XII Jornadas STIC CCN-CERT

Ciberseguridad,
hacia una respuesta y disuasión efectivas

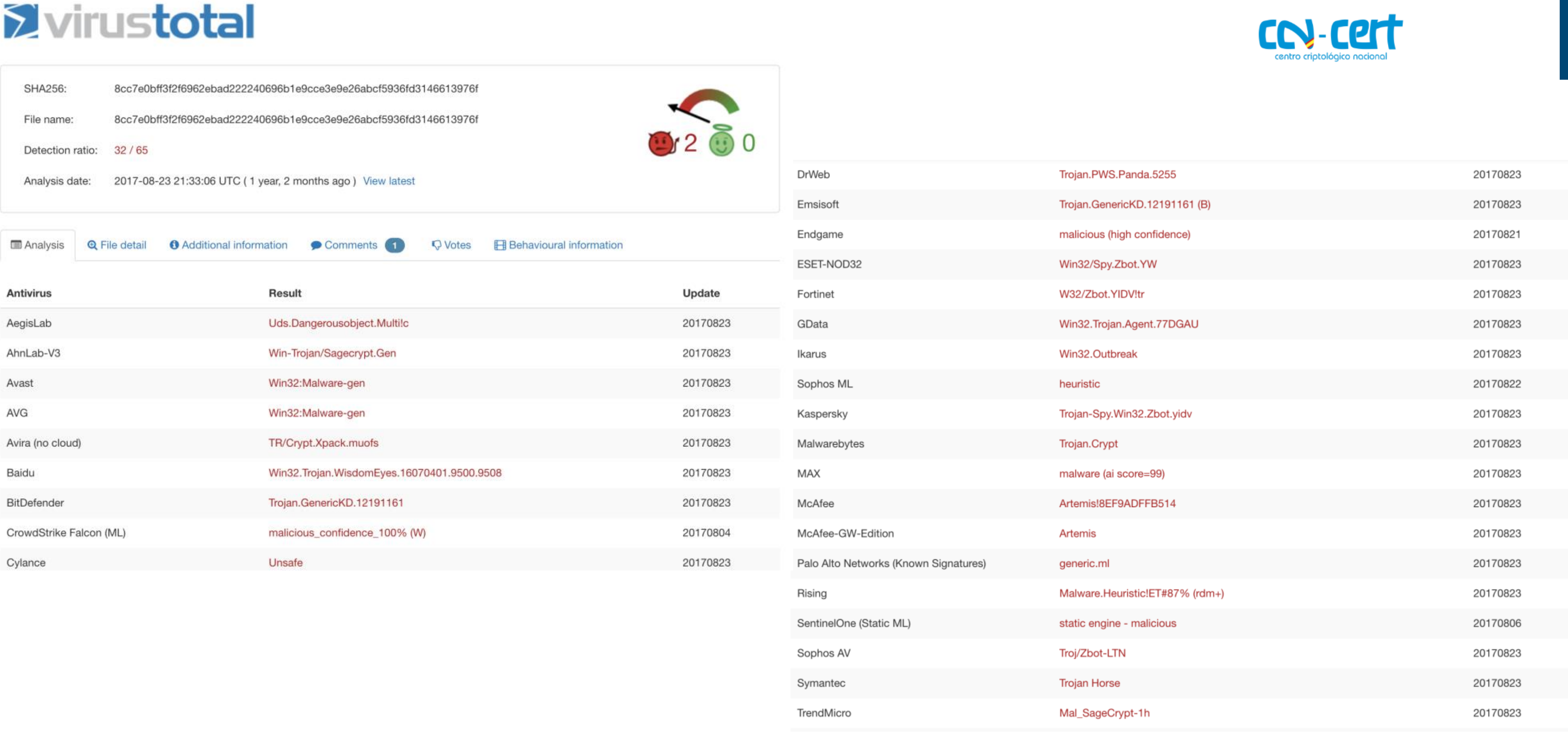
Conociendo a tus enemigos: cómo generar y usar TTPs y no morir en el intento

ccn-cert
centro criptológico nacional

- David Barroso Berrueta
- CounterCraft
- dbarroso@countercraft.eu
  @lostinsecurity

The Tower of Babel by Pieter Bruegel the Elder(1563)

Toda la Tierra hablaba una misma lengua y usaba las mismas palabras. «Edifiquemos una ciudad y una torre cuya cúspide llegue hasta el cielo. Hagámonos así famosos y no andemos más dispersos sobre la faz de la Tierra». Pero Yahveh descendió para ver la ciudad y la torre que los hombres estaban edificando y dijo: «He aquí que todos forman un solo pueblo y todos hablan una misma lengua; siendo este el principio de sus empresas, nada les impedirá que lleven a cabo todo lo que se propongan. Pues bien, descendamos y allí mismo confundamos su lenguaje de modo que no se entiendan los unos con los otros».



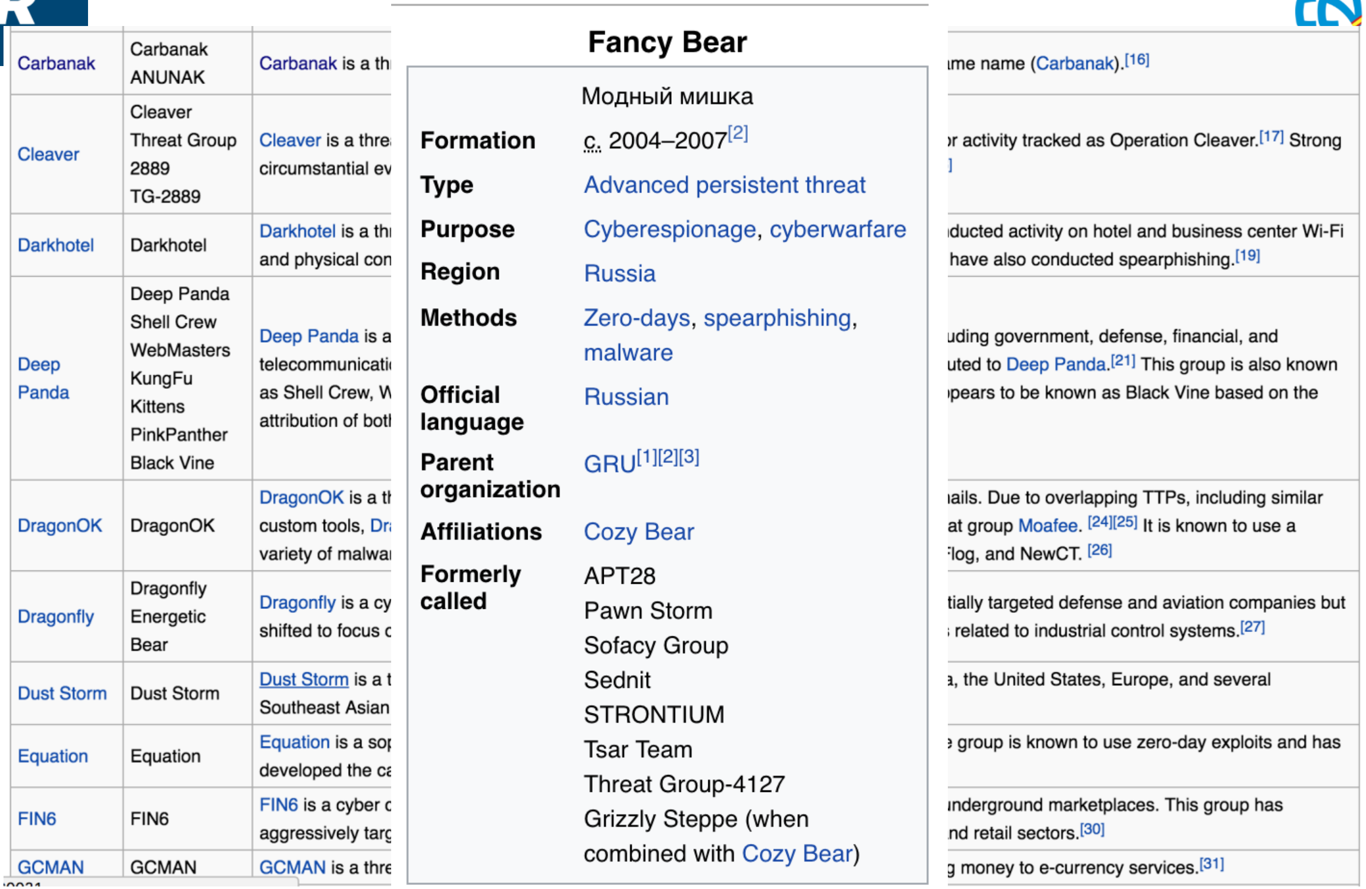
SHA256: 8cc7e0bff3f2f6962ebad222240696b1e9cce3e9e26abcf5936fd3146613976f

File name: 8cc7e0bff3f2f6962ebad222240696b1e9cce3e9e26abcf5936fd3146613976f

Detection ratio: 32 / 65

Analysis date: 2017-08-23 21:33:06 UTC (1 year, 2 months ago) View latest

Antivirus	Result	Update
AegisLab	Uds.Dangerousobject.Multi!c	20170823
AhnLab-V3	Win-Trojan/Sagecrypt.Gen	20170823
Avast	Win32:Malware-gen	20170823
AVG	Win32:Malware-gen	20170823
Avira (no cloud)	TR/Crypt.Xpack.muofs	20170823
Baidu	Win32.Trojan.WisdomEyes.16070401.9500.9508	20170823
BitDefender	Trojan.GenericKD.12191161	20170823
CrowdStrike Falcon (ML)	malicious_confidence_100% (W)	20170804
Cylance	Unsafe	20170823
DrWeb	Trojan.PWS.Panda.5255	20170823
Emsisoft	Trojan.GenericKD.12191161 (B)	20170823
Endgame	malicious (high confidence)	20170821
ESET-NOD32	Win32/Spy.Zbot.YW	20170823
Fortinet	W32/Zbot.YIDV!tr	20170823
GData	Win32.Trojan.Agent.77DGAU	20170823
Ikarus	Win32.Outbreak	20170823
Sophos ML	heuristic	20170822
Kaspersky	Trojan-Spy.Win32.Zbot.yidv	20170823
Malwarebytes	Trojan.Crypt	20170823
MAX	malware (ai score=99)	20170823
McAfee	Artemis!8EF9ADFFB514	20170823
McAfee-GW-Edition	Artemis	20170823
Palo Alto Networks (Known Signatures)	generic.ml	20170823
Rising	Malware.Heuristic!ET#87% (rdm+)	20170823
SentinelOne (Static ML)	static engine - malicious	20170806
Sophos AV	Troj/Zbot-LTN	20170823
Symantec	Trojan Horse	20170823
TrendMicro	Mal_SageCrypt-1h	20170823



Carbanak	Carbanak ANUNAK	Carbanak is a thr	me name (Carbanak).[16]
Cleaver	Cleaver Threat Group 2889 TG-2889	Cleaver is a threa circumstantial ev	r activity tracked as Operation Cleaver.[17] Strong]
Darkhotel	Darkhotel	Darkhotel is a thr and physical con	ducted activity on hotel and business center Wi-Fi have also conducted spearphishing.[19]
Deep Panda	Deep Panda Shell Crew WebMasters KungFu Kittens PinkPanther Black Vine	Deep Panda is a telecommunicatio as Shell Crew, W attribution of both	uding government, defense, financial, and uted to Deep Panda.[21] This group is also known pears to be known as Black Vine based on the
DragonOK	DragonOK	DragonOK is a th custom tools, Dra variety of malwa	ails. Due to overlapping TTPs, including similar at group Moafee. [24][25] It is known to use a log, and NewCT. [26]
Dragonfly	Dragonfly Energetic Bear	Dragonfly is a cy shifted to focus c	tially targeted defense and aviation companies but related to industrial control systems.[27]
Dust Storm	Dust Storm	Dust Storm is a t Southeast Asian	a, the United States, Europe, and several
Equation	Equation	Equation is a sop developed the ca	group is known to use zero-day exploits and has
FIN6	FIN6	FIN6 is a cyber c aggressively targ	nderground marketplaces. This group has nd retail sectors.[30]
GCMAN	GCMAN	GCMAN is a thre	g money to e-currency services.[31]

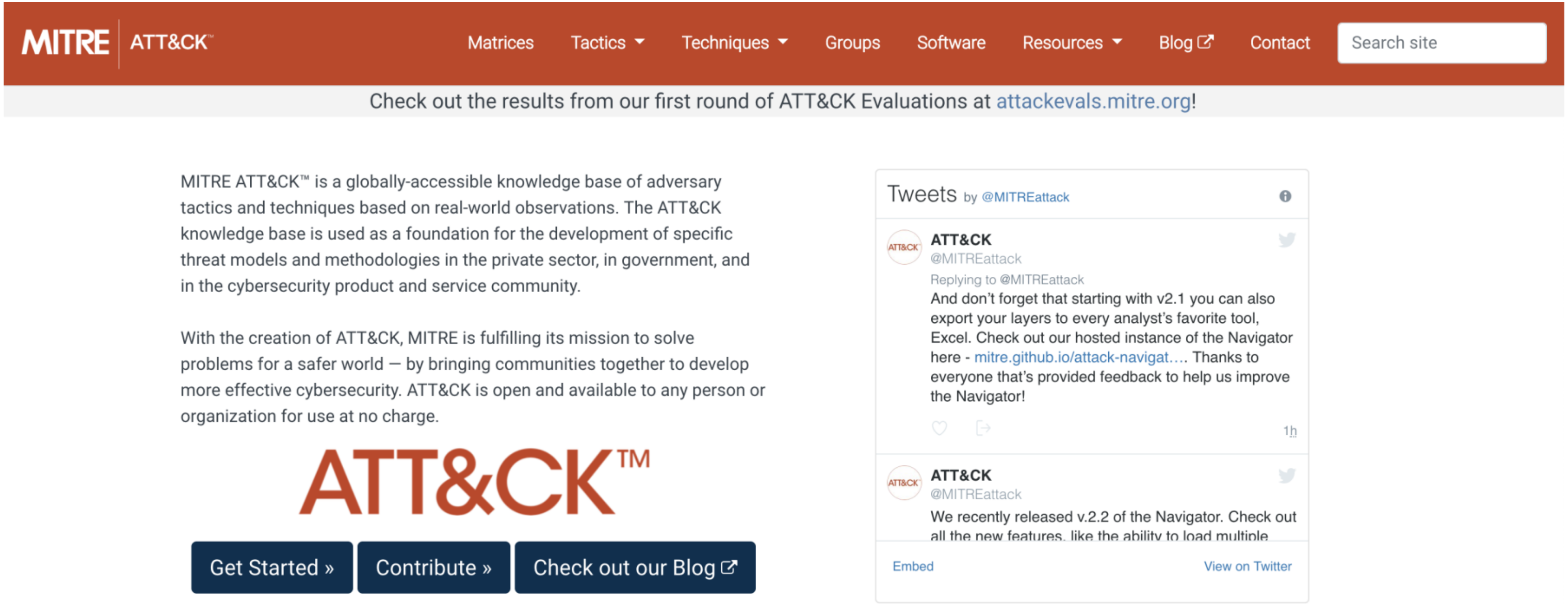
Fancy Bear

Модный мишка

Formation	c. 2004–2007[2]
Type	Advanced persistent threat
Purpose	Cyberespionage, cyberwarfare
Region	Russia
Methods	Zero-days, spearphishing, malware
Official language	Russian
Parent organization	GRU[1][2][3]
Affiliations	Cozy Bear
Formerly called	APT28 Pawn Storm Sofacy Group Sednit STRONTIUM Tsar Team Threat Group-4127 Grizzly Steppe (when combined with Cozy Bear)

Fuente: https://attack.mitre.org/wiki/Groups

MITRE ATT&CK



Check out the results from our first round of ATT&CK Evaluations at attackevals.mitre.org!

MITRE ATT&CK™ is a globally-accessible knowledge base of adversary tactics and techniques based on real-world observations. The ATT&CK knowledge base is used as a foundation for the development of specific threat models and methodologies in the private sector, in government, and in the cybersecurity product and service community.

With the creation of ATT&CK, MITRE is fulfilling its mission to solve problems for a safer world — by bringing communities together to develop more effective cybersecurity. ATT&CK is open and available to any person or organization for use at no charge.

Tweets by @MITREattack

ATT&CK @MITREattack
Replying to @MITREattack
And don't forget that starting with v2.1 you can also export your layers to every analyst's favorite tool, Excel. Check out our hosted instance of the Navigator here - mitre.github.io/attack-navigat…. Thanks to everyone that's provided feedback to help us improve the Navigator!
1h

ATT&CK @MITREattack
We recently released v.2.2 of the Navigator. Check out all the new features, like the ability to load multiple

https://attack.mitre.org/

Síndrome Cyber-Diogenes

Threat intelligence

- Fuentes (cuál escojo):
  - Muchos proveedores de threat intelligence
  - CERTs (nacionales, verticales, etc.)
  - Organizaciones (FS-ISAC)
- Integración con productos de seguridad existentes:
  - SIEM
  - IDS, Firewalls, Endpoint
- Necesidad de analistas que puedan entender y utilizarlos
- A veces es información que no nos afecta directamente

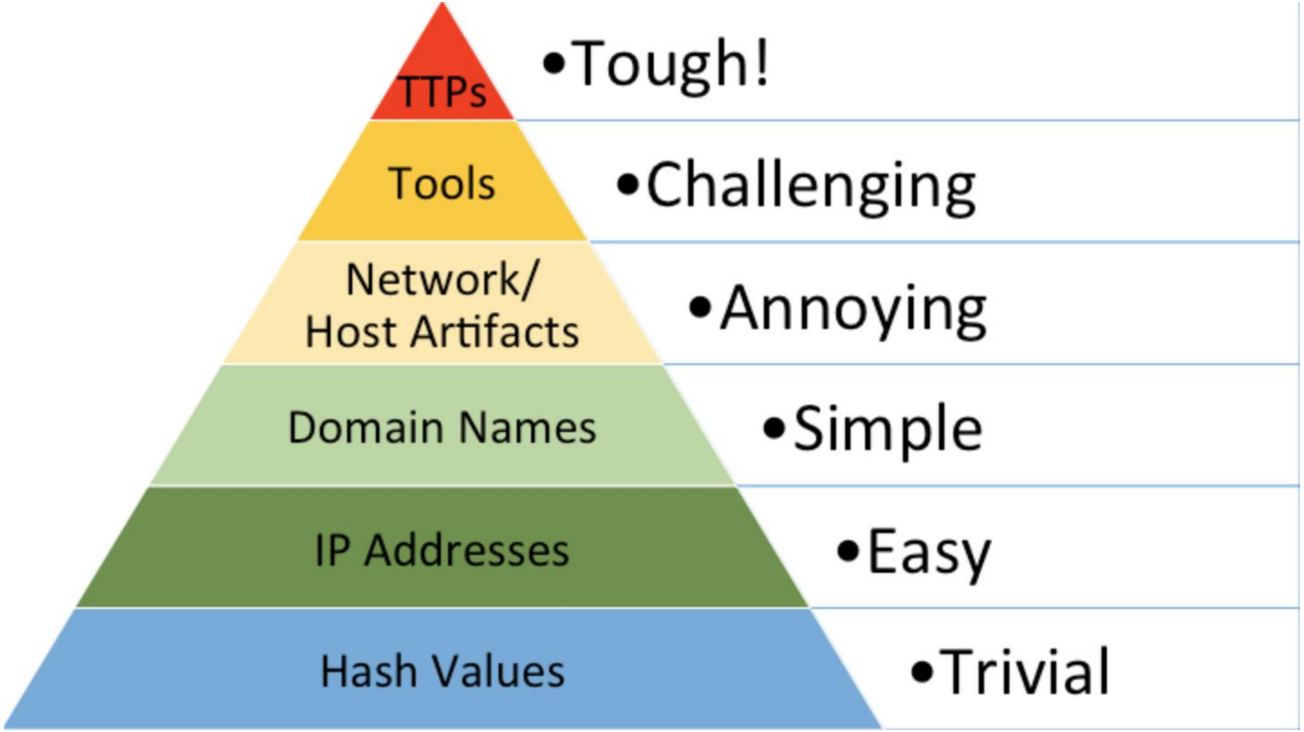
IOCs

1. Contexto
2. Volatilidad
3. Usabilidad

IOCs

- Difíciles de categorizar:
  - – **Confianza** (threat intelligence sharing en círculos de confianza)
  - – **Utilidad** (threat intelligence sharing con entidades ‘útiles’): la pirámide del dolor
  - – **Frescura** (threat intelligence sharing con entidades que tienen datos frescos)

Pirámide del dolor



http://detect-respond.blogspot.com/2013/03/the-pyramid-of-pain.html

TTPs

TTPS: Tactics/Tools, Techniques and Procedures

Tácticas: describe la forma en la que un adversario realiza su ataque desde el inicio hasta el final.

Técnicas: qué herramientas y tecnología utiliza para ello

Procedimientos: pasos a seguir en el ataque

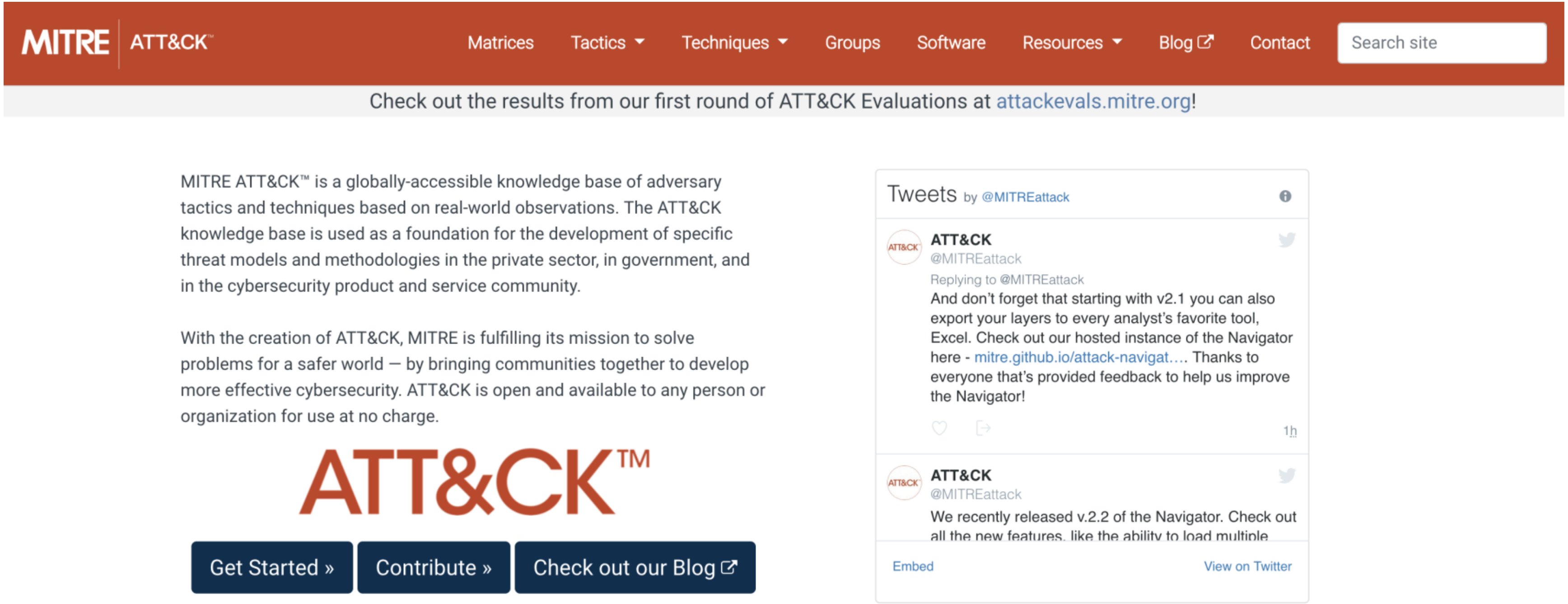
TTPs

- No pensemos siempre en grupos APT
  - Seguramente nunca te enfrentes a ellos
- Pon foco en tus adversarios reales:
  - Insiders – Fraude interno, robo de información, sabotaje
  - Outsiders: competidores, bandas criminales, lobos solitarios.
- Pueden ser más o menos avanzados técnicamente.
- Pero son los que te tienen en el punto de mira.

Análisis de TTPs

Análisis	Resultado
Incidente	¿Es similar a otros incidentes?
Vulnerabilidades/Exploits	Herramientas, métodos de ataque
Patrones	Clasificación de la actividad
Herramientas	¿Qué habilidades y recursos tiene?
Acceso	Motivos, manejabilidad, familiaridad
OPSEC	Anti-forense, técnicas de alteración

MITRE ATT&CK



Check out the results from our first round of ATT&CK Evaluations at attackevals.mitre.org!

MITRE ATT&CK™ is a globally-accessible knowledge base of adversary tactics and techniques based on real-world observations. The ATT&CK knowledge base is used as a foundation for the development of specific threat models and methodologies in the private sector, in government, and in the cybersecurity product and service community.

With the creation of ATT&CK, MITRE is fulfilling its mission to solve problems for a safer world — by bringing communities together to develop more effective cybersecurity. ATT&CK is open and available to any person or organization for use at no charge.

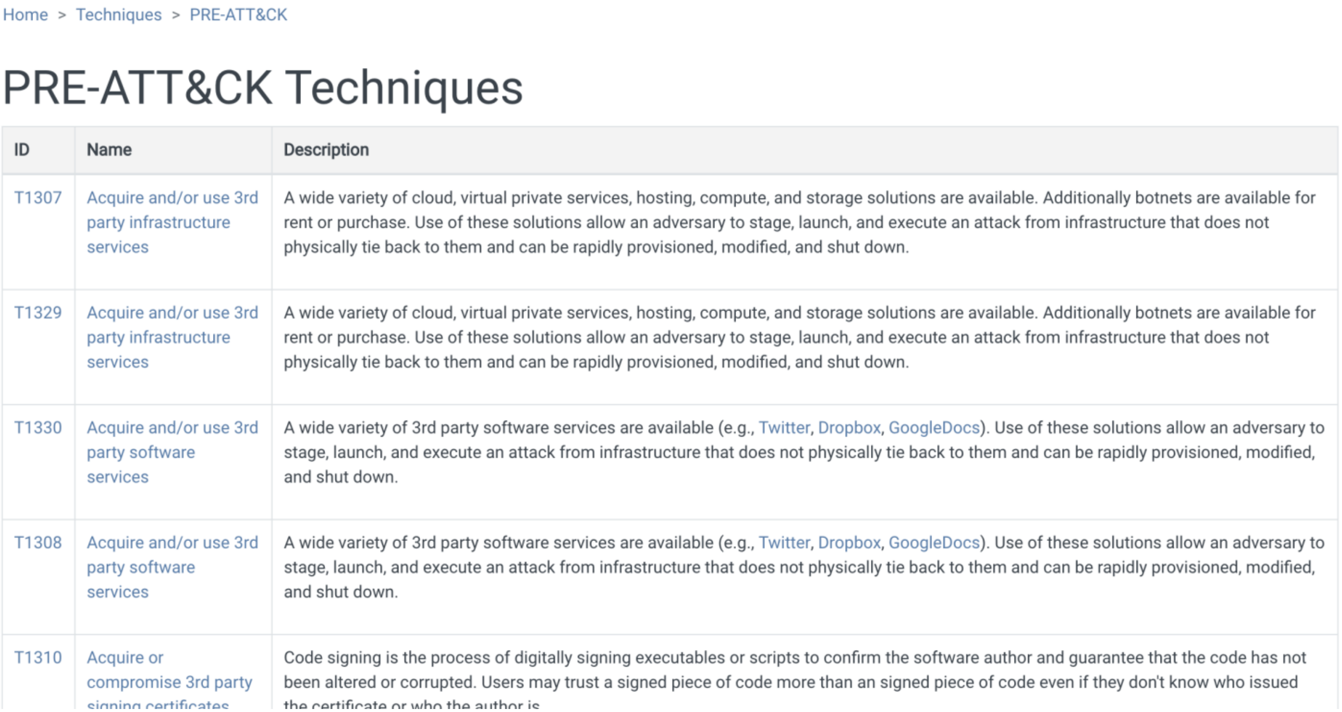
Tweets by @MITREattack

ATT&CK @MITREattack
Replying to @MITREattack
And don't forget that starting with v2.1 you can also export your layers to every analyst's favorite tool, Excel. Check out our hosted instance of the Navigator here - mitre.github.io/attack-navigat…. Thanks to everyone that's provided feedback to help us improve the Navigator!
1h

ATT&CK @MITREattack
We recently released v.2.2 of the Navigator. Check out all the new features, like the ability to load multiple

https://attack.mitre.org/

Pre-ATT&CK

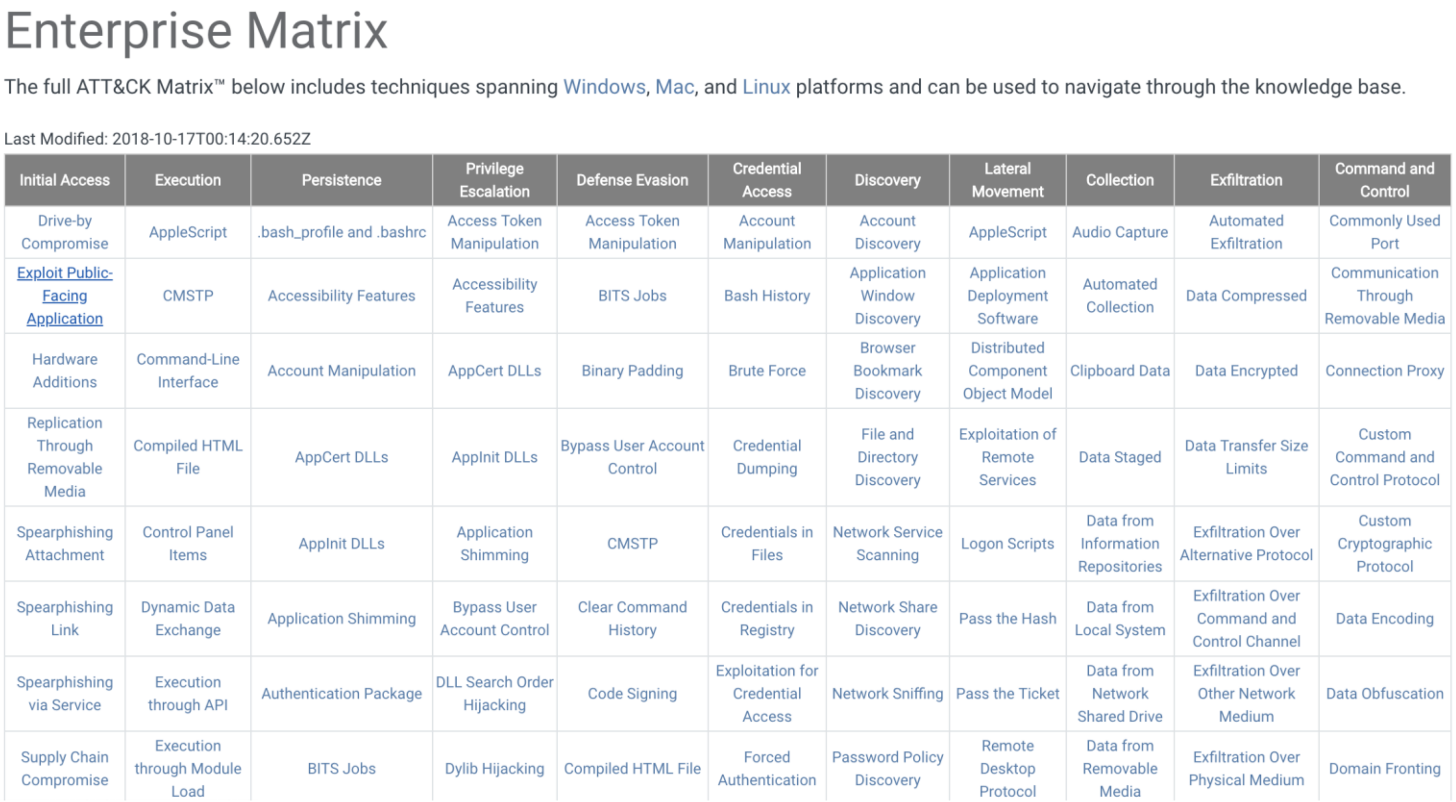


Home > Techniques > PRE-ATT&CK

PRE-ATT&CK Techniques

ID	Name	Description
T1307	Acquire and/or use 3rd party infrastructure services	A wide variety of cloud, virtual private services, hosting, compute, and storage solutions are available. Additionally botnets are available for rent or purchase. Use of these solutions allow an adversary to stage, launch, and execute an attack from infrastructure that does not physically tie back to them and can be rapidly provisioned, modified, and shut down.
T1329	Acquire and/or use 3rd party infrastructure services	A wide variety of cloud, virtual private services, hosting, compute, and storage solutions are available. Additionally botnets are available for rent or purchase. Use of these solutions allow an adversary to stage, launch, and execute an attack from infrastructure that does not physically tie back to them and can be rapidly provisioned, modified, and shut down.
T1330	Acquire and/or use 3rd party software services	A wide variety of 3rd party software services are available (e.g., Twitter, Dropbox, GoogleDocs). Use of these solutions allow an adversary to stage, launch, and execute an attack from infrastructure that does not physically tie back to them and can be rapidly provisioned, modified, and shut down.
T1308	Acquire and/or use 3rd party software services	A wide variety of 3rd party software services are available (e.g., Twitter, Dropbox, GoogleDocs). Use of these solutions allow an adversary to stage, launch, and execute an attack from infrastructure that does not physically tie back to them and can be rapidly provisioned, modified, and shut down.
T1310	Acquire or compromise 3rd party signing certificates	Code signing is the process of digitally signing executables or scripts to confirm the software author and guarantee that the code has not been altered or corrupted. Users may trust a signed piece of code more than an signed piece of code even if they don't know who issued the certificate or who the author is.

MITRE ATT&CK



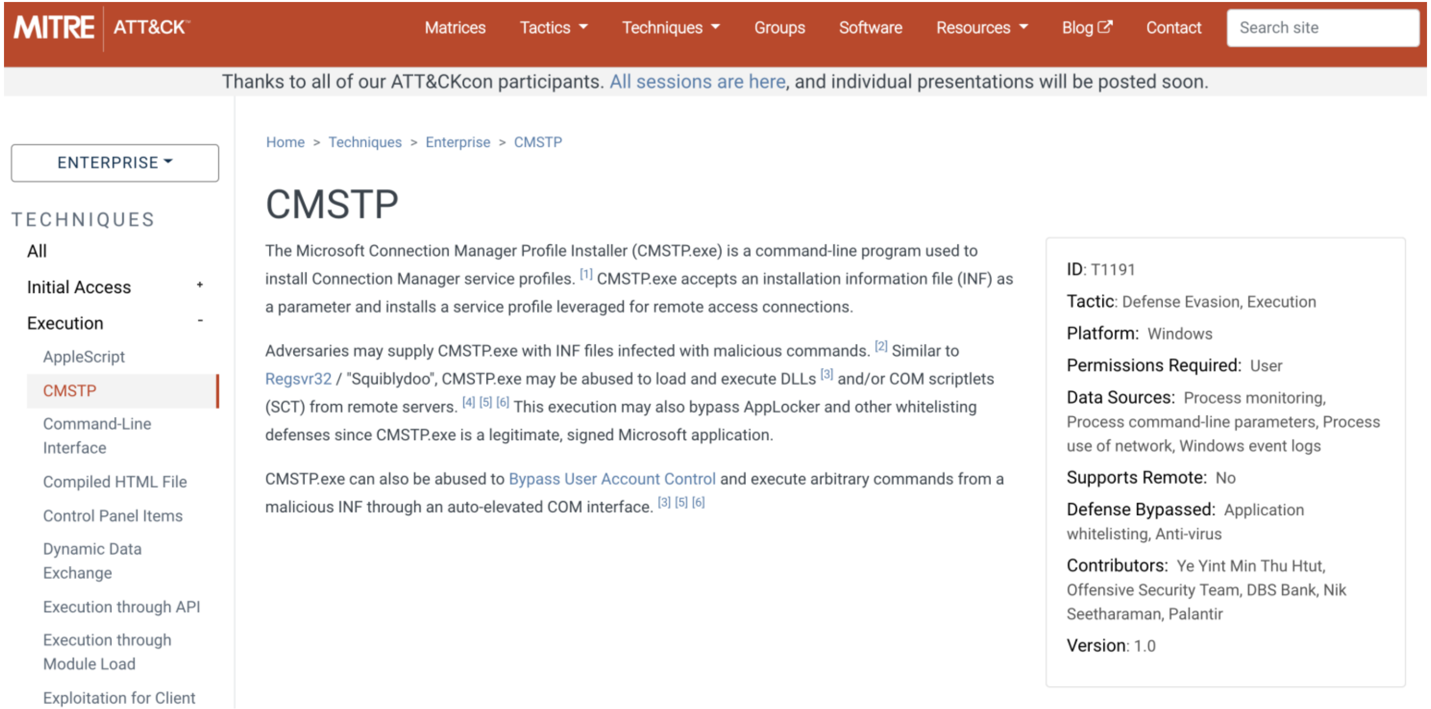
Enterprise Matrix

The full ATT&CK Matrix™ below includes techniques spanning Windows, Mac, and Linux platforms and can be used to navigate through the knowledge base.

Last Modified: 2018-10-17T00:14:20.652Z

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control
Drive-by Compromise	AppleScript	.bash_profile and .bashrc	Access Token Manipulation	Access Token Manipulation	Account Manipulation	Account Discovery	AppleScript	Audio Capture	Automated Exfiltration	Commonly Used Port
Exploit Public-Facing Application	CMSTP	Accessibility Features	Accessibility Features	BITS Jobs	Bash History	Application Window Discovery	Application Deployment Software	Automated Collection	Data Compressed	Communication Through Removable Media
Hardware Additions	Command-Line Interface	Account Manipulation	AppCert DLLs	Binary Padding	Brute Force	Browser Bookmark Discovery	Distributed Component Object Model	Clipboard Data	Data Encrypted	Connection Proxy
Replication Through Removable Media	Compiled HTML File	AppCert DLLs	AppInit DLLs	Bypass User Account Control	Credential Dumping	File and Directory Discovery	Exploitation of Remote Services	Data Staged	Data Transfer Size Limits	Custom Command and Control Protocol
Spearphishing Attachment	Control Panel Items	AppInit DLLs	Application Shimming	CMSTP	Credentials in Files	Network Service Scanning	Logon Scripts	Data from Information Repositories	Exfiltration Over Alternative Protocol	Custom Cryptographic Protocol
Spearphishing Link	Dynamic Data Exchange	Application Shimming	Bypass User Account Control	Clear Command History	Credentials in Registry	Network Share Discovery	Pass the Hash	Data from Local System	Exfiltration Over Command and Control Channel	Data Encoding
Spearphishing via Service	Execution through API	Authentication Package	DLL Search Order Hijacking	Code Signing	Exploitation for Credential Access	Network Sniffing	Pass the Ticket	Data from Network Shared Drive	Exfiltration Over Other Network Medium	Data Obfuscation
Supply Chain Compromise	Execution through Module Load	BITS Jobs	Dylib Hijacking	Compiled HTML File	Forced Authentication	Password Policy Discovery	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Physical Medium	Domain Fronting

Ejemplo: CMSTP



Thanks to all of our ATT&CKcon participants. All sessions are here, and individual presentations will be posted soon.

Home > Techniques > Enterprise > CMSTP

CMSTP

The Microsoft Connection Manager Profile Installer (CMSTP.exe) is a command-line program used to install Connection Manager service profiles. [1] CMSTP.exe accepts an installation information file (INF) as a parameter and installs a service profile leveraged for remote access connections.

Adversaries may supply CMSTP.exe with INF files infected with malicious commands. [2] Similar to Regsvr32 / "Squiblydoo", CMSTP.exe may be abused to load and execute DLLs [3] and/or COM scriptlets (SCT) from remote servers. [4] [5] [6] This execution may also bypass AppLocker and other whitelisting defenses since CMSTP.exe is a legitimate, signed Microsoft application.

CMSTP.exe can also be abused to Bypass User Account Control and execute arbitrary commands from a malicious INF through an auto-elevated COM interface. [3] [5] [6]

ID: T1191

Tactic: Defense Evasion, Execution

Platform: Windows

Permissions Required: User

Data Sources: Process monitoring, Process command-line parameters, Process use of network, Windows event logs

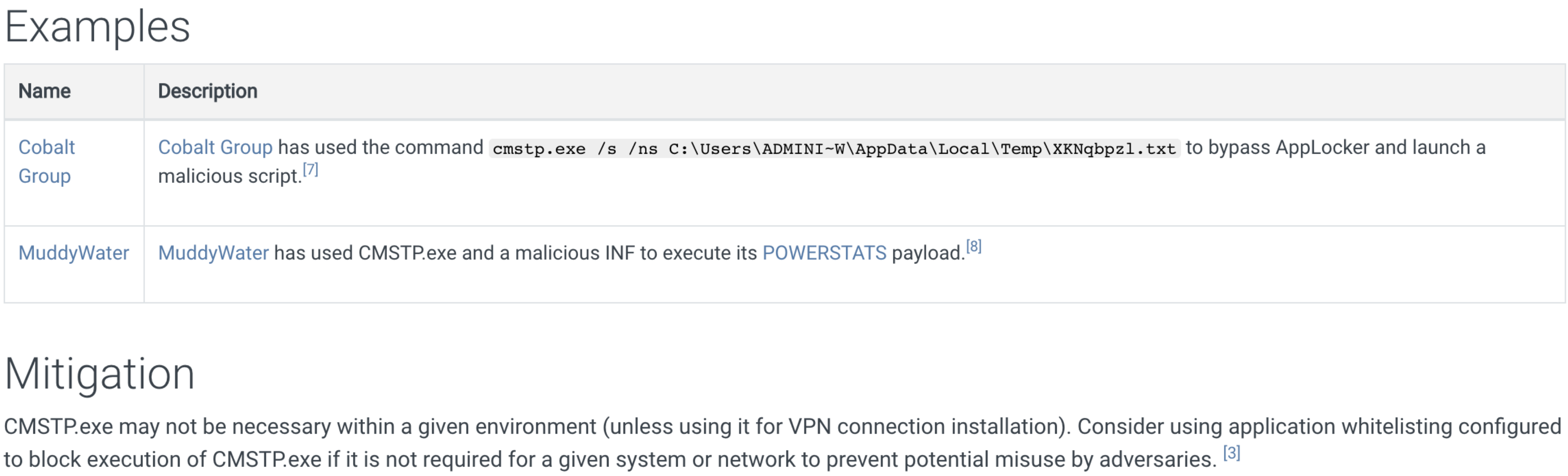
Supports Remote: No

Defense Bypassed: Application whitelisting, Anti-virus

Contributors: Ye Yint Min Thu Htut, Offensive Security Team, DBS Bank, Nik Seetharaman, Palantir

Version: 1.0

Ejemplo: CMSTP



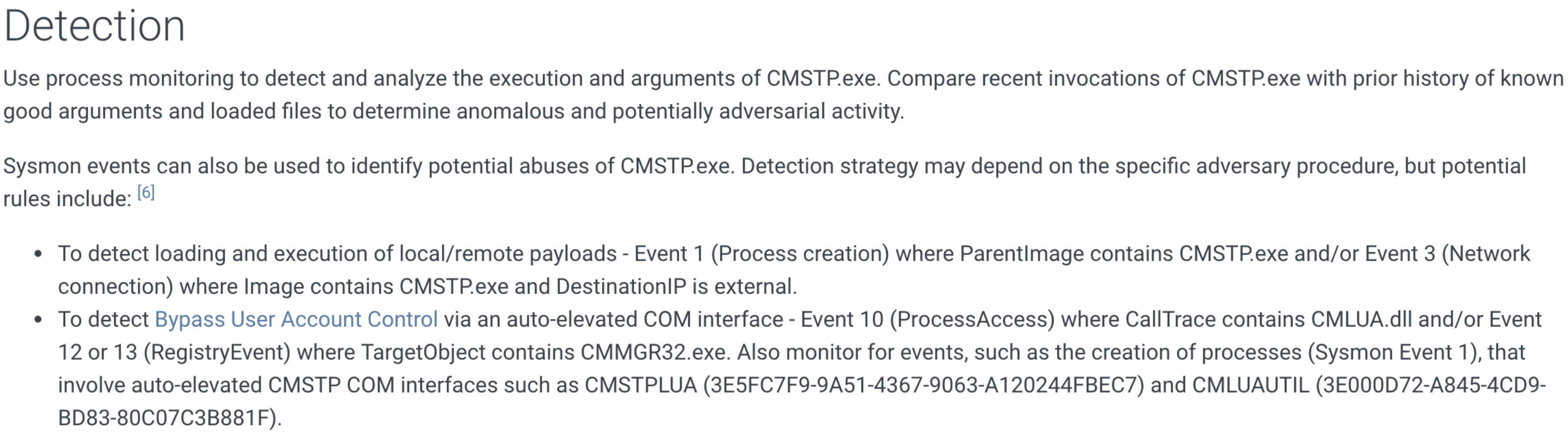
Examples

Name	Description
Cobalt Group	Cobalt Group has used the command `cmstp.exe /s /ns C:\Users\ADMINI~W\AppData\Local\Temp\XKNqbpzl.txt` to bypass AppLocker and launch a malicious script.[7]
MuddyWater	MuddyWater has used CMSTP.exe and a malicious INF to execute its POWERSTATS payload.[8]

Mitigation

CMSTP.exe may not be necessary within a given environment (unless using it for VPN connection installation). Consider using application whitelisting configured to block execution of CMSTP.exe if it is not required for a given system or network to prevent potential misuse by adversaries. [3]

Ejemplo: CMSTP



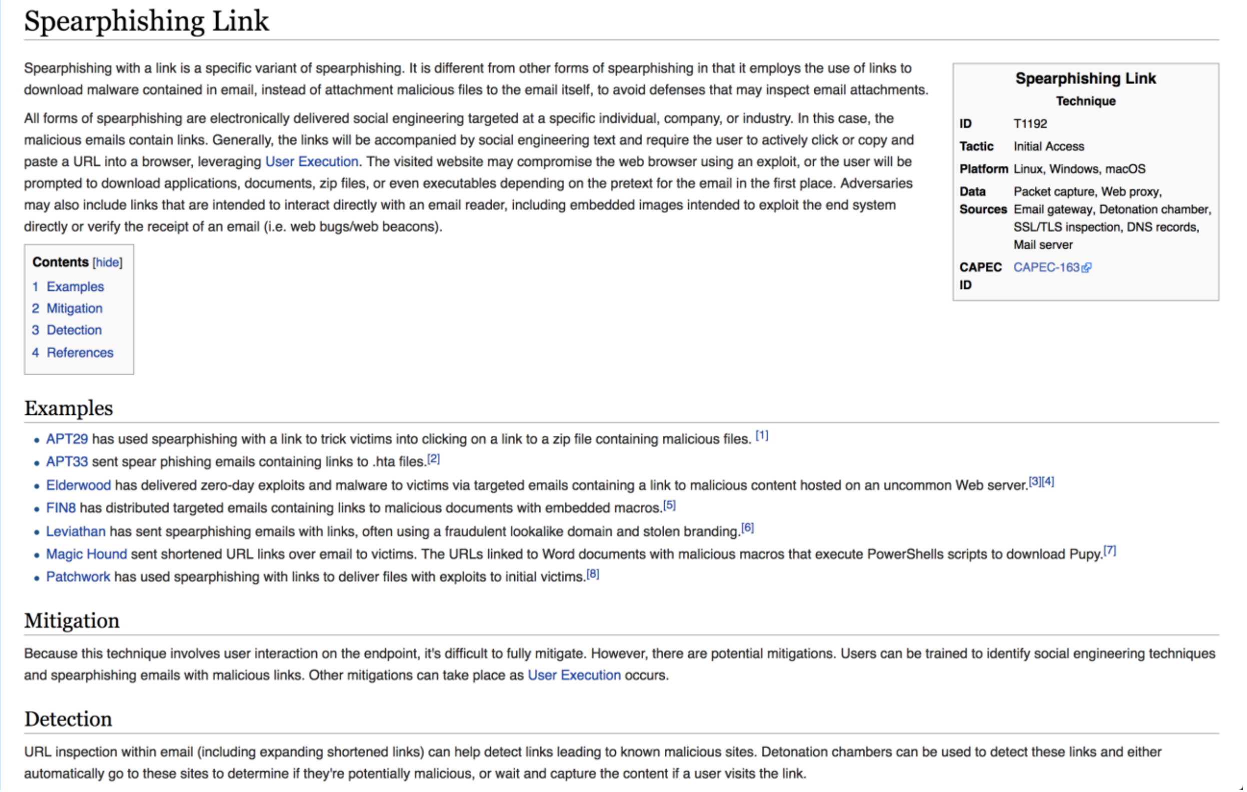
Detection

Use process monitoring to detect and analyze the execution and arguments of CMSTP.exe. Compare recent invocations of CMSTP.exe with prior history of known good arguments and loaded files to determine anomalous and potentially adversarial activity.

Sysmon events can also be used to identify potential abuses of CMSTP.exe. Detection strategy may depend on the specific adversary procedure, but potential rules include: [6]

- To detect loading and execution of local/remote payloads - Event 1 (Process creation) where ParentImage contains CMSTP.exe and/or Event 3 (Network connection) where Image contains CMSTP.exe and DestinationIP is external.
- To detect Bypass User Account Control via an auto-elevated COM interface - Event 10 (ProcessAccess) where CallTrace contains CMLUA.dll and/or Event 12 or 13 (RegistryEvent) where TargetObject contains CMMGR32.exe. Also monitor for events, such as the creation of processes (Sysmon Event 1), that involve auto-elevated CMSTP COM interfaces such as CMSTPLUA (3E5FC7F9-9A51-4367-9063-A120244FBEC7) and CMLUAUTIL (3E000D72-A845-4CD9-BD83-80C07C3B881F).

Ejemplo – Spear Phishing



Spearphishing Link

Spearphishing with a link is a specific variant of spearphishing. It is different from other forms of spearphishing in that it employs the use of links to download malware contained in email, instead of attachment malicious files to the email itself, to avoid defenses that may inspect email attachments.

All forms of spearphishing are electronically delivered social engineering targeted at a specific individual, company, or industry. In this case, the malicious emails contain links. Generally, the links will be accompanied by social engineering text and require the user to actively click or copy and paste a URL into a browser, leveraging User Execution. The visited website may compromise the web browser using an exploit, or the user will be prompted to download applications, documents, zip files, or even executables depending on the pretext for the email in the first place. Adversaries may also include links that are intended to interact directly with an email reader, including embedded images intended to exploit the end system directly or verify the receipt of an email (i.e. web bugs/web beacons).

Spearphishing Link Technique	
ID	T1192
Tactic	Initial Access
Platform	Linux, Windows, macOS
Data Sources	Packet capture, Web proxy, Email gateway, Detonation chamber, SSL/TLS inspection, DNS records, Mail server
CAPEC ID	CAPEC-163

Contents [hide]

Examples

- APT29 has used spearphishing with a link to trick victims into clicking on a link to a zip file containing malicious files. [1]
- APT33 sent spear phishing emails containing links to .hta files.[2]
- Elderwood has delivered zero-day exploits and malware to victims via targeted emails containing a link to malicious content hosted on an uncommon Web server.[3][4]
- FIN8 has distributed targeted emails containing links to malicious documents with embedded macros.[5]
- Leviathan has sent spearphishing emails with links, often using a fraudulent lookalike domain and stolen branding.[6]
- Magic Hound sent shortened URL links over email to victims. The URLs linked to Word documents with malicious macros that execute PowerShells scripts to download Pupy.[7]
- Patchwork has used spearphishing with links to deliver files with exploits to initial victims.[8]

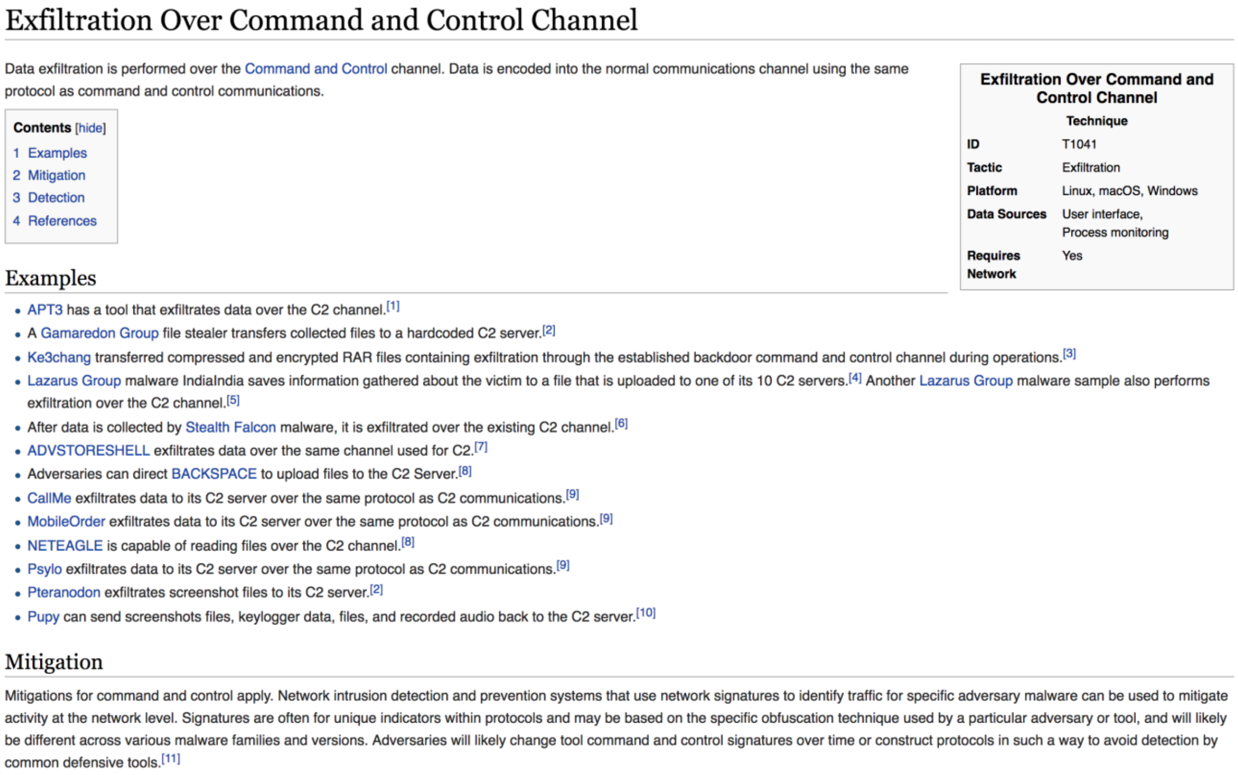
Mitigation

Because this technique involves user interaction on the endpoint, it's difficult to fully mitigate. However, there are potential mitigations. Users can be trained to identify social engineering techniques and spearphishing emails with malicious links. Other mitigations can take place as User Execution occurs.

Detection

URL inspection within email (including expanding shortened links) can help detect links leading to known malicious sites. Detonation chambers can be used to detect these links and either automatically go to these sites to determine if they're potentially malicious, or wait and capture the content if a user visits the link.

Ejemplo – Exfiltration over C2



Exfiltration Over Command and Control Channel

Data exfiltration is performed over the Command and Control channel. Data is encoded into the normal communications channel using the same protocol as command and control communications.

Exfiltration Over Command and Control Channel	
	Technique
ID	T1041
Tactic	Exfiltration
Platform	Linux, macOS, Windows
Data Sources	User interface, Process monitoring
Requires Network	Yes

Contents [hide]

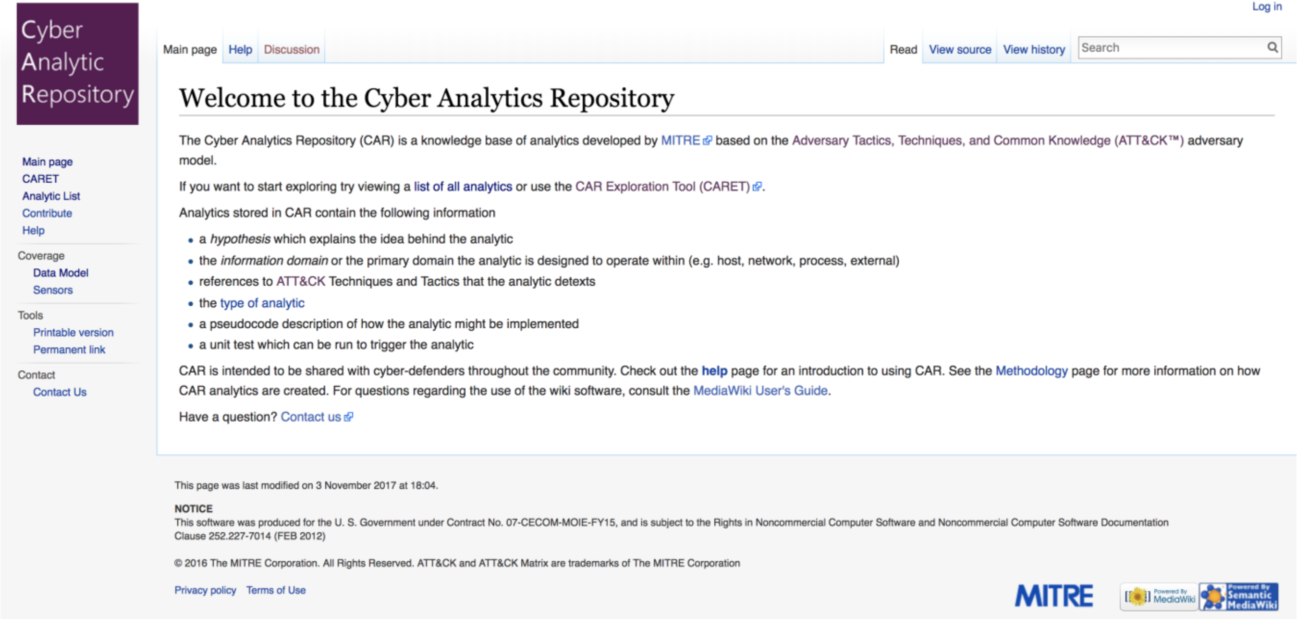
Examples

- APT3 has a tool that exfiltrates data over the C2 channel.[1]
- A Gamaredon Group file stealer transfers collected files to a hardcoded C2 server.[2]
- Ke3chang transferred compressed and encrypted RAR files containing exfiltration through the established backdoor command and control channel during operations.[3]
- Lazarus Group malware IndiaIndia saves information gathered about the victim to a file that is uploaded to one of its 10 C2 servers.[4] Another Lazarus Group malware sample also performs exfiltration over the C2 channel.[5]
- After data is collected by Stealth Falcon malware, it is exfiltrated over the existing C2 channel.[6]
- ADVSTORESHELL exfiltrates data over the same channel used for C2.[7]
- Adversaries can direct BACKSPACE to upload files to the C2 Server.[8]
- CallMe exfiltrates data to its C2 server over the same protocol as C2 communications.[9]
- MobileOrder exfiltrates data to its C2 server over the same protocol as C2 communications.[9]
- NETEAGLE is capable of reading files over the C2 channel.[8]
- Psylo exfiltrates data to its C2 server over the same protocol as C2 communications.[9]
- Pteranodon exfiltrates screenshot files to its C2 server.[2]
- Pupy can send screenshots files, keylogger data, files, and recorded audio back to the C2 server.[10]

Mitigation

Mitigations for command and control apply. Network intrusion detection and prevention systems that use network signatures to identify traffic for specific adversary 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 obfuscation technique used by a particular adversary or tool, and will likely be different across various malware families and versions. Adversaries will likely change tool command and control signatures over time or construct protocols in such a way to avoid detection by common defensive tools.[11]

Cyber Analytics Repository



Welcome to the Cyber Analytics Repository

The Cyber Analytics Repository (CAR) is a knowledge base of analytics developed by MITRE based on the Adversary Tactics, Techniques, and Common Knowledge (ATT&CK™) adversary model.

If you want to start exploring try viewing a list of all analytics or use the CAR Exploration Tool (CARET).

Analytics stored in CAR contain the following information

- a *hypothesis* which explains the idea behind the analytic
- the *information domain* or the primary domain the analytic is designed to operate within (e.g. host, network, process, external)
- references to ATT&CK Techniques and Tactics that the analytic detexts
- the type of analytic
- a pseudocode description of how the analytic might be implemented
- a unit test which can be run to trigger the analytic

CAR is intended to be shared with cyber-defenders throughout the community. Check out the **help** page for an introduction to using CAR. See the Methodology page for more information on how CAR analytics are created. For questions regarding the use of the wiki software, consult the MediaWiki User's Guide.

Have a question? Contact us

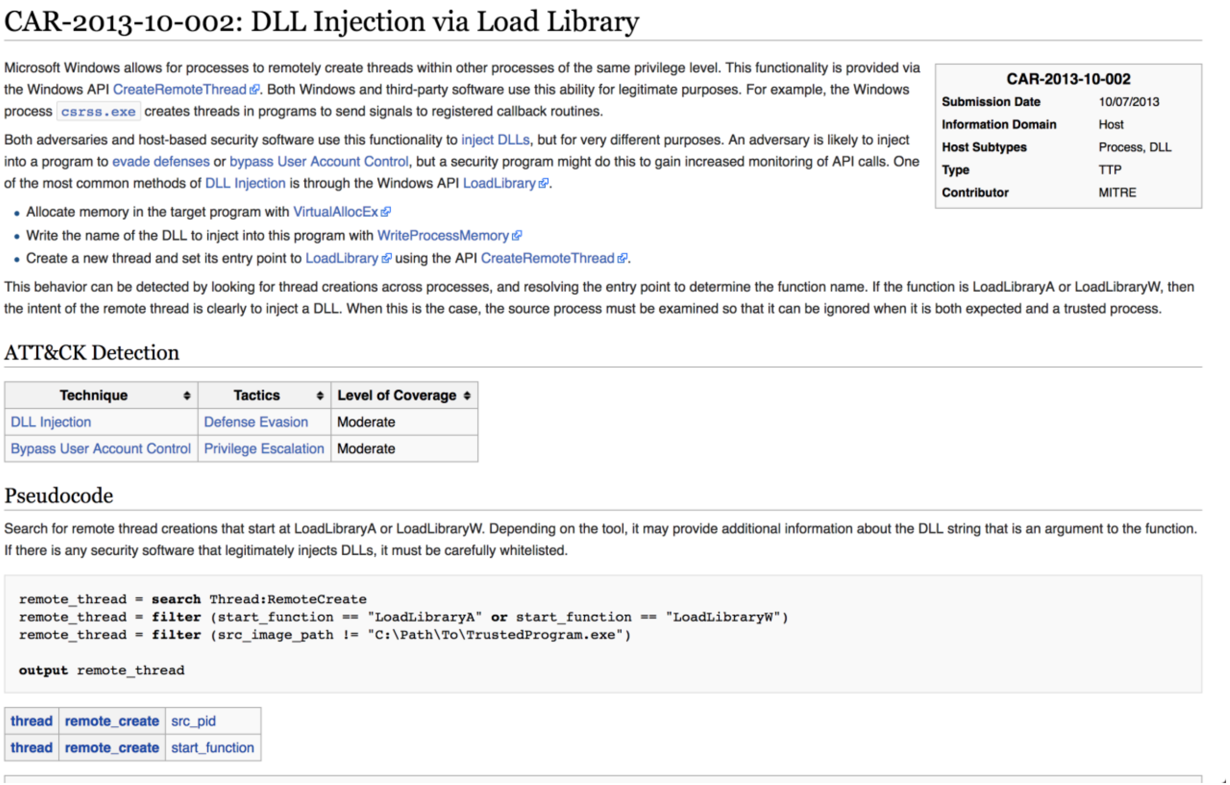
This page was last modified on 3 November 2017 at 18:04.

NOTICE
This software was produced for the U. S. Government under Contract No. 07-CECOM-MOIE-FY15, and is subject to the Rights in Noncommercial Computer Software and Noncommercial Computer Software Documentation Clause 252.227-7014 (FEB 2012)

© 2016 The MITRE Corporation. All Rights Reserved. ATT&CK and ATT&CK Matrix are trademarks of The MITRE Corporation

https://car.mitre.org/wiki/Main_Page

Ejemplo – DLL Injection



CAR-2013-10-002: DLL Injection via Load Library

Microsoft Windows allows for processes to remotely create threads within other processes of the same privilege level. This functionality is provided via the Windows API CreateRemoteThread. Both Windows and third-party software use this ability for legitimate purposes. For example, the Windows process `csrss.exe` creates threads in programs to send signals to registered callback routines.

Both adversaries and host-based security software use this functionality to inject DLLs, but for very different purposes. An adversary is likely to inject into a program to evade defenses or bypass User Account Control, but a security program might do this to gain increased monitoring of API calls. One of the most common methods of DLL Injection is through the Windows API LoadLibrary.

- Allocate memory in the target program with VirtualAllocEx
- Write the name of the DLL to inject into this program with WriteProcessMemory
- Create a new thread and set its entry point to LoadLibrary using the API CreateRemoteThread.

This behavior can be detected by looking for thread creations across processes, and resolving the entry point to determine the function name. If the function is LoadLibraryA or LoadLibraryW, then the intent of the remote thread is clearly to inject a DLL. When this is the case, the source process must be examined so that it can be ignored when it is both expected and a trusted process.

CAR-2013-10-002	
Submission Date	10/07/2013
Information Domain	Host
Host Subtypes	Process, DLL
Type	TTP
Contributor	MITRE

ATT&CK Detection

Technique	Tactics	Level of Coverage
DLL Injection	Defense Evasion	Moderate
Bypass User Account Control	Privilege Escalation	Moderate

Pseudocode

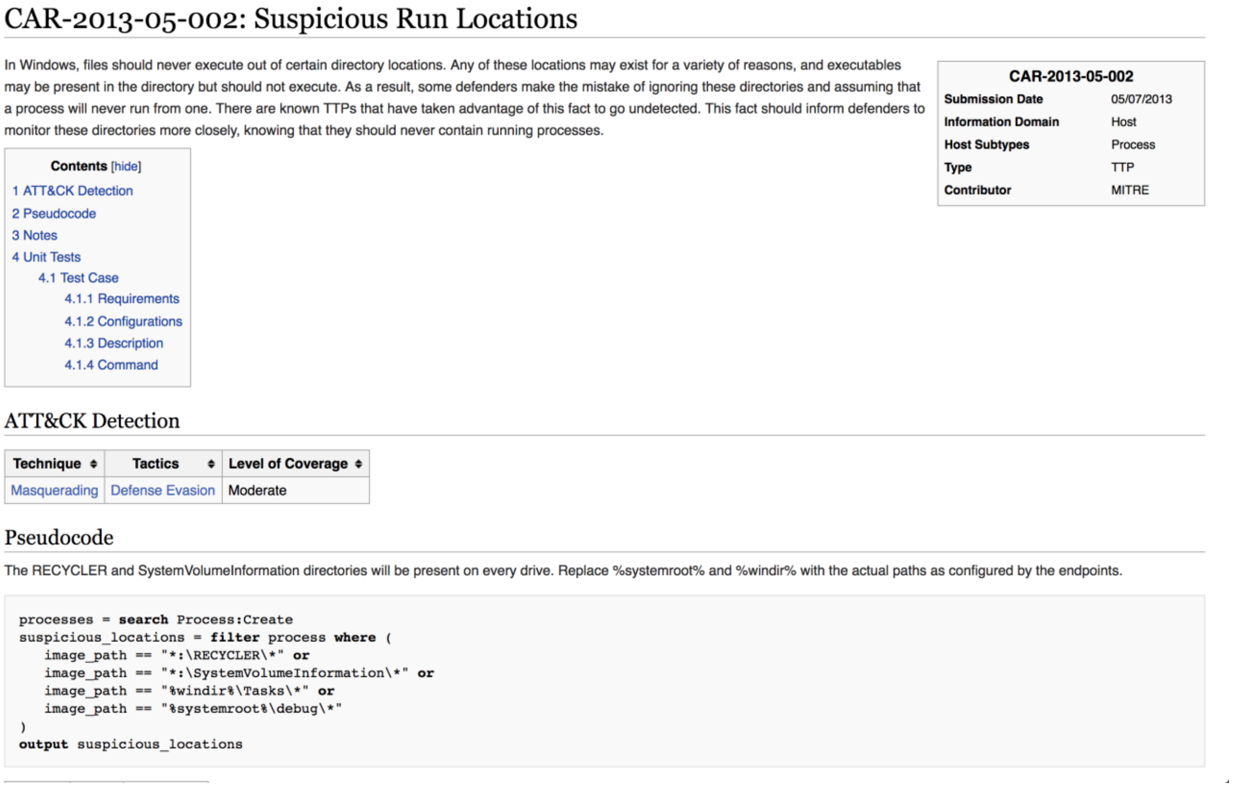
Search for remote thread creations that start at LoadLibraryA or LoadLibraryW. Depending on the tool, it may provide additional information about the DLL string that is an argument to the function. If there is any security software that legitimately injects DLLs, it must be carefully whitelisted.

```
remote_thread = search Thread:RemoteCreate
remote_thread = filter (start_function == "LoadLibraryA" or start_function == "LoadLibraryW")
remote_thread = filter (src_image_path != "C:\Path\To\TrustedProgram.exe")

output remote_thread
```

thread	**remote_create**	src_pid
thread	**remote_create**	start_function

Ejemplo – Suspicious Run Locations



CAR-2013-05-002: Suspicious Run Locations

In Windows, files should never execute out of certain directory locations. Any of these locations may exist for a variety of reasons, and executables may be present in the directory but should not execute. As a result, some defenders make the mistake of ignoring these directories and assuming that a process will never run from one. There are known TTPs that have taken advantage of this fact to go undetected. This fact should inform defenders to monitor these directories more closely, knowing that they should never contain running processes.

CAR-2013-05-002	
Submission Date	05/07/2013
Information Domain	Host
Host Subtypes	Process
Type	TTP
Contributor	MITRE

Contents [hide]

ATT&CK Detection

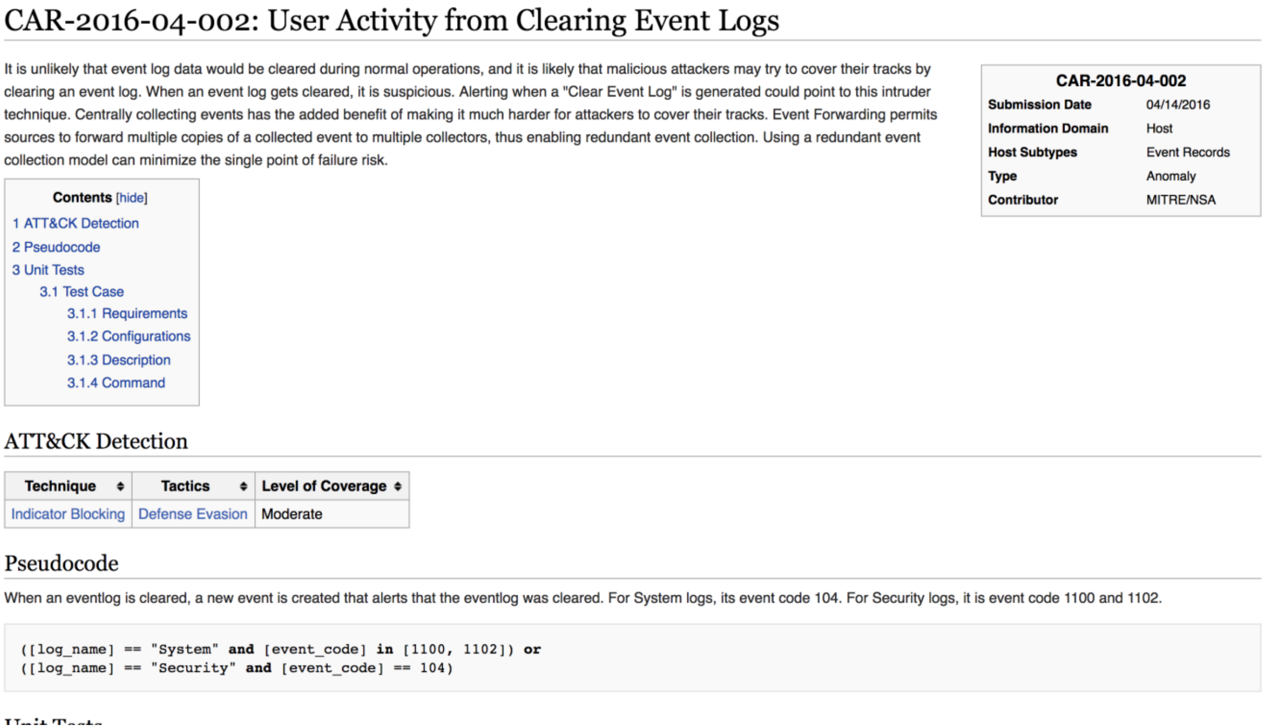
Technique	Tactics	Level of Coverage
Masquerading	Defense Evasion	Moderate

Pseudocode

The RECYCLER and SystemVolumeInformation directories will be present on every drive. Replace %systemroot% and %windir% with the actual paths as configured by the endpoints.

```
processes = search Process:Create
suspicious_locations = filter process where (
   image_path == "*:\RECYCLER\*" or
   image_path == "*:\SystemVolumeInformation\*" or
   image_path == "%windir%\Tasks\*" or
   image_path == "%systemroot%\debug\*"
)
output suspicious_locations
```

Ejemplo – Clearing logs



CAR-2016-04-002: User Activity from Clearing Event Logs

It is unlikely that event log data would be cleared during normal operations, and it is likely that malicious attackers may try to cover their tracks by clearing an event log. When an event log gets cleared, it is suspicious. Alerting when a "Clear Event Log" is generated could point to this intruder technique. Centrally collecting events has the added benefit of making it much harder for attackers to cover their tracks. Event Forwarding permits sources to forward multiple copies of a collected event to multiple collectors, thus enabling redundant event collection. Using a redundant event collection model can minimize the single point of failure risk.

CAR-2016-04-002	
Submission Date	04/14/2016
Information Domain	Host
Host Subtypes	Event Records
Type	Anomaly
Contributor	MITRE/NSA

Contents [hide]

ATT&CK Detection

Technique ⬍	Tactics ⬍	Level of Coverage ⬍
Indicator Blocking	Defense Evasion	Moderate

Pseudocode

When an eventlog is cleared, a new event is created that alerts that the eventlog was cleared. For System logs, its event code 104. For Security logs, it is event code 1100 and 1102.

```
([log_name] == "System" and [event_code] in [1100, 1102]) or
([log_name] == "Security" and [event_code] == 104)
```

Unit Tests

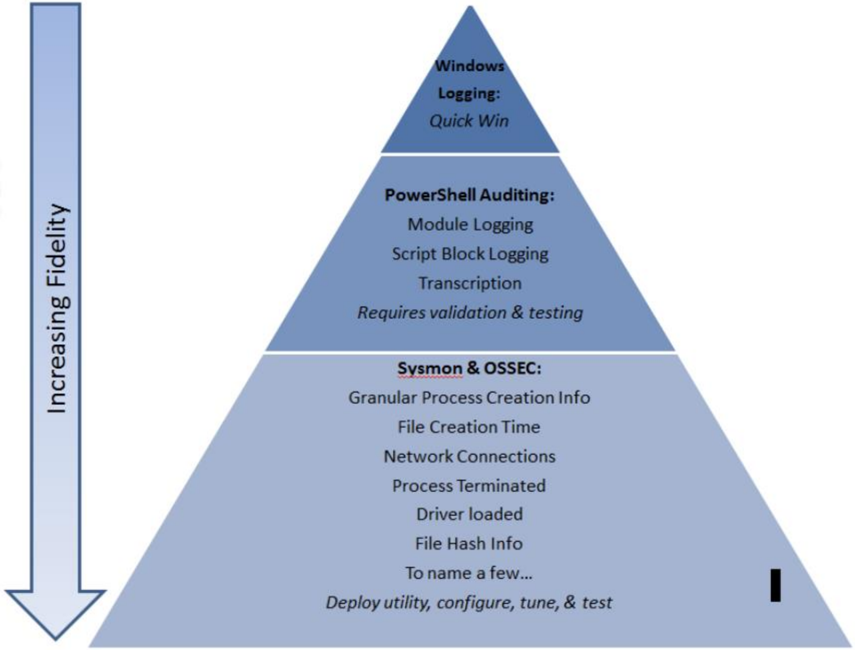
MITRE ATT&CK es…

- Es una gran oportunidad de usar una taxonomia ‘standard’
- Lecciones aprendidas de intentos previos (CyberKillChain, STIX, STIX2, CyBoX, attack graphs, threat modeling, etc.)
- Pero aún no es perfecta. Por ejemplo, ¿cómo se pueden modelar incidents de fraude?
  - Mulas
  - Procedimientos de cash out

¿Y ahora cómo creo esos TTPs?

1. Logs, Logs y más Logs
2. Threat Hunting
    1. Crea hipótesis
    2. Comprueba
    3. Automatiza

Dame logs



Windows Logging:
Quick Win

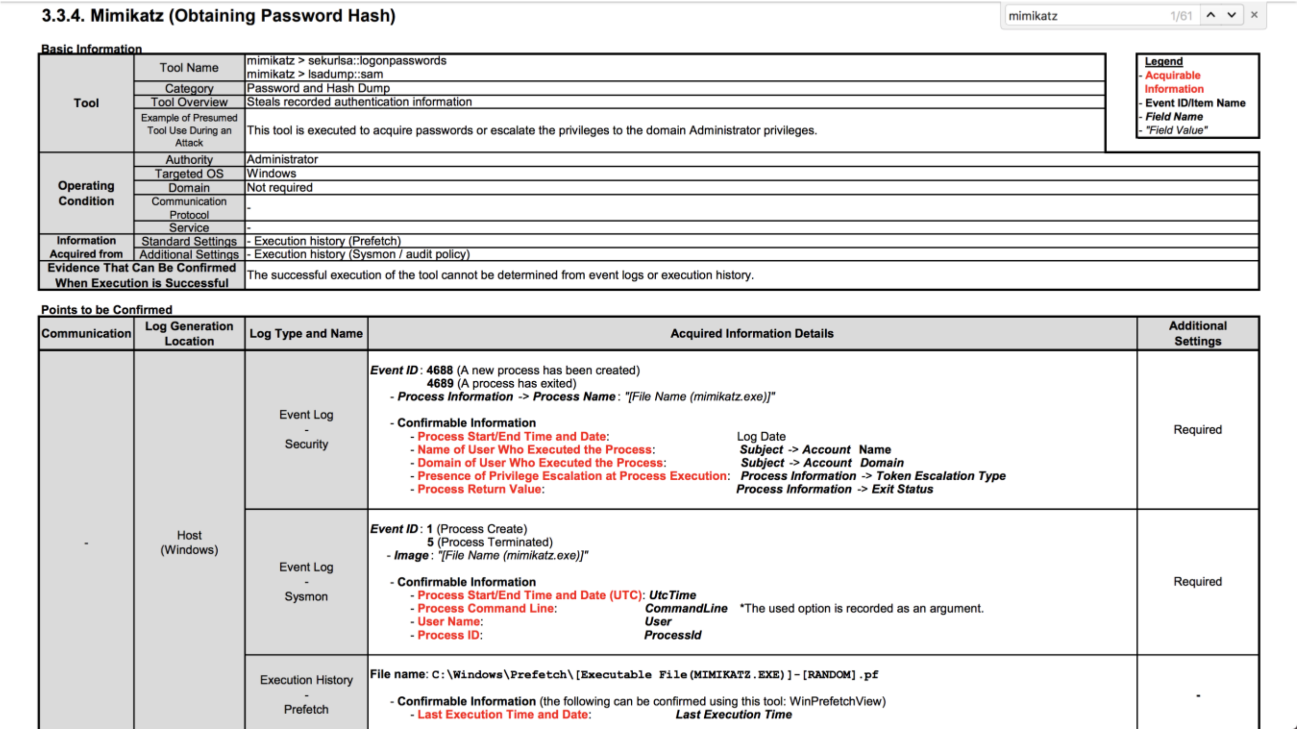
PowerShell Auditing:
Module Logging
Script Block Logging
Transcription
Requires validation & testing

Sysmon & OSSEC:
Granular Process Creation Info
File Creation Time
Network Connections
Process Terminated
Driver loaded
File Hash Info
To name a few...
Deploy utility, configure, tune, & test

Dame logs

- Recursos recomendados:
  - https://github.com/SwiftOnSecurity/sysmon-config
  - https://www.malwarearchaeology.com/cheat-sheets/
  - https://github.com/ThreatHuntingProject/ThreatHunting
  - https://github.com/Neo23x0/sigma/tree/master/rules
  - https://www.jpcert.or.jp/english/pub/sr/20170612ac-ir_research_en.pdf

Ejemplo – Detectando Mimikatz



3.3.4. Mimikatz (Obtaining Password Hash)

Basic Information

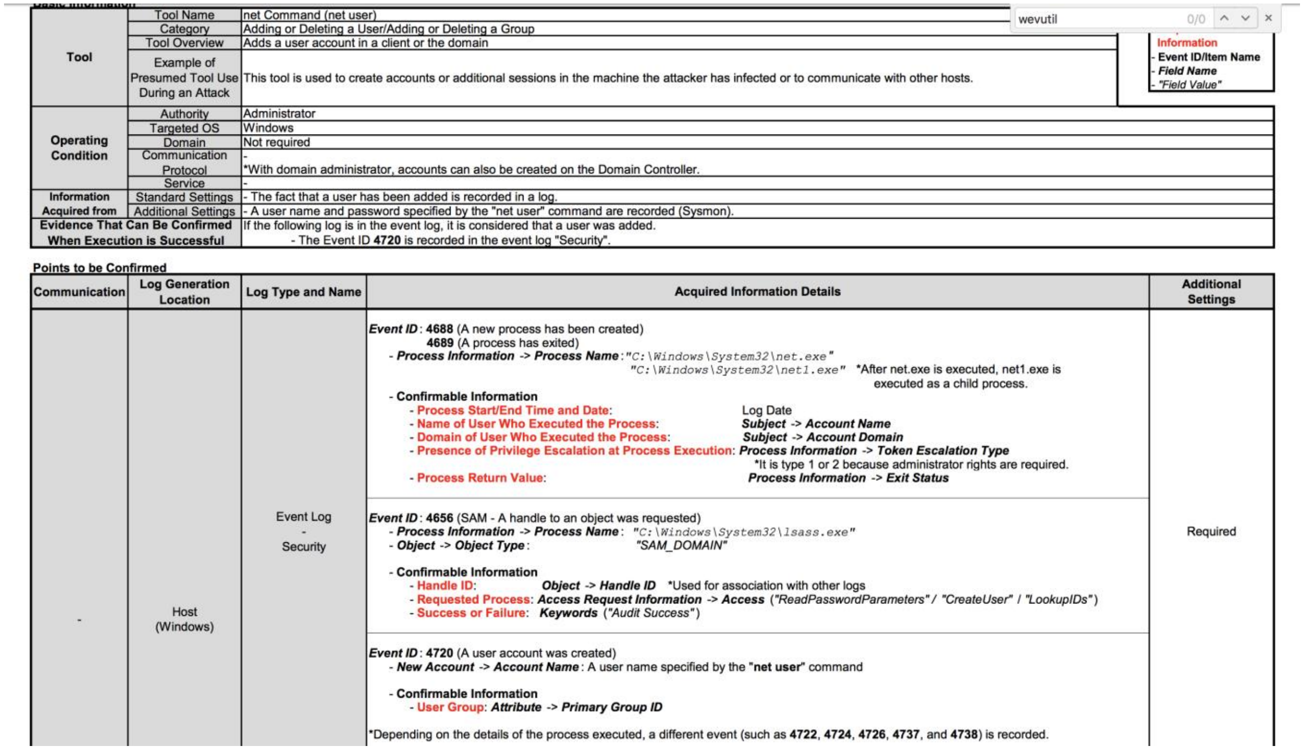
Tool	Tool Name	mimikatz > sekurlsa::logonpasswords mimikatz > lsadump::sam
	Category	Password and Hash Dump
	Tool Overview	Steals recorded authentication information
	Example of Presumed Tool Use During an Attack	This tool is executed to acquire passwords or escalate the privileges to the domain Administrator privileges.
Operating Condition	Authority	Administrator
	Targeted OS	Windows
	Domain	Not required
	Communication Protocol	-
	Service	-
Information Acquired from	Standard Settings	- Execution history (Prefetch)
	Additional Settings	- Execution history (Sysmon / audit policy)
Evidence That Can Be Confirmed When Execution is Successful		The successful execution of the tool cannot be determined from event logs or execution history.

Legend
- Acquirable Information
- **Event ID/Item Name**
- ***Field Name***
- *"Field Value"*

Points to be Confirmed

Communication	Log Generation Location	Log Type and Name	Acquired Information Details	Additional Settings
-	Host (Windows)	Event Log - Security	***Event ID*** : **4688** (A new process has been created) **4689** (A process has exited) - ***Process Information*** -> ***Process Name*** : *"[File Name (mimikatz.exe)]"* - **Confirmable Information** - **Process Start/End Time and Date**: Log Date - **Name of User Who Executed the Process**: ***Subject*** -> ***Account*** **Name** - **Domain of User Who Executed the Process**: ***Subject*** -> ***Account*** ***Domain*** - **Presence of Privilege Escalation at Process Execution**: ***Process Information*** -> ***Token Escalation Type*** - **Process Return Value**: ***Process Information*** -> ***Exit Status***	Required
		Event Log - Sysmon	***Event ID*** : **1** (Process Create) **5** (Process Terminated) - ***Image*** : *"[File Name (mimikatz.exe)]"* - **Confirmable Information** - **Process Start/End Time and Date (UTC)**: ***UtcTime*** - **Process Command Line**: ***CommandLine*** *The used option is recorded as an argument. - **User Name**: ***User*** - **Process ID**: ***ProcessId***	Required
		Execution History - Prefetch	**File name**: `C:\Windows\Prefetch\[Executable File(MIMIKATZ.EXE)]-[RANDOM].pf` - **Confirmable Information** (the following can be confirmed using this tool: WinPrefetchView) - **Last Execution Time and Date**: ***Last Execution Time***	-

Ejemplo – net user



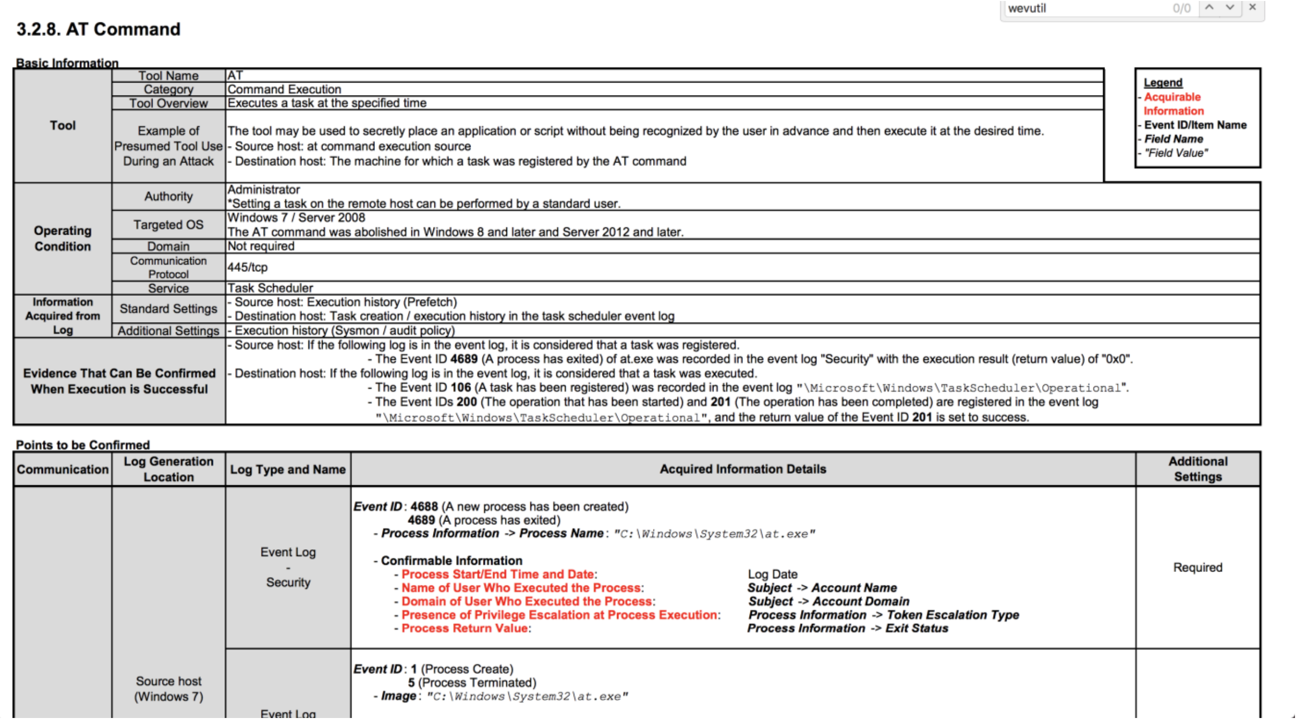
Basic Information

Tool	Tool Name	net Command (net user)
	Category	Adding or Deleting a User/Adding or Deleting a Group
	Tool Overview	Adds a user account in a client or the domain
	Example of Presumed Tool Use During an Attack	This tool is used to create accounts or additional sessions in the machine the attacker has infected or to communicate with other hosts.
Operating Condition	Authority	Administrator
	Targeted OS	Windows
	Domain	Not required
	Communication Protocol	- *With domain administrator, accounts can also be created on the Domain Controller.
	Service	-
Information Acquired from	Standard Settings	- The fact that a user has been added is recorded in a log.
	Additional Settings	- A user name and password specified by the "net user" command are recorded (Sysmon).
Evidence That Can Be Confirmed When Execution is Successful		If the following log is in the event log, it is considered that a user was added. - The Event ID **4720** is recorded in the event log "Security".

Points to be Confirmed

Communication	**Log Generation Location**	**Log Type and Name**	**Acquired Information Details**	**Additional Settings**
-	Host (Windows)	Event Log - Security	***Event ID*** : **4688** (A new process has been created) **4689** (A process has exited) - ***Process Information -> Process Name*** : "C:\Windows\System32\net.exe" "C:\Windows\System32\net1.exe" *After net.exe is executed, net1.exe is executed as a child process. - **Confirmable Information** - **Process Start/End Time and Date**: Log Date - **Name of User Who Executed the Process**: ***Subject -> Account Name*** - **Domain of User Who Executed the Process**: ***Subject -> Account Domain*** - **Presence of Privilege Escalation at Process Execution**: ***Process Information -> Token Escalation Type*** *It is type 1 or 2 because administrator rights are required. - **Process Return Value**: ***Process Information -> Exit Status***	Required
			Event ID : **4656** (SAM - A handle to an object was requested) - ***Process Information -> Process Name*** : "C:\Windows\System32\lsass.exe" - ***Object -> Object Type*** : *"SAM_DOMAIN"* - **Confirmable Information** - **Handle ID**: ***Object -> Handle ID*** *Used for association with other logs - **Requested Process**: ***Access Request Information -> Access*** (*"ReadPasswordParameters" / "CreateUser" / "LookupIDs"*) - **Success or Failure**: ***Keywords*** (*"Audit Success"*)	
			Event ID : **4720** (A user account was created) - ***New Account -> Account Name*** : A user name specified by the "**net user**" command - **Confirmable Information** - **User Group**: ***Attribute -> Primary Group ID*** *Depending on the details of the process executed, a different event (such as **4722**, **4724**, **4726**, **4737**, and **4738**) is recorded.	

Ejemplo – AT (I)



3.2.8. AT Command

Basic Information

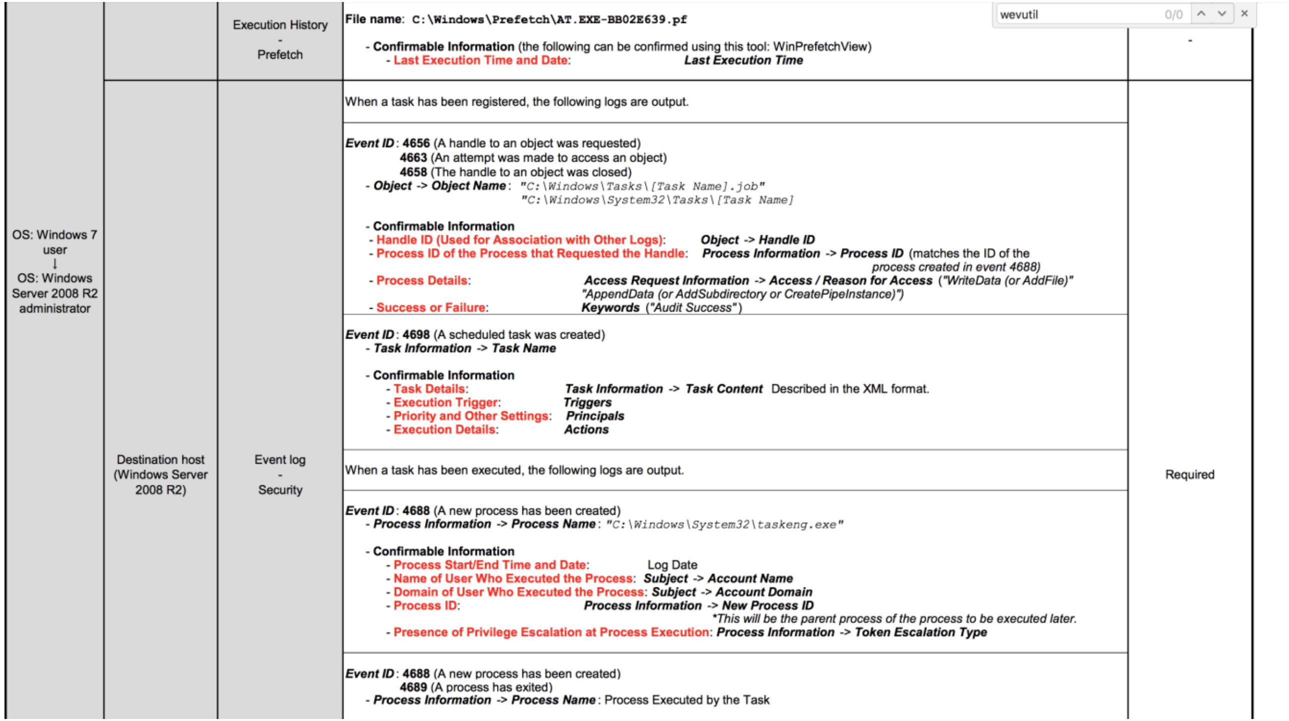
Tool	Tool Name	AT
	Category	Command Execution
	Tool Overview	Executes a task at the specified time
	Example of Presumed Tool Use During an Attack	The tool may be used to secretly place an application or script without being recognized by the user in advance and then execute it at the desired time. - Source host: at command execution source - Destination host: The machine for which a task was registered by the AT command
Operating Condition	Authority	Administrator *Setting a task on the remote host can be performed by a standard user.
	Targeted OS	Windows 7 / Server 2008 The AT command was abolished in Windows 8 and later and Server 2012 and later.
	Domain	Not required
	Communication Protocol	445/tcp
	Service	Task Scheduler
Information Acquired from Log	Standard Settings	- Source host: Execution history (Prefetch) - Destination host: Task creation / execution history in the task scheduler event log
	Additional Settings	- Execution history (Sysmon / audit policy)
Evidence That Can Be Confirmed When Execution is Successful		- Source host: If the following log is in the event log, it is considered that a task was registered. - The Event ID **4689** (A process has exited) of at.exe was recorded in the event log "Security" with the execution result (return value) of "0x0". - Destination host: If the following log is in the event log, it is considered that a task was executed. - The Event ID **106** (A task has been registered) was recorded in the event log "\Microsoft\Windows\TaskScheduler\Operational". - The Event IDs **200** (The operation that has been started) and **201** (The operation has been completed) are registered in the event log "\Microsoft\Windows\TaskScheduler\Operational", and the return value of the Event ID **201** is set to success.

Legend
- Acquirable Information
- **Event ID/Item Name**
- ***Field Name***
- *"Field Value"*

Points to be Confirmed

Communication	Log Generation Location	Log Type and Name	Acquired Information Details	Additional Settings
	Source host (Windows 7)	Event Log - Security	***Event ID***: **4688** (A new process has been created) **4689** (A process has exited) - ***Process Information*** -> ***Process Name***: *"C:\Windows\System32\at.exe"* - **Confirmable Information** - **Process Start/End Time and Date**: Log Date - **Name of User Who Executed the Process**: ***Subject*** -> ***Account Name*** - **Domain of User Who Executed the Process**: ***Subject*** -> ***Account Domain*** - **Presence of Privilege Escalation at Process Execution**: ***Process Information*** -> ***Token Escalation Type*** - **Process Return Value**: ***Process Information*** -> ***Exit Status***	Required
		Event Log	***Event ID***: **1** (Process Create) **5** (Process Terminated) - ***Image***: *"C:\Windows\System32\at.exe"*	

Ejemplo – AT (II)



OS: Windows 7 user ↓ OS: Windows Server 2008 R2 administrator		Execution History - Prefetch	File name: `C:\Windows\Prefetch\AT.EXE-BB02E639.pf` - **Confirmable Information** (the following can be confirmed using this tool: WinPrefetchView) - Last Execution Time and Date: ***Last Execution Time***	-
	Destination host (Windows Server 2008 R2)	Event log - Security	When a task has been registered, the following logs are output.	Required
			Event ID: **4656** (A handle to an object was requested) **4663** (An attempt was made to access an object) **4658** (The handle to an object was closed) - ***Object -> Object Name***: *"C:\Windows\Tasks\[Task Name].job"* *"C:\Windows\System32\Tasks\[Task Name]* - **Confirmable Information** - Handle ID (Used for Association with Other Logs): ***Object -> Handle ID*** - Process ID of the Process that Requested the Handle: ***Process Information -> Process ID*** (matches the ID of the *process created in event 4688)* - Process Details: ***Access Request Information -> Access / Reason for Access*** *("WriteData (or AddFile)" "AppendData (or AddSubdirectory or CreatePipeInstance)")* - Success or Failure: ***Keywords*** *("Audit Success")*	
			Event ID: **4698** (A scheduled task was created) - ***Task Information -> Task Name*** - **Confirmable Information** - Task Details: ***Task Information -> Task Content*** Described in the XML format. - Execution Trigger: ***Triggers*** - Priority and Other Settings: ***Principals*** - Execution Details: ***Actions***	
			When a task has been executed, the following logs are output.	
			Event ID: **4688** (A new process has been created) - ***Process Information -> Process Name***: *"C:\Windows\System32\taskeng.exe"* - **Confirmable Information** - Process Start/End Time and Date: Log Date - Name of User Who Executed the Process: ***Subject -> Account Name*** - Domain of User Who Executed the Process: ***Subject -> Account Domain*** - Process ID: ***Process Information -> New Process ID*** **This will be the parent process of the process to be executed later.* - Presence of Privilege Escalation at Process Execution: ***Process Information -> Token Escalation Type***	
			Event ID: **4688** (A new process has been created) **4689** (A process has exited) - ***Process Information -> Process Name***: Process Executed by the Task	

Threat Hunting

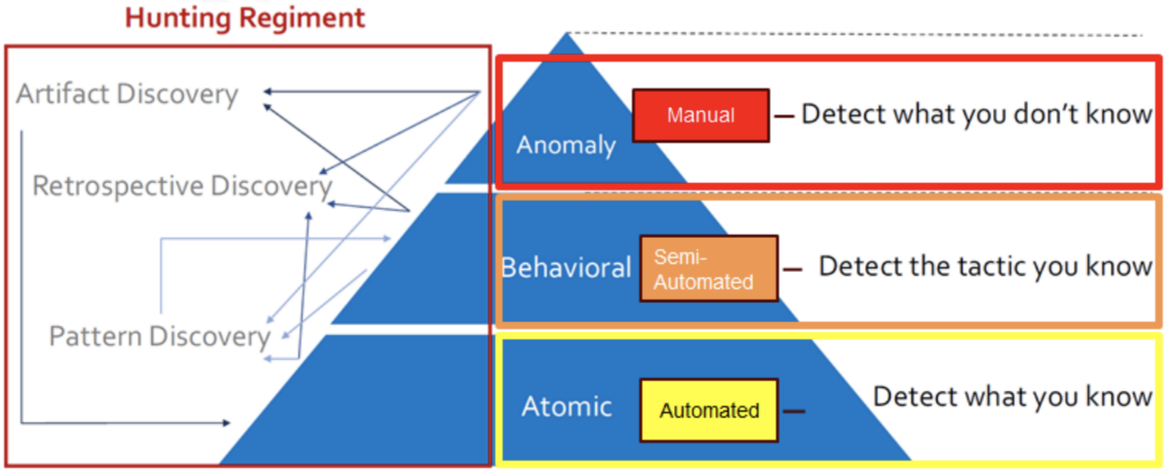


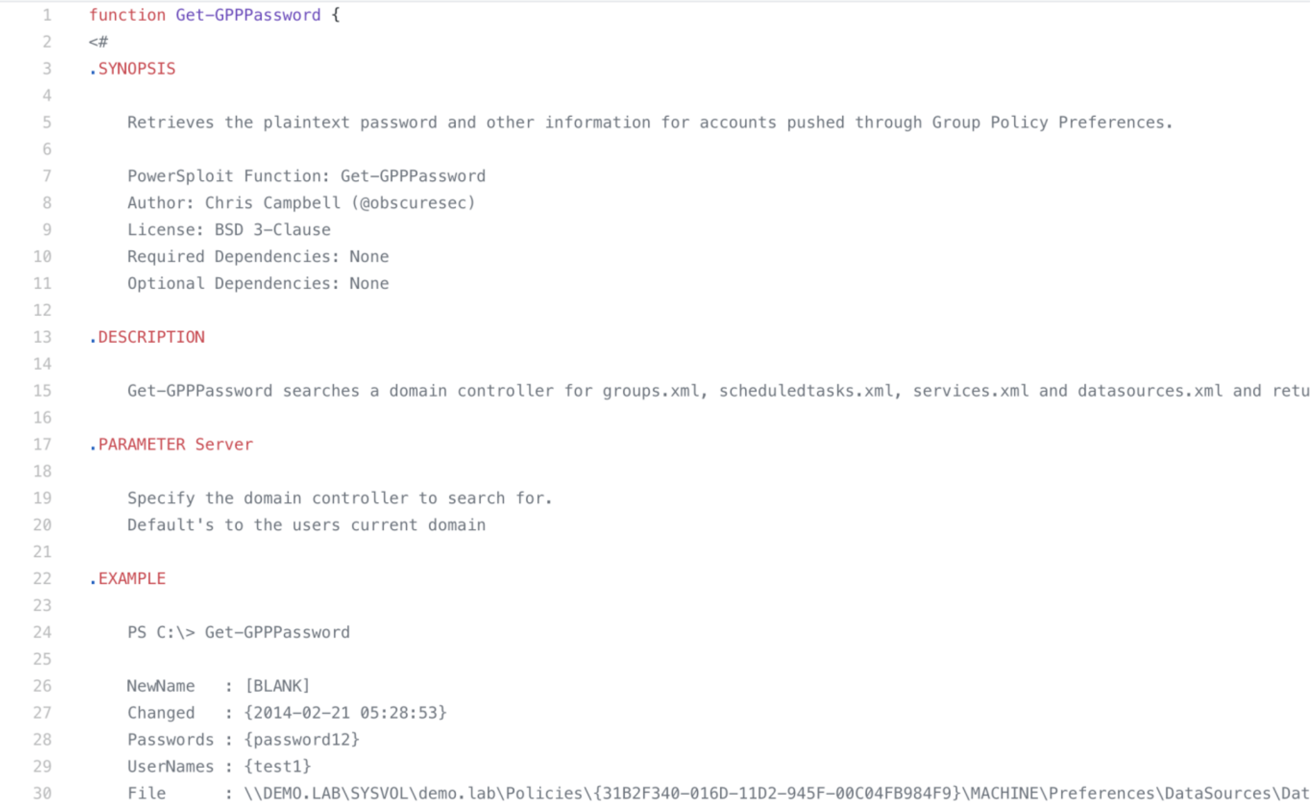
Figure 3. The Hunting Regiment in Relation to The Organization's Detection Strategy (Merritt & Concannon, 2017).

https://www.giac.org/paper/gcih/20661/offensive-intrusion-analysis-uncovering-insiders-threat-hunting-active-defense/128770

Mi hipótesis

“Atacantes internos utilizan Directorio Activo para obtener credenciales”

Mi hipótesis



```
function Get-GPPPassword {
<#
.SYNOPSIS

    Retrieves the plaintext password and other information for accounts pushed through Group Policy Preferences.

    PowerSploit Function: Get-GPPPassword
    Author: Chris Campbell (@obscuresec)
    License: BSD 3-Clause
    Required Dependencies: None
    Optional Dependencies: None

.DESCRIPTION

    Get-GPPPassword searches a domain controller for groups.xml, scheduledtasks.xml, services.xml and datasources.xml and retu

.PARAMETER Server

    Specify the domain controller to search for.
    Default's to the users current domain

.EXAMPLE

    PS C:\> Get-GPPPassword

    NewName   : [BLANK]
    Changed   : {2014-02-21 05:28:53}
    Passwords : {password12}
    UserNames : {test1}
    File      : \\DEMO.LAB\SYSVOL\demo.lab\Policies\{31B2F340-016D-11D2-945F-00C04FB984F9}\MACHINE\Preferences\DataSources\Dat
```

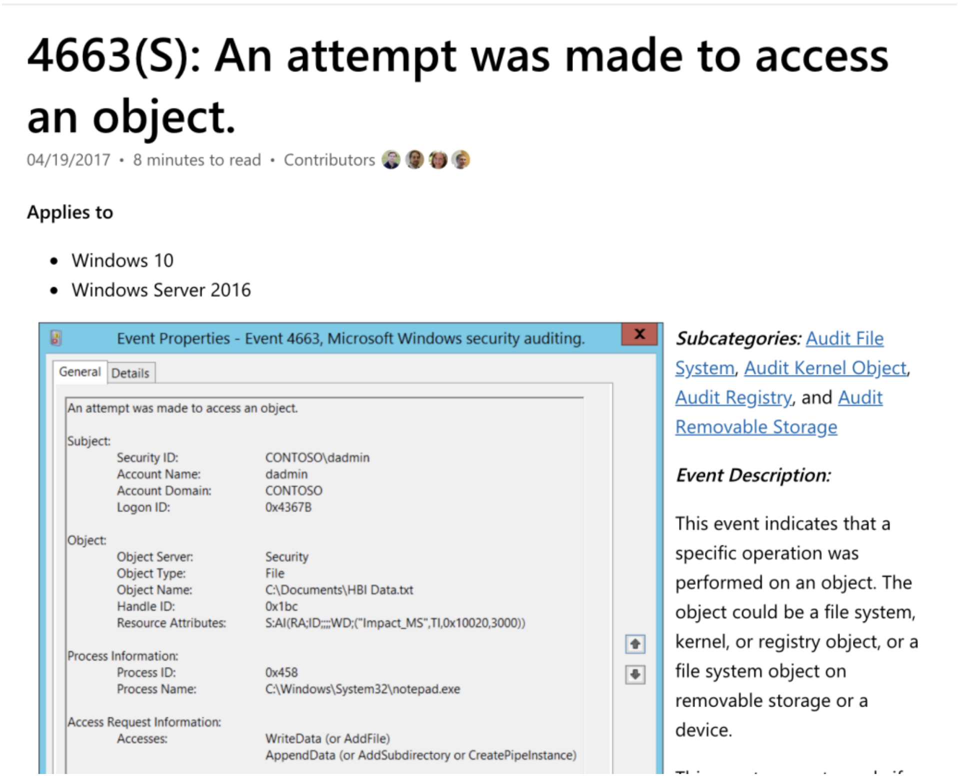
Tengo una hipótesis, ¿y ahora qué?

1. Intento detectarlo con los logs
2. Creo escenarios sintéticos para ver si es cierto.
3. Utilizo equipos de Red Team o simulaciones de adversarios con esa hipótesis.

Detectarlo con logs

1. Creo una GPO con una tarea periódica que se autentica con usuario y contraseña.
2. Añado auditoria de objeto sobre el fichero services.xml de esa GPO en SYSVOL
3. Detecto evento 4663

Detectarlo con logs



4663(S): An attempt was made to access an object.

04/19/2017 • 8 minutes to read • Contributors

Applies to

- Windows 10
- Windows Server 2016

Event Properties - Event 4663, Microsoft Windows security auditing.

```
An attempt was made to access an object.

Subject:
        Security ID:            CONTOSO\dadmin
        Account Name:           dadmin
        Account Domain:         CONTOSO
        Logon ID:               0x4367B

Object:
        Object Server:          Security
        Object Type:            File
        Object Name:            C:\Documents\HBI Data.txt
        Handle ID:              0x1bc
        Resource Attributes:    S:AI(RA;ID;;;;WD;("Impact_MS",TI,0x10020,3000))

Process Information:
        Process ID:             0x458
        Process Name:           C:\Windows\System32\notepad.exe

Access Request Information:
        Accesses:               WriteData (or AddFile)
                                AppendData (or AddSubdirectory or CreatePipeInstance)
```

Subcategories: Audit File System, Audit Kernel Object, Audit Registry, and Audit Removable Storage

Event Description:

This event indicates that a specific operation was performed on an object. The object could be a file system, kernel, or registry object, or a file system object on removable storage or a device.

Crear escenarios sintéticos

1. En la tarea periódica añado un powershell que hace backup de una base de datos con sus credenciales.
2. Monitorizo accesos a la base de datos.

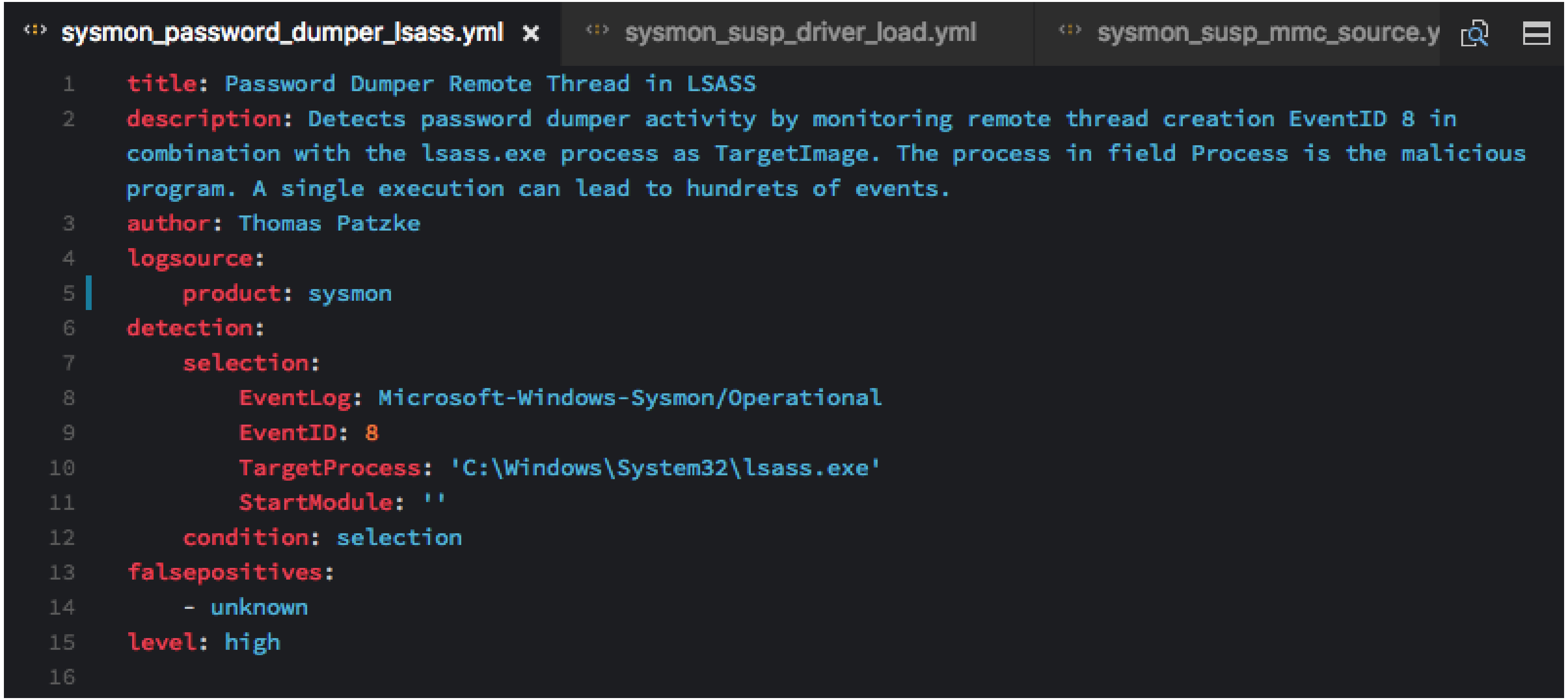
Sigma: una herramienta de la comunidad.

Sigma

Generic Signature Format for SIEM Systems

Sigma is for log files what Snort is for network traffic and YARA is for files.

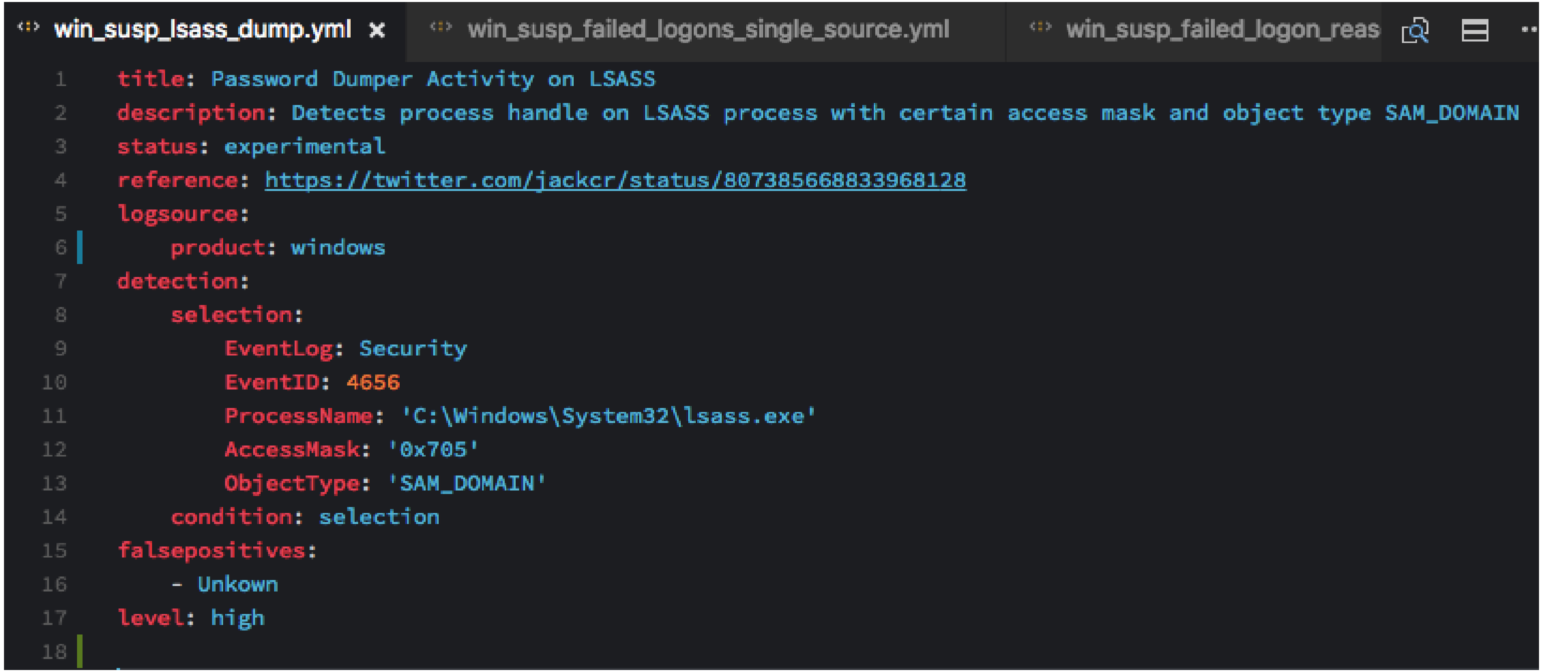
Ejemplo : LSASS access


sysmon_password_dumper_lsass.yml ×
sysmon_susp_driver_load.yml
sysmon_susp_mmc_source.y

```yaml
title: Password Dumper Remote Thread in LSASS
description: Detects password dumper activity by monitoring remote thread creation EventID 8 in combination with the lsass.exe process as TargetImage. The process in field Process is the malicious program. A single execution can lead to hundrets of events.
author: Thomas Patzke
logsource:
    product: sysmon
detection:
    selection:
        EventLog: Microsoft-Windows-Sysmon/Operational
        EventID: 8
        TargetProcess: 'C:\Windows\System32\lsass.exe'
        StartModule: ''
    condition: selection
falsepositives:
    - unknown
level: high

```

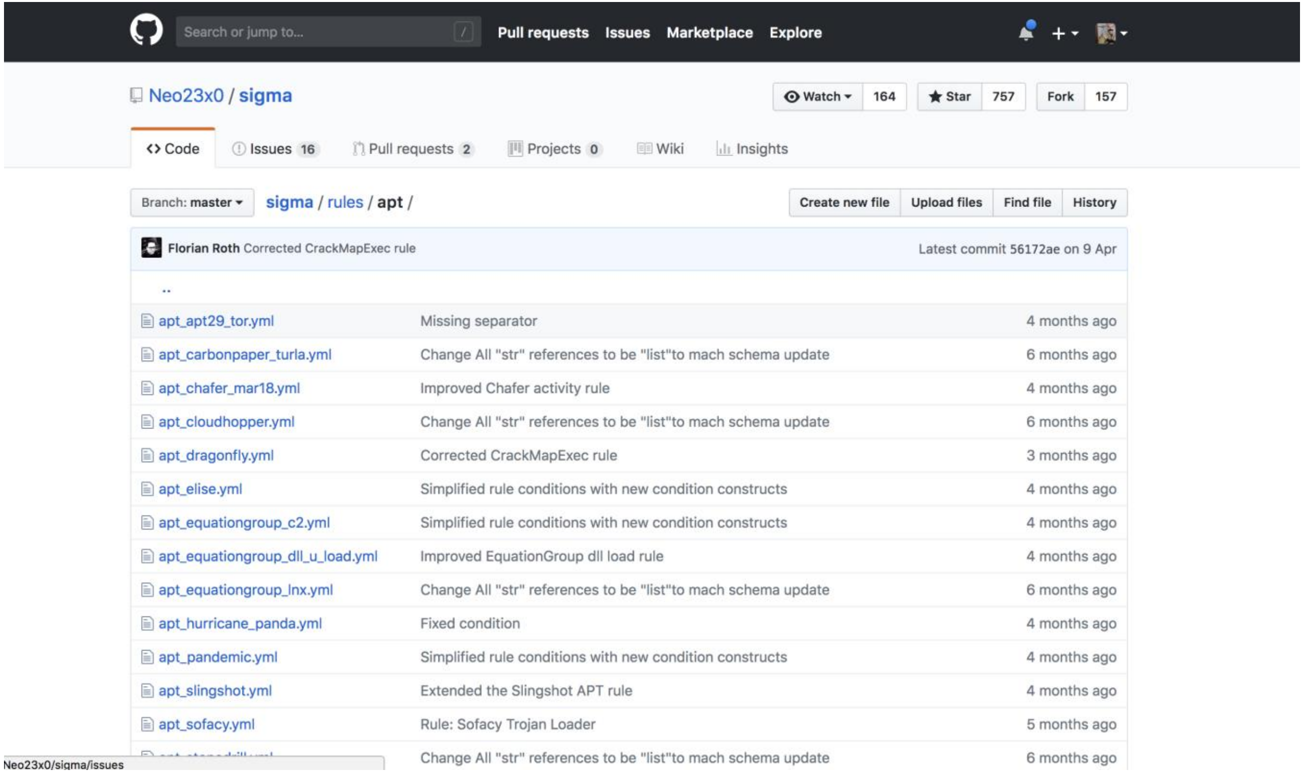
Ejemplo: CreateRemoteThread


win_susp_lsass_dump.yml ×
win_susp_failed_logons_single_source.yml
win_susp_failed_logon_reas

```yaml
title: Password Dumper Activity on LSASS
description: Detects process handle on LSASS process with certain access mask and object type SAM_DOMAIN
status: experimental
reference: https://twitter.com/jackcr/status/807385668833968128
logsource:
    product: windows
detection:
    selection:
        EventLog: Security
        EventID: 4656
        ProcessName: 'C:\Windows\System32\lsass.exe'
        AccessMask: '0x705'
        ObjectType: 'SAM_DOMAIN'
    condition: selection
falsepositives:
    - Unkown
level: high

```

TTPs sources



Neo23x0 / sigma

sigma / rules / apt /

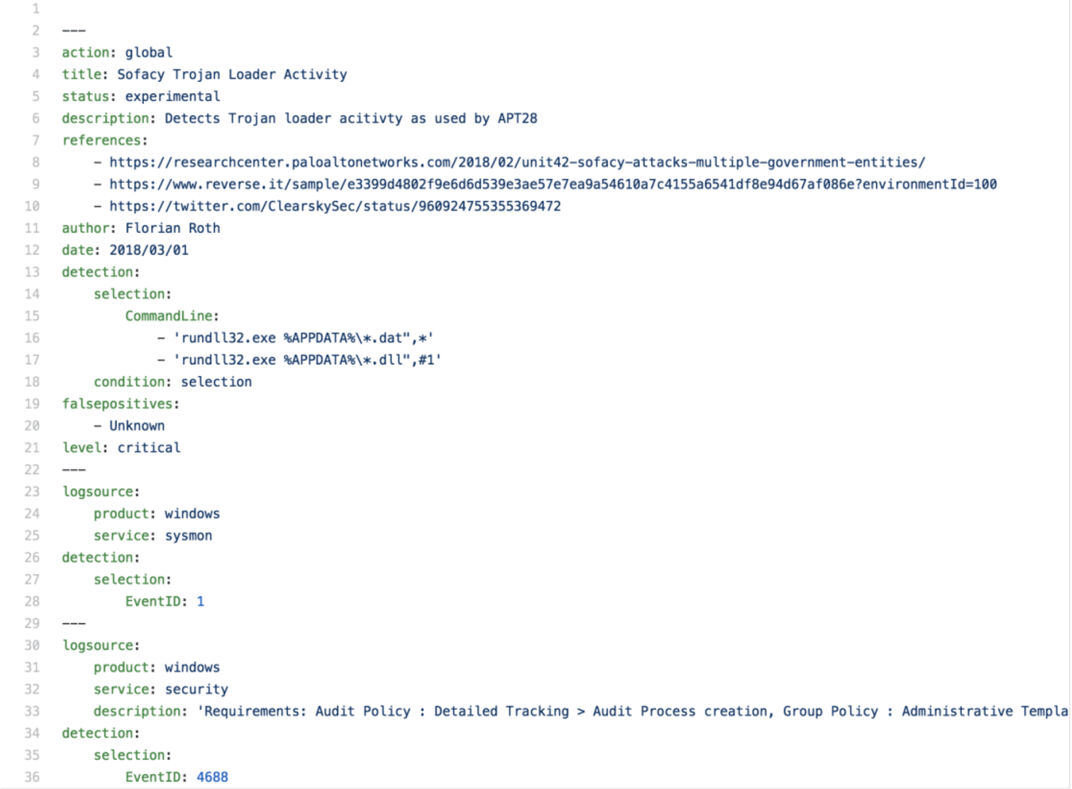
Florian Roth Corrected CrackMapExec rule — Latest commit 56172ae on 9 Apr

..		
apt_apt29_tor.yml	Missing separator	4 months ago
apt_carbonpaper_turla.yml	Change All "str" references to be "list"to mach schema update	6 months ago
apt_chafer_mar18.yml	Improved Chafer activity rule	4 months ago
apt_cloudhopper.yml	Change All "str" references to be "list"to mach schema update	6 months ago
apt_dragonfly.yml	Corrected CrackMapExec rule	3 months ago
apt_elise.yml	Simplified rule conditions with new condition constructs	4 months ago
apt_equationgroup_c2.yml	Simplified rule conditions with new condition constructs	4 months ago
apt_equationgroup_dll_u_load.yml	Improved EquationGroup dll load rule	4 months ago
apt_equationgroup_lnx.yml	Change All "str" references to be "list"to mach schema update	6 months ago
apt_hurricane_panda.yml	Fixed condition	4 months ago
apt_pandemic.yml	Simplified rule conditions with new condition constructs	4 months ago
apt_slingshot.yml	Extended the Slingshot APT rule	4 months ago
apt_sofacy.yml	Rule: Sofacy Trojan Loader	5 months ago
apt_stonedrill.yml	Change All "str" references to be "list"to mach schema update	6 months ago

Neo23x0/sigma/issues

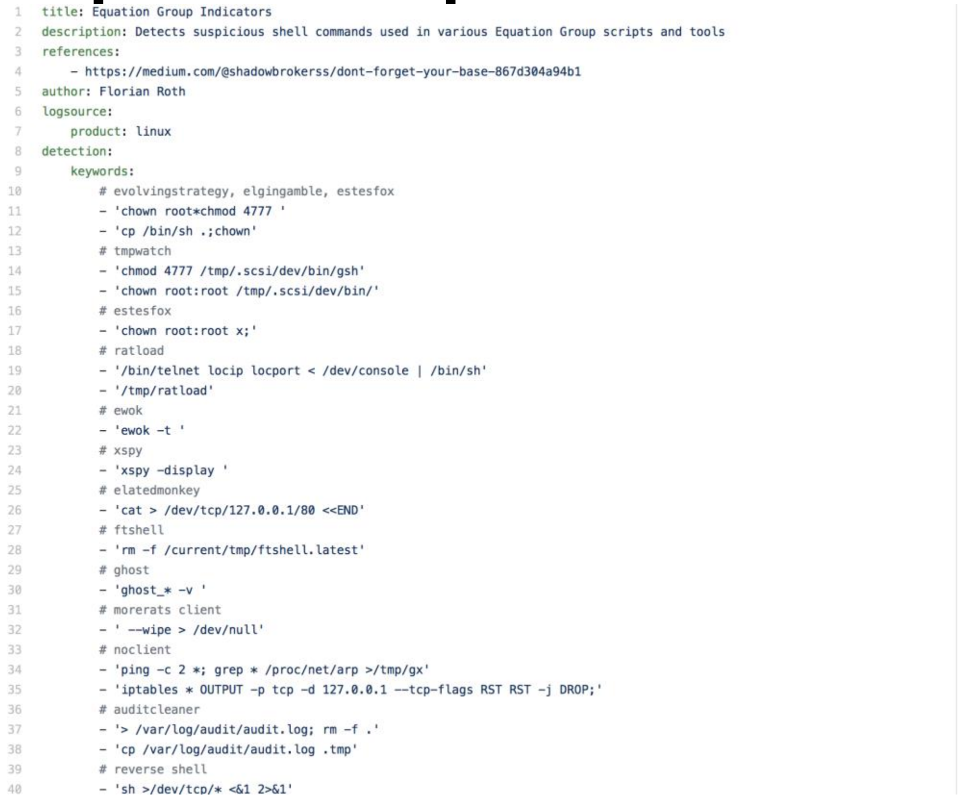
https://github.com/Neo23x0/sigma/tree/master/rules

Ejemplo - Sofacy



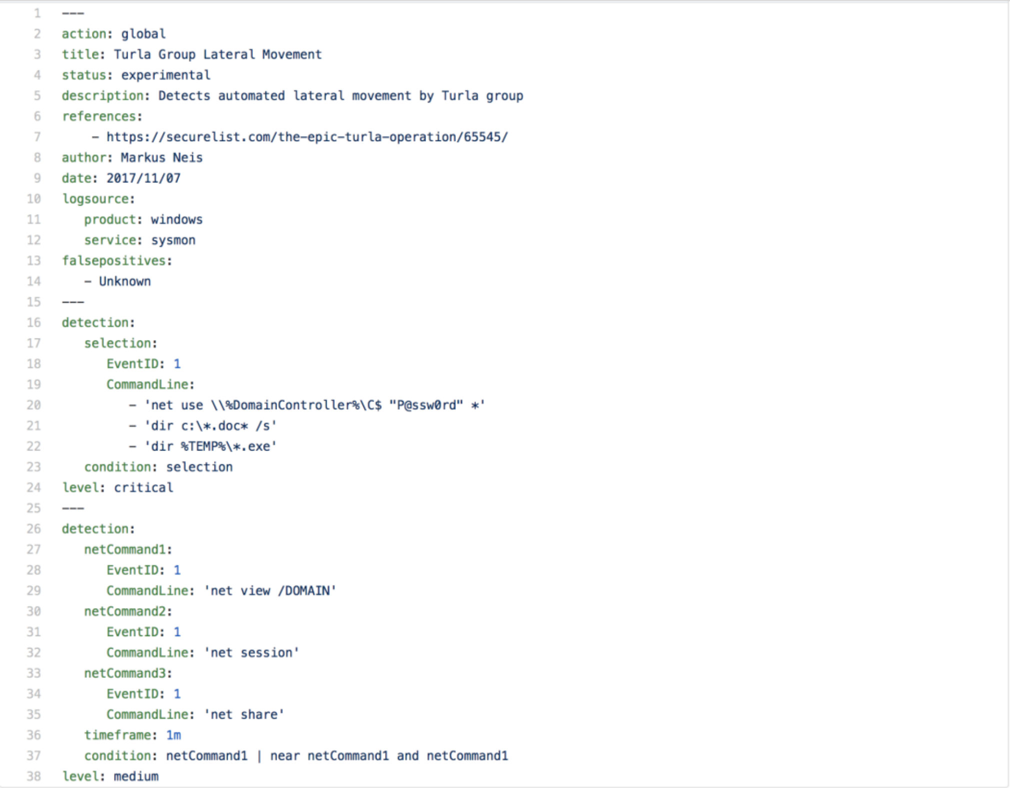
```
---
action: global
title: Sofacy Trojan Loader Activity
status: experimental
description: Detects Trojan loader acitivty as used by APT28
references:
    - https://researchcenter.paloaltonetworks.com/2018/02/unit42-sofacy-attacks-multiple-government-entities/
    - https://www.reverse.it/sample/e3399d4802f9e6d6d539e3ae57e7ea9a54610a7c4155a6541df8e94d67af086e?environmentId=100
    - https://twitter.com/ClearskySec/status/960924755355369472
author: Florian Roth
date: 2018/03/01
detection:
    selection:
        CommandLine:
            - 'rundll32.exe %APPDATA%\*.dat",*'
            - 'rundll32.exe %APPDATA%\*.dll",#1'
    condition: selection
falsepositives:
    - Unknown
level: critical
---
logsource:
    product: windows
    service: sysmon
detection:
    selection:
        EventID: 1
---
logsource:
    product: windows
    service: security
    description: 'Requirements: Audit Policy : Detailed Tracking > Audit Process creation, Group Policy : Administrative Templa
detection:
    selection:
        EventID: 4688
```

Ejemplo – Equation Group



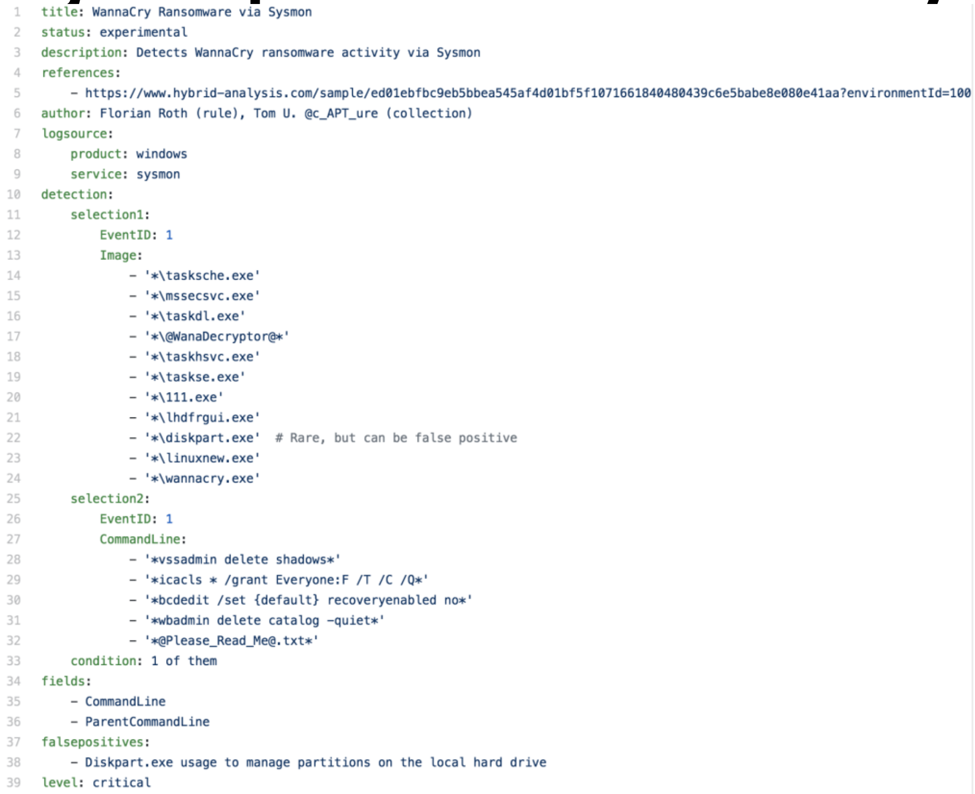
```
title: Equation Group Indicators
description: Detects suspicious shell commands used in various Equation Group scripts and tools
references:
    - https://medium.com/@shadowbrokerss/dont-forget-your-base-867d304a94b1
author: Florian Roth
logsource:
    product: linux
detection:
    keywords:
        # evolvingstrategy, elgingamble, estesfox
        - 'chown root*chmod 4777 '
        - 'cp /bin/sh .;chown'
        # tmpwatch
        - 'chmod 4777 /tmp/.scsi/dev/bin/gsh'
        - 'chown root:root /tmp/.scsi/dev/bin/'
        # estesfox
        - 'chown root:root x;'
        # ratload
        - '/bin/telnet locip locport < /dev/console | /bin/sh'
        - '/tmp/ratload'
        # ewok
        - 'ewok -t '
        # xspy
        - 'xspy -display '
        # elatedmonkey
        - 'cat > /dev/tcp/127.0.0.1/80 <<END'
        # ftshell
        - 'rm -f /current/tmp/ftshell.latest'
        # ghost
        - 'ghost_* -v '
        # morerats client
        - ' --wipe > /dev/null'
        # noclient
        - 'ping -c 2 *; grep * /proc/net/arp >/tmp/gx'
        - 'iptables * OUTPUT -p tcp -d 127.0.0.1 --tcp-flags RST RST -j DROP;'
        # auditcleaner
        - '> /var/log/audit/audit.log; rm -f .'
        - 'cp /var/log/audit/audit.log .tmp'
        # reverse shell
        - 'sh >/dev/tcp/* <&1 2>&1'
```

Ejemplo - Turla



```
---
action: global
title: Turla Group Lateral Movement
status: experimental
description: Detects automated lateral movement by Turla group
references:
    - https://securelist.com/the-epic-turla-operation/65545/
author: Markus Neis
date: 2017/11/07
logsource:
   product: windows
   service: sysmon
falsepositives:
   - Unknown
---
detection:
   selection:
      EventID: 1
      CommandLine:
         - 'net use \\%DomainController%\C$ "P@ssw0rd" *'
         - 'dir c:\*.doc* /s'
         - 'dir %TEMP%\*.exe'
   condition: selection
level: critical
---
detection:
   netCommand1:
      EventID: 1
      CommandLine: 'net view /DOMAIN'
   netCommand2:
      EventID: 1
      CommandLine: 'net session'
   netCommand3:
      EventID: 1
      CommandLine: 'net share'
   timeframe: 1m
   condition: netCommand1 | near netCommand1 and netCommand1
level: medium
```

Ejemplo - Wannacry



```
title: WannaCry Ransomware via Sysmon
status: experimental
description: Detects WannaCry ransomware activity via Sysmon
references:
    - https://www.hybrid-analysis.com/sample/ed01ebfbc9eb5bbea545af4d01bf5f1071661840480439c6e5babe8e080e41aa?environmentId=100
author: Florian Roth (rule), Tom U. @c_APT_ure (collection)
logsource:
    product: windows
    service: sysmon
detection:
    selection1:
        EventID: 1
        Image:
            - '*\tasksche.exe'
            - '*\mssecsvc.exe'
            - '*\taskdl.exe'
            - '*\@WanaDecryptor@*'
            - '*\taskhsvc.exe'
            - '*\taskse.exe'
            - '*\111.exe'
            - '*\lhdfrgui.exe'
            - '*\diskpart.exe'  # Rare, but can be false positive
            - '*\linuxnew.exe'
            - '*\wannacry.exe'
    selection2:
        EventID: 1
        CommandLine:
            - '*vssadmin delete shadows*'
            - '*icacls * /grant Everyone:F /T /C /Q*'
            - '*bcdedit /set {default} recoveryenabled no*'
            - '*wbadmin delete catalog -quiet*'
            - '*@Please_Read_Me@.txt*'
    condition: 1 of them
fields:
    - CommandLine
    - ParentCommandLine
falsepositives:
    - Diskpart.exe usage to manage partitions on the local hard drive
level: critical
```

En resúmen

- No tengas el sindrome de ciber-Diógenes.
- Haz foco en tus adversaries reales.
- Intenta usar y crear tus propios TTPs.
- Logs, logs, logs.
- Ciclo de Threat Hunting:
  - Crea tu hipótesis
  - Comprueba su validez
  - Automatiza y a por la siguiente

XII Jornadas STIC CCN-CERT

Ciberseguridad, hacia una respuesta y disuasión efectivas

- **E-Mails**
  - info@ccn-cert.cni.es
  - ccn@cni.es
  - organismo.certificacion@cni.es

  Websites
  - www.ccn.cni.es
  - www.ccn-cert.cni.es
  - oc.ccn.cni.es
- **Síguenos en**

ccn-cert
centro criptológico nacional