shares on client computers. Retrieved November 20, 2014.

^ ↑ Microsoft. (n.d.). Net Use. Retrieved November 25, 2016.

^ ↑ Microsoft. (n.d.). Windows Remote Management. Retrieved November 12, 2014.

^ ↑ Jacobsen, K. (2014, May 16). Lateral Movement with PowerShell[slides]. Retrieved November 12, 2014.

LOG CONVERTER

https://cyber-defense.sans.org/blog/2009/06/30/dump-windows-event-logs-to-csv-text-vbscript

https://www.sans.org/course/open-source-intelligence-gathering#__utma=247151638.1452178913.1526516745.1526516745.1526516745.1

SUPPORTING BOOKMARKS

https://whitepages.plus/n/Martin_Barrios/Socorro_Tx/b0af46b32d3d4d6dae465b670c2641da

https://whitepages.plus/n/Jose_M_Barrios/Socorro_Tx/18ce6c5ee82a8c1ab4506ec75c4795c4

https://whitepages.plus/n/Jose_Barrios/Socorro_TX/5d136e5585b13680041cf7debf7fd616?%7B'name':%20u'jose%20barrios',%20'location':%20u'socorro%20tx'%7D

https://docs.groundlabs.com/landing/index.htm

PORT Zero Linux

http://programmer.97things.oreilly.com/wiki/index.php/Linux_in_a_Windows_World/Remote_Login_Tools/Running_GUI_Programs_Remotely

http://programmer.97things.oreilly.com/wiki/index.php/Linux_in_a_Windows_World/Remote_Login_Tools/Running_GUI_Programs_Remotely#Using_a_VNC_Client

https://superuser.com/questions/919808/why-ssh-r-allows-port-0-but-ssh-l-needs-a-port-number

https://googleprojectzero.blogspot.com/2015/07/one-font-vulnerability-to-rule-them-all.html

https://iptv.social/threads/client-area-for-users-who-have-a-iptvforest-subscription.19/

https://www.youtube.com/watch?v=RKOuHDddvow

SQLi Dumper V.8 SQL Injectionf

https://github.com/tesseract-ocr/tesseract/wiki/TrainingTesseract2

3DMarkAdvancedEdition1.3.708

https://archive.org/details/Office.16.December.17.x64

FAKE OFFICE with SQL Injection

https://github.com/tesseract-ocr/tesseract/wiki

Tesseract is an open source text recognizer (OCR) Engine, available under the Apache 2.0 license. It can be used directly, or (for programmers) using an API to extract printed text from images. It supports a wide variety of languages.

http://osintframework.com/

OSINT Framework

https://www.youtube.com/watch?v=QhJiOCwz-_I

Convert PDF to high resolution image then extract text

http://chillyfacts.com/convert-image-to-text-using-cmd-prompt/

Detailed instructions convert image to text

https://tesseract-ocr.repairfaq.org/allaboutdawg.html

What does Tesseract use DAWG for?

Tesseract uses the Directed Acyclic Word Graphs to very compactly store and efficiently search several list(s) of words. There are four DAWGs in tesseract: (right?)

•1. word_dawg (pre-set/fixed list read in from "tessdata/word-dawg")

(this one is read in raw/directly for speed, user can't change this right now)

•2. document_words (document-words that have already been recognized)

(built during execution; FIX: is/isn't cleared per-document/baseapi call)

•3. pending_words (words tess is working on, at the moment, before they are added to document_word)

•4. user_words (user-adjustable list read in from "tessdata/user-words")

(add here custom words that tesseract tends to corrupt)

Disclosure: I don't know the order of preference - which DAWG does tesseract check first AND which DAWG over-rides the others. ex. "thls" is not in #1 but, say, is in #4 - will tesseract NOT jiggle the 'l' into an 'i' (which then matches in #1) or will it go with #4? Ray?

Let's say that tesseract thinks it found a word with four letters, "thls". Before this word is output, tesseract will:

•look-up "thls" in DAWG #1 (see above)

•(when does it check user-words?)

•By looking through the sorted list for each of the classes, tesseract will note that the third character had a second-best choice to be an 'i' so it changes that letter and

•look-up "this" in DAWG #1 and this time it DOES match.

•(fmg has seen tess KEEP ON permuting even after a match in both #1 and #4 so is not sure what the ending conditions are - maybe someone who knows better can explain) which can only mean that:

•until the certainty of the word isn't moved beyond some threshold, permuting of other letters continues...

So, the answer to "Why does tesseract bother with DAWGs" is that when a typical English word has one or two letters that have permutations possible, WITHOUT using the compact and fast DAWG's this lookup task would quickly become a huge bottle-neck.

========== DAWG-related ToDo's ==========

Todo:Need to add info here on: •how to view/list words ALREADY IN "tessdata/word-dawg"

•how to CREATE A NEW "tessdata/word-dawg"

•which constants need to be tweaked when adding words to "tessdata/word-dawg"

•which constants need to be tweaked when adding words to "tessdata/user-words" (because a poster on the forums said that after about 5000 words are added guano happens)

•why/what for is rand() used in add_word_to_dawg()

•what to do when the dreaded "DAWG Table is too full" error occurs AFTER Ray Smith's patch is already applied...

Sentry_MBA.exe DLL files,

advapi32.dll

CryptAcquireContextA	CryptCreateHash	CryptDecrypt	CryptDeriveKey
CryptDestroyHash	CryptEncrypt	CryptGenRandom	CryptHashData
CryptReleaseContext	RegCloseKey	RegFlushKey	RegOpenKeyExA

avifil32.dll

AVIFileExit	AVIFileGetStream	AVIFileInit	AVIFileOpenW
AVIFileRelease	AVISaveOptionsFree	AVIStreamGetFrame	AVIStreamGetFrameClose
AVIStreamGetFrameOpen	AVIStreamInfoW	AVIStreamRelease	

comctl32.dll

ImageList_Add	ImageList_BeginDrag	ImageList_Create	ImageList_Destroy
ImageList_DragEnter	ImageList_DragLeave	ImageList_DragMove	ImageList_DragShowNolo
ImageList_Draw	ImageList_DrawEx	ImageList_EndDrag	ImageList_GetBkColor
ImageList_GetDragImage	ImageList_GetIcon	ImageList_GetIconSize	ImageList_GetImageCoun
ImageList_Read	ImageList_Remove	ImageList_Replace	ImageList_ReplaceIcon
ImageList_SetBkColor	ImageList_SetDragCursorImage	ImageList_SetIconSize	ImageList_Write
InitCommonControls			

comdlg32.dll

ChooseColorA	ChooseFontA	GetOpenFileNameA	GetSaveFileNameA

gdi32.dll

Arc	BitBlt	CombineRgn	CopyEnhMetaFileA
CreateBitmap	CreateBrushIndirect	CreateCompatibleBitmap	CreateCompatibleDC
CreateDCA	CreateDIBitmap	CreateDIBSection	CreateEllipticRgn
CreateFontIndirectA	CreateHalftonePalette	CreateICA	CreatePalette

CreatePenIndirect	CreatePolygonRgn	CreateRectRgn	CreateRectRgnIndirect
CreateRoundRectRgn	CreateSolidBrush	DeleteDC	DeleteEnhMetaFile
DeleteObject	Ellipse	EndDoc	EndPage
ExcludeClipRect	ExtCreatePen	ExtCreateRegion	ExtTextOutA
GdiFlush	GetBitmapBits	GetBrushOrgEx	GetClipBox
GetClipRgn	GetCurrentObject	GetCurrentPositionEx	GetDCOrgEx
GetDeviceCaps	GetDIBColorTable	GetDIBits	GetEnhMetaFileBits
GetEnhMetaFileHeader	GetEnhMetaFilePaletteEntries	GetGlyphOutlineA	GetGraphicsMode
GetNearestPaletteIndex	GetObjectA	GetObjectType	GetPaletteEntries
GetPixel	GetStockObject	GetSystemPaletteEntries	GetTextExtentPoint32A
GetTextExtentPointA	GetTextMetricsA	GetViewportOrgEx	GetWindowOrgEx
GetWinMetaFileBits MaskBlt	IntersectClipRect	LineDDA MoveToEx	LineTo PatBlt
ModifyWorldTransform	PlayEnhMetaFile	Polygon	Polyline
RealizePalette	Rectangle	RectVisible	RestoreDC
RoundRect	SaveDC	SelectClipRgn	SelectObject
SelectPalette	SetAbortProc	SetBkColor	SetBkMode
SetBrushOrgEx	SetDIBColorTable	SetEnhMetaFileBits	SetGraphicsMode
SetMapMode	SetPaletteEntries	SetPixel	SetROP2
SetStretchBltMode	SetTextAlign	SetTextColor	SetViewportOrgEx
SetWindowOrgEx	SetWinMetaFileBits	SetWorldTransform	StartDocA
StartPage	StretchBlt	StretchDIBits	UnrealizeObject

kernel32.dll

CloseHandle	CompareStringA	CompareStringW	CopyFileA

CreateDirectoryA	CreateEventA	CreateFileA	CreateFileMappingA
CreateFileW	CreateMutexA	CreateThread	DeleteCriticalSection
DeleteFileA	EnterCriticalSection	EnumCalendarInfoA	ExitProcess
ExitThread	FileTimeToDosDateTime	FileTimeToLocalFileTime	FindClose
FindFirstFileA	FindNextFileA	FindResourceA	FlushInstructionCache
FormatMessageA	FreeLibrary	FreeResource	GetACP
GetCommandLineA	GetCPInfo GetCurrentProcess	GetCurrentProcessId	GetCurrentThreadId
GetDateFormatA	GetDiskFreeSpaceA	GetExitCodeThread	GetFileAttributesA
GetFileAttributesW	GetFileSize	GetFileType	GetFullPathNameA
GetLastError	GetLocaleInfoA	GetLocalTime	GetModuleFileNameA
GetModuleHandleA	GetProcAddress	GetProfileStringA	GetStartupInfoA
GetStdHandle	GetStringTypeExA	GetSystemInfo	GetTempPathA
GetThreadLocale	GetTickCount	GetVersion	GetVersionExA
GlobalAddAtomA	GlobalAlloc	GlobalDeleteAtom	GlobalFindAtomA
GlobalFree	GlobalHandle	GlobalLock	GlobalMemoryStatus
GlobalReAlloc	GlobalSize	GlobalUnlock	InitializeCriticalSection
InterlockedCompareExchange	InterlockedDecrement	InterlockedExchange	InterlockedIncrement
IsBadReadPtr	LeaveCriticalSection	LoadLibraryA	LoadLibraryExA
LoadResource	LocalAlloc	LocalFree	LockResource
lstrcmpA	lstrcpyA	lstrcpynA	lstrlenA
MapViewOfFile	MulDiv	MultiByteToWideChar	OpenFileMappingA
OutputDebugStringA	QueryPerformanceCo	RaiseException	ReadFile

	unter		
ReleaseMutex	ResetEvent ResumeThread	RtlUnwind	SearchPathA
SetCurrentDirectoryA	SetEndOfFile	SetErrorMode	SetEvent
SetFilePointer	SetLastError	SetProcessWorkingSetSize	SetThreadLocale
SetThreadPriority	SizeofResource	Sleep	TlsGetValue
TlsSetValue	UnhandledExceptionFilter	UnmapViewOfFile	VirtualAlloc
VirtualFree	VirtualProtect	VirtualQuery	WaitForSingleObject
WideCharToMultiByte	WriteFile	WriteProcessMemory	

MsVfW32.dll

DrawDibClose	DrawDibDraw	DrawDibOpen	DrawDibRealize

ole32.dll

CoCreateGuid	CoCreateInstance	CoInitialize	CoTaskMemAlloc
CoUninitialize	OleInitialize	OleUninitializ	

oleaut32.dll

GetErrorInfo	SafeArrayAccessData	SafeArrayCreate	SafeArrayGetElement
SafeArrayGetLBound	SafeArrayGetUBound	SafeArrayPtrOfIndex	SafeArrayPutElement
SafeArrayUnaccessData	SysAllocStringLen	SysFreeString	SysReAllocStringLen
VariantChangeType	VariantClear	VariantCopy	VariantCopyInd
VariantInit			

shell32.dll

SHBrowseForFolderA	Shell_NotifyIconA	ShellExecuteA	SHGetDesktopFolder
SHGetMalloc	SHGetPathFromIDListA		

user32.dll

ActivateKeyboardLayout	AdjustWindowRectEx	BeginDeferWindowPos	BeginPaint
CallNextHookEx	CallWindowProcA	CharLowerA	CharLowerBuffA

CharNextA	CharToOemA	CharUpperBuffA	CheckMenuItem
ChildWindowFromPoint	ClientToScreen	CloseClipboard	CopyImage
CreateCaret	CreateIcon	CreateMenu	CreatePopupMenu
CreateWindowExA	DeferWindowPos	DefFrameProcA	DefMDIChildProcA
DefWindowProcA	DeleteMenu	DestroyCaret DestroyCursor	DestroyIcon
DestroyMenu	DestroyWindow	DispatchMessageA	DrawAnimatedRects
DrawEdge	DrawFocusRect	DrawFrameControl	DrawIcon
DrawIconEx	DrawMenuBar	DrawTextA	EmptyClipboard
EnableMenuItem	EnableScrollBar	EnableWindow	EndDeferWindowPos
EndPaint	EnumClipboardFormats	EnumThreadWindows	EnumWindows
EqualRect	FillRect	FindWindowA	FindWindowExA
FrameRect	GetActiveWindow	GetAsyncKeyState	GetCapture
GetClassInfoA	GetClassNameA	GetClientRect	GetClipboardData
GetCursor	GetCursorPos	GetDC	GetDCEx
GetDesktopWindow	GetDlgItem	GetDoubleClickTime	GetFocus
GetForegroundWindow	GetIconInfo	GetKeyboardLayout	GetKeyboardLayoutList
GetKeyboardState	GetKeyboardType	GetKeyNameTextA	GetKeyState
GetLastActivePopup	GetMenu	GetMenuItemCount	GetMenuItemID
GetMenuItemInfoA	GetMenuState	GetMenuStringA	GetMessageA
GetMessagePos	GetParent	GetPropA	GetScrollInfo
GetScrollPos	GetScrollRange	GetSubMenu	GetSysColor
GetSysColorBrush	GetSystemMenu	GetSystemMetrics	GetTopWindow
GetUpdateRect	GetWindow	GetWindowDC	GetWindowLongA
GetWindowPlacement	GetWindowRect	GetWindowTextA	GetWindowTextLengthA
GetWindowThreadProc	HideCaret	InflateRect	InsertMenuA

essId			
InsertMenuItemA	IntersectRect	InvalidateRect	InvalidateRgn
IsChild	IsClipboardFormatAvailable	IsDialogMessageA	IsIconic
IsRectEmpty	IsWindow	IsWindowEnabled	IsWindowVisible
IsZoomed	KillTimer	LoadBitmapA	LoadCursorA
LoadIconA	LoadImageA	LoadKeyboardLayoutA	LoadStringA
MapVirtualKeyA	MapWindowPoints	MessageBeep	MessageBoxA
MsgWaitForMultipleObjects	OemToCharA	OffsetRect	OpenClipboard
PeekMessageA	PostMessageA	PostQuitMessage	PtInRect
RedrawWindow	RegisterClassA	RegisterClipboardFormatA	RegisterWindowMessageA
ReleaseCapture	ReleaseDC	RemoveMenu	RemovePropA
ScreenToClient	ScrollWindow	SendDlgItemMessageA	SendMessageA
SetActiveWindow	SetCapture	SetCaretPos	SetClassLongA
SetClipboardData	SetCursor	SetFocus	SetForegroundWindow
SetMenu	SetMenuItemInfoA	SetParent	SetPropA
SetRect	SetScrollInfo	SetScrollPos	SetScrollRange
SetTimer	SetWindowLongA	SetWindowPlacement	SetWindowPos
SetWindowsHookExA	SetWindowTextA	ShowCaret	ShowCursor
ShowOwnedPopups	ShowScrollBar	ShowWindow	SystemParametersInfoA
TrackPopupMenu	TranslateMDISysAccel	TranslateMessage	UnhookWindowsHookEx
UnregisterClassA	UpdateWindow	WaitMessage	WindowFromPoint
WinHelpA	wvsprintfA		

version.dll

GetFileVersionInfoA	GetFileVersionInfoSizeA	VerQueryValueA	

wininet.dll

InternetQueryOptionA	InternetSetOptionA

winmm.dll

sndPlaySoundA	timeGetTime

winspool.drv

ClosePrinter	DocumentPropertiesA	EnumPrintersA	OpenPrinterA

wsock32.dll.

gethostbyname	inet_addr inet_ntoa	WSACleanup	WSAStartup