Alpha & Omega Wellness Center

Cyber Incident Threat Response Intelligence Report

Prepared for Alpha & Omega Wellness Center

By

Anthony Sullivan

8/18/2018

FOR OFFICIAL USE ONLY

This page intentionally left blank

Properties

Size	66.7MB
Pages	98
Words	16407
Total Editing Time	3820 Minutes
Title	Cyber Threat Intelligence and In.
Tags	Add a tag
Comments	Add comments

Related Dates

Last Modified	Today, 9:19 AM
Created	8/15/2018 7:56 PM
Last Printed	Today, 9:19 AM

Related People

Author	Anthony Sullivan
	Add an author
Last Modified By	HP

Alpha & Omega Wellness Center

Cyber Incident Threat Response Intelligence Report

Executive Summary

"Electronic Vandalism" attacks are rippling across the world crippling companies, encrypting files and causing major business interruptions. Cyber Actors wait till late on Friday afternoons to launch major crypto worm attacks. On Friday the 8th of June 2018, Alpha & Omega Wellness Center, was a victim of "Electronic Vandalism".

The new improved variant of the "WannaCry" crypto worm named "WorldCry" exploited a vulnerable Windows 2008 R2 server which was not patched with MS17-010. The WorldCry@cock.li crypto worm, executed on the 9th of June 2018 at 8:56 am rendering information processing systems unusable, causing a major business interruption. Entry point is believed to be via port zero, MikroTik VoIP router, which was not patched for the "SLINGSHOT" vulnerability, utilizing BUSYBOX and Apple Script to laterally traverse the network to the file server. The 2008 R2 server was not patched to protect against the "EternalBlue" attack tool, all files were encrypted. Previous IT support contractor attempted to "Decrypt" file structure to no avail. The "Mirrored HDD" was reformatted and counterfeit Windows Server 2008 R2 installed, because he did not have the original media, in another failed attempt to "Decrypt" and "Repair" with unsupported software. After 48 days of no progress or success in restoring systems to an operational capability, Karen Ruja then called Monica Velasquez of AR Billing Company, Wednesday July 25th, and asked for help. On Thursday July 26th, AR Billing Company executed a "Business Associate Agreement", for forensic analysis, data analysis, data retrieval and recreation, post ransomware attack. AR Billing Company then executed a "Cyber Incident Response Plan" in accordance with HIPPA/HITECH Act requirements. HDD evidence preserved, logs captured, forensic analysis completed, FBI notified. Data sets recovered, repaired and recreated, workstation and server operating systems recovered, repaired and recreated. Security Technical Implementation Guides desktop/server lockdowns implemented, Fortiguard Security Solution deployed, FortiClient workstation compliance, telemetry and Veriato 360 monitoring software deployed. AOWC's file server was rebuilt over the weekend, program specific datasets recovered and restored, user specific datasets recovered and restored. Workstations repaired, recovered and restored the following week, full mission capability achieved within 10 days.

Alpha & Omega Wellness Center

Cyber Incident Threat Response Intelligence Report

Table of Contents

The list of "WorldCry" victims is long and includes notorious names across all sectors. It soon became clear that the victims of this new "WannaCry: variant were much larger than usual. According to the last estimates, the ransomware infected more than 350,000 systems in more than one hundred countries. The new variant WorldCry, infected 10,000 machines at Taiwan Semiconductor Manufacturing Company (chip manufacture for the Apple iPhone) forcing a shutdown of its advanced chip-fabrication factories on August 6th, 2018. The company's CEO C.C. Wei said an "operational error" occurred when a new fab tool was not taken offline during installation and the virus quickly spread to over 10,000 machines in its factories across Taiwan. "This is the first time it happened. I was shocked and surprised," he told reporters in Taipei, adding that the company had enhanced its information security systems and protective measures. "It's impossible that humans would never make mistakes and we have changed the system to automatically detect (virus) and such a mistake would never be made again."

The Shadow Brokers (TSB) is a hacker group who first appeared in the summer of 2016. They published several leaks containing hacking tools from the National Security Agency (NSA), including several zero-day exploits. Specifically, these exploits and vulnerabilities targeted enterprise firewalls, routers, antivirus software, and Microsoft products.

The Shadow Brokers attribute the leaks to the Equation Group cyber threat actor, who have been tied to the NSA's Tailored Access Operations unit. EternalBlue, sometimes stylized as ETERNALBLUE, is an exploit developed by the U.S. National Security Agency (NSA) according to testimony by former NSA employees. It was leaked by the Shadow Brokers hacker group on April 14, 2017, and was used as part of the worldwide WannaCry ransomware attack on May 12, 2017. The exploit was also used to help carry out the 2017 NotPetya cyberattack on June 27, 2017 and reported to be used as part of the Retefe banking trojan since at least September 5, 2017. While Microsoft had released patches previously to close the exploit, much of WannaCry's spread was from organizations that had not applied these, or were using older Windows systems that were past their end-of-life. WannaCry also took advantage of installing backdoors onto infected systems.

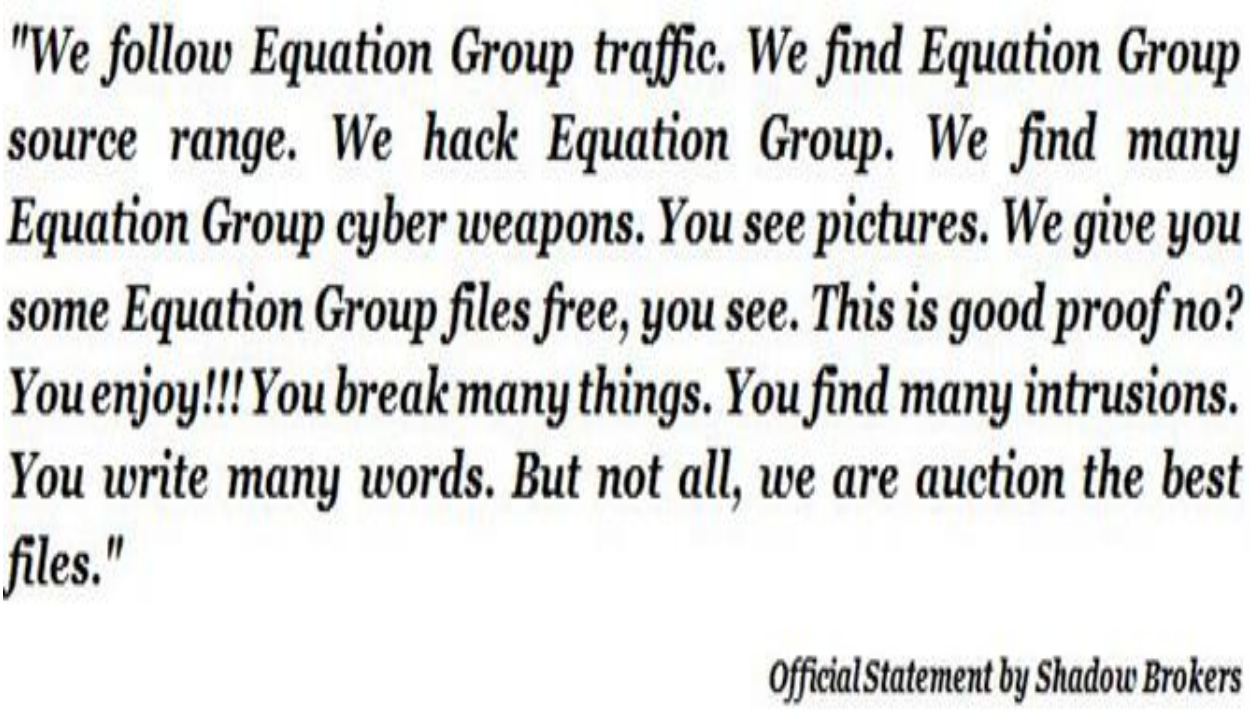
So who are the Equation Group and Shadow Brokers? Edward Snowden stated on Twitter on August 16, 2016 that "circumstantial evidence and conventional wisdom indicates Russian responsibility" and that the leak "is likely a warning that someone can prove US responsibility for any attacks that originated from this malware server" summarizing that it looks like "somebody sending a message that an escalation in the attribution game could get messy fast". Russians wanted to send a clear message that they can and will release exceptionally embarrassing information. The New York Times put the incident in the context of the Democratic National Committee cyber-attacks and hacking of the Podesta emails. As US intelligence agencies were contemplating counter-attacks, the Shadow Brokers code release was to be seen as a warning: "Retaliate for the D.N.C., and there are a lot more secrets, from the hackings of the State Department, the White House and the Pentagon, that might be spilled as well. One senior official compared it to the scene in The Godfather where the head of a favorite horse is left in a bed, as a warning."[44] Experts believed from preliminary evaluation of the worm that the attack originated from North Korea or agencies working for the country. In December 2017, the United States, United Kingdom and Australia formally asserted that North Korea was responsible for the attack. A number of experts highlighted the NSA's non-disclosure of the underlying vulnerability, and their loss of control over the EternalBlue attack tool that exploited it. Edward Snowden said that if the NSA had "privately disclosed the flaw used to attack hospitals when they found it, not when they lost it, the attack may not have happened".[155]

British cybersecurity expert Graham Cluley also sees "some culpability on the part of the U.S. intelligence services". According to Cluley and others, "they could have done something ages ago to get this problem fixed, and they didn't do it". He also said that despite obvious uses for such tools to spy on people of interest, they have a duty to protect their countries' citizens.[156] Others have also commented that this attack shows that the practice of intelligence agencies to stockpile exploits for offensive purposes rather than disclosing them for defensive purposes may be problematic.[108] Microsoft president and chief legal officer Brad Smith wrote, "Repeatedly, exploits in the hands

of governments have leaked into the public domain and caused widespread damage. An equivalent scenario with conventional weapons would be the U.S. military having some of its Tomahawk missiles stolen."[157][158][159]

Russian President Vladimir Putin placed the responsibility of the attack on U.S. intelligence services, for having created EternalBlue.[144] The attack was stopped within a few days of its discovery due to emergency patches released by Microsoft, and the discovery of a kill switch that prevented infected computers from spreading WannaCry further. The attack was estimated to have affected more than 200,000 computers across 150 countries, with total damages ranging from hundreds of millions to billions of dollars.

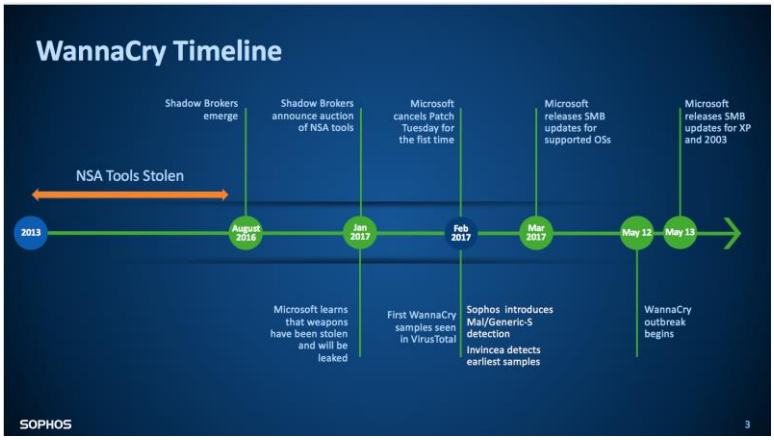
On 17 May 2018, United States bipartisan lawmakers introduced the PATCH Act[160] that aims to have exploits reviewed by an independent board to "balance the need to disclose vulnerabilities with other national security interests while increasing transparency and accountability to maintain public trust in the process".[161]



The Adversary's Actions and Tactics

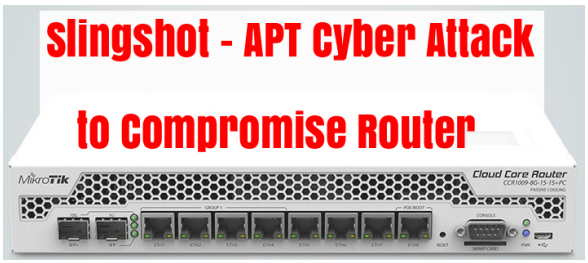
A new class of threats, appropriately dubbed the "Advanced Persistent Threat" (APT), represents well-resourced and trained adversaries that conduct multi-year intrusion campaigns targeting highly sensitive economic, proprietary, or national security information. These adversaries accomplish their goals using advanced tools and techniques designed to defeat most conventional computer network defense mechanisms. Network defense techniques which leverage knowledge about these adversaries can create an intelligence feedback loop, enabling defenders to establish a state of information superiority which decreases the adversary's likelihood of success with each subsequent intrusion attempt. Using a kill chain model to describe phases of intrusions, mapping adversary kill chain indicators to defender courses of action, identifying patterns that link individual intrusions into broader campaigns, and understanding the iterative nature of intelligence gathering from the basis of intelligence-driven computer network defense (CND). Institutionalization of this approach reduces the likelihood of adversary success, informs network defense investment and resource prioritization, and yields relevant metrics of performance and effectiveness. The evolution of advanced persistent threats necessitates an intelligence-based model because in this model the defenders mitigate not just vulnerability, but the threat component of risk, too.

The malware encrypts and adds the extension ".WCRY" to all files that match a list of 176 specific extensions including documents, database and backup files. The victim is requested to pay between USD 300 and 600 in Bitcoins to get its files back. There is no evidence that a payment will effectively provide the key for decrypting the files.

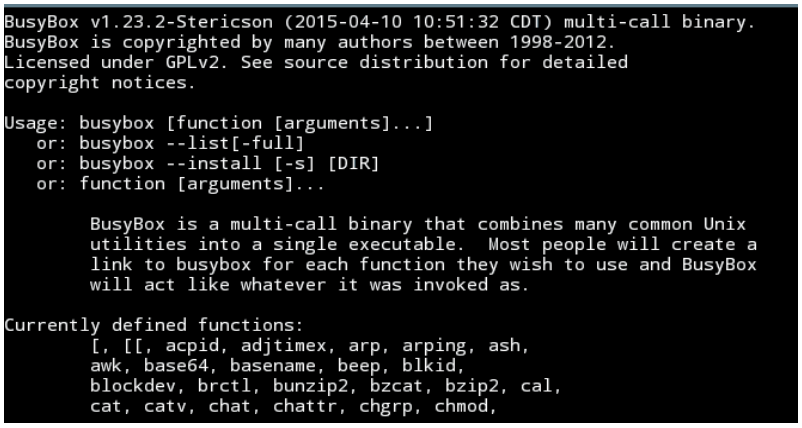


In their message, the authors threaten to delete the file forever if their request is not met within eight days. The international ambitions of this campaign are made clear by the fact that the ransom message is translated in 28 languages. Once the initial host has been infected, the ransomware dropper makes use of the MS17-010 vulnerability of the Server Message Block (SMB) protocol to spread laterally through the network. The exploit using this vulnerability has been made public by the group Shadow Broker on 14 April 2017 in a leak of hacking tools allegedly crafted by a state actor. The number of victims rose steeply, as there are 1000's directly connected to the Internet over a SMB protocol. Despite overwhelming information, some points still remain unclear. First, it is not yet known how the dropper is initially delivered to the

victims. US-CERT claimed that hackers gained access to the victims' network either through Remote Desktop Protocol or through the exploitation of the critical Windows SMB vulnerability mentioned above. Second, the identity of the authors is wrapped in mystery. The Alpha & Omega Wellness Center VoIP system was vulnerable to the SLINGSHOT attack, because of the MikroTik router.



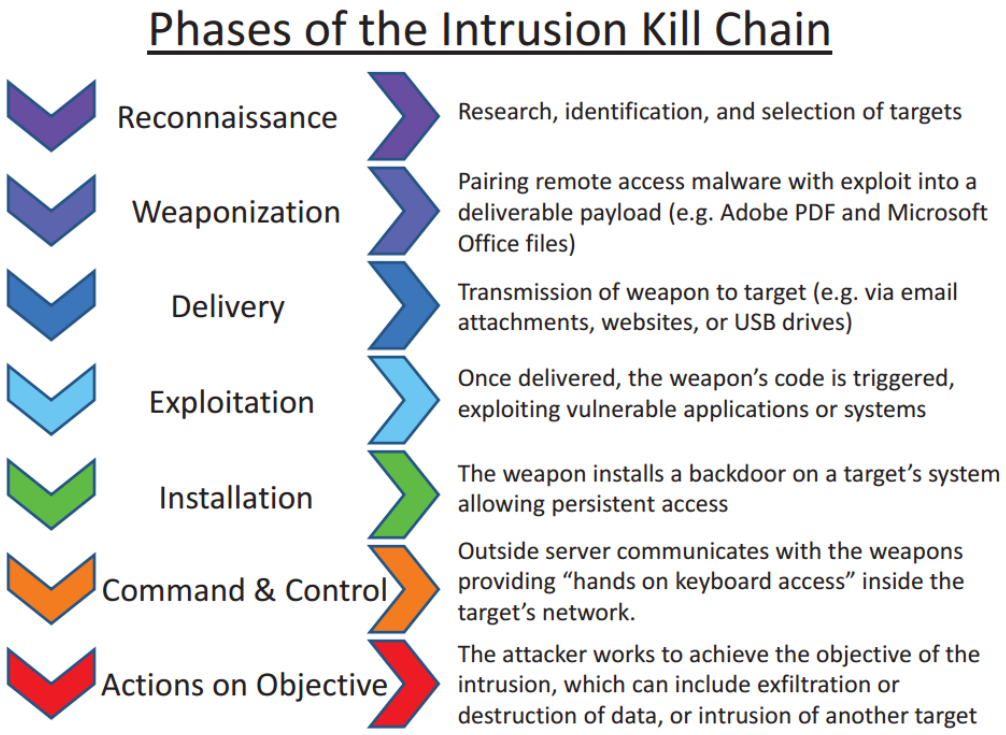
It is believed the attackers used port zero to send commands and drop the WorldCry payload via BUSYBOX and Apple Script directly on the file server. As previously mentioned, the exploit used in this attack was originally leaked in April of 2017 At that time, the vendor had already released a patch to correct the flaws. Unfortunately, many users ignored this threat and were not much eager to install the patch. This should serve as a reminder that threat actors will reuse leaked tools. As reported by the media, a young IT-security researcher temporarily stopped the attack by registering a "kill-switch" domain that told the ransomware to stop spreading itself. Unfortunately, new versions of the malware without this feature are active in the wild. Furthermore, the threat intelligence community generously shared a lot of indicators and advices helping organizations to identify prevent and dwarf the impact of infections.



The HIPAA/HITECH Security Rule requires implementation of security measures that can help prevent the introduction of malware, including ransomware. Additionally implementation of a security management process, which includes conducting a risk analysis to identify threats and vulnerabilities to electronic protected health information (ePHI) must be deployed. Along with the implementation of security measures to mitigate or remove identified risks with Kill Chain procedures to guard against and detect malicious software.

Intrusion Kill Chain

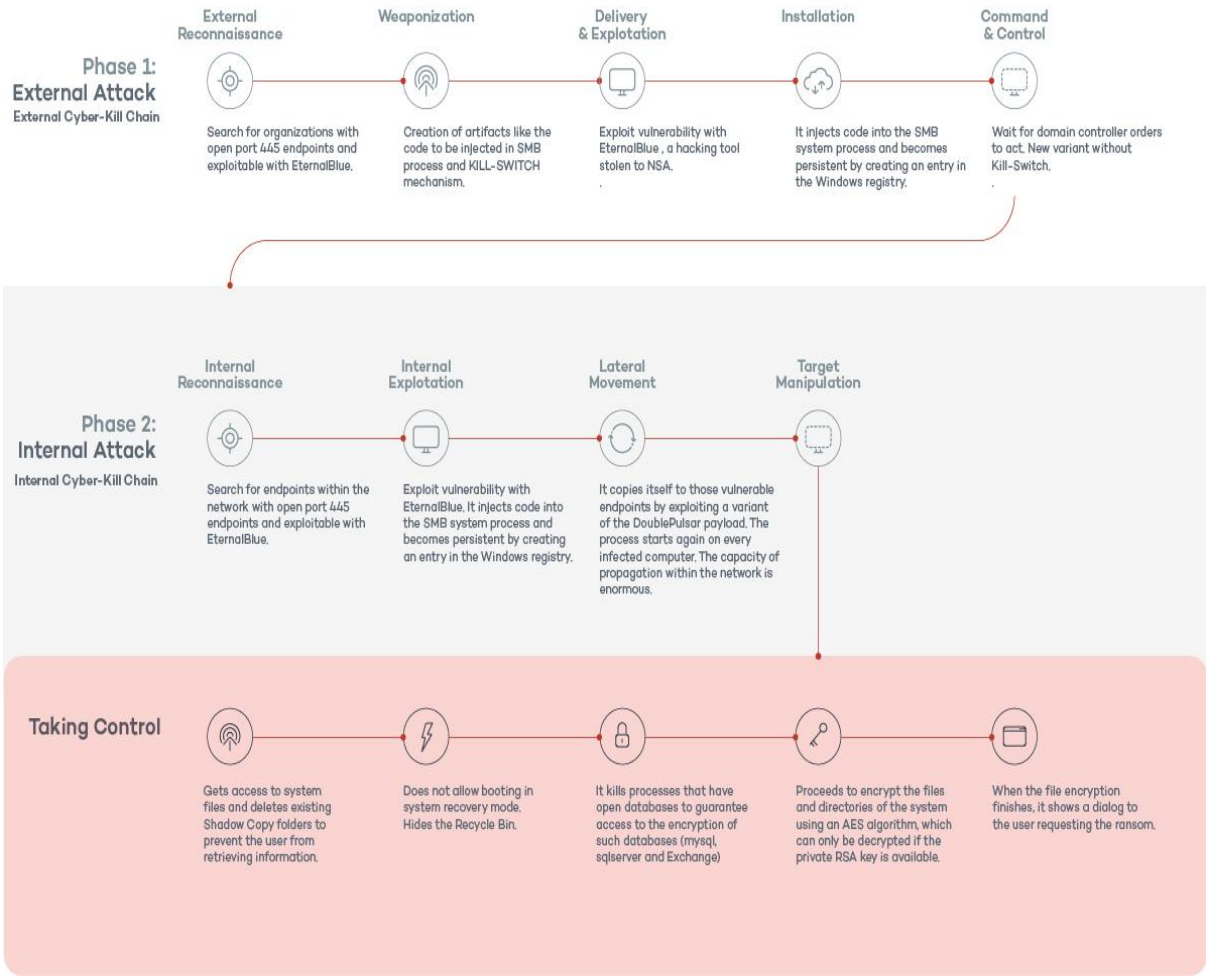
A kill chain is a systematic process to target and engage an adversary to create desired effects. U.S. military targeting doctrine defines the steps of this process as find, fix, track, target, engage, assess(F2T2EA): find adversary targets suitable for engagement; fix their location; track and observe; target with suitable weapon or asset to create desired effects; engage adversary; assess effects (U.S. Department of Defense, 2007). This is an integrated, end-to-end process described as a "chain" because any one deficiency will interrupt the entire process. Expanding on this concept, this paper presents a new kill chain model, one specifically for intrusions. The essence of an intrusion is that the aggressor must develop a payload to breach a trusted boundary, establish a presence inside a trusted environment, and from that presence, take actions towards their objectives, be they moving laterally inside the environment or violating the confidentiality, integrity, or availability of a system in the environment. The intrusion kill chain is defined as reconnaissance, weaponization, delivery, exploitation, installation, command and control (C2), and actions on objectives. With respect to computer network attack (CNA) or computer network espionage (CNE), the definitions for these kill chain phases are as follows:



Alpha & Omega Wellness Center

Cyber Incident Threat Response Intelligence Report

Anatomy of #WorldCry@Cock.Li



This graphic provides a description of the adversary's capabilities in terms of tactics, techniques and procedures (TTPs). Tools and tradecraft employed by the intrusion perpetrators, exploits backdoors, staging methods and situational awareness.

The Adversary's Infrastructure

It is impossible to exactly determine the infrastructure, such as IP addresses, domain names, program names, etc. used by the adversary. But we can look at affected systems and gain insight into just how extensive the adversary's infrastructure is. Once compromise, a network becomes part of the adversary's infrastructure. Industrial controls systems are exceptionally vulnerable and a major national security concern.

WannaCry Ransomware Hits U.S. Critical Infrastructure

By Jeff Goldman,
Posted May 18, 2017
A Department of Homeland Security official told Reuters earlier this week that some U.S. critical infrastructure operators have been affected by the recent WannaCry ransomware campaign. The official didn't provide any further information, except to say that there have been no victims of the cyber attack within the U.S. federal government. Dragos CEO Robert M. Lee told Forbes that his company is "aware of infections that occurred in the industrial control system community and had impact," including small utilities and manufacturing sites in the United States -- though he said "no one's been hurt and no safety was at risk." The news should put all companies that rely on industrial control systems (ICS) on high alert, PAS Global CEO Eddie Habibi told *eSecurity Planet* by email, because the choices available to protect the systems within an industrial process facility are much more limited than those in corporate IT. "In a corporate IT network, cyber security professionals have the option of isolating traffic or entire systems if they are compromised," Habibi said. "Personnel can also apply patches in real time with confidence that patching will not impact system performance."

A Challenge for ICS

But in an industrial process facility, it's rarely possible to isolate traffic or systems. "Those systems may have primary responsibility for controlling volative processes or ensuring worker and environmental safety," Habibi said. "System uptime is paramount." "Real-time patches are also no-nos within a facility's network," Habibi added. "First, any Microsoft patch must have ICS vendor approval before application. Even with approval, patching typically occurs during maintenance windows and turnarounds when systems are offline -- something that may occur only once or twice per year." And patches may never get applied if there's a potential for process disruption. "In these cases, asset owners may place additional security controls in front of the unpatched system to mitigate risk," Habibi said. "This assumes that there is a closed-loop, enterprise-wide patch management process in place that can evaluate the steps required to mitigate risk; many companies are missing this capability."

So while it's great that Microsoft has issued patches for older operating systems in response to WannaCry, Habibi said that may not be enough for critical infrastructure operators, which have limited ability to apply those patches.

"As we watch WannaCry continue to proliferate and see new variants spring up, the risk to industrial process facilities remains high," he said. Langner founder and CEO Ralph Langner told Forbes that a competent attacker could hit industrial targets and force a product halt. "We haven't seen that on a large scale yet, but I predict it's coming, with ransom demands in the six and seven digits," he said.

Hospital Equipment

Separately, an unidentified source in the healthcare industry provided Forbes with an image of a Bayer Medrad radiology device in a U.S. hospital infected with WannaCry ransomware. A Bayer spokesperson told Forbes that it had received two reports of customers in the U.S. with devices hit by the malware. "Operations at both sites were restored within 24 hours," the spokesperson said. "If a hospital's network is compromised, this may affect Bayer's Windows-based devices connected to that network." The company said it will be deploying a patch for its Windows-based devices "soon."

According to the HITRUST Alliance, medical devices from Siemens and other unnamed manufacturers have also been infected. "HITRUST is reaching out to healthcare organizations and trade associations to provide information to detect, prevent and remediate the threat and associated malware," the organization stated.

"Select Siemens Healthineers products may be affected by the Microsoft vulnerability being exploited by the WannaCry ransomware," Siemens stated in a security bulletin [PDF]. "The exploitability of any such vulnerability depends on the actual configuration and deployment environment of each product."

The Victims and Affected Assets

WannaCry: List of major companies and networks hit by ransomware around the globe. High-profile organizations such as the NHS, Renault, FedEx, Bank of China and more were affected.
By Agamoni Ghosh, India Ashok
Updated May 16, 2017 12:36 BST

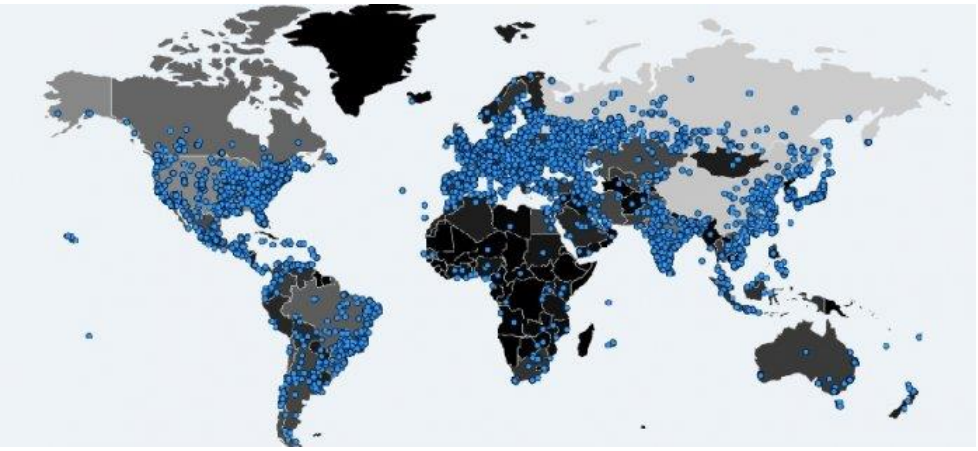
FedEx is the only major US company to have openly acknowledged the attacks on its systems until now REUTERS. The massive WannaCry ransomware attacks wreaked havoc across the globe over the weekend, with experts estimating that the ransomware hit between 100,000 to 200,000 computers across nearly 150 countries.

Although the attacks were stopped by a 22-year old British security researcher, who prefers being referred to as MalwareTech, the fix is temporary and only applies to the original ransomware strain. Security researchers have warned that the attackers will likely upgrade the malware to renew their global onslaught soon.

IBTimes UK brings you a list major government and private organizations affected by the global WannaCry ransomware attacks. These are just a handful of companies that have acknowledged or been reported about among the massive number of systems affected.

Deutsche Bahn: The German train operator was hit as traveler's tweeted pictures of hijacked departure boards showing the ransom demand instead of train times. The company, however, insisted trains were running as normal

Patrick Coomans (@patrickcoomans)
May 13, 2017 WOW! even in train stations #WannaCry #wannacrypt



The map shows the affected countries MalwareTech

- NHS: Hundreds of clinics and hospitals across UK suffered a massive outage in the wake of the attacks, with the administration being forced to delay or even cancel surgeries and X-rays of numerous patients.
- Telefonica: The Spanish telephone giant said it was attacked, clarifying that "the infected equipment is under control and being reinstalled".
- **Renault:** The French automobile giant was hit, forcing it to halt production at sites in France and its factory in Slovenia as part of measures to stop the spread of the virus
- **FedEx:** The US package delivery group acknowledged it had been hit by malware and said it was "implementing remediation steps as quickly as possible"
- **Nissan:** The firm's manufacturing plant in Sunderland, northeast England, was affected by the ransomware attack
- **Hitachi:** The Japanese firm said that its email service was hit, and that some of their staff were unable to access attachments or send and receive messages.
- **Russia Central Bank:** The bank said they detected the ransomware but had successfully thwarted the attack
- **Russian Railways:** The ransomware infected the Russian railways' IT systems. The organization said that they were working to eliminate the threat and upgrade their anti-virus protections
- **Russian Interior Ministry:** The ransomware also affected the government organisation, though the scope of the infection remains unknown
- **Iberdrola:** The Spanish electric utility firm was also affected and disconnected its systems from the internet as a precautionary measure
- **Indian police in the state of Andhra Pradesh:** The state police said they were locked out of their systems according to the Indian daily Economic Times
- **Electricity boards in India:** A handful of electricity boards in the country have said their systems have been affected. One of them is the West Bengal State Electricity Distribution Company Ltd (WBSEDCL), whose 4 office caters to around 8,00,000 households

- **MegaFon:** The biggest Russian telecom firm also confirmed having been affected by the attack
- **Sberbank:** Russia's largest bank said they detected the ransomware but defended against the attack
- **Bank Of China:** Many ATMs went dark and non functional in the wake of the attacks
- **China gas stations:** Payment systems of gas stations in parts of China were shut down by the attacks
- **Chinese traffic police, immigration and public security bureaus:** The agencies suspended many of its operations until the issues related to its systems were resolved, according to South China Morning Post
- **Singapore malls:** Display boards of Tiong Bahru Plaza and White Sands showed the ransomware message
- **Japan government offices :** Several city offices including the City Council of Osaka were locked out of their systems post the attacks
- **Multiplex chain in South Korea:** Major theatre chain CJ CGV said around 50 of its complexes are estimated to have been attacked by the malware
- **Sandvik:** The Swedish IT firm's computers in both administration and production were hit
- **Petrobras:** Brazil's state-owned oil company was also affected by the ransomware attack and turned off its computers as a precaution
- **Brazil's Foreign Ministry:** The government organization also fell victim to the attacks and switched off its computers
- **Brazil's social security system:** The attacks affected Brazil's social security systems, forcing it to disconnect computers and cancel public access to the agency
- **Portugal Telecom**: The firm acknowledged being hit by the attack but said it has managed to contain the ransomware from spreading according to Reuters.

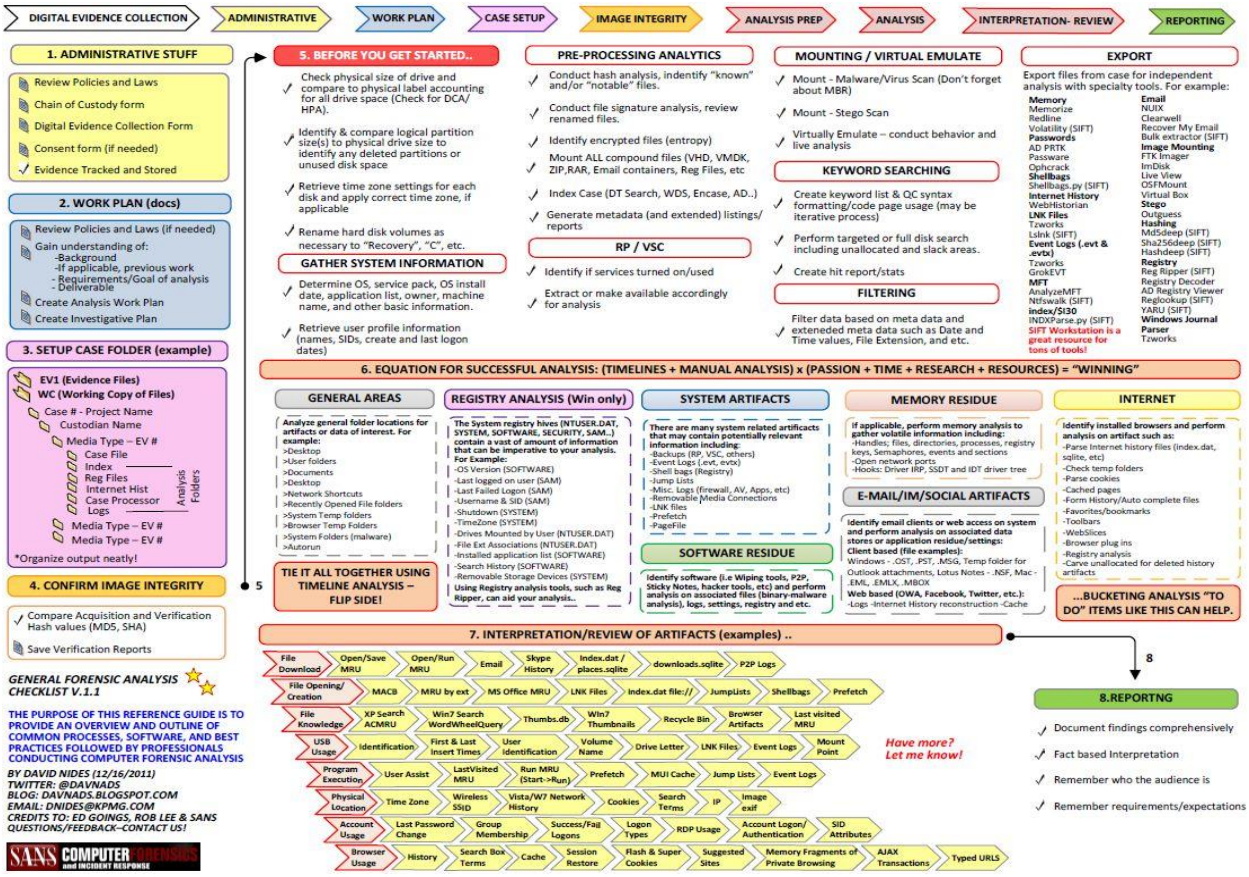
More from IBTimes UK

- Is WannaCry ransomware back? 2 new variants emerge hinting at future global attacks
- WannaCry: How to stay safe from the deadly ransomware if you own a Windows PC
- Global cyberattack: Full list of countries affected by ransomware campaign

Alpha & Omega Wellness Center

Cyber Incident Threat Response Intelligence Report

Course of Action Incident Response



Forensic Analysis and Data Recovery:

Reconnaissance	Port 445 Scan, EternalBlue Vulnerability, Lateral Traversal
Weaponization	SlingShot Port Zero BUSYBOX VoIP router exploited
Delivery	WorldCry dropped 2018-06-09 @ 8:56am
Exploitation	Encrypt files; require payment in BIT COIN to decrypt. Establish persistent presence expand attack
Installation	Install remote access software
Command and Control	Establish total & complete C2 capability, QUIC TOR MPTCP SSL
Actions on Objectives	Primary objective is to create a business interruption

Alpha & Omega Wellness Center

Cyber Incident Threat Response Intelligence Report

1. Contact Information for this Incident	
Name:	Marius Ruja D.O. & Karen Ruja
Title:	Alpha & Omega Wellness Center (Owners)
Office Location	2630 Montana El Paso Texas 79903
Work Phone:	(915) 521-2020
Mobile Phone:	(915) 494-1503 (915) 494-4468
Email address:	rujahealth@gmail.com
Fax Number:	(915)

2. Incident Description.

On Friday 8th of June 2018, Alpha & Omega Wellness Center, was a victim of "Electronic Vandalism". The new improved variant of the "WannaCry" crypto worm named "WorldCry" exploited \\SERVER08 which was not patched with MS17-010. Entry point is believed to be via port zero, MikroTik VoIP router, which was not patched for "SLINGSHOT" vulnerability, utilizing BUSYBOX and Apple Script to laterally traverse the network to the file server. The 2008 R2 server was not patched to protect against the "EternalBlue" attack tool, all files were encrypted. Previous IT support contractor attempted to "Decrypt" file structure to no avail. The "Mirrored HDD" was reformatted and counterfeit Windows Server 2008 R2 installed, because he did not have the original media, in another failed attempt to "Decrypt" and "Repair" with unsupported software. After 48 days of no progress or success in restoring systems to an operational capability, Karen Ruja then called Monica Velasquez of AR Billing Company, Wednesday July 25th, and asked for help. On Thursday July 26th, AR Billing Company executed a "Business Associate Agreement", for forensic analysis, data analysis, data retrieval and recreation, post ransomware attack. AR Billing Company then executed a "Cyber Incident Response Plan" in accordance with HIPPA/HITECH Act requirements. HDD evidence preserved, logs captured, forensic analysis completed, FBI notified. Data sets recovered, repaired and recreated, workstation and server operating systems recovered, repaired and recreated. Security Technical Implementation Guides desktop/server lockdowns implemented, Fortiguard Security Solution deployed, FortiClient workstation compliance, telemetry and Veriato 360 monitoring software deployed.

3. Impact / Potential Impact Check that apply to this incident.

- Loss / Compromise of Data
- Damage to Systems
- System Downtime
- Financial Loss
- Other Organizations' Systems Affected
- Damage to the Integrity and Delivery of Critical Services Information

Unable to bill for services, process insurance claims, provide critical personal injuring case evidentiary reports for attorneys. Electronic vandalism of system, combined with appointment cancellations, poor technical support with inadequate resources, combined for a perfect storm that affected business associates and partners. Although the total exact financial loss is difficult to calculated, it can be estimated based on historical qualitative and quantitative data. As a result of this "Electronic Vandalism" incident, AOWC has implemented "DISA STIG's", enforced security, training, operations, plans, and procedures standardization.

4. Sensitivity of Data/Information Involved
Check all of the following that apply to this incident.

Category	Description
Public	Marketing brochures and material posted to Alpha & Omega Wellness Center web pages.
Internal Use Only	This information is intended for use within Alpha & Omega Wellness Center or between agencies, and in some cases within affiliated organizations, such as business partners. Unauthorized disclosure of this information to outsiders may be against laws and regulations, or may cause problems for the Alpha & Omega Wellness Center, its customers, or its business partners.
ePHI Electronic Protected Health Information (Privacy Violation)	Examples are patient identifiable data, transaction account information and electronic medical records. Other examples include data and legal information protected by doctor patient privilege.

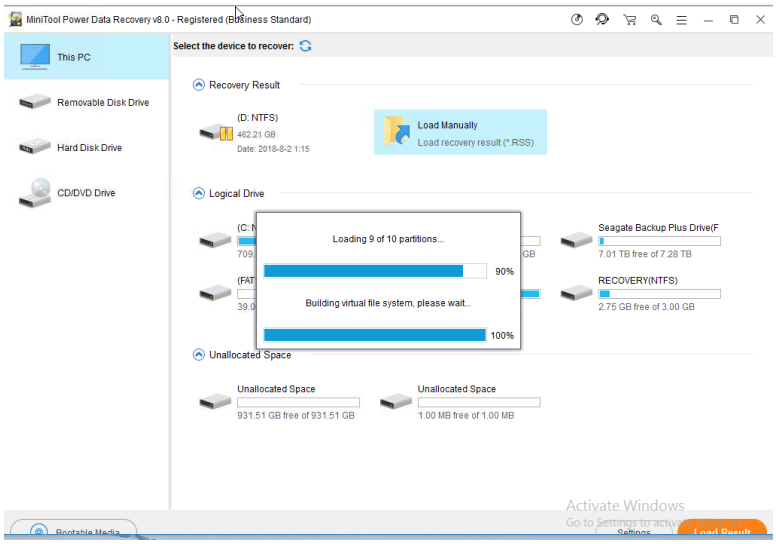
Provide a brief description of data that was compromised:
Microsoft Office documents, marketing materials, patient data, patient reports, billing statements, billing scans and billing lists. Complete destruction of data stores, operating systems, archives and profiles. ChiroTouch databases, reports and claims and Report Master client files all encrypted. However, using very expensive specialized tools, low level forensic analysis of HDD yielded a bounty of information, lost data sets, hidden partitions, corrupted partitions and RAW data. The forensic log is a PDF file 100Mb large and almost 65,000 pages long, report log has been parsed into usable extracts for the recreation of directory tree, recreation of data sets, recreation of profiles and restoration of lost data that was recovered. Approximately 97% of lost data sets have been recovered, restored and/or recreated. The other 3% can potentially be recreated utilizing forensic directory data structures and patient sign in sheets in an attempt to identify the recovered patient folder number, then recreate data record importing previously unidentified folder with TIFF records of original patient scans.
5. Who Else Has Been Notified?
SSA JR Reisinger FBI Cyber El Paso Texas JRReisinger@FBI.Gov
6. What Steps Have Been Taken So Far? Check all of the following that apply to this incident.
See AOWC Cyber Threat Intelligence Response Report, cyber incident response plan and supplementary logs/reports.
Provide a brief description: AOWC is fully mission capable, lost datasets are being recreated from forensic metadata.

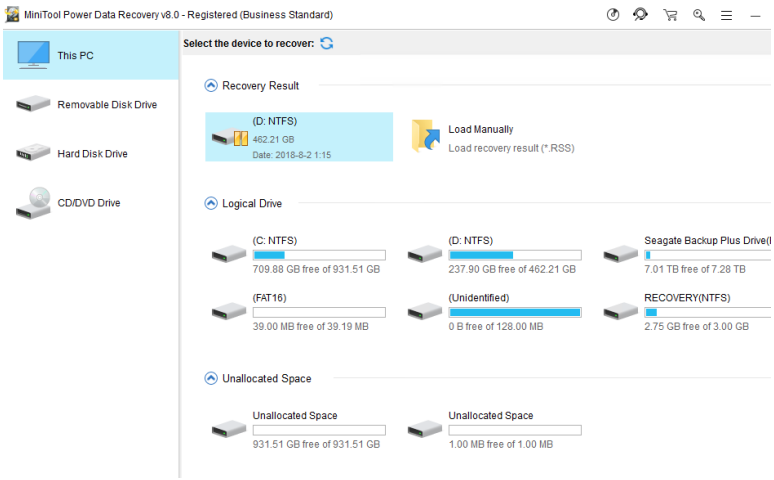
7. Incident Details	
Date and Time the Incident was discovered:	8th of June 2018
Has the incident been resolved?	Yes
Physical location of affected system(s):	2630 Montana Avenue El Paso Texas 79903
Number of sites affected by the incident:	3
Approximate number of systems affected by the incident:	15
Approximate number of users affected by the incident:	15
Are non-AOWC systems, such a business partners, affected by the incident? (Y or N – if Yes, please describe)	Yes, billing companies unable to process claims, directly impacting cash flow, ability to make payroll and pay bills.
Please provide any additional information that you feel is important but has not been provided elsewhere on this form.	This attack was the work of an ADVANCE PERSISTANT THREAT, utilizing stolen Top-Secret NSA hacking tools, which exploit known and unknown code vulnerabilities.

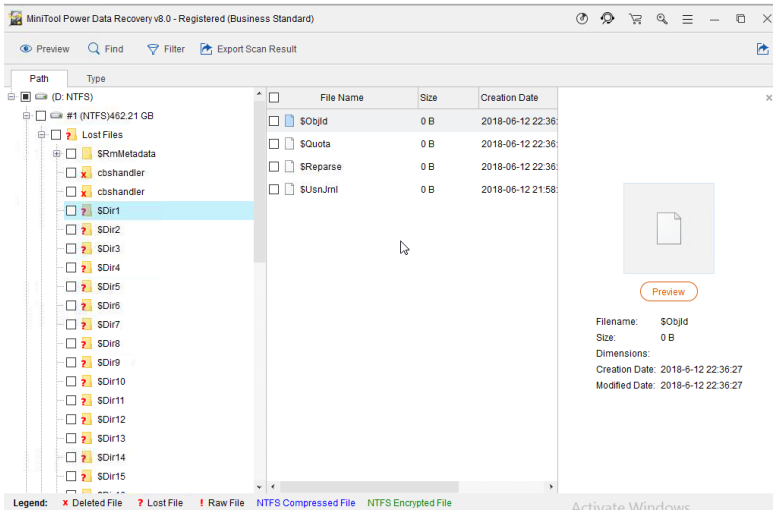
Electronic Vandalism Recovery Costs Worksheet

Items	Hourly Rate	Itemized Cost ($)		Total Cost ($)	
Digital Evidence Collection		Hrs Estimated	Actual Hrs	Estimated Cost	Actual Cost
Review policies and laws, execute Business Associate Agreement with AOWC, preserve chain of evidence, secure HDD for forensic analysis and law enforcement, procure replacement HDD's, secure evidence, backup images determine need to notify FBI	120	8	6	960	720
Work Plan		Estimated	Actual	Estimated	Actual
Interview end-users to gain understanding, document background, document failed procedure and actions by previous contractor, obtain passwords, usernames and key codes, create investigative plan, create analysis work plan, and contact FBI.	120	3	7	360	840
Case Setup		Estimated	Actual	Estimated	Actual
Collect evidence files, create working copy of files, and prepare to analyze, repair, recover and recreate data sets.	120	3	1	360	120
Image Integrity		Estimated	Actual	Estimated	Actual
Compare acquisition HASH and MD5 values, save report, determine extent of damage and begin repair, save report and begin recover, save report and begin recreation of data sets, save report, check physical size of drive and compare with logical size.	120	20	16	2400	1920
Check drive for lost or damaged partitions, retrieve file date time stamps, determine partition sizes, operating system, patch level, previously installed software, determine users, file structures and share points. Gather as much information as possible about each user's needs and lost data that must be recreated, attempt to contact previous contractor for support data to include passwords and usernames.	120	20	18	2400	2160

Analysis Preparation		Estimated	Actual	Estimated	Actual
Create CROWDSTRICK Falcon View automated malware analysis sandbox and BitNinja Virtual Machine sandbox for forensic analysis, testing, reverse engineering of malware, encryption cyphers, HASH and MD5 signatures. Isolate system to prevent infection while working with infected live files. Obtain decryption key utilizing specialized tools for analysis of memory stacks.	120	3	4	360	480
Analysis		Estimated	Actual	Estimated	Actual
Forensic analysis, threat analysis intelligence, data repair, recovery and recreation of directory structures. Extraction of data sets, logs, and files structure. Extraction of client files, insurance files, and databases.	120	20	25	2400	3000
Extraction of TIFF and PDF scans database, image database directories, folder and files structure. Recovery of data stores, restoration of data stores and validation of datasets.	120	8	15	960	1800
Interpretation & Review		Estimated	Actual	Estimated	Actual
Determine what data is corrupted, destroyed or lost and which datasets must be recreated, report on findings.	120	5	5	600	600
Server Recovery		Estimated	Actual	Estimated	Actual
Operating System	120	5	3	600	360
ChiroTouch/Report Master	120	5	8	600	960
Active Directory/Directory Services	120	3	1	360	120
Remote Desktop Services	120	2	1	240	120
Workstation Recovery		Estimated	Actual	Estimated	Actual
Operating systems, data sets, profiles, share points, productivity applications and specialized software.	120	60	40	7200	4800
Data Recovery		Estimated	Actual	Estimated	Actual
Recovery, restoration and recreation of data sets.	120	10	19	1200	2280
		175	**169**		
Subtotal				21000	20280
Sales Tax				Estimated	Actual
Add 8.25%				1732.5	0
Total				$22,732.50	$20,280.00

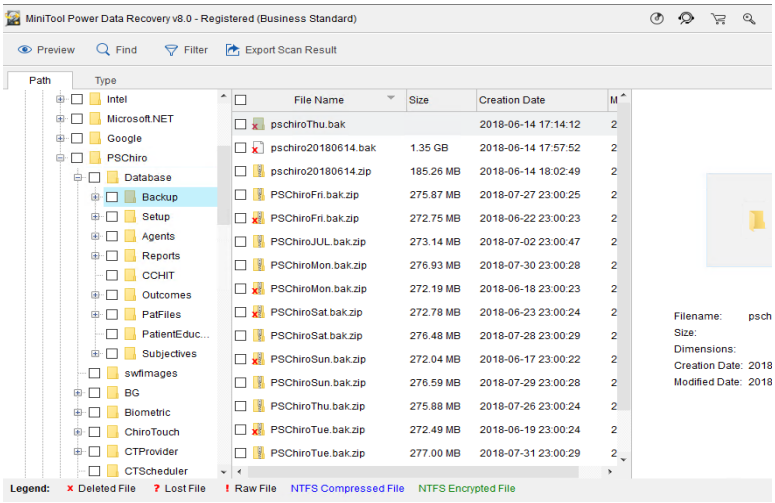

MiniTool Power Data Recovery v8.0 - Registered (Business Standard)
This PC
Removable Disk Drive
Hard Disk Drive
CD/DVD Drive
Select the device to recover:
Recovery Result
(D: NTFS)
462.21 GB
Date: 2018-8-2 1:15
Load Manually
Load recovery result (*.RSS)
Logical Drive
Loading 9 of 10 partitions...
90%
Building virtual file system, please wait...
100%
Seagate Backup Plus Drive(F
7.01 TB free of 7.28 TB
RECOVERY(NTFS)
2.75 GB free of 3.00 GB
Unallocated Space
Unallocated Space
931.51 GB free of 931.51 GB
Unallocated Space
1.00 MB free of 1.00 MB
Activate Windows

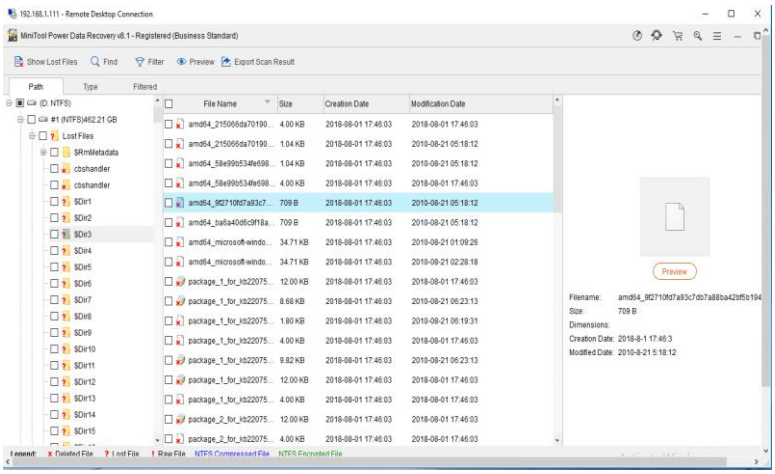

MiniTool Power Data Recovery v8.0 - Registered (Business Standard)
This PC
Removable Disk Drive
Hard Disk Drive
CD/DVD Drive
Select the device to recover:
Recovery Result
(D: NTFS)
462.21 GB
Date: 2018-8-2 1:15
Load Manually
Load recovery result (*.RSS)
Logical Drive
(C: NTFS)
709.88 GB free of 931.51 GB
(D: NTFS)
237.90 GB free of 462.21 GB
Seagate Backup Plus Drive(I
7.01 TB free of 7.28 TB
(FAT16)
39.00 MB free of 39.19 MB
(Unidentified)
0 B free of 128.00 MB
RECOVERY(NTFS)
2.75 GB free of 3.00 GB
Unallocated Space
Unallocated Space
931.51 GB free of 931.51 GB
Unallocated Space
1.00 MB free of 1.00 MB

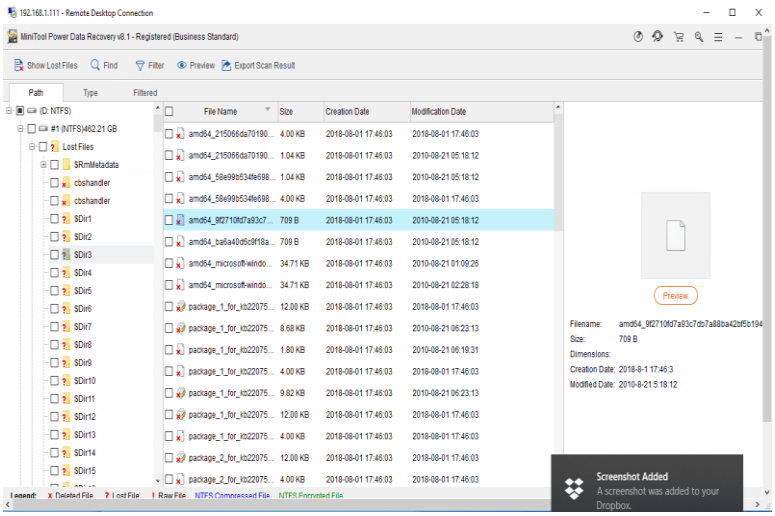

MiniTool Power Data Recovery v8.0 - Registered (Business Standard)
Preview
Find
Filter
Export Scan Result
Path
Type
(D: NTFS)
#1 (NTFS)462.21 GB
Lost Files
$RmMetadata
cbshandler
cbshandler
$Dir1
$Dir2
$Dir3
$Dir4
$Dir5
$Dir6
$Dir7
$Dir8
$Dir9
$Dir10
$Dir11
$Dir12
$Dir13
$Dir14
$Dir15
File Name
Size
Creation Date
$ObjId
0 B
2018-06-12 22:36:
$Quota
0 B
2018-06-12 22:36:
$Reparse
0 B
2018-06-12 22:36:
$UsnJrnl
0 B
2018-06-12 21:58:
Preview
Filename: $ObjId
Size: 0 B
Dimensions:
Creation Date: 2018-6-12 22:36:27
Modified Date: 2018-6-12 22:36:27
Legend: Deleted File Lost File Raw File NTFS Compressed File NTFS Encrypted File

Alpha & Omega Wellness Center

Cyber Incident Threat Response Intelligence Report

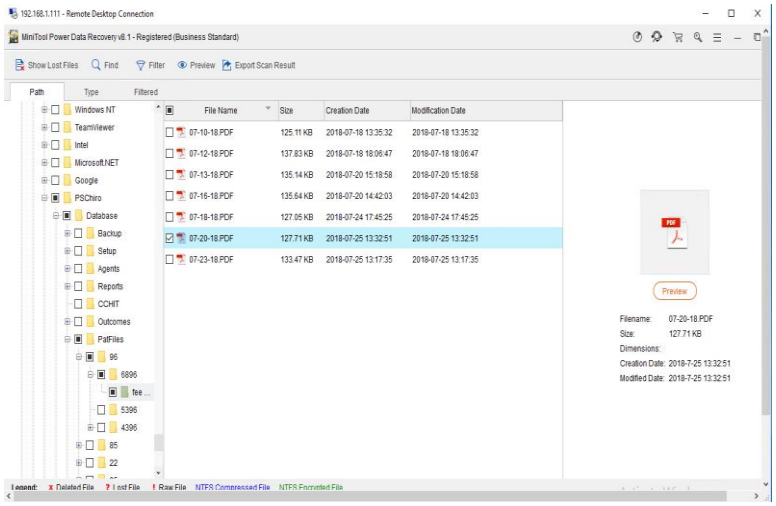


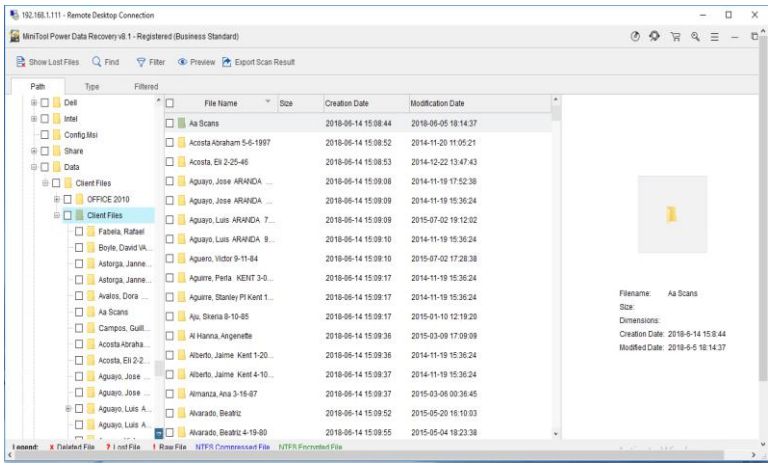


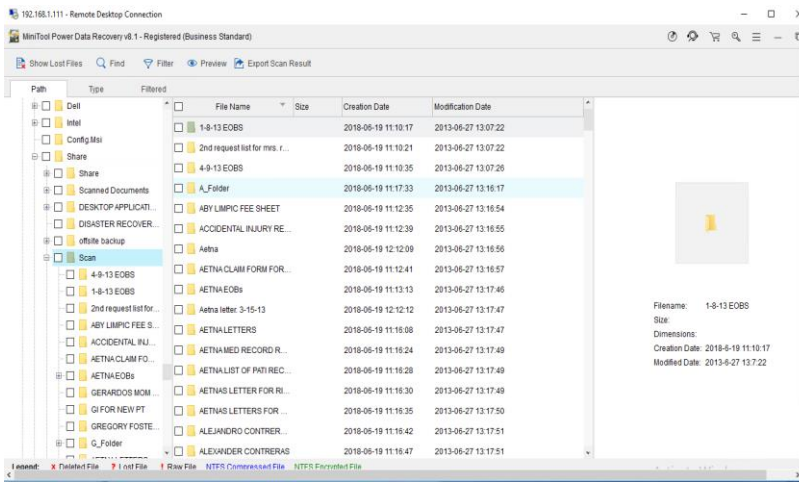


Alpha & Omega Wellness Center

Cyber Incident Threat Response Intelligence Report

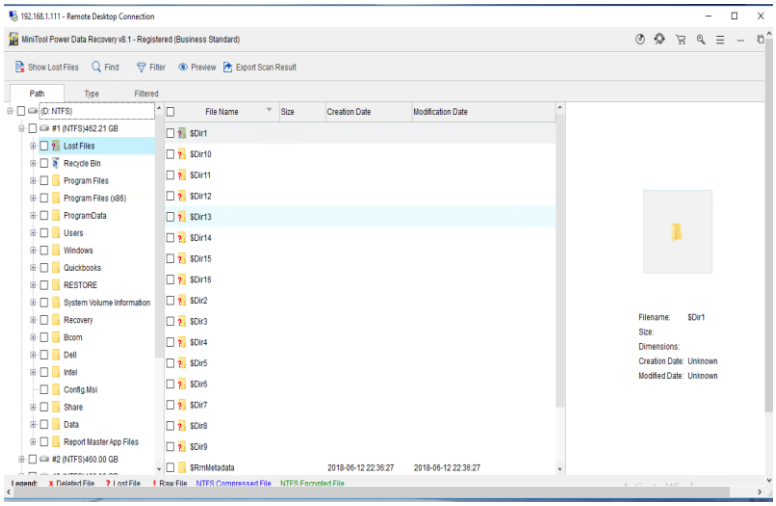


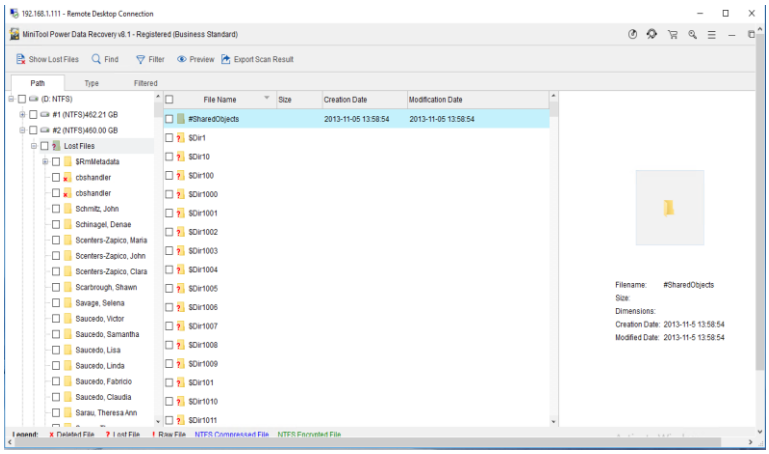


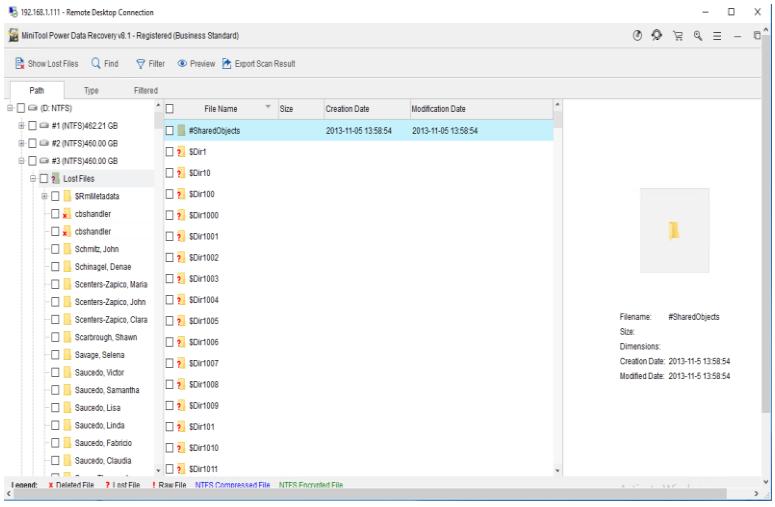


Alpha & Omega Wellness Center

Cyber Incident Threat Response Intelligence Report

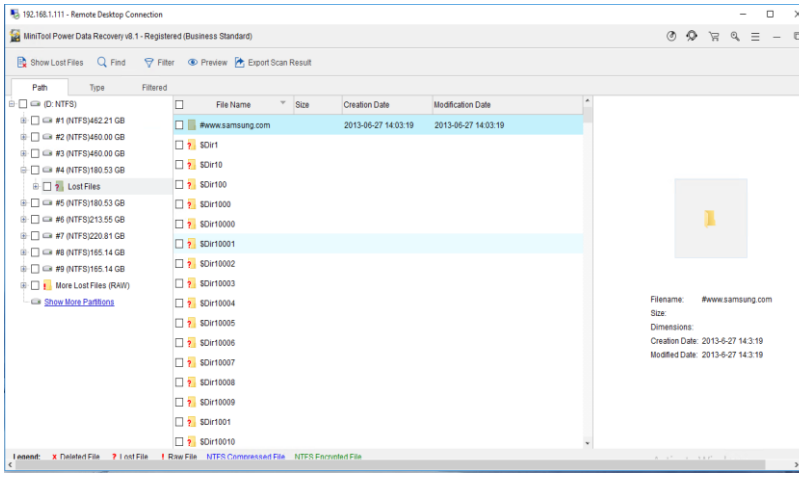


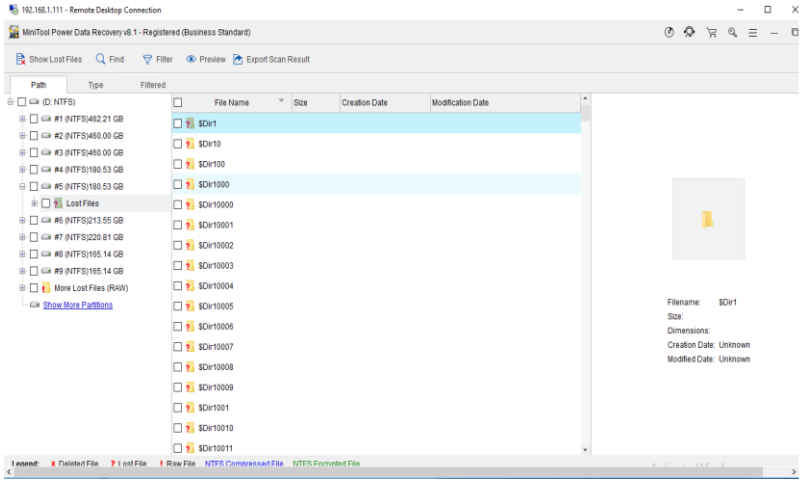


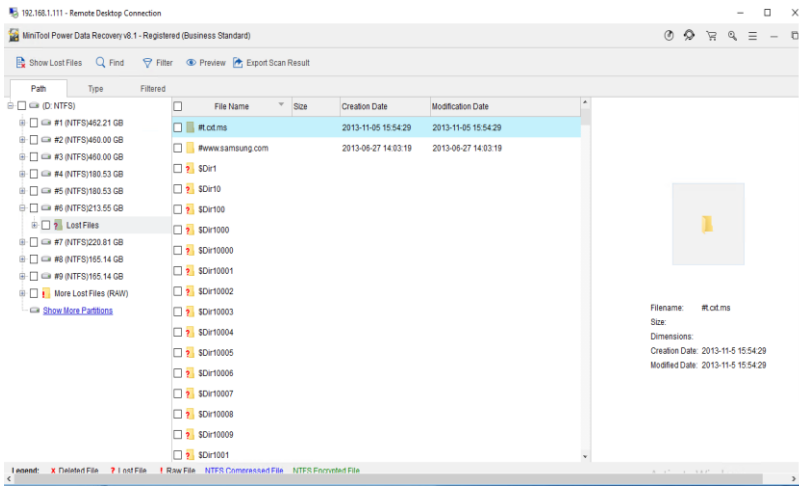


Alpha & Omega Wellness Center

Cyber Incident Threat Response Intelligence Report

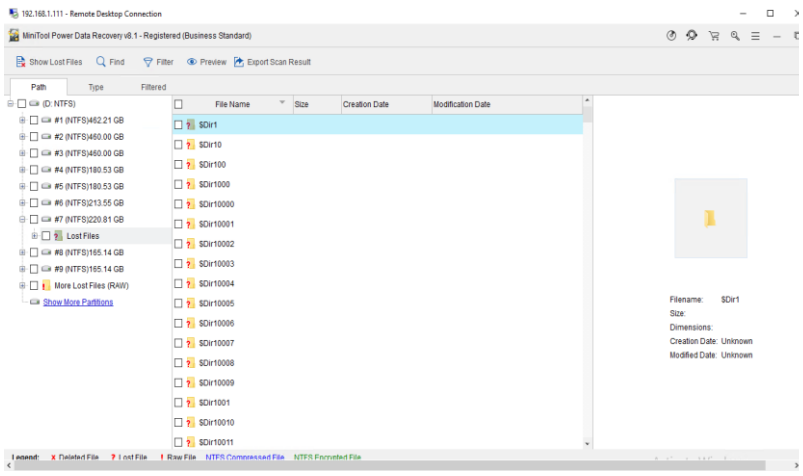


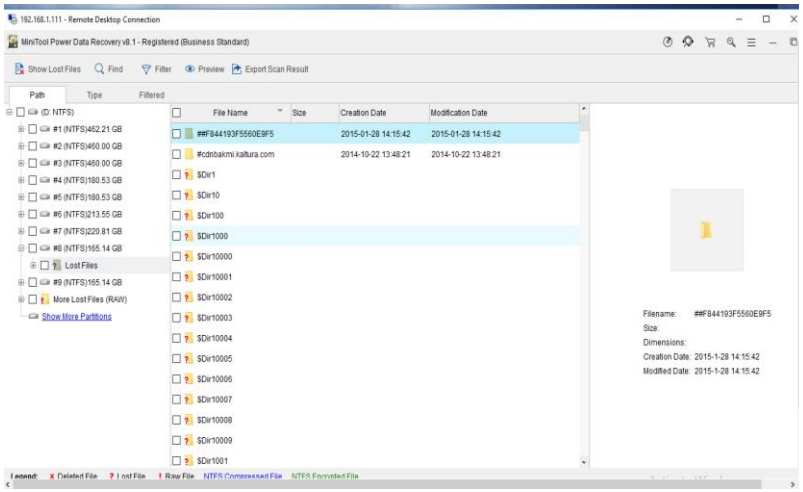


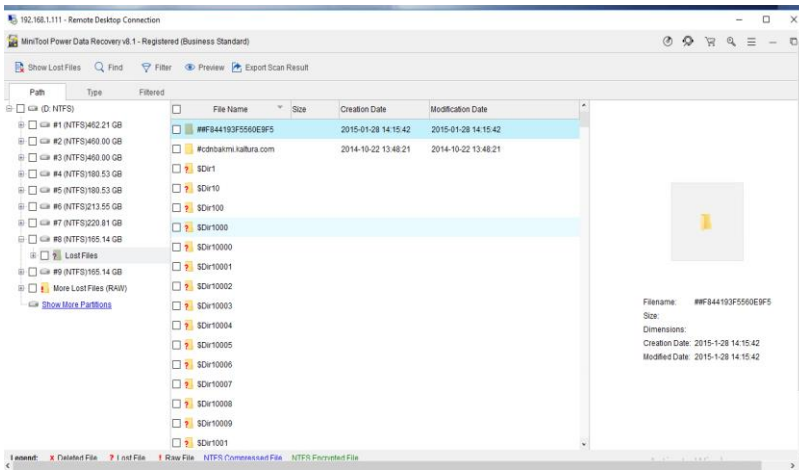


Alpha & Omega Wellness Center

Cyber Incident Threat Response Intelligence Report

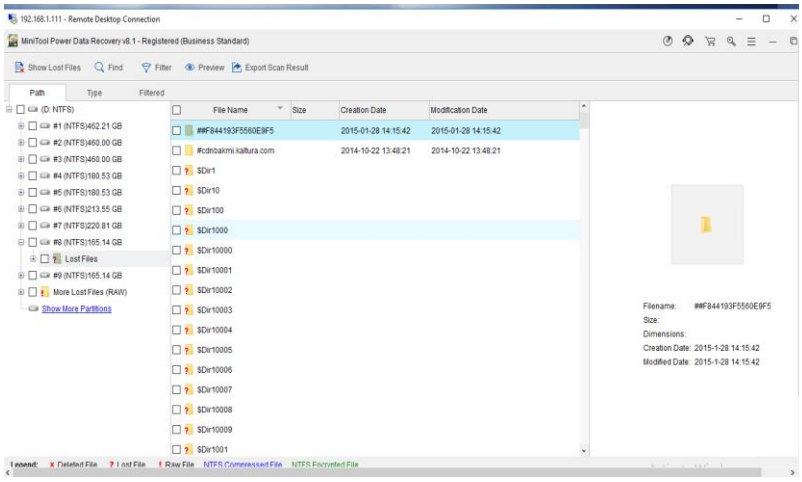


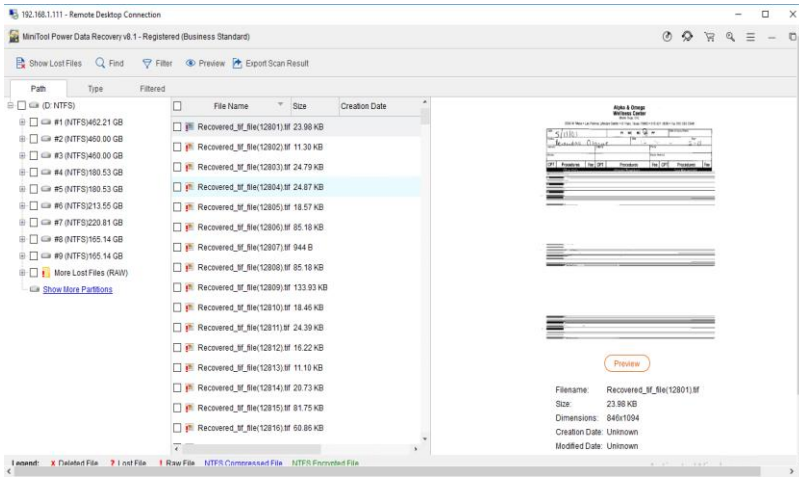


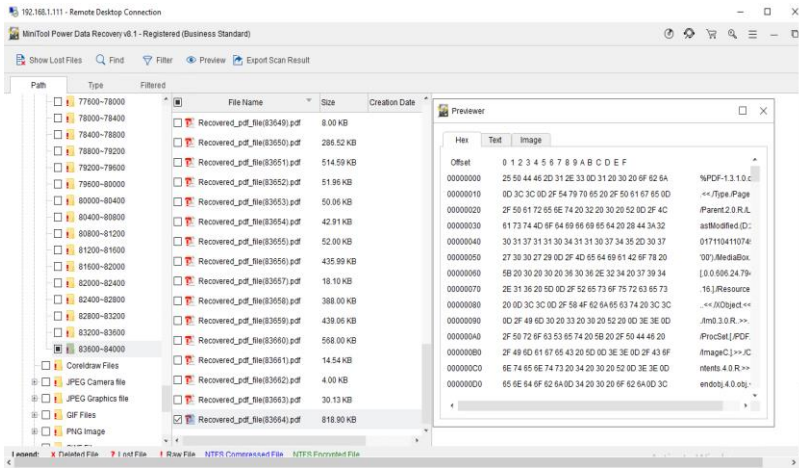


Alpha & Omega Wellness Center

Cyber Incident Threat Response Intelligence Report

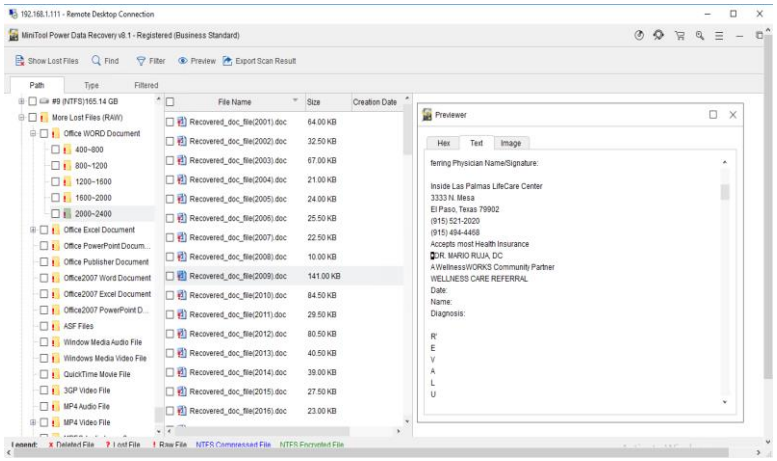


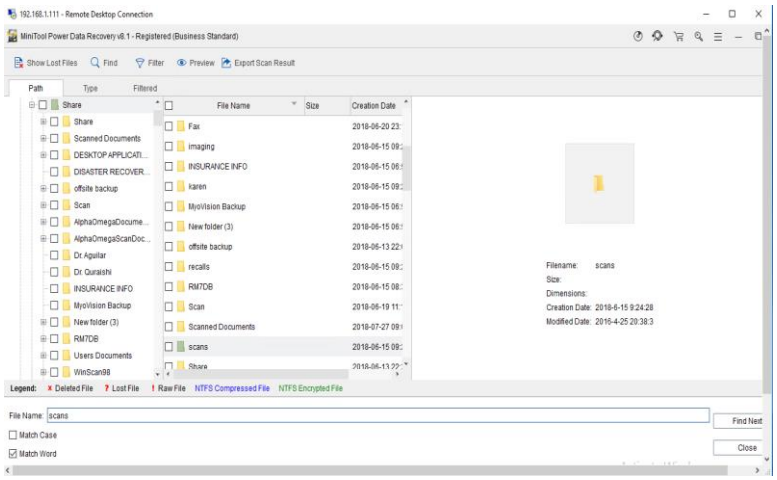


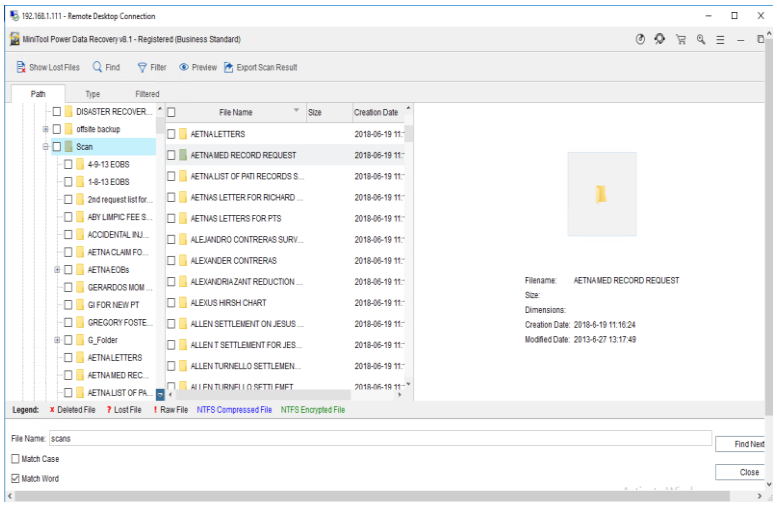


Alpha & Omega Wellness Center

Cyber Incident Threat Response Intelligence Report







Tue, Jun 12, 7:44 AM

Good morning.
What is the expected time for having the server back up ?

Tue, Jun 12, 9:52 AM

I spent yesterday and this morning trying to decrypt. Going to start reinstalling shortly.

Okay. Thank you.

Wed, Jun 13, 10:50 AM

Hi Don. What is the current status of the server?

I spent most Monday and Tuesday am trying to decrypt. If that had worked, would have saved me many hours. Did not work. Tuesday afternoon, I made the decision to wipe server and start clean. That takes about 6hr of installing

The DATA is restored, I need to install the software. Quickbooks

When when can she get access again?

Not yet. I need to build VPN, install QB, make her an account. Configure QB. Then send her new instructions on connecting. I'll be ready late today. She can log in tomorrow

Ok

Tue, Jun 19, 4:37 PM

Download link expired for quickbooks. Try clicking it, says expired.... :/ do you recall version? 2016?

I'll see if I can find 2016 QB pro download

It is 2016. I don't know anything about it.

Started updating last night, running updates this morning

Started updating last night, running updates this morning

Restoring user data later today. Returning server to job site tomorrow. Itll take a few hours tomorrow for install.

Chirotouch will need to remote in and install software and restore my backups.

Quickbooks data is also good. Along with some large data folders, like scans

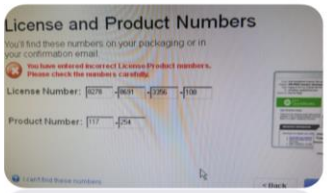
Thank you

For security reasons I'd reccomend we stop using " remote desktop"

Gonna need to find another remote method

It is 2016. I don't know anything about it.

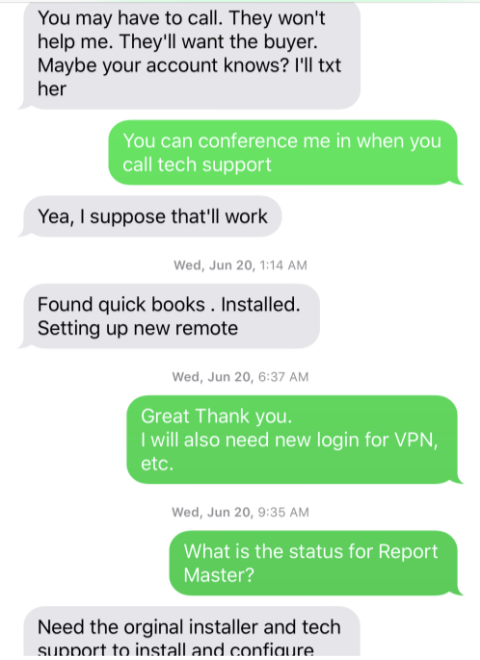
Tue, Jun 19, 6:30 PM

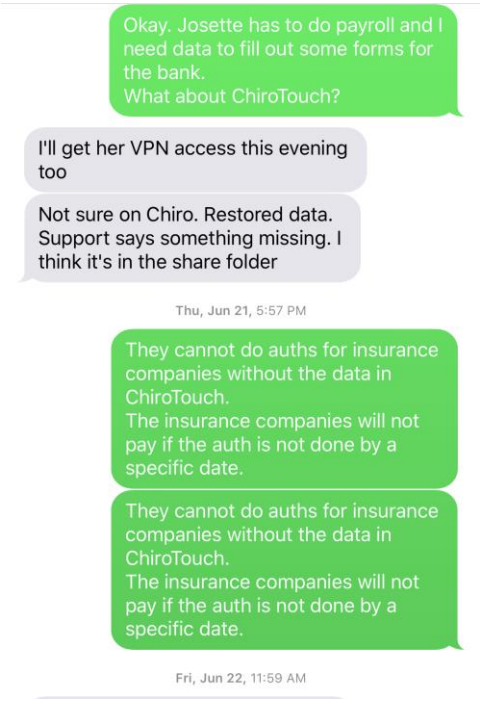


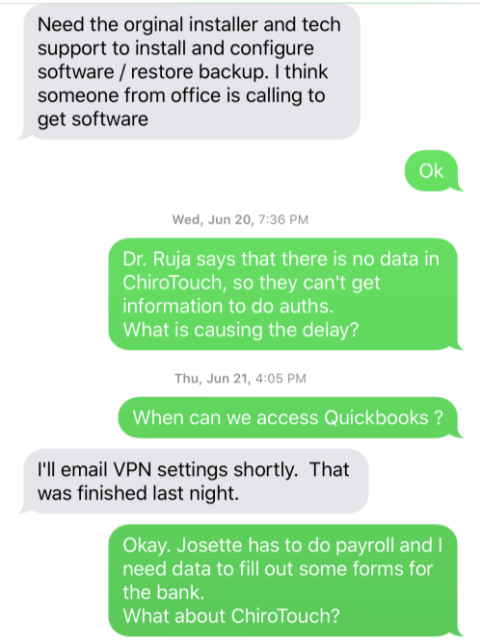
Who bought originally? Need to know version of QB

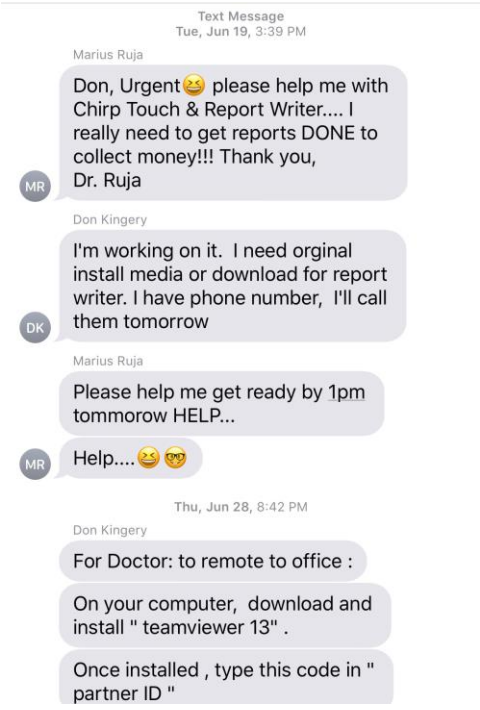
I just emailed what I could find from 2012. We have had QB since 2002. I don't have access to any original docs. Everything is packed in boxes.
With the order numbers, they should have access to our account history

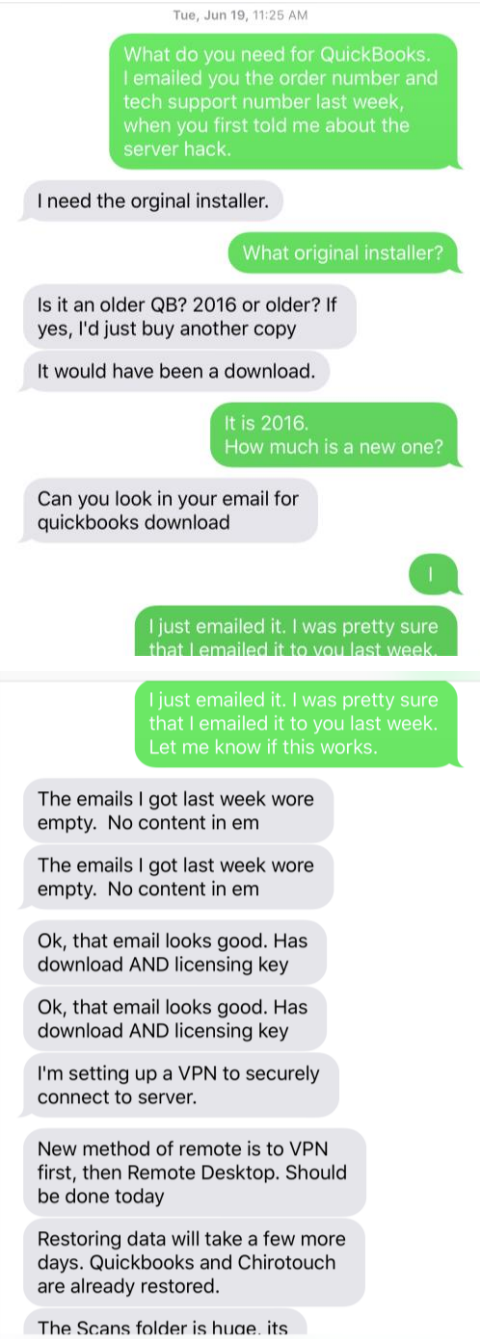
You may have to call. They won't help me. They'll want the buyer.

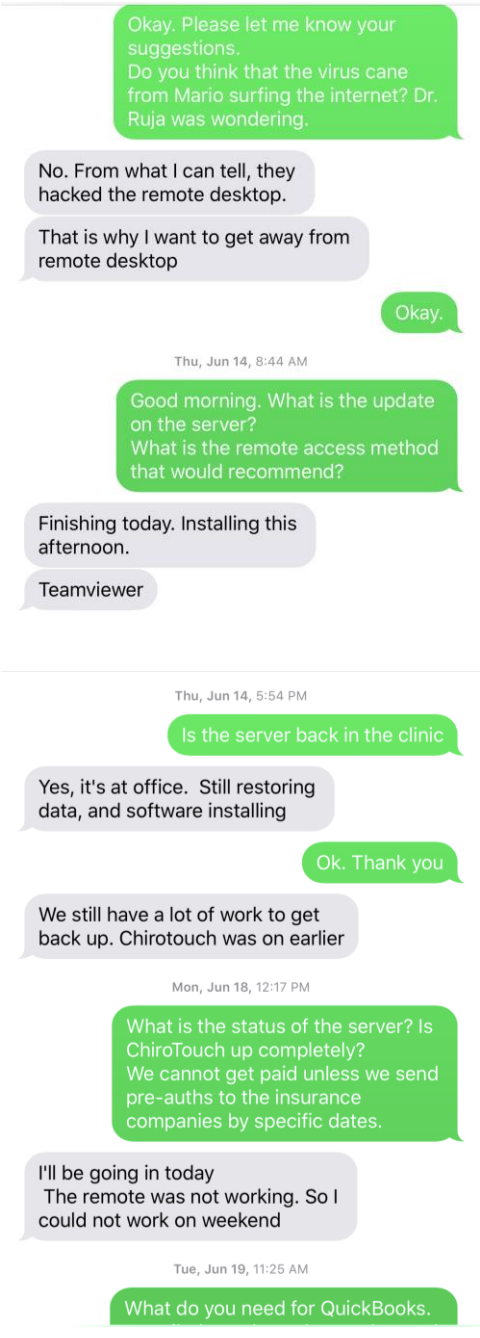

You may have to call. They won't help me. They'll want the buyer. Maybe your account knows? I'll txt her
You can conference me in when you call tech support
Yea, I suppose that'll work
Wed, Jun 20, 1:14 AM
Found quick books . Installed. Setting up new remote
Wed, Jun 20, 6:37 AM
Great Thank you.
I will also need new login for VPN, etc.
Wed, Jun 20, 9:35 AM
What is the status for Report Master?
Need the orginal installer and tech support to install and configure

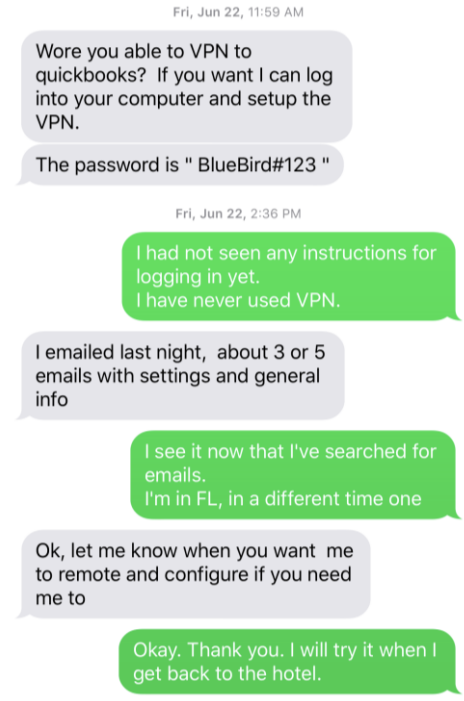

Okay. Josette has to do payroll and I need data to fill out some forms for the bank.
What about ChiroTouch?
I'll get her VPN access this evening too
Not sure on Chiro. Restored data. Support says something missing. I think it's in the share folder
Thu, Jun 21, 5:57 PM
They cannot do auths for insurance companies without the data in ChiroTouch.
The insurance companies will not pay if the auth is not done by a specific date.
They cannot do auths for insurance companies without the data in ChiroTouch.
The insurance companies will not pay if the auth is not done by a specific date.
Fri, Jun 22, 11:59 AM

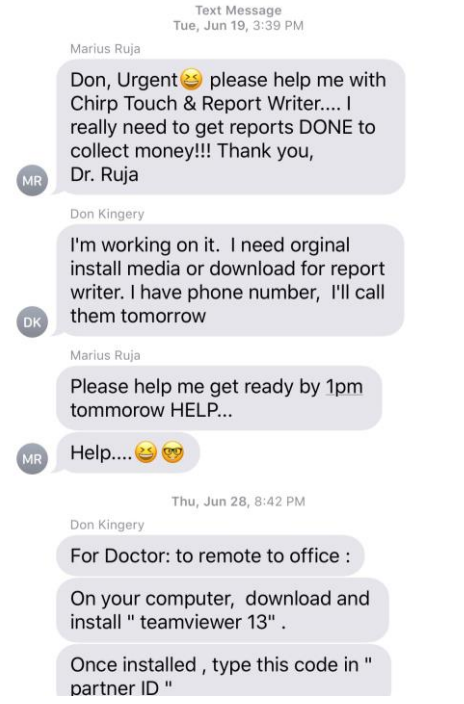

Need the orginal installer and tech support to install and configure software / restore backup. I think someone from office is calling to get software
Ok
Wed, Jun 20, 7:36 PM
Dr. Ruja says that there is no data in ChiroTouch, so they can't get information to do auths.
What is causing the delay?
Thu, Jun 21, 4:05 PM
When can we access Quickbooks ?
I'll email VPN settings shortly. That was finished last night.
Okay. Josette has to do payroll and I need data to fill out some forms for the bank.
What about ChiroTouch?

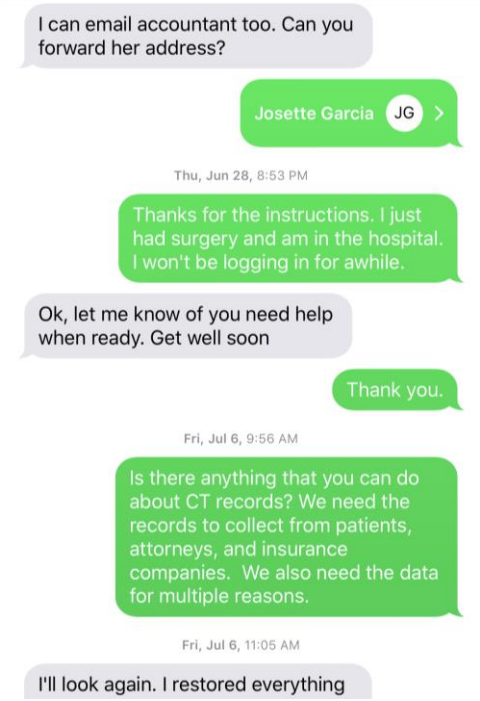

Text Message
Tue, Jun 19, 3:39 PM
Marius Ruja
Don, Urgent please help me with Chirp Touch & Report Writer.... I really need to get reports DONE to collect money!!! Thank you,
Dr. Ruja
MR
Don Kingery
I'm working on it. I need orginal install media or download for report writer. I have phone number, I'll call them tomorrow
DK
Marius Ruja
Please help me get ready by 1pm tommorow HELP...
Help....
MR
Thu, Jun 28, 8:42 PM
Don Kingery
For Doctor: to remote to office :
On your computer, download and install " teamviewer 13" .
Once installed , type this code in " partner ID "

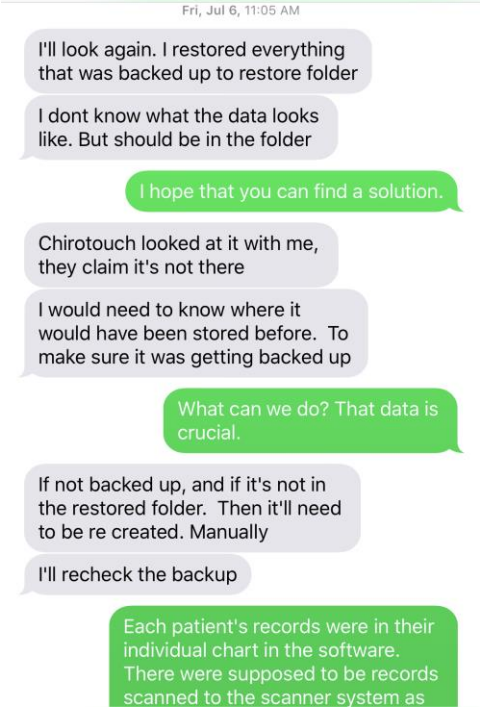

Tue, Jun 19, 11:25 AM
What do you need for QuickBooks. I emailed you the order number and tech support number last week, when you first told me about the server hack.
I need the orginal installer.
What original installer?
Is it an older QB? 2016 or older? If yes, I'd just buy another copy
It would have been a download.
It is 2016.
How much is a new one?
Can you look in your email for quickbooks download
I
I just emailed it. I was pretty sure that I emailed it to you last week.
I just emailed it. I was pretty sure that I emailed it to you last week. Let me know if this works.
The emails I got last week wore empty. No content in em
The emails I got last week wore empty. No content in em
Ok, that email looks good. Has download AND licensing key
Ok, that email looks good. Has download AND licensing key
I'm setting up a VPN to securely connect to server.
New method of remote is to VPN first, then Remote Desktop. Should be done today
Restoring data will take a few more days. Quickbooks and Chirotouch are already restored.
The Scans folder is huge. its

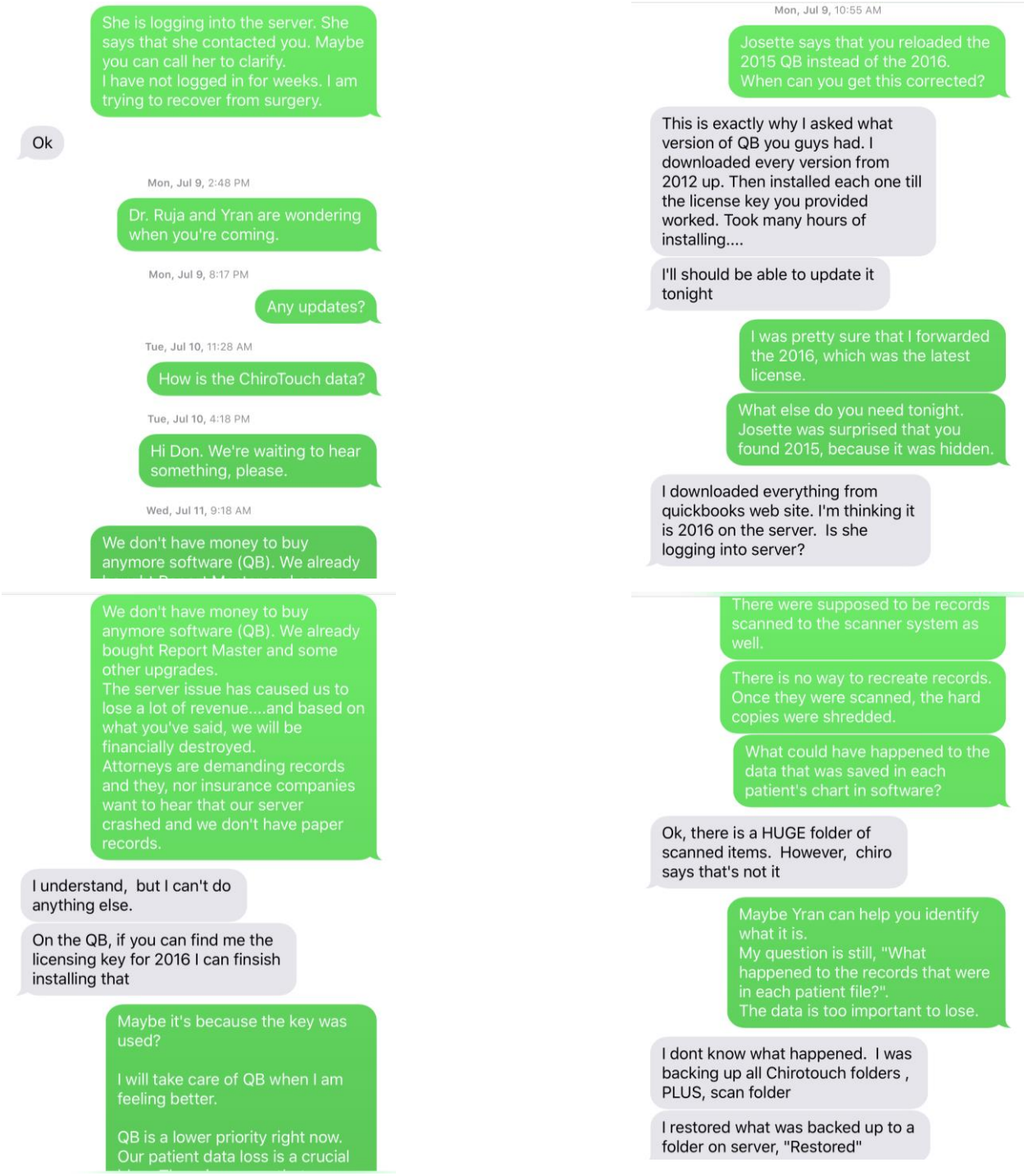

Okay. Please let me know your suggestions.
Do you think that the virus cane from Mario surfing the internet? Dr. Ruja was wondering.
No. From what I can tell, they hacked the remote desktop.
That is why I want to get away from remote desktop
Okay.
Thu, Jun 14, 8:44 AM
Good morning. What is the update on the server?
What is the remote access method that would recommend?
Finishing today. Installing this afternoon.
Teamviewer
Thu, Jun 14, 5:54 PM
Is the server back in the clinic
Yes, it's at office. Still restoring data, and software installing
Ok. Thank you
We still have a lot of work to get back up. Chirotouch was on earlier
Mon, Jun 18, 12:17 PM
What is the status of the server? Is ChiroTouch up completely?
We cannot get paid unless we send pre-auths to the insurance companies by specific dates.
I'll be going in today
The remote was not working. So I could not work on weekend
Tue, Jun 19, 11:25 AM
What do you need for QuickBooks.


Fri, Jun 22, 11:59 AM
Wore you able to VPN to quickbooks? If you want I can log into your computer and setup the VPN.
The password is " BlueBird#123 "
Fri, Jun 22, 2:36 PM
I had not seen any instructions for logging in yet.
I have never used VPN.
I emailed last night, about 3 or 5 emails with settings and general info
I see it now that I've searched for emails.
I'm in FL, in a different time one
Ok, let me know when you want me to remote and configure if you need me to
Okay. Thank you. I will try it when I get back to the hotel.


Text Message
Tue, Jun 19, 3:39 PM
Marius Ruja
Don, Urgent please help me with Chirp Touch & Report Writer.... I really need to get reports DONE to collect money!!! Thank you,
Dr. Ruja
MR
Don Kingery
I'm working on it. I need orginal install media or download for report writer. I have phone number, I'll call them tomorrow
DK
Marius Ruja
Please help me get ready by 1pm tommorow HELP...
Help....
MR
Thu, Jun 28, 8:42 PM
Don Kingery
For Doctor: to remote to office :
On your computer, download and install " teamviewer 13" .
Once installed , type this code in " partner ID "


I can email accountant too. Can you forward her address?
Josette Garcia JG
Thu, Jun 28, 8:53 PM
Thanks for the instructions. I just had surgery and am in the hospital. I won't be logging in for awhile.
Ok, let me know of you need help when ready. Get well soon
Thank you.
Fri, Jul 6, 9:56 AM
Is there anything that you can do about CT records? We need the records to collect from patients, attorneys, and insurance companies. We also need the data for multiple reasons.
Fri, Jul 6, 11:05 AM
I'll look again. I restored everything


Fri, Jul 6, 11:05 AM
I'll look again. I restored everything that was backed up to restore folder
I dont know what the data looks like. But should be in the folder
I hope that you can find a solution.
Chirotouch looked at it with me, they claim it's not there
I would need to know where it would have been stored before. To make sure it was getting backed up
What can we do? That data is crucial.
If not backed up, and if it's not in the restored folder. Then it'll need to be re created. Manually
I'll recheck the backup
Each patient's records were in their individual chart in the software. There were supposed to be records scanned to the scanner system as


She is logging into the server. She says that she contacted you. Maybe you can call her to clarify.
I have not logged in for weeks. I am trying to recover from surgery.
Ok
Mon, Jul 9, 2:48 PM
Dr. Ruja and Yran are wondering when you're coming.
Mon, Jul 9, 8:17 PM
Any updates?
Tue, Jul 10, 11:28 AM
How is the ChiroTouch data?
Tue, Jul 10, 4:18 PM
Hi Don. We're waiting to hear something, please.
Wed, Jul 11, 9:18 AM
We don't have money to buy anymore software (QB). We already
We don't have money to buy anymore software (QB). We already bought Report Master and some other upgrades.
The server issue has caused us to lose a lot of revenue....and based on what you've said, we will be financially destroyed.
Attorneys are demanding records and they, nor insurance companies want to hear that our server crashed and we don't have paper records.
I understand, but I can't do anything else.
On the QB, if you can find me the licensing key for 2016 I can finsish installing that
Maybe it's because the key was used?
I will take care of QB when I am feeling better.
QB is a lower priority right now. Our patient data loss is a crucial
Mon, Jul 9, 10:55 AM
Josette says that you reloaded the 2015 QB instead of the 2016. When can you get this corrected?
This is exactly why I asked what version of QB you guys had. I downloaded every version from 2012 up. Then installed each one till the license key you provided worked. Took many hours of installing....
I'll should be able to update it tonight
I was pretty sure that I forwarded the 2016, which was the latest license.
What else do you need tonight. Josette was surprised that you found 2015, because it was hidden.
I downloaded everything from quickbooks web site. I'm thinking it is 2016 on the server. Is she logging into server?
There were supposed to be records scanned to the scanner system as well.
There is no way to recreate records. Once they were scanned, the hard copies were shredded.
What could have happened to the data that was saved in each patient's chart in software?
Ok, there is a HUGE folder of scanned items. However, chiro says that's not it
Maybe Yran can help you identify what it is.
My question is still, "What happened to the records that were in each patient file?".
The data is too important to lose.
I dont know what happened. I was backing up all Chirotouch folders , PLUS, scan folder
I restored what was backed up to a folder on server, "Restored"

The Scans folder is huge, its restoring now

Thank you Don. Sorry about the empty emails. Glad that I found the right one.
So...Josette can access QB now?

Not yet. I need to build VPN, install QB, make her an account. Configure QB. Then send her new instructions on connecting. I'll be ready late today. She can log in tomorrow

I'll need her text number AND email so I can send her info

I thought that you said QB was ready to go.
How long will it take to be accessible?

Josette Garcia JG >

The DATA is restored, I need to

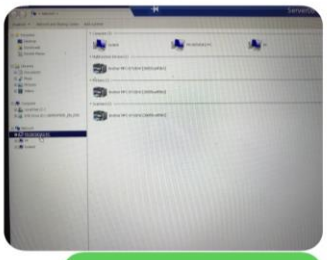
Where can I look for the missing scanned files that we need?

Should only say Server08.

Bunch of stuff in share folder

I found that when I searched. The other remote has the new address also

Most everything in share folder



Where is the share folder?

Delete that other remote, it will no longer work

The data for ChiroTouch was scanned and shredded.
I was not aware that anyone rushed you to the point of asking you to skip crucial steps, such as imaging the crypto ed server.

We have no other options. We relied on your back ups to help in these situations.

We have serious cases that we cannot settle unless we get those records to attorneys. We can not "Re-create" anything. We don't have records (or the manpower even if we did have records).

We need your help to find a solution.
There is too much on the line to leave this unresolved.
Thank you

What about the scan folder that documents were scanned into?

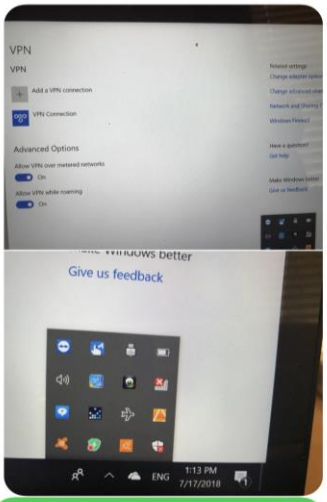
Don Kingery

There are gigabytes of scanned

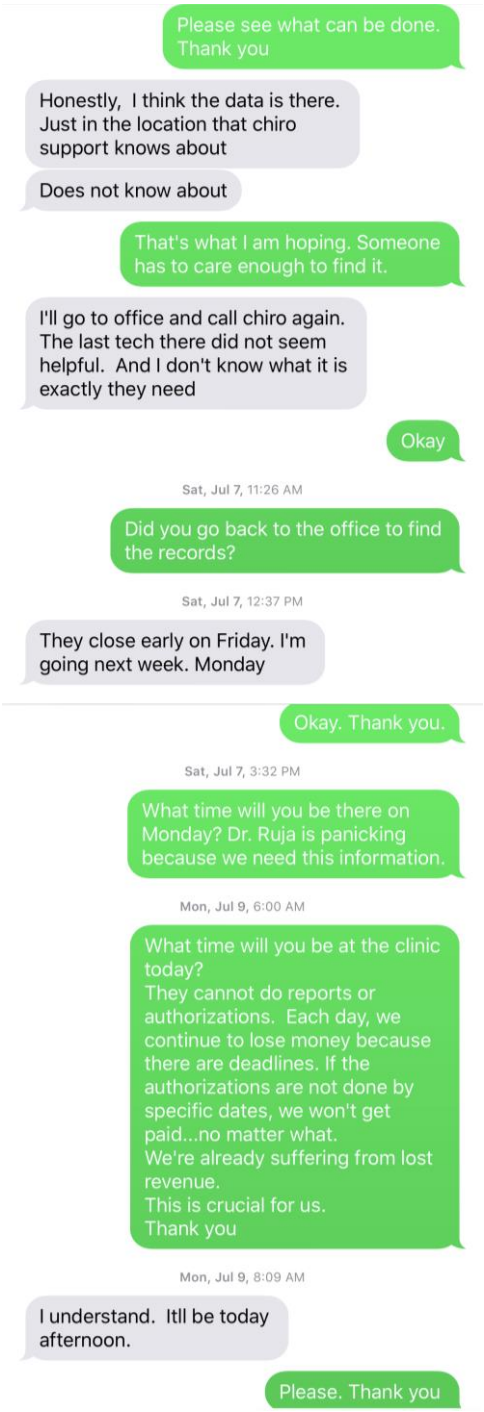
Apply

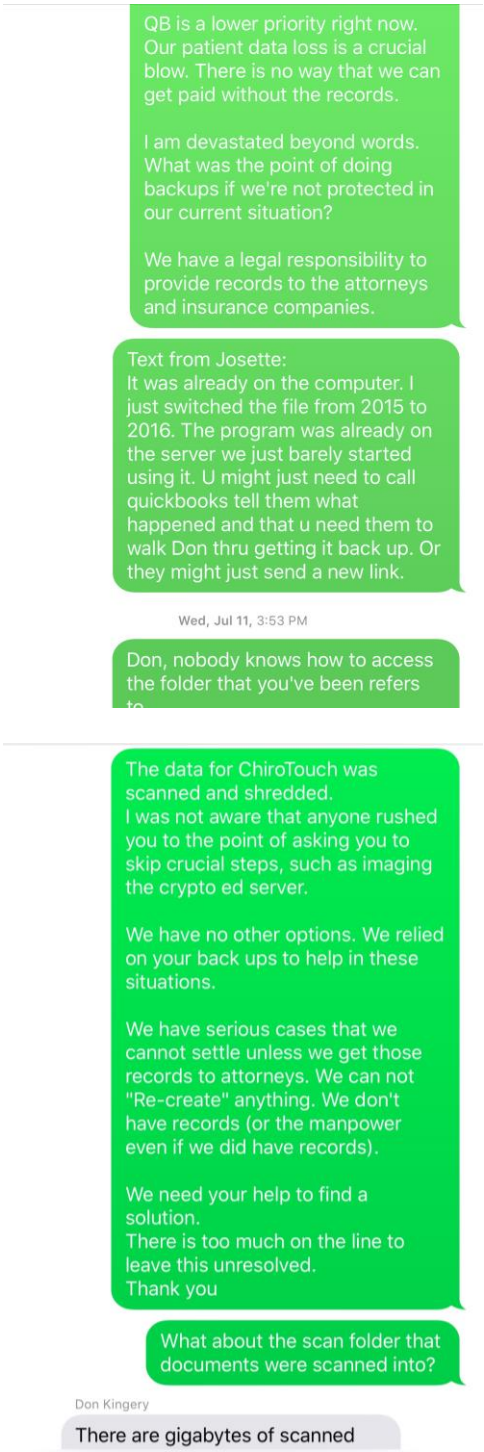
Then far right, bottom next to time, look fo network icon

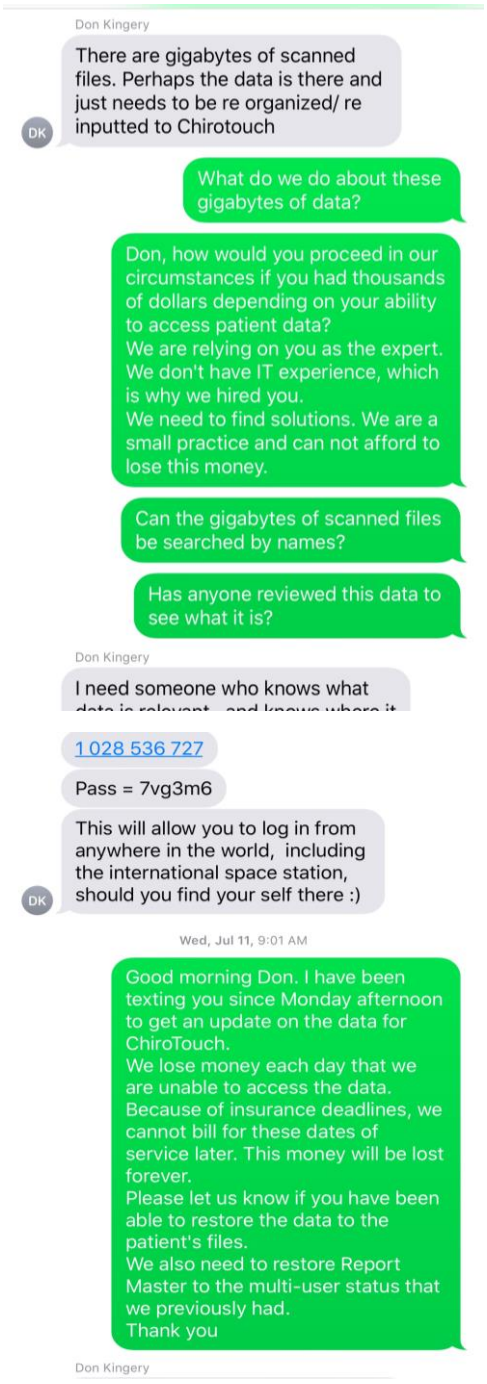
Click than, select VPN

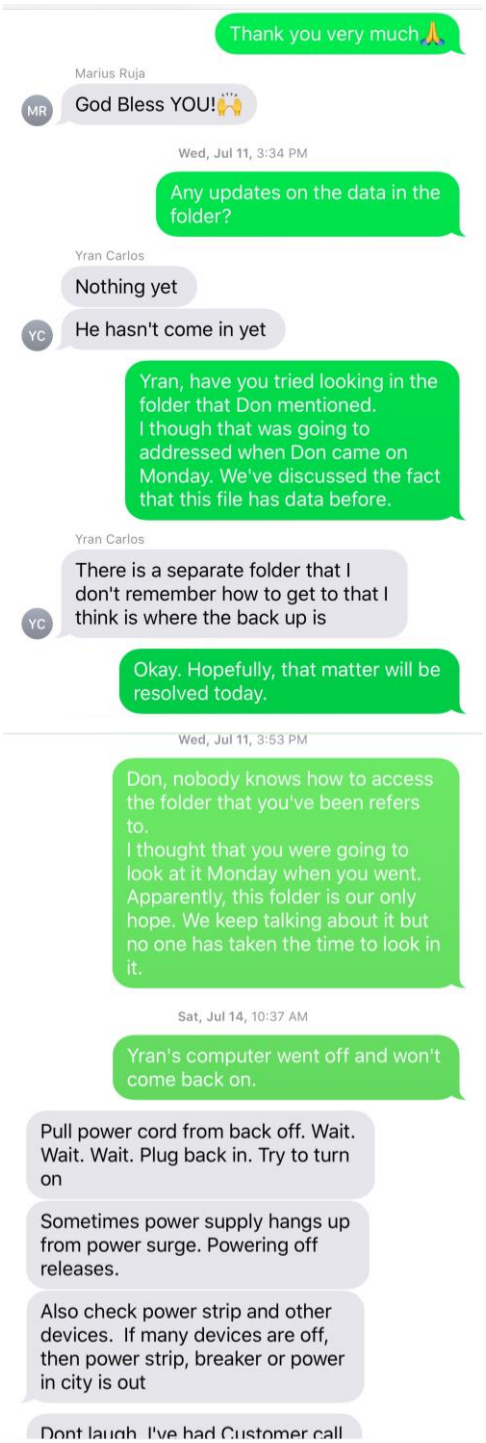


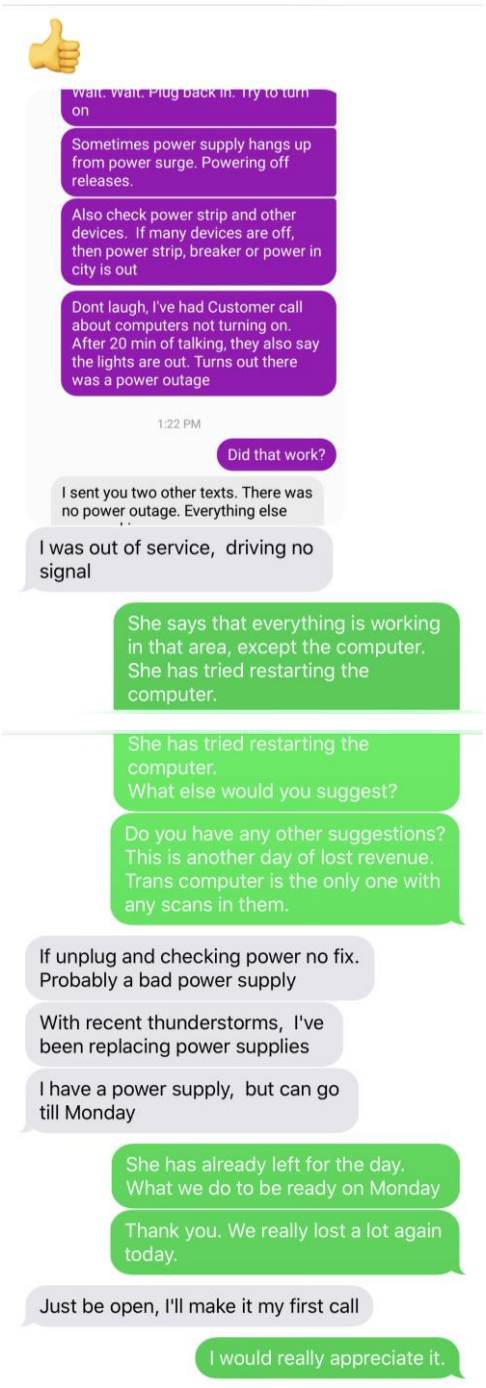
I have removed and recreated the VPN 3 times

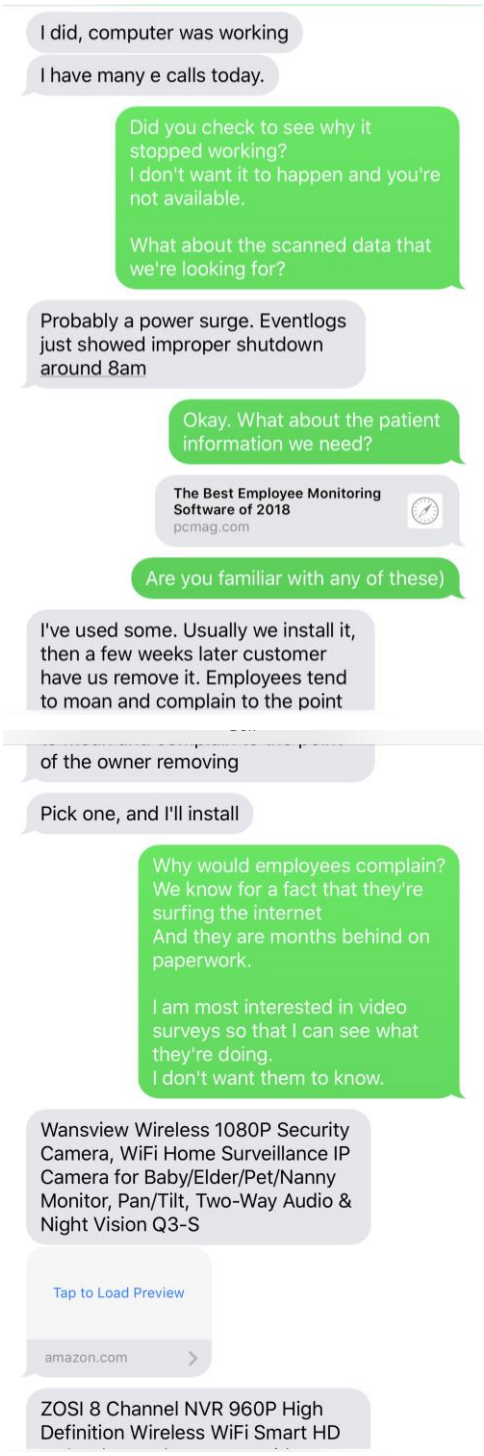

Please see what can be done. Thank you
Honestly, I think the data is there. Just in the location that chiro support knows about
Does not know about
That's what I am hoping. Someone has to care enough to find it.
I'll go to office and call chiro again. The last tech there did not seem helpful. And I don't know what it is exactly they need
Okay
Sat, Jul 7, 11:26 AM
Did you go back to the office to find the records?
Sat, Jul 7, 12:37 PM
They close early on Friday. I'm going next week. Monday
Okay. Thank you.
Sat, Jul 7, 3:32 PM
What time will you be there on Monday? Dr. Ruja is panicking because we need this information.
Mon, Jul 9, 6:00 AM
What time will you be at the clinic today?
They cannot do reports or authorizations. Each day, we continue to lose money because there are deadlines. If the authorizations are not done by specific dates, we won't get paid...no matter what.
We're already suffering from lost revenue.
This is crucial for us.
Thank you
Mon, Jul 9, 8:09 AM
I understand. Itll be today afternoon.
Please. Thank you

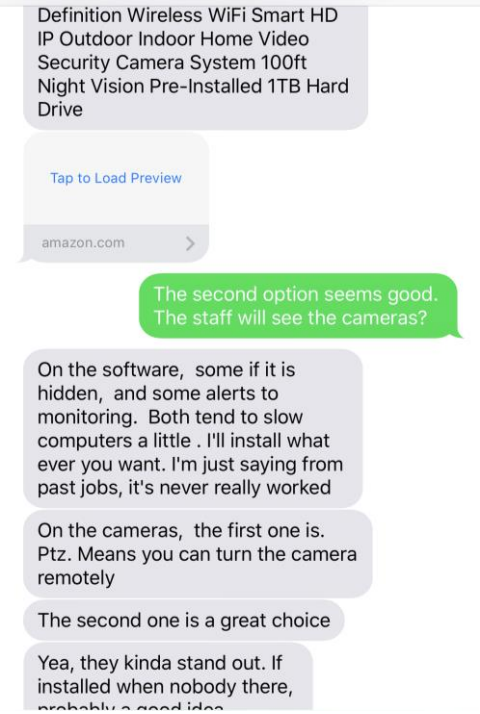

QB is a lower priority right now. Our patient data loss is a crucial blow. There is no way that we can get paid without the records.
I am devastated beyond words. What was the point of doing backups if we're not protected in our current situation?
We have a legal responsibility to provide records to the attorneys and insurance companies.
Text from Josette:
It was already on the computer. I just switched the file from 2015 to 2016. The program was already on the server we just barely started using it. U might just need to call quickbooks tell them what happened and that u need them to walk Don thru getting it back up. Or they might just send a new link.
Wed, Jul 11, 3:53 PM
Don, nobody knows how to access the folder that you've been refers
The data for ChiroTouch was scanned and shredded.
I was not aware that anyone rushed you to the point of asking you to skip crucial steps, such as imaging the crypto ed server.
We have no other options. We relied on your back ups to help in these situations.
We have serious cases that we cannot settle unless we get those records to attorneys. We can not "Re-create" anything. We don't have records (or the manpower even if we did have records).
We need your help to find a solution.
There is too much on the line to leave this unresolved.
Thank you
What about the scan folder that documents were scanned into?
Don Kingery
There are gigabytes of scanned


Don Kingery
There are gigabytes of scanned files. Perhaps the data is there and just needs to be re organized/ re inputted to Chirotouch
DK
What do we do about these gigabytes of data?
Don, how would you proceed in our circumstances if you had thousands of dollars depending on your ability to access patient data?
We are relying on you as the expert. We don't have IT experience, which is why we hired you.
We need to find solutions. We are a small practice and can not afford to lose this money.
Can the gigabytes of scanned files be searched by names?
Has anyone reviewed this data to see what it is?
Don Kingery
I need someone who knows what
1 028 536 727
Pass = 7vg3m6
This will allow you to log in from anywhere in the world, including the international space station, should you find your self there :)
DK
Wed, Jul 11, 9:01 AM
Good morning Don. I have been texting you since Monday afternoon to get an update on the data for ChiroTouch.
We lose money each day that we are unable to access the data.
Because of insurance deadlines, we cannot bill for these dates of service later. This money will be lost forever.
Please let us know if you have been able to restore the data to the patient's files.
We also need to restore Report Master to the multi-user status that we previously had.
Thank you
Don Kingery

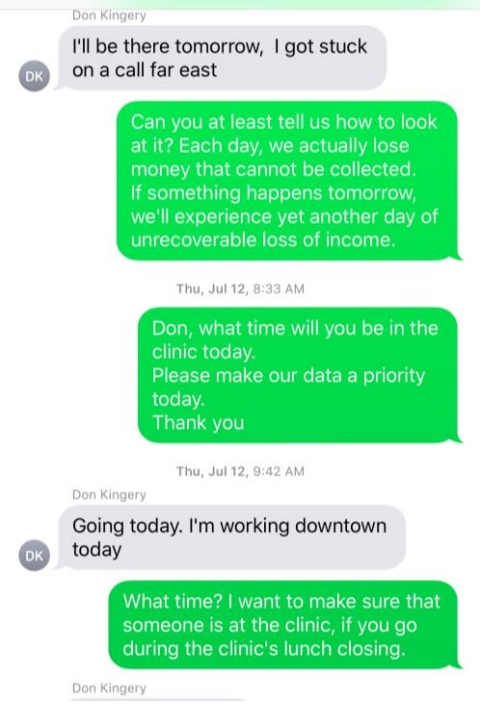

Thank you very much🙏
Marius Ruja
MR
God Bless YOU!🙌
Wed, Jul 11, 3:34 PM
Any updates on the data in the folder?
Yran Carlos
Nothing yet
YC
He hasn't come in yet
Yran, have you tried looking in the folder that Don mentioned.
I though that was going to addressed when Don came on Monday. We've discussed the fact that this file has data before.
Yran Carlos
There is a separate folder that I don't remember how to get to that I think is where the back up is
YC
Okay. Hopefully, that matter will be resolved today.
Wed, Jul 11, 3:53 PM
Don, nobody knows how to access the folder that you've been refers to.
I thought that you were going to look at it Monday when you went.
Apparently, this folder is our only hope. We keep talking about it but no one has taken the time to look in it.
Sat, Jul 14, 10:37 AM
Yran's computer went off and won't come back on.
Pull power cord from back off. Wait. Wait. Wait. Plug back in. Try to turn on
Sometimes power supply hangs up from power surge. Powering off releases.
Also check power strip and other devices. If many devices are off, then power strip, breaker or power in city is out
Dont laugh. I've had Customer call

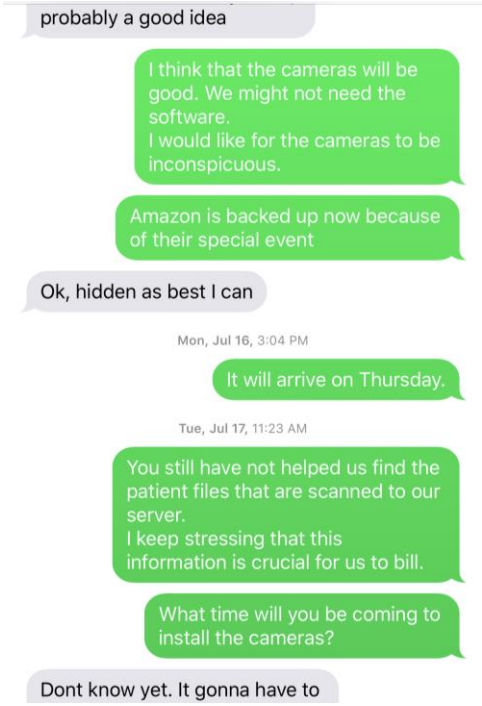

Wait. Wait. Plug back in. Try to turn on
Sometimes power supply hangs up from power surge. Powering off releases.
Also check power strip and other devices. If many devices are off, then power strip, breaker or power in city is out
Dont laugh, I've had Customer call about computers not turning on. After 20 min of talking, they also say the lights are out. Turns out there was a power outage
1:22 PM
Did that work?
I sent you two other texts. There was no power outage. Everything else
I was out of service, driving no signal
She says that everything is working in that area, except the computer. She has tried restarting the computer.
She has tried restarting the computer.
What else would you suggest?
Do you have any other suggestions? This is another day of lost revenue. Trans computer is the only one with any scans in them.
If unplug and checking power no fix. Probably a bad power supply
With recent thunderstorms, I've been replacing power supplies
I have a power supply, but can go till Monday
She has already left for the day. What we do to be ready on Monday
Thank you. We really lost a lot again today.
Just be open, I'll make it my first call
I would really appreciate it.


I did, computer was working
I have many e calls today.
Did you check to see why it stopped working?
I don't want it to happen and you're not available.
What about the scanned data that we're looking for?
Probably a power surge. Eventlogs just showed improper shutdown around 8am
Okay. What about the patient information we need?
The Best Employee Monitoring Software of 2018
pcmag.com
Are you familiar with any of these)
I've used some. Usually we install it, then a few weeks later customer have us remove it. Employees tend to moan and complain to the point
of the owner removing
Pick one, and I'll install
Why would employees complain? We know for a fact that they're surfing the internet
And they are months behind on paperwork.
I am most interested in video surveys so that I can see what they're doing.
I don't want them to know.
Wansview Wireless 1080P Security Camera, WiFi Home Surveillance IP Camera for Baby/Elder/Pet/Nanny Monitor, Pan/Tilt, Two-Way Audio & Night Vision Q3-S
Tap to Load Preview
amazon.com
ZOSI 8 Channel NVR 960P High Definition Wireless WiFi Smart HD


Definition Wireless WiFi Smart HD IP Outdoor Indoor Home Video Security Camera System 100ft Night Vision Pre-Installed 1TB Hard Drive
Tap to Load Preview
amazon.com
The second option seems good. The staff will see the cameras?
On the software, some if it is hidden, and some alerts to monitoring. Both tend to slow computers a little . I'll install what ever you want. I'm just saying from past jobs, it's never really worked
On the cameras, the first one is. Ptz. Means you can turn the camera remotely
The second one is a great choice
Yea, they kinda stand out. If installed when nobody there,


Don Kingery
I only opened a few, looked like scans of body reports
Thu, Jul 12, 4:38 PM
Don, are you available yet?
Thu, Jul 12, 6:07 PM
Don, it's been more than three hours.
Fri, Jul 13, 11:25 AM
Don, I know that you're busy but we are dealing with a major crisis.
Please make it a priority to help us deal with this without losing more than we already have.
We also need to make sure that we are protected in the future.
Don Kingery
I'll call shortly.
Thank you.
Mon, Jul 23, 10:03 AM


Don Kingery
I'll be there tomorrow, I got stuck on a call far east
Can you at least tell us how to look at it? Each day, we actually lose money that cannot be collected.
If something happens tomorrow, we'll experience yet another day of unrecoverable loss of income.
Thu, Jul 12, 8:33 AM
Don, what time will you be in the clinic today.
Please make our data a priority today.
Thank you
Thu, Jul 12, 9:42 AM
Don Kingery
Going today. I'm working downtown today
What time? I want to make sure that someone is at the clinic, if you go during the clinic's lunch closing.
Don Kingery


probably a good idea
I think that the cameras will be good. We might not need the software.
I would like for the cameras to be inconspicuous.
Amazon is backed up now because of their special event
Ok, hidden as best I can
Mon, Jul 16, 3:04 PM
It will arrive on Thursday.
Tue, Jul 17, 11:23 AM
You still have not helped us find the patient files that are scanned to our server.
I keep stressing that this information is crucial for us to bill.
What time will you be coming to install the cameras?
Dont know yet. It gonna have to

You have to run wiring for wireless? If you have to send a cabling guy, it is probably outside our budget.

We have to think low budget. Our staff's lacksdaisacal attitude has put us in a financial vice. The computer hack and resulting problems have only made it worse.

Wireless world be cheapest, but won't last as long. A few years, 3 maybe 12 years.

Let me get some numbers on costs

We're not even going to last more than three years. The Titanic is hitting the iceberg soon.

Don't spend too much time. Just find the cheapest, yet effective method?

Nanny cams?

Mon, Jul 16, 12:06 PM

You said that you would be going to

Please tell me where to find the folder to look for our scanned patient files
Thank you

Wed, Jul 18, 9:04 AM

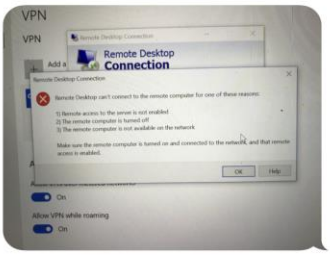
Our billing company still cannot print the notes that aré needed for billing our claims.
This is another step that is causing a cash flow problem.
Our billing is more than a month behind and will take weeks to get paid, after the claims are actually able to be transmitted.

I fixed it lastnight

Lots of little things to to go back into place as we get everything backup and working

Monica tried printing this morning and still cannot print.

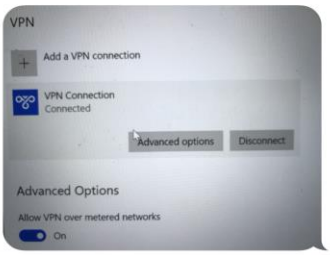
Wed, Jul 18, 11:18 AM



VPN has to be connected first

Then use the new remote desktop icon

I did.



I was trying to access yahoo mail and this screen popped up. I can't get out or close it.

Not good

That's how crypto gets in

Log off, dont close screen. Need to go to start then log off

Something was showing that it was downloading on the bottom of the screen.
I don't know what it was.

I'll log in

Thank you

Thu, Jul 19, 4:07 PM

We still have unresolved issues:

QuickBooks software cannot be accessed,

Cannot find files that were scanned to server. They should have been a

I'll log in

Thank you

Thu, Jul 19, 4:07 PM

We still have unresolved issues:

QuickBooks software cannot be accessed,

Cannot find files that were scanned to server. They should have been a part of your standard backup.

Have you checked to make sure that ChiroTouch files are actually being backed up properly, so that we do not find ourselves in a bind again?

Wed, Jul 25, 10:33 PM

What's happening with QuickBooks? I can't login

Thu, Jul 26, 7:23 AM

What happened with QuickBooks?

I'll need to call back. Later. When you can, please call them and add me to contacts. Itll make this go quicker.

I will

Don,
I have added you as a contact.
Please call QuickBooks and give the following information:
Don Kingery
dkingery@elp.tech

Business address:
4437 Lazy Willow Dr.
ELP, TX 79922

License # 827886913356108
Thank you

Case # 525106326 for reference

Wed, Jul 25, 1:54 AM

Don Kingery

Ok, thanks

Thu, Jul 26, 7:23 AM

What happened with QuickBooks?
I gave you the information yesterday morning but I have not heard from you.
I tried logging into QuickBooks, but it still has the same installation problem.
We are months behind on getting documents to the banks that are requesting them.
Please let me know what the status is.
Thsnk you

I'm working with QB support to fix

Great. Thank you

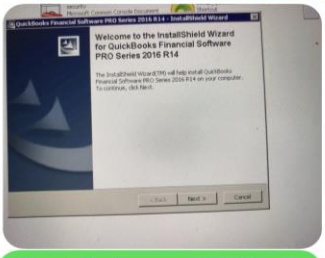
Thu, Jul 26, 9:46 AM

I also need the network details that I asked you for yesterday. Yran still cannot connect to Monica's network.

Thu, Jul 26, 2:38 PM

The password is " BlueBird#123 "

before?



When I tried to open QuickBooks

I can install Adobe, I'll see if I can find a copy of office

I tried to install QB, but its crashes. Could be compatibility issue. The newer versions of QB don't work on older operating systems. I'm still researching

So, we can't use QB?

Try clicking next, see if it installs.

Would calling tech support work?

Would calling tech support work?

It was giving error

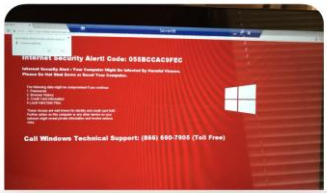
Also, that's incorrect version, there is 2018

2016 installed and worked. But someone said it was too old, and gave a link for newer version

I clicked next but didn't finish because I didn't want to do anything wrong without asking.
I thought that it was already up and running since we upgraded

Try the newer version

I only see icons for 2016



Can't this be resolved with QB tech support?

Don Kingery

Maybe. But they won't help me. I'm not the owner. I dont have account info

DK If you want to call and authorize me, add to support contact

Okay. Then you can conference me in when you call.

Don Kingery

DK Ok, I'll call tomorrow

Okay. I can add you but it's better if you conference me when you're ready. I think that they have 24 hour support

Don Kingery

DK On the user data, most everything is in the share folder. And there is some other data in a folder C:\data

They sent you an email, forward it

On monica, I installed drivers. Should have worked, but did not. May need to reboot server

I'll log in and load more print drivers, and reboot

Also look for a folder called restore in C drive

I'm looking for files in the server. Most are very old. One doc would not open

May need Adobe reader and office installed in order to open files documents

Under restore file, share folder is empty.
I see report master files, but we need the scanned patient files in order to create report master reports.

Will you be installing Adobe or Office?
Did it get uninstalled?
How were we able to open files

Don Kingery

DK I need someone who knows what data is relevant, and knows where it should go.

Yran Carlos

YC Don if you send me the folder where the back up info is at I can start looking thru it

That would be Yran or Maria. Would you please go to the clinic today to begin the process of identifying the data?

Don Kingery

Data can be organized by date. I dont think it can be searched by name.. although, when the data was saved it looks like they used humans names, and not just random numbers. So, looks like search by name can be done

DK I'll stop by.

Yran Carlos

YC Ok thank you

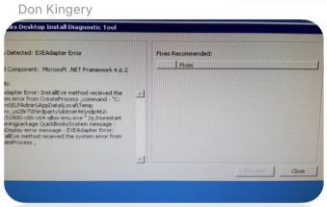
Thank you very much 🙏

DK They sent you an email, forward it to me when you can. Ot should contain a tool I need to fix QB install error

DK It may speed things up if you call QB and add me as a tech contact. They wore hesitant on helping me. I had to convince the to send you the fix. They definitely wore not going to send it to me

I just emailed you

Don Kingery



The tool says no fix for this error.

DK I'll need to call back. Later. When you can, please call them and add me to contacts. Itll make this go quicker.

Don Kingery

After 2, maybe 230

DK I may go next, if I finish this call soon

We would be grateful.

Yran Carlos

YC Also Monica just messaged that she can't get into chirotouch

Don Kingery

DK Its asking for serial number, someone gonna need to call chiro to get that number

Thu, Jul 12, 2:52 PM

What is the information in the files that you have mentioned?

Don Kingery

DK I'll call shortly, with Customer.

Please do. Thank you.

Don Kingery

I only opened a few, looked like scans of body reports

Please take care of everything today,

Including

QuickBooks

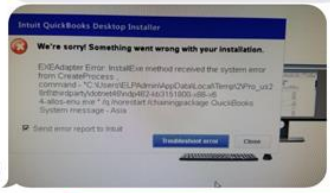
Scanned patient data.

Thank you

Tue, Jul 24, 11:26 PM

Don Kingery

Quickbooks will not install on server. QB2018 may not be comparable with server 2012. May want to install on a different computer



DK

Mon, Jul 23, 10:03 AM

Good morning Don.
Yran can't access the server and Dr. Ruja can not access Report Master. Please go to the clinic and help resolve this morning.

Without access to the server, we will have even more delays in our billing which affects our cash flow. We have already experienced a major setback because of the hack.

Also, we still need to find the folder that has the scanned patient files. We need this information to do authorizations and reports for insurance billing.

Also, we still need to access Chirotouch. Please help us resolve all of these problems. This has been lingering for weeks even though we keep asking for help.

Thank you

Don Kingery

I'm out of town. Trying to make it

I'm out of town. Trying to make it back today. I'll see if I can remote in to look

Thank you

Marius Ruja

Please 🙏

Tue, Jul 24, 11:30 AM

Don, the issues still have not been resolved.
We continue to have delays each day. Some of this revenue will never be recovered.

Don Kingery

Going today. I'm in town

Please take care of everything today,

Including

QuickBooks

Scanned patient data.

Wed, Jul 25, 2:15 PM

Don,
The login Instructions that you emailed me in June is the administrative login credentials, right?

Don Kingery

Yes

Thank you

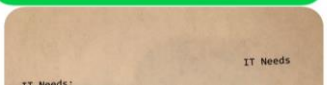
Don Kingery

The user Administrator is disabled for security reasons. ELPAdmin is equal

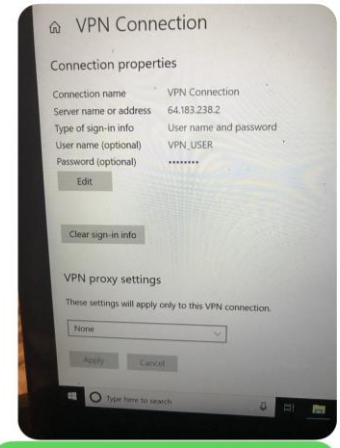
Thank you

Wed, Jul 25, 4:18 PM

Don,
Please provide me with the information requested in this note.
Thank you



each camera



I'm trying to set up the VPN vine tío It I do not see how to put in password to text.
I do not see the computer icon in task bar but I found VPN under available networks.

Apply

Thu, Jul 26, 1:28 PM

Yran, have you been able to connect to the billing software yet? Has Don contacted you?

Yran Carlos

No not yet.

Fri, Jul 27, 7:16 AM

Good morning Don. Monica's IT person was finally able to get Yran connected to their server.

We still have pending tasks that you have not resolved for us.

You have promised to take care of QuickBooks, but I have not received a response to my numerous texts to you.

Marius Ruja

Don !!!! Show dome LOVE! Pleaase care of Mrs. Ruja.... she just had surgery 3 weeks ago. She doesn't need more stress.
Thank you

From: *Anthony Sullivan <anthony.sullivan3@yahoo.com>*
To: *"karenruja@sbcglobal.net" <karenruja@sbcglobal.net>; Monica <monica@arbillingcompany.com>*
Sent: *Tuesday, July 24, 2018 1:10 PM*
Subject: *IT Support*

Good afternoon Ms. Ruja,
Monica has told me about your concerns regarding your ePHI processing systems. While helping Monica configure her VPN connection to not use the remote gateway, so her internet would work while connect to your VPN, noticed some very serious security related issues on your system.
I was able to open the registry editor, open a command prompt with elevated privileges, able to see all file shares, drives, and network computers. Your system as it is configured now is WIDE OPEN and exploitable. I have attached the Security Technical Implementation Guide or STIG's for ePHI systems that we implemented at AR Billing Company. We can implement these exact same controls on all your servers and workstations; it is a requirement to do this.
The security controls lock down the systems in accordance with Federal Regulations set forth by the HIPPA/HITECH/MACRA Act. Additionally using Microsoft VPN is not as secure as using the FortiGate Security Solution.
I left my phone at Monica's office yesterday; I will be in El Paso tomorrow to retrieve it. If you would like to meet, schedule an appointment with Monica. I look forward to working with your TEAM as we secure your network and optimize network performance.
Best regards,
Anthony Sullivan, MCP, CISSP
(915) 549-6810

Karen Ruja <karenruja@sbcglobal.net>
Jul 24 at 4:21 PM
To Anthony Sullivan
CC Ruja Health

Mr. Sullivan,
Thank you very much for your feedback about the vulnerability of our network. I am in PHX, but my husband (Dr. Ruja) and our receptionist (Yran Carlos) will be in the office tomorrow. Please call Dr. Ruja at 915-494-4468 or Yran at 915-521-2020 to schedule an appointment with you.
Thank you,
Mrs. Ruja

Karen Ruja <karenruja@sbcglobal.net>
Jul 27 at 9:22 AM
To Anthony Sullivan

Good morning Anthony. I am authorizing you to use forensic tools in order to reset administrative passwords.

As far as I know, there are not software DVDs anymore. Our IT had to contact tech support for each software company, in order to reinstall all software.

Thank you

From: *Anthony Sullivan <anthony.sullivan3@yahoo.com>*
To: *Karen Ruja <karenruja@sbcglobal.net>; Monica <monica@arbillingcompany.com>; Monica Velasquez <mvelasquez2@elp.rr.com>; Pat Saxman <pat@arbillingcompany.com>*
Sent: *Friday, July 27, 2018 9:17 AM*
Subject: *Re: Authorization to Reset Passwords*

Good morning Ms. Ruja,

In accordance with the HITECH Act of 2013 we have executed a Business Associate Agreement.

I will coordinate with your husband and work around his schedule.

AR Billing will provide you with a scope of work for those action plan items which must be resolved immediately. Short version is, I will reset the password, perform an analysis of the HDD, if evidence of any nefarious activity is found, we will proceed in accordance with rules and regulations set forth by the HITECH Act of 2013.

Yran's computer has already been upgraded to Windows 10 Pro, the use of Network Level Authentication and ability to audit user logins is a requirement, which means we will need to deploy Active Directory Services and perform a DCPROMO to your existing server to make it a Domain Controller.

Each Windows 10 Home computer can connect to the Microsoft Store for the purchase of an upgrade license for $99, upon completion of the transaction, the operating system upgrades automatically in about 20 minutes.

Please give me some time to pull all this together into a nice concise executive brief, analysis of the current HDD will tell us the real story.

Best regards,

Anthony

From: *Anthony Sullivan <anthony.sullivan3@yahoo.com>*
To: *Karen Ruja <karenruja@sbcglobal.net>; Monica <monica@arbillingcompany.com>; Pat Saxman <pat@arbillingcompany.com>*
Sent: *Friday, July 27, 2018 3:20 PM*
Subject: *Re: ChiroTouch Re: Anthony Sullivan, your appointment is confirmed*

Good afternoon Ms. Ruja,

Yes I did, have discussed the matter with Monica, and we both feel that an analysis of the HDD needs to be done first. We would prefer to comment with facts instead of educated guesses, everything may be as he said, so we are going to verify.

We will know by this time tomorrow, fear not, your are in good hands.

My hobby is painting 24 x 30 Oil on gallery canvas, "Yeshua"

Best regards,

Anthony

On Friday, July 27, 2018 03:51:47 PM,
Karen Ruja <karenruja@sbcglobal.net> wrote:

Thank you for your prompt attention to this matter.

Did you see my email about my questions regarding Don Kingery?

From: Anthony Sullivan <anthony.sullivan3@yahoo.com>
To: Monica <Mvelasquez2@elp.rr.com>; Karen Ruja <karenruja@sbcglobal.net>; Pat Saxman <pat@arbillingcompany.com>
Sent: Saturday, July 28, 2018 7:52 PM
Subject: re AOWC Ruja update

Good morning Ms. Ruja,

Monica, have configured Ms. Ruja's mobile unit, had to uninstall multiple competing products before FortiClient would load.

All loaded, updated and configured, showed her how to login, and was in the process of rebooting her computer to apply critical updates, when KABOOM.

Massive lightning strike, poof, no power, no internet for a couple hours.

Ms. Ruja, this is the state of your network at this time, and the steps that will be taken to fix compliance and security related issues.

Currently your server is loaded with Server 2008 R2 without Service Pack 1 (SP1)

1. Without SP1 the server is exceptionally vulnerable a host of well documented exploits,
2. Without SP1 FortiClient will not load because of inherent vulnerabilities.
3. Without SP1, .NET 4.6.2 can not be loaded which in turn means QB-2018 will NOT load.
4. Currently the server as configured, does NOT meet the minimum standards mandated by The HITECH Act
5. 5 workstations need to be upgraded to Windows 10 Pro before they can join the AOWC.local domain.
6. Deployment of a Domain Controller with Audit Trails and login restrictions are REQUIRED by The HITECH Act

Proposed plan of immediate action to fix regulatory deficiencies and gross security related issues.

7. Immediate upgrade of 5 workstation to Win 10 Pro via Microsoft Store, cost $99 per machine, purchased online directly from Microsoft.
8. Immediate installation of SP1 to fix critical security related issue on the Server 2008 R2 operating system
9. Installation of .NET 4.6.2 and cumulative security rollup in preparation for installing QB 2018
10. Installation of QB2018.

Recommended path forward based on observations and limited available resources

- Purchase QTY 2, 500GB or better HDD's, 1 drive will be a dedicated backup drive, backups will run twice a day
- Purchase QTY 1, 2TB or better mobile USB External HDD for backup transfer for storage OFFSITE
- Deploy employee monitoring system for acceptable computer use policy enforcement.

- Deploy Web Filtering, Content Filtering and Organizational Unit desktop lockdown policies.
- Enforcement of HITECH Act ePHI processing regulations, policies and procedures.
- Install Server 2016 R2, Remote Desktop Services, Active Directory Services and Windows Backup on the new drives.
- Migrate and transfer DATABASE from SERVER08 to new AOWC Domain Controller 1 on the AOWC.LOCAL domain
- Create OU users, assigns rights and lockdown the server in accordance with The HITECH Act Security Technical Implementation Guides, (STIG's) for short.
- Purchase a FortiGate 30E WiFi with security bundle and subscriptions from Amazon Prime for $399,00.

Fortinet FG-30E-BDL FORTIGATE-30E HW PLUS 1YR 8X5 FC & FG BNDL

https://www.amazon.com/Fortinet-FG-30E-BDL-FORTIGATE-30E-PLUS-BNDL/dp/B016TSL8HA/ref=pd_lpo_sbs_147_t_0?_encoding=UTF8&refRID=7Q4D0VMQDGS8Z33X0B7W&th=1

Jul 29 at 7:53 PM
Good evening Ms. Ruja,

Started the AOWC HITECH Act Compliance initiative today.

- Upgraded all production workstations Windows 10 Pro
- Upgraded Office 2007 to Office 2010 Pro + on all workstations Installed Softros Lan Messenger on all workstations
- Installed Disk2VHD and created VHDD images of all workstation for disaster recovery.
- Installed VNC for remote support and surveillance
- User Access Control implemented on all workstations
- Require Ctr,Alt,Del to login,
- Edited Registry and set keys for a login banner SECURITY WARNING
- Edited HOST file on all workstation to block, Facebook, YouTube, Ebay, Netflix, Hulu, Instagram

- Analysis of \\SERVER08 has revealed that the software is NOT GENUINE,
- Unable to install Service Packs, Updates and Security Cumulative Rollups because it is fake software.
- Analysis of \\REPORTMASTER revealed exceptionally unproductive information process behavior
- logs reveal that approximate, 3 out of every 4 hours is used for Facebook, YouTube and EBay activities,
- furthermore, analysis of \\PP and \\Frontdesk_2 indicate similar unproductive information processing behaviors

Before any user can login they must acknowledge by clicking okay. It is expected that end-user are going to test barriers, tomorrow when they go to Facebook and YouTube, the page will not come up. On Tuesday when they try to go to Facebook, YouTube, Ebay, the AWOC Acceptable Computer Use policy will display so that enduser can refresh their memory on what they agreed to login in. The 3rd time a violation occurs a formal counseling document MUST be done, informing the Enduser they are in violation of the AOWC Acceptable Computer Use Policy. The violation after that will be bundled with evidentiary VIDEO support via VERIATO 360 in preparation to debunk a Texas Workforce Commission investigation.

SECURITY WARNING

This computer system is the property of Alpha & Omega Wellness Center. All activity on this system is monitored. Users have no personal privacy rights to any materials or activities on this system. Alpha & Omega Wellness Center complies with all State and Federal law regarding legally protected confidential information. Unauthorized or improper use of this system my result in disciplinary actions and/or referral to appropriate law enforcement agencies. Using streaming video, social networks, gaming and pornographic sites is STRICKLY PROHIBITED and subject to immediate dismissal. By use of this system user indicates awareness and consent to these terms.

CLAIM # DHX3803 Email Thread

Anthony Sullivan <anthony.sullivan3@yahoo.com>

Aug 15 at 3:57 PM

To Karen Ruja Monica
urgent Re: CLAIM # DHX3803

Afternoon,

Do not forget that attorneys also take 33 % of any moneys, I have a check list of stuff and most of it is providing loss of income, expenses incurred during recovery, please DO NOT just copy my tiny paragraph, the adjuster is liable to use that instead of letting me do my due diligence.

Please do not rush this; it is an insurance tactic to take advantage of the insured so that they do not take a big hit. It is the adjusters job to pay as little as possible, it is our job to document loss and expense, Monica tells me she gave you some preliminary numbers for certain aspects of the incident.

We just need some time to do document this please; we have been concentrating on restoring services, upgrading systems and securing the network. I am exhausted, Monica will be out of town all next week, and I just plain need time to get this done. Please understand that we are talking about 15 or 20 hours to document this debacle, basically my entire weekend, family will not be happy with me.

Best regards,

Anthony

From: Karen Ruja <karenruja@sbcglobal.net>
To: Anthony Sullivan <anthony.sullivan3@yahoo.com>
Sent: Wednesday, August 15, 2018 2:12 PM
Subject: Re: CLAIM # DHX3803

Thank you Anthony. May I just copy and paste the paragraph that refers to the VOIP system and terminal server to send to the new adjuster who has been assigned?

The attorney has been in contact with me and requested the complete commercial policy. I emailed the complete policy to him yesterday. He has advised me that he will give me some guidance buy his firm will probably too expensive to represent us. The fees at his firm range from $550.00 per hour to $850.00 per hour. H partner referred me to him because he is the lower billing partner. He will refer us to another, more affordable firm, if necessary.

From: Anthony Sullivan <anthony.sullivan3@yahoo.com>
To: Karen Ruja <karenruja@sbcglobal.net>; Monica <monica@arbillingcompany.com>; "KSHEIKH@travelers.com" <KSHEIKH@travelers.com>
Sent: Wednesday, August 15, 2018 6:03 AM
Subject: Re: CLAIM # DHX3803

Good morning Ms. Ruja,

It is going to take at least 3 days to compile, author, edit and publish the "Cyber Threat Intelligence and Incident Response Report, and that is assuming we do nothing else. Additionally, Monica and I need to provide a current expense report and forecast of future expenses to remediate incident response report findings.

You can inform the insurance company that the VoIP system and Terminal Services provided the entry points for various exploits associated with SLINGSHOT, APPLE SCRIPT, and BUSY BOX. The file server appears to have been exploited to mine Crypto Currency as part of a BOTNET. That is the short version of a long string of events that culminated in an unbootable server, the situation was made worse by a computer technician who panicked, in an attempt to restore services.

Ideally it is our hope that the insurance company will afford us the time to produce an acceptable document that will meet their needs, explain what happened, provide details on what was done to remediate the findings, the new detailed security protocols that have ALREADY been implemented, and deployment of specialized tools such as Veriato 360, FortiGuard Security Fabric Solution with locked down desktops/servers.

Perhaps if we provide everything they need as fast as we can they will reciprocate with a fast timely reimbursement for this "BUSINESS INTERUPTION", this is not just about a server that crashed, it is mostly about the BUSINESS INTERUPTION, I want us to keep focused on that fact.

Best regards,

Anthony Sullivan

9(915) 549-6810

From: Karen Ruja <karenruja@sbcglobal.net>
To: Anthony Sullivan <anthony.sullivan3@yahoo.com>
Sent: Tuesday, August 14, 2018 8:57 AM
Subject: Re: CLAIM # DHX3803

Thank you.. Safe travels.

From: Anthony Sullivan <anthony.sullivan3@yahoo.com>
To: Karen Ruja <karenruja@sbcglobal.net>
Sent: Tuesday, August 14, 2018 6:16 AM
Subject: Re: CLAIM # DHX3803

Morning,

Got it, will work on this tonight, traveling today.

Best regards,

Anthony

From: Karen Ruja <karenruja@sbcglobal.net>
To: Anthony Sullivan <anthony.sullivan3@yahoo.com>
Sent: Thursday, August 9, 2018 3:24 PM
Subject: Fw: CLAIM # DHX3803

----- Forwarded Message -----
From: "Sheikh,Kamran" <KSHEIKH@travelers.com>
To: "KARENRUJA@SBCGLOBAL.NET" <KARENRUJA@SBCGLOBAL.NET>
Sent: Thursday, August 9, 2018 2:21 PM
Subject: CLAIM # DHX3803

Mrs. Ruja,

Per our conversation please E-mail documents and/or contact information of the IT tech whom we can contact to determine cause of loss that resulted in computer server crash. Also, please confirm the loss date and any reason for the late reporting?

Thank you

Kamran Sheikh | **Claim Professional**

P.O. Box 650293

Dallas, TX 75265-0293

W: 281.606.7042 F: 877.749.0075

Anthony Sullivan <anthony.sullivan3@yahoo.com> Aug 29 at 9:02 AM

To Karen Ruja Monica admin@arbillingcompany.com

Good morning Ms. Ruja,

No she has not, plus Monica and I are still compiling the billing, we are going as fast as we can, I will send you a copy of the RECOVERY report shortly, I have to login to your server to compile it and save as a PDF.

Best regards,

Anthony

From: Karen Ruja <karenruja@sbcglobal.net>
To: Anthony Sullivan <anthony.sullivan3@yahoo.com>
Sent: Tuesday, August 28, 2018 5:47 PM
Subject: Travelers Claim

Has Josette sent the numbers to you yet?

Anthony Sullivan <anthony.sullivan3@yahoo.com>

Aug 22 at 8:32 AM

To JRReisinger@FBI.Gov Karen Ruja Ruja Health
Notification: WorldCry@Cock.Li attack, Alpha & Omega Wellness Center
Attachments: AOWC Cyber Incident Threat Response Intelligence Report.pdf

Good morning SSA Reisinger,

It was a pleasure to work with your associates yesterday.

On June the 8th, 2018 Friday afternoon, WorldCry Cryptoworm exploited MS17-010 vulnerability; refer to Indicators Associated With WannaCry Ransomware the payload dropper executed at 9:03 am on Saturday June 9th, 2018.

Attach is a rough draft cyber incident report.

POC's

Alpha & Omega Wellness Center

2630 Montana, El Paso, TX

Office 915-521-2020 Dr. Ruja 915-494-4468, Karen Ruja 915-494-1503

Yran Carlos 915-929-5879, Anthony Sullivan 915-549-6810

Alpha & Omega Wellness Center

Cyber Incident Threat Response Intelligence Report

Fortinet Security Operations Solution

Description of the measures put in place to identify the adversary's future activities related to the applicable intrusion phase. Policy defined and deployed, indicators and signatures, additional sensors or instrumentation, security event data monitors, deployed.

Deny

Fortinet security operations solution deployed.

Disrupt

Fortinet intrusion detection system and advanced artificial intelligence analysis.

Degrade

All unnecessary ports are blocked by FortiGate policy.

Deceive

Umbutu Linux BitNinja Honey Pot

Destroy

No offensive actions have been taken at this time.

Intrusion Campaign Analysis

Rafael Amado
More From This Author

On 12 May 2017, as the WannaCry ransomware spread across computer networks across the world, a variety of explanations also began to worm their way through the information security community. Who was responsible for the WannaCry campaign? And what was the objective? Ransomware suggested it was the work of cybercriminals, although, given the sheer scale of infections and disruption, some commentators suspected the hand of a nation state. Despite relentless analysis from the security research community that has brought fragments of new information to the fore, no consensus has yet been reached on an attribution for the campaign.
One of the most recent theories put forward rests on a possible connection between WannaCry and the Lazarus Group, an actor that has previously been linked with several high-profile network intrusions and assessed as highly likely to have some association with the Democratic People's Republic of Korea (DPRK).

Analysis has indicated that WannaCry samples from February 2017 contained a small section of code identical to those used in previous Lazarus campaigns. At the time of writing, however, we assessed there to be insufficient evidence to corroborate this claim of attribution to this group, and alternative hypotheses should be considered. While malware may initially be developed and used by a single actor, this does not mean that it will permanently remain unique to that actor. Malware samples might be accidentally or intentionally leaked, stolen, sold, or used in independent operations by individual members of a group. It is therefore important to consider other factors, such as the consistency of an operation with previous activity attributed to an actor.

Digital Shadows has, therefore, applied the Analysis of Competing Hypothesis (ACH) technique to the information currently available through sources. ACH uses a weighted inconsistency algorithm to assign numeric values – weighted by the assessed reliability and relevance of each data point – to represent how consistent the available evidence is with a given hypothesis. While the aim here was not to provide a conclusive attribution for the WannaCry campaign, this structured analytical technique allows us to assess the reliability and relevance of the data presented thus far, as well as make some tentative assessments over the type of actor most likely to have been behind last week's attacks. As such, we compared four hypotheses for the purposes of this exercise. That the campaign was the work of:

- A sophisticated financially-motivated cybercriminal actor – H1
- An unsophisticated financially-motivated cybercriminal actor – H2
- A nation state or state-affiliated actor conducting a disruptive operation – H3
- A nation state or state-affiliated actor aiming to discredit the National Security Agency (NSA) – H4

Using a mixture of primary and secondary reporting, as well as assessments from Digital Shadows analysts, we have included a collection of the most salient data points to have emerged at the time of writing. As well as the widely-discussed use of the DOUBLEPULSAR backdoor dropper, ETERNALBLUE exploit, and SMB vulnerability, the latter for propagation, we have included several other pieces of evidence to drive our assessment. These are presented in the ACH table below, though some of the more significant points include:

- So-called "kill-switch" probably an anti-sandboxing feature – MalwareTech, who discovered the unregistered domain, now believes this was most likely included as a badly-thought out anti-analysis measure.
- Low number of Bitcoin wallets a result of an unintentional bug – Symantec have reported that the creation of only three Bitcoin wallets for victims to transfer payment into was the result of a bug in the malware's code, referred to as a race condition.
- No evidence that the malware was delivered via phishing emails – IBM X-Force, for example, scanned over one billion emails passing through its honeypots and found no evidence suggesting spam/phishing was the initial infection vector.
- Unconfirmed links to Lazarus Group and North Korean campaigns – Some researchers have now claimed that WannaCry contained pieces of code previously associated with the Lazarus Group, as well as two malware variants (called Joanap and Brambul) used in attacks against South Korean organizations. This connection, however, was assessed to be primarily based on the ordering of ciphers and public libraries used by the Lazarus Group, and inconclusive at the time of writing.

ACH reveals the most plausible scenario is that an unsophisticated cybercriminal actor launched the WannaCry campaign

Figure 1 – ACH diagram

Though by no means definitive, **we assessed that a WannaCry campaign launched by an unsophisticated cybercriminal actor was the most plausible scenario based on the information that is currently available.** While there were numerous data points that were consistent with this assessment, a few stand out:

- Coordination and implementation of the campaign was relatively poor: victims who paid reportedly did not receive decryption keys
- No discernible pattern to the organizations that were targeted
- Only three Bitcoin wallets were created for the receipt of payment
- An inability to monetize effectively
- Failed anti-sandboxing measure and race condition bug

These inconsistencies are not errors we normally associate with a sophisticated cybercriminal operation. The Carbanak (AKA Anunak) organized criminal group, in comparison, are known for conducting highly-targeted, lucrative, and efficient operations relying on the strategic use of social engineering attacks and network intrusions that more resemble the tactics used by Advanced Persistent Threat (APT) groups.

H3 and H4, which posit that the campaign was the work of a state-affiliated actor, also contain inconsistencies:

- If the attacks were aimed to discredit the NSA (H4), then why the lack of a supporting media narrative driving this message home? In the 2016 attacks on the US Presidential election, for example, network intrusions against the Democratic Party and subsequent data leaks were accompanied by blog posts and media commentary critical of Hillary Clinton. Were this to be a nation state campaign intended to cause disruption (H3), we would also expect to see some level of target specification alongside clear campaign objectives.
- During their previous destructive campaigns, the Lazarus Group, for example, have generally displayed a consistent level of geographic targeting – primarily against organizations in South Korea and the US. Specific industries such as media companies, financial institutions and critical national infrastructure have been the main targets of attack, but in the case of WannaCry, infections were widely distributed across the world, and the malware appeared to spread virtually indiscriminately with no control by its operators. Had the attackers used a phishing vector, they would have been able to limit the malware's capability to spread outside a network and instead used spear phishing emails to target selected organizations.

Such tactics would have been more consistent with the activities of a sophisticated criminal outfit or a technically-competent nation-state actor. It is entirely possible that new information will come to light in future that further supports, or even discredits, some of the hypotheses proposed in this exercise.

While attribution may be exciting and fulfill our insatiable desire to put a face to the crime, perhaps what is more important in this instance is reviewing what lessons we can learn from the WannaCry campaign? For this we advise checking out the recent blog from the Digital Shadows Security Engineering Team, which outlines five fundamental and widely used security principles that are reusable across different types of attackers, be it nation-state or petty cybercriminal.

Recorded Future Blog

What Is WannaCry? Analyzing the Global Ransomware Attack
By John Wetzel on May 15, 2017
Key Takeaways

- WannaCry ransomware is a new variant of WanaCypt0r, which uses the ETERNALBLUE SMBv1 exploit to infect connected systems.
- Over 100 countries were affected by the ransomware.
- Three Bitcoin wallets are associated with the WannaCry 2.0 ransomware, which have received almost $26,000 in transfers since the beginning of the latest infection, a small sum considering the scope of damage.
- As of this posting, no money appears to have been moved from the Bitcoin wallets.
- Criminals behind WannaCry piggybacked on publicly dumped Equation Group exploits in an attempt to abuse free tools for easy money.
- We believe the criminals behind WannaCry didn't intend for such a widespread attack, nor did they possess the expertise to properly enable or protect the malware from reverse engineering.
- WannaCry variants that mitigated the kill-switch may have spread over the weekend.

In an attack predicted by cyber security experts for months, a yet unknown actor or actors integrated the EQUATIONGROUP APT exploits leaked by ShadowBrokers in a worldwide ransomware worm attack, infecting tens of thousands of endpoints in a matter of hours.

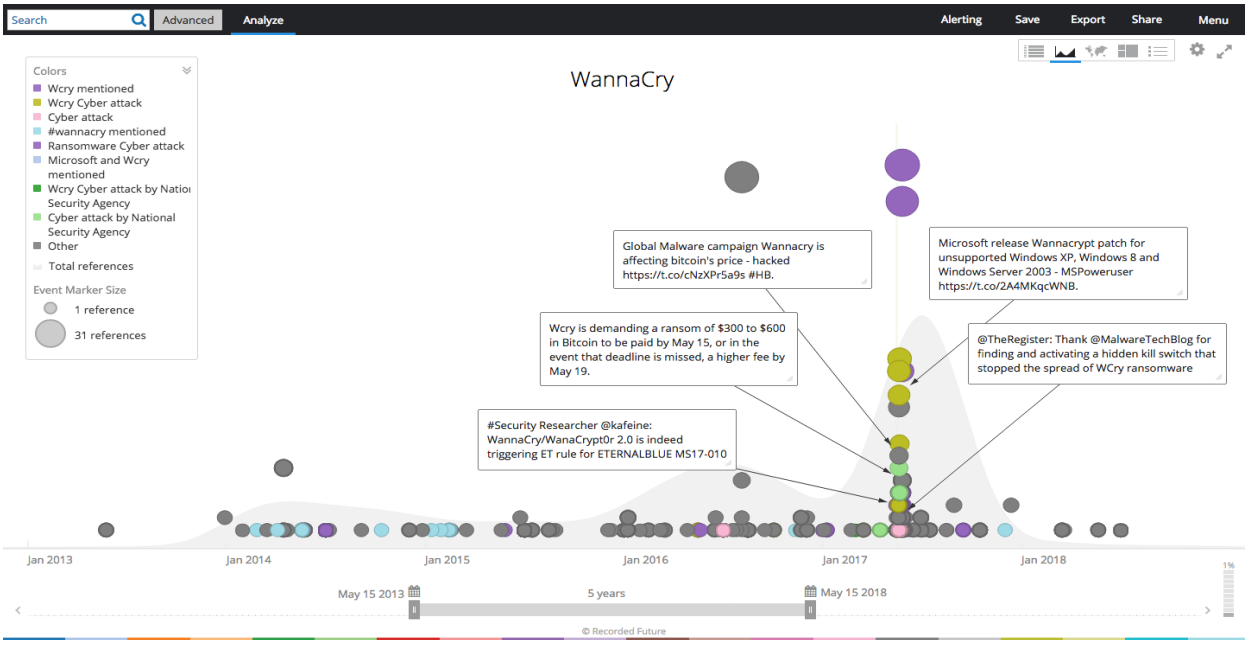
On Friday, May 12, a new ransomware, called WannaCry, began circulating throughout the United Kingdom and Spain, rapidly infecting over 45,000 exposed servers at healthcare, financial, and other business sectors. This ransomware stood out for several reasons, including being the largest ransomware attack in history, and the first widely spread ransomware worm.

The ransomware infection is Version 2.0 of WanaCypt0r (also known as WCry, WannaCry, and WannaCryptor). Unlike previous instances, this version takes advantage of the SMB vulnerability outlined in Microsoft Security Bulletin (MS17-010). This vulnerability was first exploited by the ETERNALBLUE malware, revealed by the ShadowBrokers leak in March, and targeted the Microsoft MS17-010 SMB vulnerabilities. SMB (Server Message Block) is a protocol primarily communicating on port 445 and is designed to provide access to shared resources on a network. Last fall, Microsoft propounded system administrators to disable SMB Version 1 on systems.
According to a FBI FLASH Alert (TLP:White) received by Recorded Future, the WannaCry ransomware infects initial endpoints via a phishing campaign or compromised RDP (remote desktop protocol). Once the ransomware gets into a network, it spreads quickly through any computers that don't have the patch applied. The worm-like capabilities are the new feature added to this ransomware.

During the May 12 attack, two of the most significant targets were Telefonica, the Spanish telecommunications giant, and the United Kingdom's National Health Service. In the United States, the shipping firm FedEx was hit by the ransomware. Infections of the new version of WannaCry started in Spain early on May 12, but quickly spread to the United Kingdom, Russia, Japan, Taiwan, the United States, and many more. In total, almost 100 countries were affected by the attack.

New instances of this ransomware worm dramatically decreased following the activation of a "kill-switch" in the ransomware. A security researcher going by the Twitter handle @MalwareTechBlog noted an unregistered domain (www.iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea[.]com) in a sample of the malware. WannaCry checked to ensure non-registration of the domain at some point prior to infection. According to the researcher, this was likely intended as a way to prevent analysis of the malware in a sandbox. If the domain is registered, WannaCry exits the system, preventing further infection. While this doesn't benefit victims already infected, it does curb further infection. Additionally, according to security researcher Didier Stevens, WannaCry isn't proxy aware, so enterprises utilizing a proxy won't benefit from the "kill-switch."
Further, researchers have been registering a new variant of WannaCry on VirusTotal:
SHA256 – 07c44729e2c570b37db695323249474831f5861d45318bf49ccf5d2f5c8ea1cd
This variant appears to have patched the domain "kill-switch," and was seen actively propagating throughout the weekend, according to our private conversations with security researchers.

Timeline



Starting on March 27, 2016, a security researcher named Karsten Hahn reported the updated version of WannaCry ransomware, and linked to a VirusTotal hash analysis on Twitter: ca29de1dc8817868c93e54b09f557fe14e40083c0955294df5bd91f52ba469c8
Interestingly, reviewing this Intel Card, we can see it's identified as Spora ransomware.

Spora ransomware, which began circulating in January of this year, is a ransomware noted for its sophistication, including top-notch customer support to victims, and was likely created by professional malicious actors.
Research in Recorded Future identified an early warning bulletin on WannaCry published on May 5, 2017 by the Spanish CERTSI (Computer Emergency Response Team for Security and Industry). The CERTSI bulletin cited numerous ransomware attacks using WannaCry targeting on equipment.
On May 12, 2017, around 11:00 AM UTC, reports of the attack began circulating on Twitter. The first mentioned companies were Spanish-based companies, including Telefónica, Vodafone, and Banco Bilbao Vizcaya Argentaria.

It appears Russian cyber criminals were equally perplexed by the WCry campaign as the rest of the world. One of the members of the popular underground community complained about the recently purchased Virtual Private Server (VPS) which was almost immediately infected by ransomware even before the system update was completed.

Bitcoin Wallets
At least three separate Bitcoin wallets, controlled by unknown criminals were identified as part of the ransomware campaign.
As of this writing, little over 15 Bitcoins or approximately $26,000 were deposited to wallets controlled by unknown criminals.

Identified WannaCry 2.0 Bitcoin Wallets

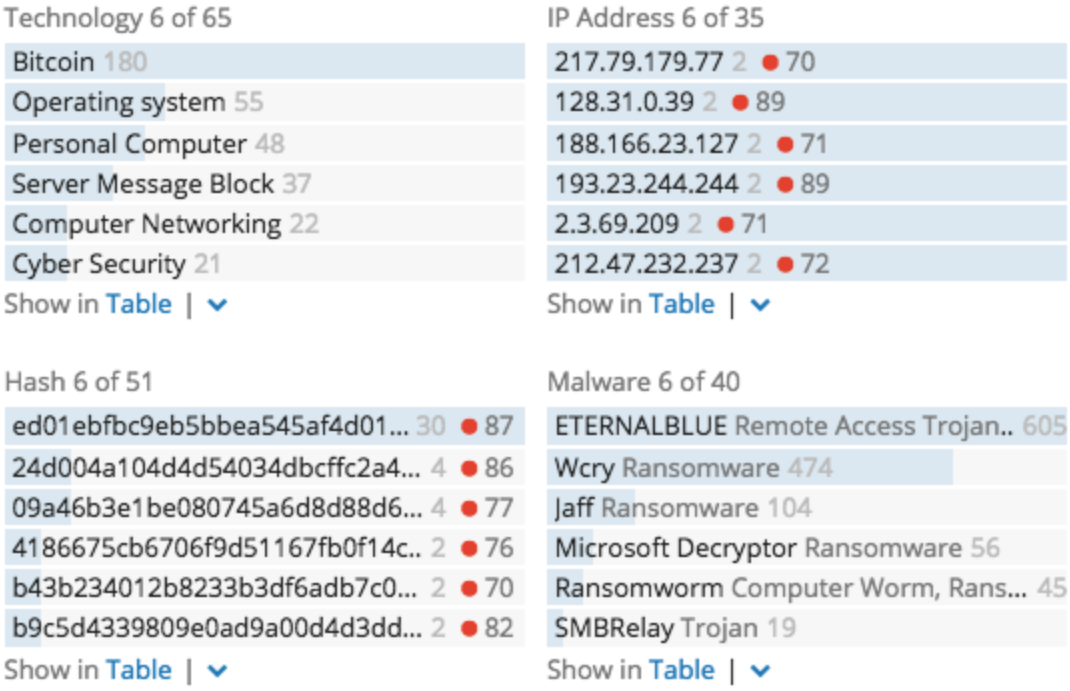
- https://blockchain.info/address/13AM4VW2dhxYgXeQepoHkHSQuy6NgaEb94
- https://blockchain.info/address/12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw
- https://blockchain.info/address/115p7UMMngoj1pMvkpHijcRdfJNXj6LrLn

Bitcoin Address Linked to WannaCry 1.0 Campaign

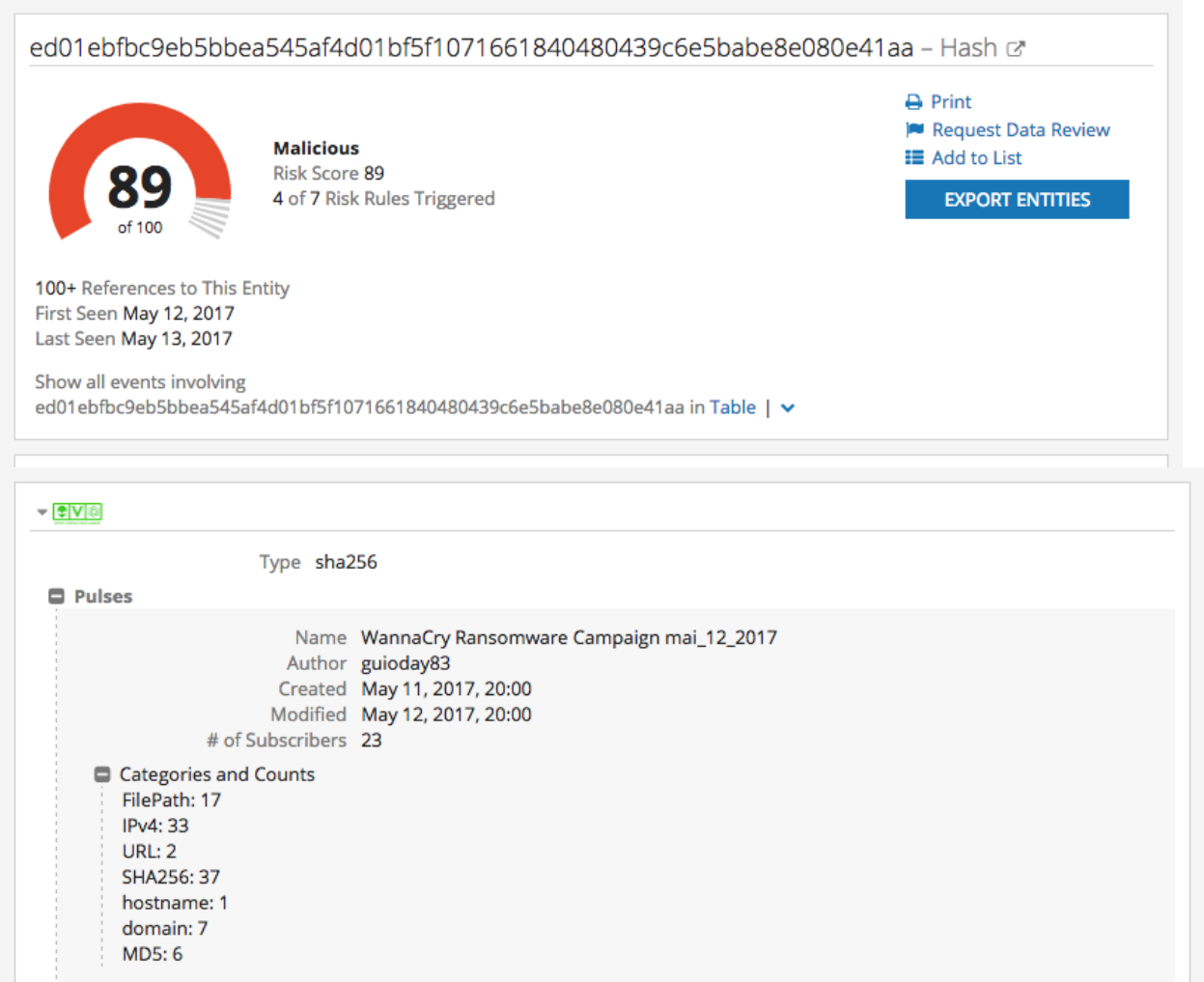
- https://blockchain.info/address/1QAc9S5EmycqjzzWDc1yiWzr9jJLC8sLiY

Link analysis of ransom transactions related to three wallets controlled by criminals.

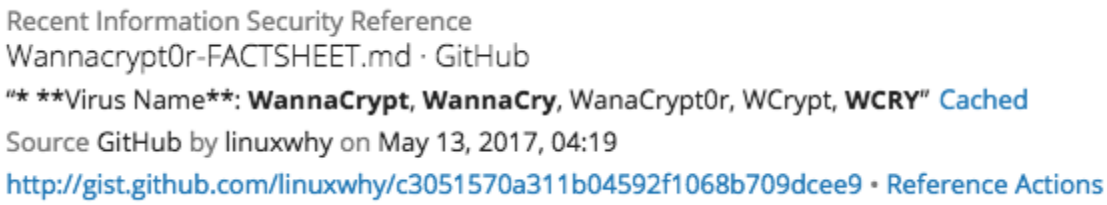
Research
Reviewing the Recorded Future Intel Card for WannaCry, we can rapidly identify any associated IP addresses and hashes.



The most prominent hash appears in early reports on May 11, according to the AlienVault extension on the Intel Card:
ed01ebfbc9eb5bbea545af4d01bf5f1071661840480439c6e5babe8e080e41aa

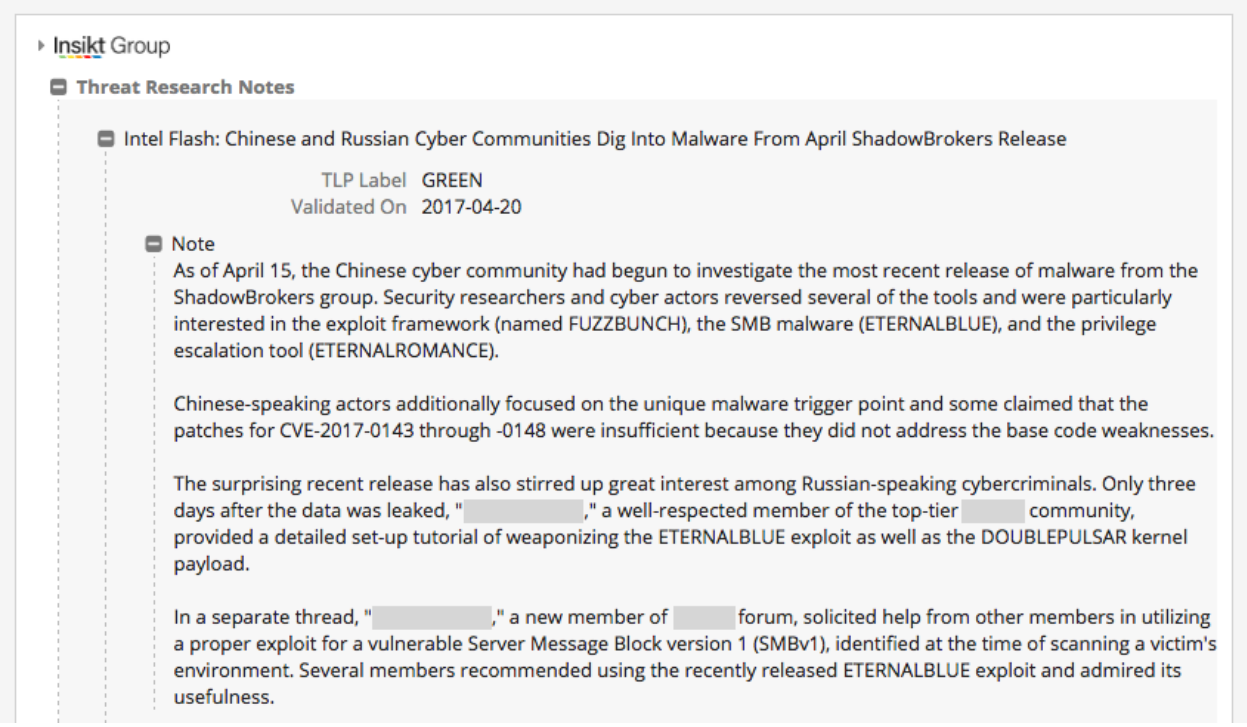


In the Reference section of the WCry Intel Card, we see this factsheet posted towards a GitHub page where security researcher Mark Lee helpfully wrote a running compilation of information on WannaCry ransomware. Early identification of these types of resources during an evolving situation can greatly assist a security analyst gain insight to the nature of the threat and crowdsource solutions.



The GitHub page cites Malwarebytes, claiming the WannaCry worm loops through every RDP session on a system to run the ransomware as that user, and also installs the DOUBLEPULSAR backdoor. This is an interesting observation. According to Cisco's Talos security research team,

WannaCry appears to scan the system to identify if the DOUBLEPULSAR backdoor is present. Only when it's not present does it use the ETERNALBLUE SMB vulnerability to infect the host.
Recorded Future recently reported on the rapid weaponization of the DOUBLEPULSAR payload, a kernel-level exploit which can inject arbitrary DLLs into user land processes. From the Insikt Group note (exclusive to Recorded Future customers):



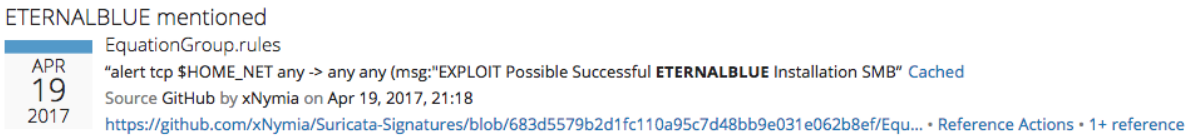
Detection and Remediation

MS17-010 is a known vulnerability which was patched by Microsoft in March 2017. Additionally, Microsoft released an emergency patch for systems in custom support only, including Windows XP, Windows 8, and Windows Server 2003.
For now, the best advice is to update your antivirus on endpoints, to ensure that all Windows systems are fully patched, to configure firewalls to block access to SMB and RDP ports, and to educate users to watch out for suspicious emails.

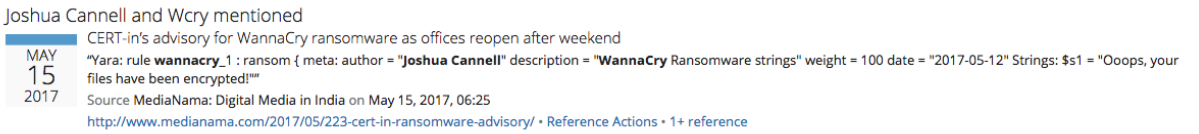
It's notable that WannaCry installs the DOUBLEPULSAR exploit on to any infected system. This is a kernel mode payload which can arbitrarily inject DLLs into user land processes.
Due to the success of this ransomware, and the ease of patching the code, we have likely not seen the last of this malware. Further monitoring in Recorded Future is advised to stay abreast of the latest changes.

IDS/IPS Rules

Using Recorded Future, we were able to identify a shared SNORT rule for MS17-010:



Additionally, Recorded Future surfaces multiple SNORT and Yara signatures for the malware:



Indicators

Open source intelligence indicates the following list of ransomware controllers, as well as the domain which led to the rapid decline of the ransomware infection, which has been sinkholed:

- iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea[dot]com (sinkholed)
- Rphjmrpwmfv6v2e[dot]onion
- Gx7ekbenv2riucmf[dot]onion
- 57g7spgrzlojinas[dot]onion
- xxlvbrloxvriy2c5[dot]onion
- 76jdd2ir2embyv47[dot]onion
- cwwnhwhlz52maqm7[dot]onion

On the MS17-010 bulletin, Microsoft states the following vulnerabilities are related:

- CVE-2017-0143
- CVE-2017-0144
- CVE-2017-0145
- CVE-2017-0146
- CVE-2017-0147
- CVE-2017-0148

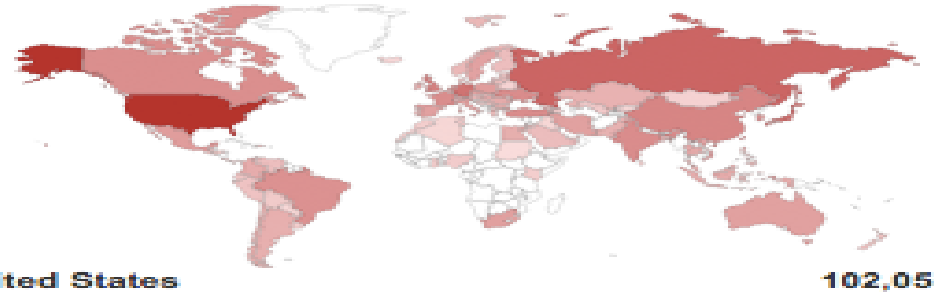
Conclusion

It's likely we haven't seen the last of these large scale attacks, however the speed of remediation by security teams around the globe is impressive. Microsoft released a patch for no longer supported Windows XP, Windows 8, and Windows Server 2003. Meanwhile, global security teams scrambled to patch vulnerable systems, or close the exposed ports. As of this blog posting, Shodan reveals approximately 230,000 Windows hosts worldwide with exposed SMB ports.

TOTAL RESULTS

263,379

TOP COUNTRIES



United States	102,055
Russian Federation	18,121
Taiwan, Province of China	16,598
Japan	14,776
Germany	11,130

TOP SERVICES

SMB	263,375
8880	3
HTTP	1

TOP ORGANIZATIONS

Enzu	16,281
HiNet	13,182
CloudRadium L.L.C	10,892
Nobis Technology Group, LLC	6,703
SpeedVM Network Group LLC	5,930

TOP OPERATING SYSTEMS

Windows Server 2008 R2 Enterpris...	50,099
Windows Server 2012 R2 Standard ...	42,492
Windows Server 2008 R2 Standard ...	29,078
Windows 6.1	14,436
Windows Server 2012 R2 Datacente...	13,532

Shodan scan of open SMB ports on Windows machines.

We expect to see further attacks from variants of this malware, due to the ease of using the exploits. Notably, the ETERNALBLUE exploit of SMBv1 wasn't the only exploit involved in this attack. The use of DOUBLEPULSAR as an infection vector shows the actors were eager to gain access to exposed systems. The use of nation-state exploits in a fairly pedestrian attack gone large reveals the lack of sophistication of the criminals behind these attacks.

A part of carefully planned large-scale ransomware attack requires a separate Bitcoin address for each victim, guaranteeing that the miscreant controlling the operation would later be able to identify the payment and decrypt the correct system. However, in the case of WannaCry 2.0 campaign, only a handful number of wallets were used, with ransomed funds remaining untouched by criminals. Such unusual behavior suggests the current epidemic was never planned by criminals, and resulted from targeted attacks going horribly wrong.

As of this blog publication, all ransomed funds remain untouched by the criminals. We believe this inaction indicates awareness of the intense scrutiny by law enforcement investigators around the world, and fear of identification or capture, which further supports our theory.

Unintended or not, the scale and scope of damage in this attack is unprecedented. Criminals will utilize any method available in their pursuit of monetary gain. While the gain in this attack was limited, the damage was massive, and possibly avoidable.

Microsoft has advocated migration away from SMBv1 since September 2016, and patched the vulnerabilities in MS17-010 in mid-March 2017. This attack occurred in the 90 to 180 day window, demonstrating the importance of patch prioritization in the security lifecycle. Threat intelligence monitoring of emerging and imminent threats against your business, including escalation of security priorities, is vital to defending your enterprise from all threats.

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

Further Analysis of WannaCry Ransomware
By McAfee Labs on May 14, 2017

McAfee Labs has closely monitored the activity around the ransomware WannaCry. Many sources have reported on this attack and its behavior, including this post by McAfee's Raj Samani and Christiaan Beek and this post by Steve Grobman. In the last 24 hours, we have learned more about this malware. These findings mainly concern the malware's network propagation, Bitcoin activity, and differences in observed variants.

Malware network behavior WannaCry uses the MS17-010 exploit to spread to other machines through NetBIOS. The malware contains exploits in its body that are used during the exploitation phase. These are related to CVE-2017-0143, CVE-2017-0144, CVE-2017-0145, CVE-2017-0146, CVE-2017-0147, and CVE-2017-0148, all based on the MS17-10 security bulletin.

In many reports we read that the malware generates a list of internal IPs. We found that the malware generates random IP addresses, not limited to the local network. The following is an example attempt at propagation:

With this, the malware can spread not only to other machines in same network, but also across the Internet if sites allow NetBIOS packets from outside networks. This could be one reason for the widespread infection seen in this outbreak and why many people are unsure about the initial infection vector of the malware.

Another interesting characteristic of the malware is that once a machine with an open NetBIOS port is found, the malware will send three NetBIOS session setup packets to it. One has the proper IP of the machine being exploited, and the other two contain two IP addresses hardcoded in the malware body:

```
SMB       185 Negotiate Protocol Response
SMB       157 Session Setup AndX Request, User: .\
SMB       175 Session Setup AndX Response
SMB       149 Tree Connect AndX Request, Path: \\192.168.0.1\IPC$
SMB       104 Tree Connect AndX Response
SMB Pip   132 PeekNamedPipe Request, FID: 0x0000
SMB        93 Trans Response, Error: STATUS_INSUFF_SERVER_RESOURCES
```

The preceding packet contains the IP of the machine being exploited. It uses the test network 192.168.0.0/24. The other two packets, below, contain different IPs that the malware has in its code:

```
SMB       191 Negotiate Protocol Request
SMB       187 Negotiate Protocol Response
SMB       194 Session Setup AndX Request, User: anonymous
SMB       251 Session Setup AndX Response
SMB       150 Tree Connect AndX Request, Path: \\192.168.56.20\IPC$
SMB       114 Tree Connect AndX Response
SMB       136 Trans2 Request, SESSION_SETUP
SMB        93 Trans2 Response, SESSION_SETUP, Error: STATUS_NOT_IMPLEMENTED
SMB       191 Negotiate Protocol Request
SMB       187 Negotiate Protocol Response
SMB       194 Session Setup AndX Request, User: anonymous
SMB       251 Session Setup AndX Response
SMB       146 Tree Connect AndX Request, Path: \\172.16.99.5\IPC$
SMB       114 Tree Connect AndX Response
SMB      1138 NT Trans Request, <unknown>
SMB        93 NT Trans Response, <unknown (0)>
```

This activity and the presence of two hardcoded IP addresses (192.168.56.20, 172.16.99.5) could be used to detect the exploit using network intrusion prevention systems.

Server message block (SMB) packets also contain the encrypted payload, which consists of exploit shellcode and the file launcher.dll. During our analysis, we found the malware is encrypted using a 4-byte XOR key, 0x45BF6313.

```
000014F0  11 9B 47 98 47 BE 8B 9A 01 9B 7F 72 87 B7 63 15  ..G.G......r..c.
00001500  9A 0F 4F 42 76 35 EE B7 45 C7 F6 34 C0 BF 58 13  ..OBv5..E..4..X.
00001510  E4 0B 63 C8 F3 09 86 13 81 9D 64 F1 45 3D 39 06  ..c.......d.E=9.
00001520  0F BF 63 22 85 34 2D 17 21 36 6B F8 41 34 07 37  ..c".4-.!6k.A4.7
00001530  4D 3C A7 03 18 E1 52 D3 21 30 63 98 63 36 27 37  M<....R.!0c.c6'7
00001540  59 8E A3 9E 08 BF EE 4E BE 96 BA 9A 9A 4C C9 9E  Y......N.....L..
00001550  08 48 EE 8E D9 4D 9C EC 6C 66 EA CC B6 15 02 D0  .H...M..lf......
00001560  AD 16 91 EC BA 54 6A 83 45 DF 33 13 44 BF 63 13  .....Tj.E.3.D.c.
00001570  08 E5 F3 13 46 BF 63 13 41 BF 63 13 BA 40 63 13  ....F.c.A.c..@c.
00001580  FD BF 63 13 45 BF 63 13 05 BF 63 13 45 BF 63 13  ..c.E.c...c.E.c.
00001590  45 BF 63 13 45 BF 63 13 45 BF 63 13 45 BF 63 13  E.c.E.c.E.c.E.c.
000015A0  45 BF 63 13 45 BF 63 13 45 BF 63 13 A5 BF 63 13  E.c.E.c.E.c...c.
000015B0  4B A0 D9 1D 45 0B 6A DE 64 07 62 5F 88 9E 37 7B  K...E.j.d.b_..7{
000015C0  2C CC 43 63 37 D0 04 61 24 D2 43 70 24 D1 0D 7C  ,.Cc7..a$.Cp$..|
000015D0  31 9F 01 76 65 CD 16 7D 65 D6 0D 33 01 F0 30 33  1..ve..}e..3..03
000015E0  28 D0 07 76 6B B2 6E 19 61 BF 63 13 45 BF 63 13  (..vk.n.a.c.E.c.
000015F0  38 23 11 4C 7C 42 7F 1F 7C 42 7F 1F 7C 42 7F 1F  8#.L|B..|B..|B..
```

Encrypted payload with the key 0x45BF6313.

```
000014F0  11 9B 47 98 47 BE 8B 9A 01 9B 7F 72 87 B7 63 15  ..G.G......r..c.
00001500  9A 0F 4F 42 76 35 EE B7 45 C7 F6 34 C0 BF 58 13  ..OBv5..E..4..X.
00001510  E4 0B 63 C8 F3 09 86 13 81 9D 64 F1 45 3D 39 06  ..c.......d.E=9.
00001520  0F BF 63 22 85 34 2D 17 21 36 6B F8 41 34 07 37  ..c".4-.!6k.A4.7
00001530  4D 3C A7 03 18 E1 52 D3 21 30 63 98 63 36 27 37  M<....R.!0c.c6'7
00001540  59 8E A3 9E 08 BF EE 4E BE 96 BA 9A 9A 4C C9 9E  Y......N.....L..
00001550  08 48 EE 8E D9 4D 9C EC 6C 66 EA CC B6 15 02 D0  .H...M..lf......
00001560  AD 16 91 EC BA 54 6A 83 45 DF 33 13 44 BF 63 13  .....Tj.E.3.D.c.
00001570  4D 5A 90 00 03 00 00 00 04 00 00 00 FF FF 00 00  MZ..............
00001580  B8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00  ........@.......
00001590  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
000015A0  00 00 00 00 00 00 00 00 00 00 00 00 E0 00 00 00  ................
000015B0  0E 1F BA 0E 00 B4 09 CD 21 B8 01 4C CD 21 54 68  ........!..L.!Th
000015C0  69 73 20 70 72 6F 67 72 61 6D 20 63 61 6E 6E 6F  is program canno
000015D0  74 20 62 65 20 72 75 6E 20 69 6E 20 44 4F 53 20  t be run in DOS
000015E0  6D 6F 64 65 2E 0D 0D 0A 24 00 00 00 00 00 00 00  mode....$.......
000015F0  7D 9C 72 5F 39 FD 1C 0C 39 FD 1C 0C 39 FD 1C 0C  }.r_9...9...9...
00001600  D1 E2 16 0C 3D FD 1C 0C 39 FD 1D 0C 36 FD 1C 0C  ....=...9...6...
00001610  FA F2 41 0C 3A FD 1C 0C D1 E2 17 0C 38 FD 1C 0C  ..A.:.......8...
00001620  81 FB 1A 0C 38 FD 1C 0C D1 E2 18 0C 3A FD 1C 0C  ....8.......:...
00001630  52 69 63 68 39 FD 1C 0C 00 00 00 00 00 00 00 00  Rich9...........
00001640  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00001650  50 45 00 00 4C 01 05 00 51 57 14 59 00 00 00 00  PE..L...QW.Y....
```

Decrypted launcher.dll payload.

We also found following x64 shellcode being transferred during network communication over SMB.

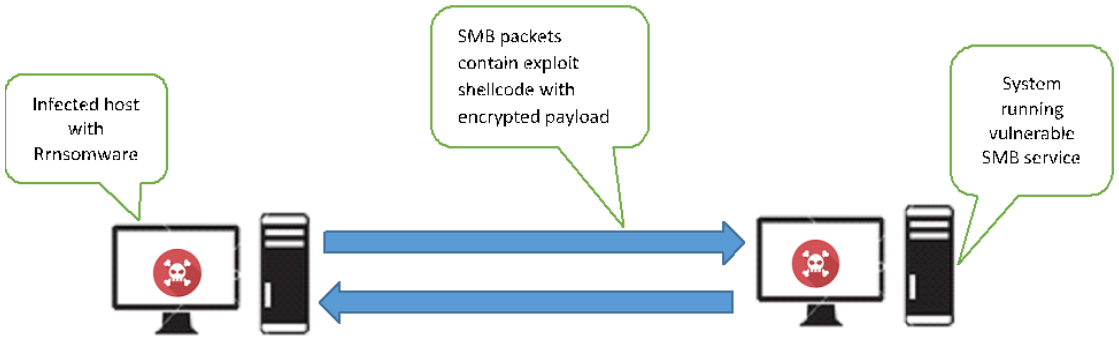
```
        assume es:nothing, ss:nothing, ds:nothing, fs:nothing, gs:nothing
        mov     ecx, 0C0000082h
        rdmsr

loc_7:                                  ; DATA XREF: seg000:000000000000002A↓w
                                        ; seg000:0000000000000055↓r ...
        mov     rbx, 0FFFFFFFFFFD00FF8h
        mov     [rbx+4], edx
        mov     [rbx], eax
        lea     rax, loc_27
        mov     rdx, rax
        shr     rdx, 20h
        wrmsr
        retn
; ---------------------------------------------------------------------------

loc_27:                                 ; DATA XREF: seg000:0000000000000016↑o
        swapgs
        mov     qword ptr gs:loc_7+9, rsp

loc_33:                                 ; DATA XREF: sub_EC+1D↓r
        mov     rsp, qword ptr gs:loc_1A8
        push    rax
        push    rbx
        push    rcx
        push    rdx
        push    rsi
        push    rdi
        push    rbp
        push    r8
        push    r9
        push    r10
        push    r11
        push    r12
        push    r13
        push    r14
        push    r15
        push    2Bh
        push    qword ptr gs:loc_7+9
```

EternalBlue code.

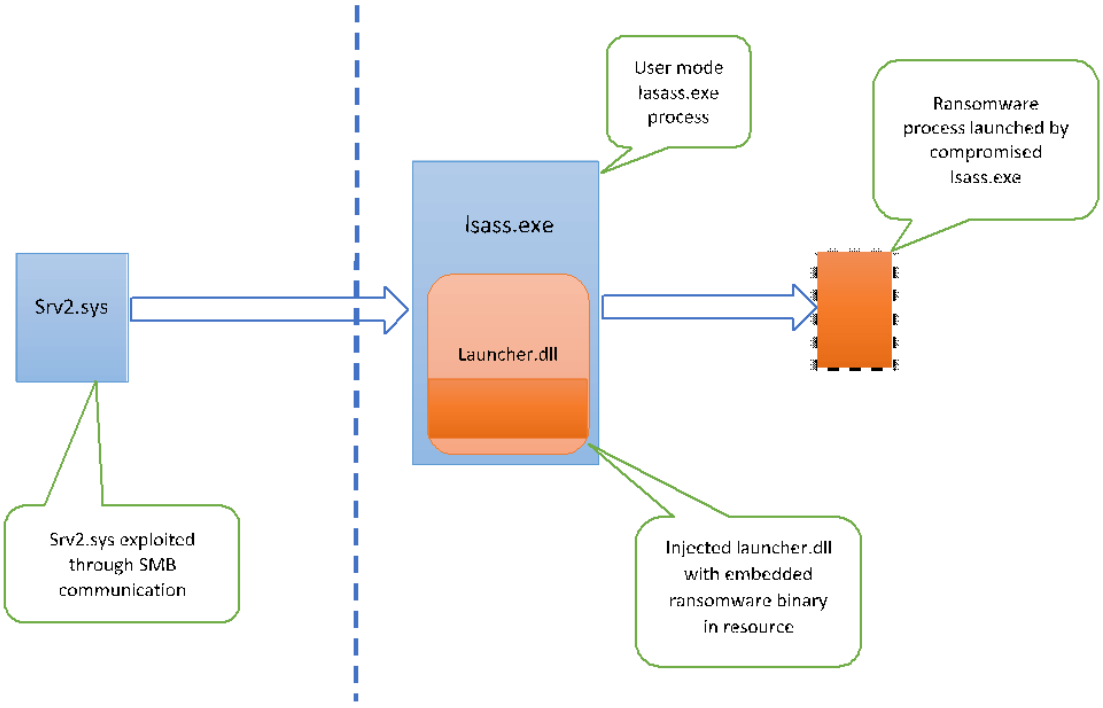
```
                push    rbx
                mov     rax, qword ptr gs:loc_36+2
                mov     rax, [rax+4]
                shr     rax, 0Ch
                shl     rax, 0Ch

loc_16:                                 ; CODE XREF: seg000:0000000000000026↓j
                mov     rbx, [rax]
                cmp     bx, 5A4Dh
                jz      short loc_28
                sub     rax, 1000h
                jmp     short loc_16
; ---------------------------------------------------------------------------

loc_28:                                 ; CODE XREF: seg000:000000000000001E↑j
                pop     rbx
                retn
; ---------------------------------------------------------------------------
```

DoublePulsar code.

Worm behavior



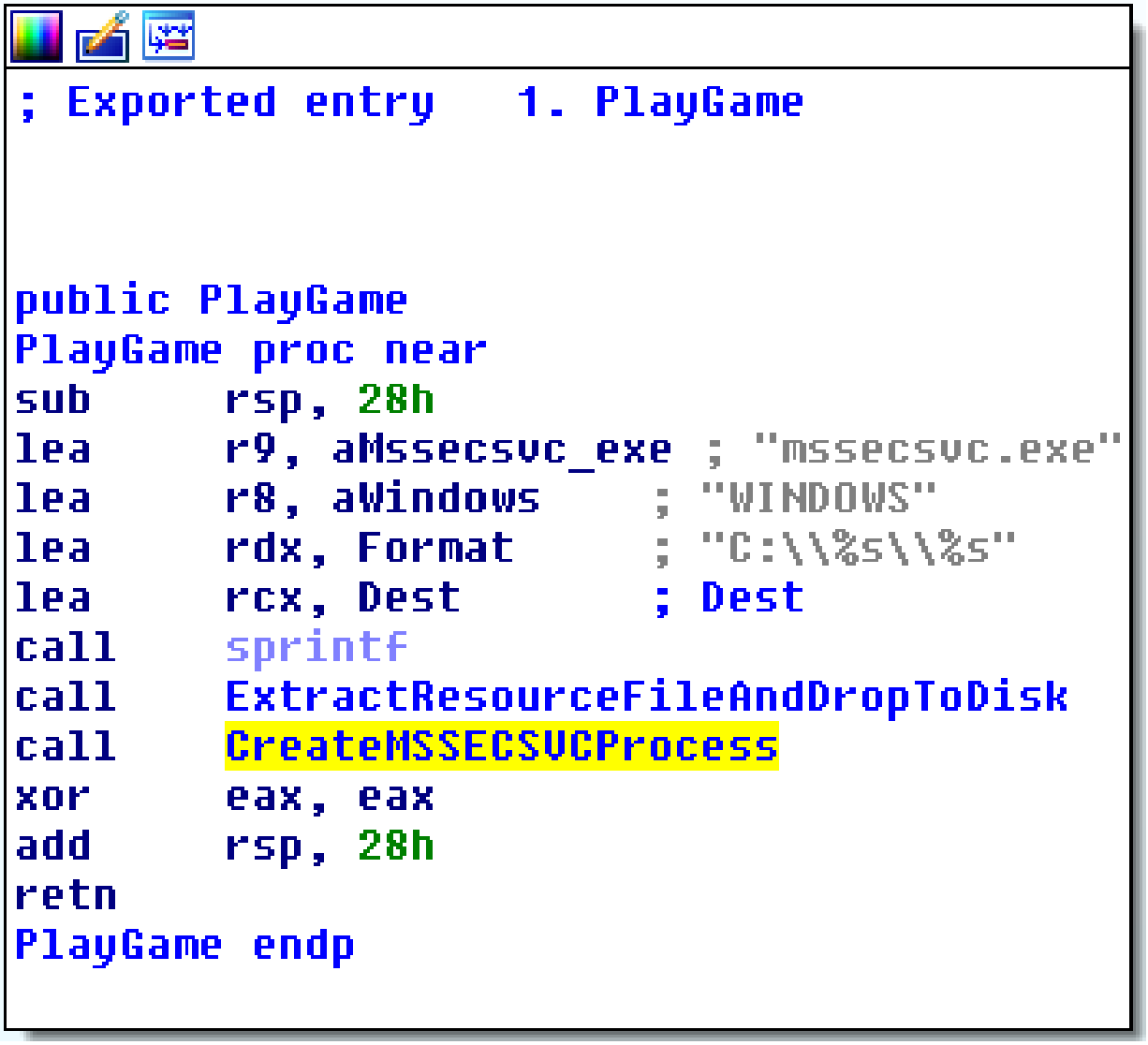
Machine A at left, Machine B at right. The infection flow to the vulnerable host (Machine B).



Kernel mode at left, user mode at right.

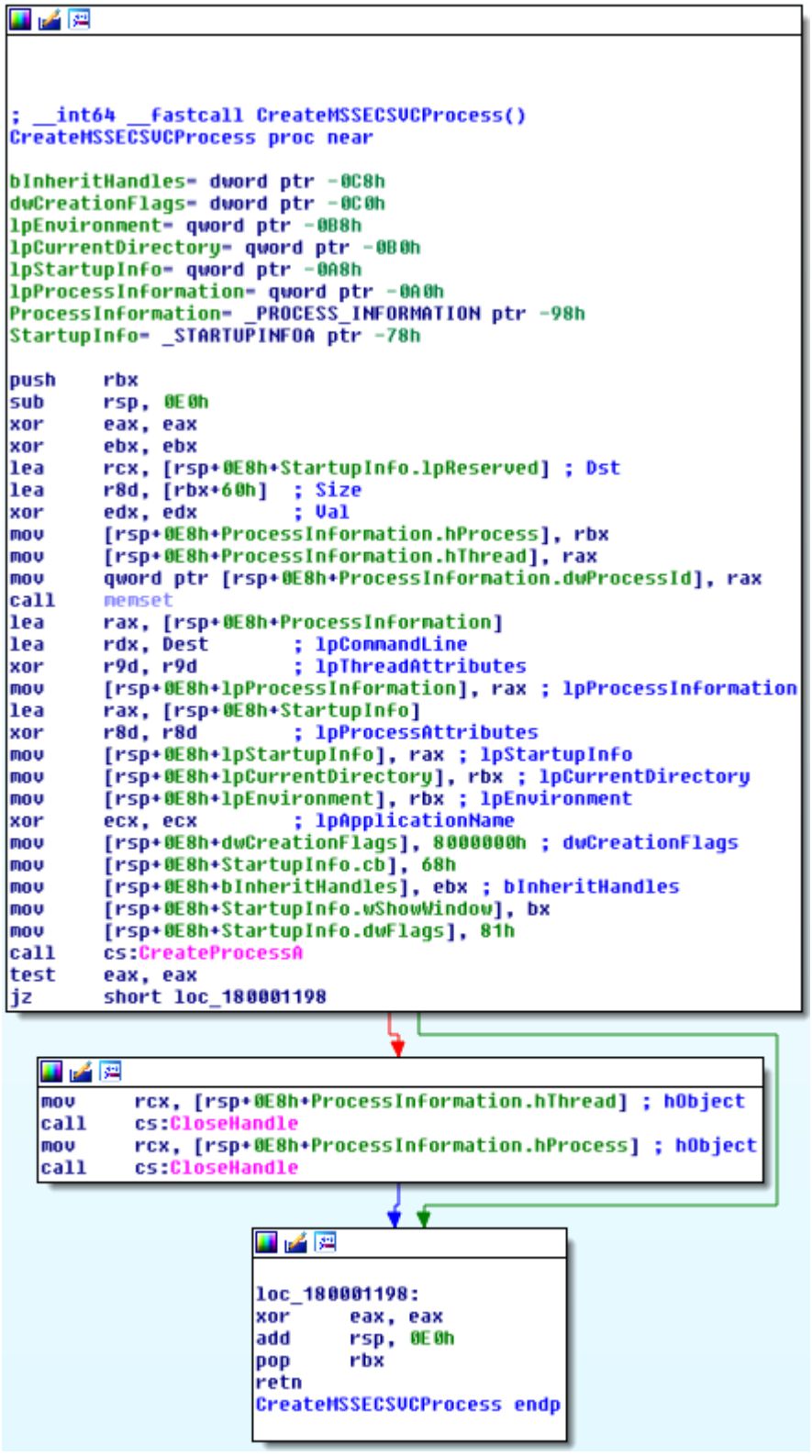
Infection using kernel exploit

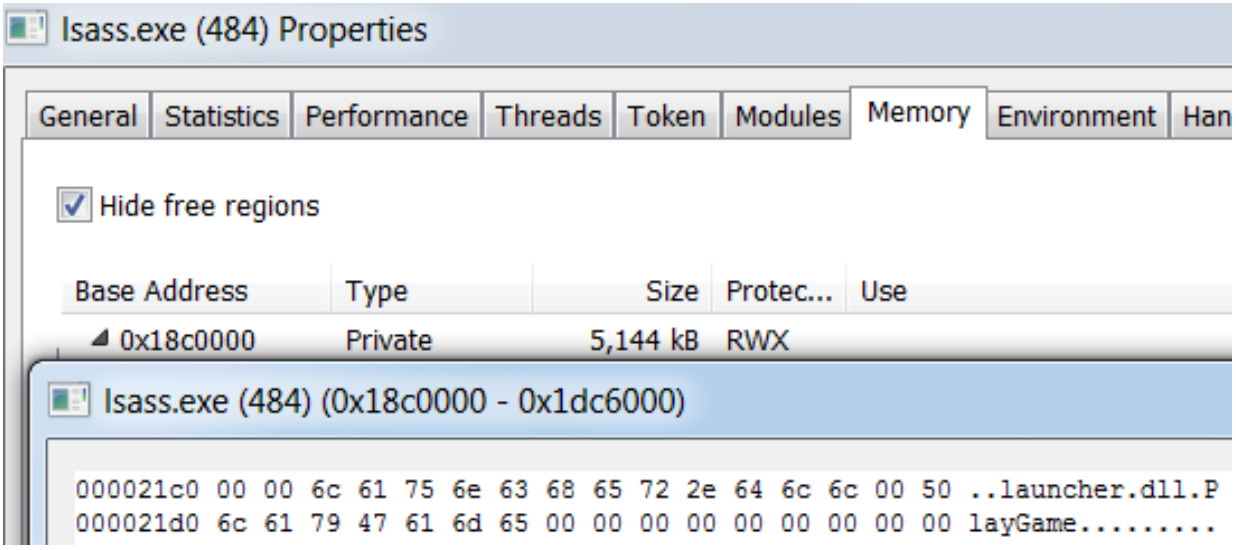
In our analysis, we found that on infected machines the SMB driver srv2.sys is vulnerable in kernel module and is exploited by the malware to spread using SMB communication.
A compromised srv2.sys will inject launcher.dll into the user-mode process lsass.exe, which acts as the loader for mssecsvc.exe. This DLL contains only one export, PlayGame:



```
; Exported entry   1. PlayGame



public PlayGame
PlayGame proc near
sub     rsp, 28h
lea     r9, aMssecsvc_exe ; "mssecsvc.exe"
lea     r8, aWindows      ; "WINDOWS"
lea     rdx, Format       ; "C:\\%s\\%s"
lea     rcx, Dest         ; Dest
call    sprintf
call    ExtractResourceFileAndDropToDisk
call    CreateMSSECSVCProcess
xor     eax, eax
add     rsp, 28h
retn
PlayGame endp
```

The code simply extracts the ransomware dropper from the resource shown previously, and starts it using the function CreateProcess:


; __int64 __fastcall CreateMSSECSVCProcess()
CreateMSSECSVCProcess proc near
bInheritHandles= dword ptr -0C8h
dwCreationFlags= dword ptr -0C0h
lpEnvironment= qword ptr -0B8h
lpCurrentDirectory= qword ptr -0B0h
lpStartupInfo= qword ptr -0A8h
lpProcessInformation= qword ptr -0A0h
ProcessInformation= _PROCESS_INFORMATION ptr -98h
StartupInfo= _STARTUPINFOA ptr -78h
push rbx
sub rsp, 0E0h
xor eax, eax
xor ebx, ebx
lea rcx, [rsp+0E8h+StartupInfo.lpReserved] ; Dst
lea r8d, [rbx+60h] ; Size
xor edx, edx ; Val
mov [rsp+0E8h+ProcessInformation.hProcess], rbx
mov [rsp+0E8h+ProcessInformation.hThread], rax
mov qword ptr [rsp+0E8h+ProcessInformation.dwProcessId], rax
call memset
lea rax, [rsp+0E8h+ProcessInformation]
lea rdx, Dest ; lpCommandLine
xor r9d, r9d ; lpThreadAttributes
mov [rsp+0E8h+lpProcessInformation], rax ; lpProcessInformation
lea rax, [rsp+0E8h+StartupInfo]
xor r8d, r8d ; lpProcessAttributes
mov [rsp+0E8h+lpStartupInfo], rax ; lpStartupInfo
mov [rsp+0E8h+lpCurrentDirectory], rbx ; lpCurrentDirectory
mov [rsp+0E8h+lpEnvironment], rbx ; lpEnvironment
xor ecx, ecx ; lpApplicationName
mov [rsp+0E8h+dwCreationFlags], 8000000h ; dwCreationFlags
mov [rsp+0E8h+StartupInfo.cb], 68h
mov [rsp+0E8h+bInheritHandles], ebx ; bInheritHandles
mov [rsp+0E8h+StartupInfo.wShowWindow], bx
mov [rsp+0E8h+StartupInfo.dwFlags], 81h
call cs:CreateProcessA
test eax, eax
jz short loc_180001198
mov rcx, [rsp+0E8h+ProcessInformation.hThread] ; hObject
call cs:CloseHandle
mov rcx, [rsp+0E8h+ProcessInformation.hProcess] ; hObject
call cs:CloseHandle
loc_180001198:
xor eax, eax
add rsp, 0E0h
pop rbx
retn
CreateMSSECSVCProcess endp



Injected launcher.dll in the lsass.exe addresses space.

Malware variants in the wild

As reported by several sources, the malware dropper contains code to check to two specific domains before executing its ransomware or the network exploit codes.

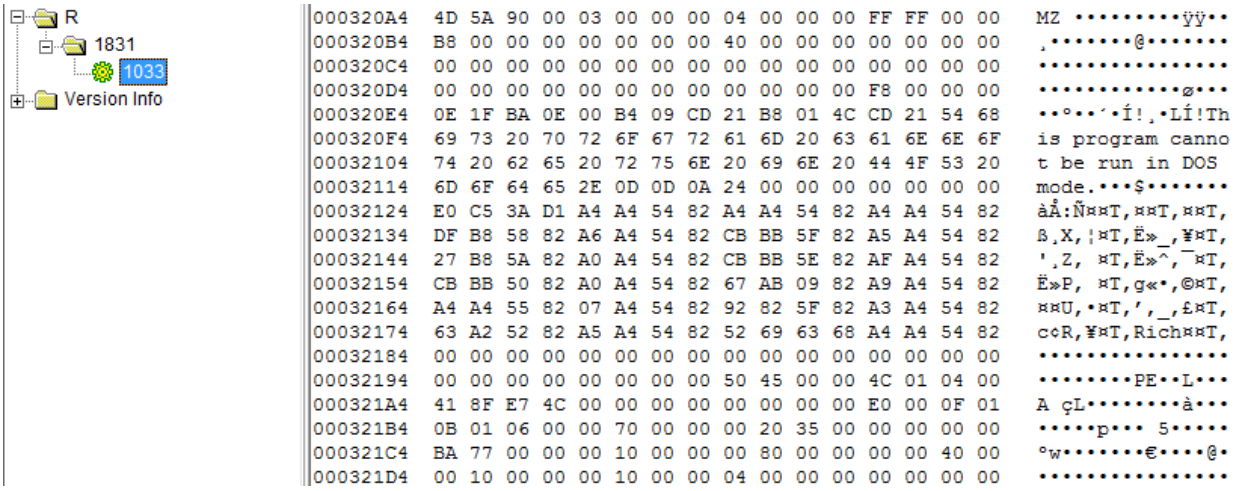
- hxxp://www[dot]iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea[dot]com
- hxxp://www[dot]ifferfsodp9ifjaposdfjhgosurijfaewrwergwea[dot]com

While looking for more samples in our malware database, we came across several other droppers (MD5: 509C41EC97BB81B0567B059AA2F50FE8) that did not exhibit this same behavior. These other droppers did not have the code to exploit machines through NetBIOS or to check for the kill-switch domain. With these samples, the ransomware code would be executed in all cases.

These samples were found in the wild, which means they are capable of infecting and spreading, but in a much less aggressive way. Once the ransomware infects a machine, it also tries to infect any network shares mounted as local disks. Anyone accessing these shares could execute the malware sample by mistake and infect themselves. This infection vector is not as effective as the network exploit but could nonetheless wreak havoc in a corporate environment.

Examination of the droppers

(MD5: DB349B97C37D22F5EA1D1841E3C89EB4) that had the exploit code to compare with the other samples. Foumd this exploit-aware dropper is a wrapper around the other droppers. Looking at the exploit-aware sample, we found that one of the resources contains a 3.4MB .exe file that is the same as the other type of droppers:



The preceding resource is extracted after the remote host is exploited and sent to the victim and installed as a service. This event starts the infection on the remote machine.

File decryption

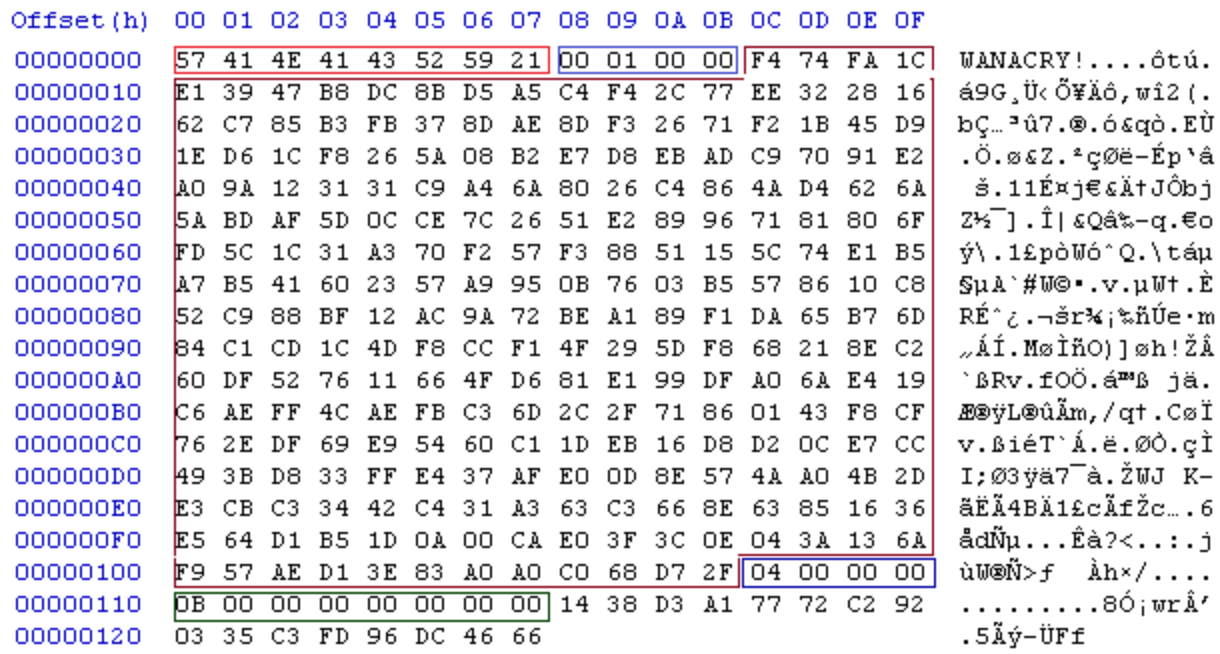
WannaCry offers free decryption for some random number of files in the folder C:\McAfee\<random folder name>\f.wnry. We have seen 10 files decrypted for free.

In the first step, the malware checks the header of each encrypted file. Once successful, it calls the decryption routine, and decrypts all the files listed in C:\McAfee\<random folder name>\ f.wnry.

A code snippet of the header check:

```
GetFileTime(v3, &CreationTime, &LastAccessTime, &LastWriteTime);
if ( !ReadFile_0(v3, v17, 8, &v25, 0)                          Signature WANNACRY!
  || memcmp(v17, aWanacry, 8u)
  || !ReadFile_0(v3, &v11, 4, &v25, 0)                         Read and verify size of Key
  || v11 != 0x100
  || !ReadFile_0(v3, v10[306], 0x100, &v25, 0)                 Read 0x100 bytes of key data
  || !ReadFile_0(v3, &v12, 4, &v25, 0)
  || !ReadFile_0(v3, &liDistanceToMove, 8, &v25, 0) )          Size of original file
{
  goto LABEL_33;
}
if ( v12 != 3 )                                                V2 has value 0x4 in encrypted files
{
  v5 = (HANDLE)CreateFileW(a3, 0x40000000, 1, 0, 2, 128, 0);
  hFile = v5;
  if ( v5 == (HANDLE)-1 )
  {
    v9 = (char *)&ms_exc.registration;
    goto LABEL_34;
  }
```

The format of the encrypted file:



Offset(h)	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	
00000000	57	41	4E	41	43	52	59	21	00	01	00	00	F4	74	FA	1C	WANACRY!....ôtú.
00000010	E1	39	47	B8	DC	8B	D5	A5	C4	F4	2C	77	EE	32	28	16	á9G¸Ü‹Õ¥Äô,wî2(.
00000020	62	C7	85	B3	FB	37	8D	AE	8D	F3	26	71	F2	1B	45	D9	bÇ…³û7.®.ó&qò.EÙ
00000030	1E	D6	1C	F8	26	5A	08	B2	E7	D8	EB	AD	C9	70	91	E2	.Ö.ø&Z.²çØë-Ép'â
00000040	A0	9A	12	31	31	C9	A4	6A	80	26	C4	86	4A	D4	62	6A	š.11É¤j€&Ä†JÔbj
00000050	5A	BD	AF	5D	0C	CE	7C	26	51	E2	89	96	71	81	80	6F	Z½¯].Î|&Qâ‰–q.€o
00000060	FD	5C	1C	31	A3	70	F2	57	F3	88	51	15	5C	74	E1	B5	ý\.1£pòWó^Q.\táµ
00000070	A7	B5	41	60	23	57	A9	95	0B	76	03	B5	57	86	10	C8	§µA`#W©•.v.µW†.È
00000080	52	C9	88	BF	12	AC	9A	72	BE	A1	89	F1	DA	65	B7	6D	RÉˆ¿.¬šr¾¡‰ñÚe·m
00000090	84	C1	CD	1C	4D	F8	CC	F1	4F	29	5D	F8	68	21	8E	C2	„ÁÍ.MøÌñO)]øh!ŽÂ
000000A0	60	DF	52	76	11	66	4F	D6	81	E1	99	DF	A0	6A	E4	19	`ßRv.fOÖ.á™ß jä.
000000B0	C6	AE	FF	4C	AE	FB	C3	6D	2C	2F	71	86	01	43	F8	CF	Æ®ÿL®ûÃm,/q†.CøÏ
000000C0	76	2E	DF	69	E9	54	60	C1	1D	EB	16	D8	D2	0C	E7	CC	v.ßiéT`Á.ë.ØÒ.çÌ
000000D0	49	3B	D8	33	FF	E4	37	AF	E0	0D	8E	57	4A	A0	4B	2D	I;Ø3ÿä7¯à.ŽWJ K-
000000E0	E3	CB	C3	34	42	C4	31	A3	63	C3	66	8E	63	85	16	36	ãËÃ4BÄ1£cÃfŽc….6
000000F0	E5	64	D1	B5	1D	0A	00	CA	E0	3F	3C	0E	04	3A	13	6A	ådÑµ...Êà?<..:.j
00000100	F9	57	AE	D1	3E	83	A0	A0	C0	68	D7	2F	04	00	00	00	ùW®Ñ>ƒ Àh×/....
00000110	0B	00	00	00	00	00	00	00	14	38	D3	A1	77	72	C2	92	.........8Ó¡wrÂ'
00000120	03	35	C3	FD	96	DC	46	66									.5Ãý–ÜFf

To decrypt all the files on an infected machine we need the file 00000000.dky, which contains the decryption keys. The decryption routine for the key and original file follows:

```
    if ( !Decrypt_Key((int)(v10 + 1), (const void *)v10[306], v11, &v22, (unsigned int *)&v23) )
    {
      if ( !Decrypt_Key((int)(v10 + 11), (const void *)v10[306], v11, &v22, (unsigned int *)&v23) )
      {
LABEL_21:
        v9 = (char *)&ms_exc.registration;
        goto LABEL_34;
      }
      v21 = 1;
    }
    Crypto_AES_FORWARD_BOX(v10 + 21, &v22, off_4213B0, v23, 0x10);
    v24 = liDistanceToMove.QuadPart;
    while ( SHIDWORD(v24) >= 0 && (SHIDWORD(v24) > 0 || (_DWORD)v24) )
    {
      v6 = (_DWORD *)v10[308];
      if ( v6 && *v6 )
        goto LABEL_33;
      if ( !ReadFile_0(v3, v10[306], 0x100000, &v25, 0) || !v25 )
      {
        v9 = (char *)&ms_exc.registration;
        goto LABEL_34;
      }
      v24 -= (unsigned int)v25;
      sub_40B3C0((int)(v10 + 21), (char *)v10[306], (_BYTE *)v10[307], v25, 1);
      if ( !WriteFile_0(v5, v10[307], v25, &v26, 0) || v26 != v25 )
        goto LABEL_33;
    }
```

File Decryption Routine

Bitcoin activity

WannaCry uses three Bitcoin wallets to receive payments from its victims. Looking at the payment activity for these wallets gives us an idea of how much money the attackers have made.

The current statistics as of May 13 show that not many people have paid to recover their files:

- Wallet 12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw

Summary		Transactions	
Address	12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw	No. Transactions	38
Hash 160	14a477964ed719135d1598da348a858b18b44fd5	Total Received	6.80581381 BTC
Tools	Related Tags - Unspent Outputs	Final Balance	6.80581381 BTC

- Wallet 13AM4VW2dhxYgXeQepoHkHSQuy6NgaEb94

Summary		Transactions	
Address	13AM4VW2dhxYgXeQepoHkHSQuy6NgaEb94	No. Transactions	35
Hash 160	17b4bd9a139158614e8f54c6b800a1822609436a	Total Received	5.00218759 BTC
Tools	Related Tags - Unspent Outputs	Final Balance	5.00218759 BTC

- Wallet 115p7UMMngoj1pMvkpHijcRdfJNXj6LrLn

Summary		Transactions	
Address	115p7UMMngoj1pMvkpHijcRdfJNXj6LrLn	No. Transactions	30
Hash 160	00e8fd98ca34f195b020af4a8b1c7238663d4212	Total Received	3.64134512 BTC
Tools	Related Tags - Unspent Outputs	Final Balance	3.64134512 BTC

-

The attackers appear to have earned a little over BTC 15.44 (US$27,724.22). That is not much considering the number of infected machines, but these numbers are increasing and might become much higher in the next few days. It's possible that the sink holing of two sites may have helped slow things down:

- hxxp://www[dot]iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea[dot]com
- hxxp://www[dot]ifferfsodp9ifjaposdfjhgosurijfaewrwergwea[dot]com

Multiple organizations across more than 90 countries have been impacted, according to reports.

Report Notice

DHS and FBI encourages recipients who identify the use of tool(s) or techniques discussed in this document to report information to DHS or law enforcement immediately. We encourage you to contact DHS's National Cybersecurity and Communications Integration Center (NCCIC) (NCCICcustomerservice@hq.dhs.gov(link sends e-mail) or 888-282-0870), or the FBI through a local field office or the FBI's Cyber Division (CyWatch@ic.fbi.gov (link sends e-mail)or 855-292-3937) to report an intrusion and to request incident response resources or technical assistance.

Original release date: May 12, 2017 | Last revised: June 07, 2018

Alert (TA17-132A)

Indicators Associated With WannaCry Ransomware

Systems Affected: Microsoft Windows operating systems

Overview

This Alert has been updated to reflect the U.S. Government's public attribution of the "WannaCry" ransomware variant to the North Korean government. Additional information on the attribution may be found in a press briefing from the White House. For more information related to WannaCry activity, go to https://www.us-cert.gov/hiddencobra.

According to numerous open-source reports, a widespread ransomware campaign is affecting various organizations with reports of tens of thousands of infections in over 150 countries, including the United States, United Kingdom, Spain, Russia, Taiwan, France, and Japan. The software can run in as many as 27 different languages. The latest version of this ransomware variant, known as WorldCry, WannaCry, WCry, or Wanna Decryptor, was originally discovered the morning of May 12, 2017, by an independent security researcher and has spread rapidly over several hours, with initial reports beginning around 4:00 AM EDT, May 12, 2017.

Open-source reporting indicates a requested ransom of .1781 bitcoins, roughly $300 U.S.

This Alert is the result of efforts between the Department of Homeland Security (DHS) National Cybersecurity and Communications Integration Center (NCCIC) and the Federal Bureau of Investigation (FBI) to highlight known cyber threats. DHS and the FBI continue to pursue related information of threats to federal, state, and local government systems and as such, further releases of technical information may be forthcoming.

Description

Initial reports indicate the hacker or hacking group behind the WannaCry campaign is gaining access to enterprise servers through the exploitation of a critical Windows SMB vulnerability. Microsoft released a security update for the MS17-010(link is external) vulnerability on March 14, 2017. Additionally, Microsoft released patches for Windows XP, Windows 8, and Windows Server 2003(link is external) operating systems on May 13, 2017.
According to open sources, one possible infection vector may be through phishing.

Technical Details

Indicators of Compromise (IOC)
See TA17-132A_WannaCry.xlsx and TA17-132A_WannaCry_stix.xml for IOCs developed immediately after WannaCry ransomware appeared. These links contain identical content in two different formats.
See TA17-132A_stix.xml for IOCs developed after further analysis of the WannaCry malware.

Analysis

Three files were submitted to US-CERT for analysis. All files are confirmed as components of a ransomware campaign identified as "WannaCry", a.k.a "WannaCrypt" or ".wnCry". The first file is a dropper, which contains and runs the ransomware, propagating via the MS17-010/EternalBlue SMBv1.0 exploit. The remaining two files are ransomware components containing encrypted plug-ins responsible for encrypting the victim users files. For a list of IOCs found during analysis, see the STIX file.

Displayed below are YARA signatures that can be used to detect the ransomware:
Yara Signatures

```
rule Wanna_Cry_Ransomware_Generic {
    meta:
        description = "Detects WannaCry Ransomware on Disk and in Virtual Page"
        author = "US-CERT Code Analysis Team"
        reference = "not set"
        date = "2017/05/12"
    hash0 = "4DA1F312A214C07143ABEEAFB695D904"
```

```
    strings:
        $s0 = {410044004D0049004E0024}
        $s1 = "WannaDecryptor"
        $s2 = "WANNACRY"
        $s3 = "Microsoft Enhanced RSA and AES Cryptographic"
        $s4 = "PKS"
        $s5 = "StartTask"
        $s6 = "wcry@123"
        $s7 = {2F6600002F72}
        $s8 = "unzip 0.15 Copyrigh"
        $s9 = "Global\\WINDOWS_TASKOSHT_MUTEX"
        $s10 = "Global\\WINDOWS_TASKCST_MUTEX"
        $s11 = {7461736B736368652E657865000000005461736B537461727400000742E776E7279000069636163}
        $s12 = {6C73202E202F6772616E742045766572796F6E653A46202F54202F43202F5100617474726962202B68}
        $s13 = "WNcry@2ol7"
        $s14 = "wcry@123"
        $s15 = "Global\\MsWinZonesCacheCounterMutexA"
    condition:
        $s0 and $s1 and $s2 and $s3 or $s4 and $s5 and $s6 and $s7 or $s8 and $s9 and $s10 or $s11 and $s12 or $s13 or $s14 or $s15
}
/*The following Yara ruleset is under the GNU-GPLv2 license (http://www.gnu.org/licenses/gpl-2.0.html) and open to any user or organization, as long as you use it under this license.*/
rule MS17_010_WanaCry_worm {
    meta:
        description = "Worm exploiting MS17-010 and dropping WannaCry Ransomware"
        author = "Felipe Molina (@felmoltor)"
        reference = "https://www.exploit-db.com/exploits/41987/"
        date = "2017/05/12"
    strings:
        $ms17010_str1="PC NETWORK PROGRAM 1.0"
        $ms17010_str2="LANMAN1.0"
        $ms17010_str3="Windows for Workgroups 3.1a"
        $ms17010_str4="__TREEID__PLACEHOLDER__"
        $ms17010_str5="__USERID__PLACEHOLDER__"
        $wannacry_payload_substr1 = "h6agLCqPqVyXi2VSQ8O6Yb9ijBX54j"
```

```
        $wannacry_payload_substr2 = "h54WfF9cGigWFEx92bzmOd0UOaZlM"
        $wannacry_payload_substr3 = "tpGFEoLOU6+5I78Toh/nHs/RAP"
    condition:
        all of them
}
```

Dropper

This artifact (5bef35496fcbdbe841c82f4d1ab8b7c2) is a malicious PE32 executable that has been identified as a WannaCry ransomware dropper. Upon execution, the dropper attempts to connect to the following hard-coded URI:
http[:]//www[.]iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com.

--Begin request—
GET HTTP/1.1
Host: www[.]iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com
Cache-Control: no-cache
--End request--

If a connection is established, the dropper will terminate execution. If the connection fails, the dropper will infect the system with ransomware. When executed, the malware is designed to run as a service with the parameters "-m security". During runtime, the malware determines the number of arguments passed during execution.

If the arguments passed are less than two, the dropper proceeds to install itself as the following service:

--Begin service--
ServiceName = "mssecsvc2.0"
DisplayName = "Microsoft Security Center (2.0) Service"
StartType = SERVICE_AUTO_START
BinaryPathName = "%current directory%5bef35496fcbdbe841c82f4d1ab8b7c2.exe -m security"
--End service—

Once the malware starts as a service named mssecsvc2.0, the dropper attempts to create and scan a list of IP ranges on the local network and attempts to connect using UDP ports 137, 138 and TCP ports 139, 445. If a connection to port 445 is successful, it creates an additional thread to propagate by exploiting the SMBv1 vulnerability documented by Microsoft Security bulliten MS17-010. The malware then extracts & installs a PE32 binary from it's resource section named "R". This binary has been identified as the ransomware component of WannaCrypt.
The dropper installs this binary into "C:\WINDOWS\tasksche.exe." The dropper executes tasksche.exe with the following command:

--Begin command--
"C:\WINDOWS\tasksche.exe /i"
--End command—

Note:
=====
When this sample was initially discovered, the domain, iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea[.]com" was not registered, allowing the malware to run and propagate freely. However within a few days, researchers learned that by registering the domain and allowing the malware to connect, its ability to spread was greatly reduced. At this time, all traffic to "iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com" is re-directed to a monitored, non-malicious server, causing the malware to terminate if it is allowed to connect. For this reason, we recommend that administrators and network security personnel not block traffic to this domain.

Impact

Ransomware not only targets home users; businesses can also become infected with ransomware, leading to negative consequences, including

- temporary or permanent loss of sensitive or proprietary information,
- disruption to regular operations,
- financial losses incurred to restore systems and files,
- potential harm to an organization's reputation.

Paying the ransom does not guarantee the encrypted files will be released; it only guarantees that the malicious actors receive the victim's money, and in some cases, their banking information. In addition, decrypting files does not mean the malware infection itself has been removed.

Recommended Steps for Prevention

- Apply the Microsoft patch for the MS17-010 SMB vulnerability dated March 14, 2017.
- Enable strong spam filters to prevent phishing emails from reaching the end users and authenticate in-bound email using technologies like Sender Policy Framework (SPF), Domain Message Authentication Reporting and Conformance (DMARC), and DomainKeys Identified Mail (DKIM) to prevent email spoofing.
- Scan all incoming and outgoing emails to detect threats and filter executable files from reaching the end users.
- Ensure anti-virus and anti-malware solutions are set to automatically conduct regular scans.
- Manage the use of privileged accounts. Implement the principle of least privilege. No users should be assigned administrative access unless absolutely needed. Those with a need for administrator accounts should only use them when necessary.
- Configure access controls including file, directory, and network share permissions with least privilege in mind. If a user only needs to read specific files, they should not have write access to those files, directories, or shares.
- Disable macro scripts from Microsoft Office files transmitted via email. Consider using Office Viewer software to open Microsoft Office files transmitted via email instead of full Office suite applications.
- Develop, institute, and practice employee education programs for identifying scams, malicious links, and attempted social engineering.
- Run regular penetration tests against the network, no less than once a year. Ideally, run these as often as possible and practical.
- Test your backups to ensure they work correctly upon use.

Recommendations for Network Protection

Apply the patch (MS17-010). If the patch cannot be applied, consider:

- Disabling SMBv1 and
- blocking all versions of SMB at the network boundary by blocking TCP port 445 with related protocols on UDP ports 137-138 and TCP port 139, for all boundary devices.

Note: *disabling or blocking SMB may create problems by obstructing access to shared files, data, or devices. The benefits of mitigation should be weighed against potential disruptions to users.*

Review US-CERT's Alert on The Increasing Threat to Network Infrastructure Devices and Recommended Mitigations and consider implementing the following best practices:

1. Segregate networks and functions.
2. Limit unnecessary lateral communications.

3. Harden network devices.
4. Secure access to infrastructure devices.
5. Perform out-of-band network management.
6. Validate integrity of hardware and software.

Recommended Steps for Remediation

- Contact law enforcement. We strongly encourage you to contact a local FBI field office upon discovery to report an intrusion and request assistance. Maintain and provide relevant logs.
- Implement your security incident response and business continuity plan. Ideally, organizations should ensure they have appropriate backups so their response is simply to restore the data from a known clean backup.

Defending Against Ransomware Generally

Precautionary measures to mitigate ransomware threats include:

- Ensure anti-virus software is up-to-date.
- Implement a data back-up and recovery plan to maintain copies of sensitive or proprietary data in a separate and secure location. Backup copies of sensitive data should not be readily accessible from local networks.
- Scrutinize links contained in emails, and do not open attachments included in unsolicited emails.
- Only download software—especially free software—from sites you know and trust.
- Enable automated patches for your operating system and Web browser.

Additional information

- Malwarebytes LABS: WanaCrypt0r ransomware hits it big just before the weekend(link is external)
- Malwarebytes LABS: The worm that spreads WanaCrypt0r(link is external)
- Microsoft: Microsoft Security Bulletin MS17-010(link is external)
- Forbes: An NSA Cyber Weapon Might Be Behind A Massive Global Ransomware Outbreak(link is external)
- Reuters: Factbox: Don't click - What is the 'ransomware' WannaCry worm?(link is external)
- GitHubGist: WannaCry|WannaDecrypt0r NSA-Cyberweapon-Powered Ransomware Worm(link is external)
- Microsoft: Microsoft Update Catalog: Patches for Windows XP, Windows 8, and Windows Server 2003, (KB4012598)(link is external)
- Cisco: Player 3 Has Entered the Game: Say Hello to 'WannaCry'(link is external)
- Washington Post: More than 150 countries affected by massive cyberattack, Europol says

Campaign Motivations

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

By now you have likely heard about the WannaCry (aka WannaCrypt) ransomware campaign that has taken the world by storm. The campaign has affected organizations and end users in at least 99 countries, shutting down hospitals in the UK and taken major companies offline.

The ransomware itself is nothing terribly unique. Like the dozens of other ransomware families out there, WannaCry encrypts your important files and then demands a ransom in the form of bitcoin payment. The campaign does not appear to be targeted and seems to spread using typical attack vectors like malicious emails and unpatched vulnerability exploitation. The malware also starts two countdown clocks. One increases the ransom from ~300$USD to ~600$USD after three days have gone by with no payment. The second clock counts down seven days, at which point all encrypted files will be deleted if no payment has been made.

The network exploitation vector allows the ransomware to spread automatically like worms of old like SQL Slammer and Nimda. This wormlike behavior accounts for the incredibly fast spread worldwide. The vulnerability exploited by the campaign is in the common SMB protocol

used in nearly every Windows network. It was disclosed as a part of the Shadow Brokers release back in April, specifically the EternalBlue exploit alleged to have come from the NSA. Microsoft patched this vulnerability back in March in the MS17-010 bulletin.

Despite a patch being available, this didn't appear to slow WannaCry down. While many blame system administrators for not patching the systems under their control, a complicating factor is the still wide spread prevalence of Windows XP and Windows Server 2003. Both of these operating systems have passed their "end-of-life" and are no longer issued patches. In order to help stem the widespread exploitation used by WannaCry, Microsoft made the rare move of pushing out a patch to end-of-life systems.

Ransomware continues to be a one of the most popular threats in the wild today, especially to large organizations with both valuable data and legacy systems hidden unpatched in the cracks and corners of their networks. Consistent and up-to-date system backups are critical to recovering from a ransomware infection. Criminals can't hold data hostage if it is recoverable. Since the exploit capitalizes on the vulnerability in the SMB, disabling SMB or blocking SMB at your perimeter firewall is a good proactive measure to stop spreading to vulnerable systems. Keeping your systems patched and upgrading legacy systems will also go a long way toward preventing infection to begin with. Microsoft has issued additional guidance for protecting your systems and networks from this specific threat.

References

1. *Ghosh, Agamoni (April 9, 2017). "'President Trump what the f**k are you doing' say Shadow Brokers and dump more NSA hacking tools". International Business Times UK. Retrieved April 10, 2017.*
2. *"'NSA malware' released by Shadow Brokers hacker group". BBC News. April 10, 2017. Retrieved April 10, 2017.*
3. *Sam Biddle (August 19, 2016). "The NSA Leak is Real, Snowden Documents Confirm". The Intercept. Retrieved April 15, 2017.*
4. *"Powerful NSA hacking tools have been revealed online".*
5. *"Equation Group - Cyber Weapons Auction - Pastebin.com". 16 August 2016. Archived from the original on 15 August 2016.*
6. *Dan Goodin (January 12, 2017). "NSA-leaking Shadow Brokers lob Molotov cocktail before exiting world stage". Ars Technica. Retrieved January 14, 2017.*
7. *"Confirmed: hacking tool leak came from "omnipotent" NSA-tied group". Ars Technica. Retrieved January 14, 2017.*
8. *"The Equation giveaway - Securelist".*

9. *"Group claims to hack NSA-tied hackers, posts exploits as proof"*.
10. *"The 'Shadow Brokers' NSA theft puts the Snowden leaks to shame - ExtremeTech"*. *19 August 2016.*
11. *"Shadow Brokers: Hackers Claim to have Breached NSA's Equation Group"*. *15 August 2016.*
12. *"Shadow Brokers: NSA Exploits of the Week"*. *Medium.com*. *15 August 2016.*
13. *"The Shadow Brokers: Lifting the Shadows of the NSA's Equation Group?"*.
14. *Rob Price (August 15, 2016).* *"'Shadow Brokers' claim to have hacked an NSA-linked elite computer security unit"*. *Business Insider*. *Retrieved April 15, 2017.*
15. *"'Shadow Brokers' Reveal List Of Servers Hacked By The NSA; China, Japan, And Korea The Top 3 Targeted Countries; 49 Total Countries, Including: China, Japan, Germany, Korea, India, Italy, Mexico, Spain, Taiwan, & Russia"*. *Fortuna's Corner. 2016-11-01. Retrieved 2017-01-14.*
16. *"MESSAGE #6 - BLACK FRIDAY / CYBER MONDAY SALE"*. *bit.no.com. bit.no.com.*
17. *"unix_screenshots.zip"*. *bit.no.com.*
18. *theshadowbrokers (April 8, 2017).* *"Don't Forget Your Base"*. *Medium. Retrieved April 9, 2017.*
19. *Cox, Joseph.* *"They're Back: The Shadow Brokers Release More Alleged Exploits"*. *Motherboard. Vice Motherboard. Retrieved April 8, 2017.*
20. https://github.com/x0rz/EQGRP
21. *"Lost in Translation"*. *Steemit. April 14, 2017. Retrieved April 14, 2017.*
22. *"Share"*. *Yandex.Disk. Retrieved 2017-04-15.*
23. *"NSA-leaking Shadow Brokers just dumped its most damaging release yet"*. *Ars Technica. Retrieved 2017-04-15.*
24. *Larson, Selena (2017-04-14).* *"NSA's powerful Windows hacking tools leaked online"*. *CNNMoney. Retrieved 2017-04-15.*
25. *"Latest Shadow Brokers dump — owning SWIFT Alliance Access, Cisco and Windows"*. *Medium. 2017-04-14. Retrieved 2017-04-15.*
26. *"misterch0c"*. *GitHub. Retrieved 2017-04-15.*
27. *"Microsoft says users are protected from alleged NSA malware"*. *AP News. Retrieved April 15, 2017.*
28. *"Protecting customers and evaluating risk"*. *MSRC. Retrieved 2017-04-15.*
29. *"Microsoft says it already patched 'Shadow Brokers' NSA leaks"*. *Engadget. Retrieved April 15, 2017.*
30. *"Leaked NSA tools, now infecting over 200,000 machines, will be weaponized for years"*. *CyberScoop. Retrieved April 24, 2017.*
31. *"An NSA-derived ransomware worm is shutting down computers worldwide"*.
32. *Perlroth, Nicole; Scott, Mark; Frenkel, Sheera (June 27, 2017).* *"Cyberattack Hits Ukraine Then Spreads Internationally"*. *The New York Times*. *Arthur Ochs Sulzberger Jr.* *p. 1. Retrieved June 27, 2017.*
33. *Sum, Zero (2017-04-21).* *"zerosum0x0: DoublePulsar Initial SMB Backdoor Ring 0 Shellcode Analysis"*. *zerosum0x0. Retrieved 2017-11-15.*

34. *"Shining Light on The Shadow Brokers". The State of Security. 2017-05-18. Retrieved 2017-11-15.*
35. *"DanderSpritz/PeddleCheap Traffic Analysis" (PDF). Forcepoint. 2018-02-06. Retrieved 2018-02-07.*
36. *"Shadow Brokers: The insider theory". August 17, 2016.*
37. *"Commentary: Evidence points to another Snowden at the NSA". Reuters. August 23, 2016.*
38. *"Hints suggest an insider helped the NSA "Equation Group" hacking tools leak". Ars Technica. August 22, 2016.*
39. *Cox, Joseph (January 12, 2017). "NSA Exploit Peddlers The Shadow Brokers Call It Quits". Motherboard.*
40. *"Circumstantial evidence and conventional wisdom indicates Russian responsibility. Here's why that is significant". Twitter. August 16, 2016. Retrieved August 22, 2016.*
41. *"This leak is likely a warning that someone can prove US responsibility for any attacks that originated from this malware server". August 16, 2016. Retrieved August 22, 2016.*
42. *"TL;DR: This leak looks like a somebody sending a message that an escalation in the attribution game could get messy fast". twitter.com. Retrieved 22 August 2016.*
43. *Price, Rob. "Edward Snowden: Russia might have leaked alleged NSA cyberweapons as a 'warning'". Business Insider. Retrieved August 22, 2016.*
44. *Eric Lipton, David E. Sanger and Scott Shane (December 13, 2016). "The Perfect Weapon: How Russian Cyberpower Invaded the U.S." New York Times. Retrieved April 15, 2017.*
45. *Ghosh, Agamoni (April 9, 2017). "'President Trump what the f**k are you doing' say Shadow Brokers and dump more NSA hacking tools". International Business Times UK. Retrieved April 10, 2017.*
46. *"'NSA malware' released by Shadow Brokers hacker group". BBC News. April 10, 2017. Retrieved April 10, 2017.*
47. *Sam Biddle (August 19, 2016). "The NSA Leak is Real, Snowden Documents Confirm". The Intercept. Retrieved April 15, 2017.*
48. *"Powerful NSA hacking tools have been revealed online".*
49. *"Equation Group - Cyber Weapons Auction - Pastebin.com". 16 August 2016. Archived from the original on 15 August 2016.*
50. *Dan Goodin (January 12, 2017). "NSA-leaking Shadow Brokers lob Molotov cocktail before exiting world stage". Ars Technica. Retrieved January 14, 2017.*
51. *"Confirmed: hacking tool leak came from "omnipotent" NSA-tied group". Ars Technica. Retrieved January 14, 2017.*
52. *"The Equation giveaway - Securelist".*
53. *"Group claims to hack NSA-tied hackers, posts exploits as proof".*
54. *"The 'Shadow Brokers' NSA theft puts the Snowden leaks to shame - ExtremeTech". 19 August 2016.*

55. *"Shadow Brokers: Hackers Claim to have Breached NSA's Equation Group"*. *15 August 2016.*
56. *"Shadow Brokers: NSA Exploits of the Week"*. *Medium.com*. *15 August 2016.*
57. *"The Shadow Brokers: Lifting the Shadows of the NSA's Equation Group?"*.
58. *Rob Price (August 15, 2016). "'Shadow Brokers' claim to have hacked an NSA-linked elite computer security unit"*. *Business Insider*. *Retrieved April 15, 2017.*
59. *"'Shadow Brokers' Reveal List Of Servers Hacked By The NSA; China, Japan, And Korea The Top 3 Targeted Countries; 49 Total Countries, Including: China, Japan, Germany, Korea, India, Italy, Mexico, Spain, Taiwan, & Russia"*. *Fortuna's Corner. 2016-11-01. Retrieved 2017-01-14.*
60. *"MESSAGE #6 - BLACK FRIDAY / CYBER MONDAY SALE"*. *bit.no.com. bit.no.com.*
61. *"unix_screenshots.zip"*. *bit.no.com.*
62. *theshadowbrokers (April 8, 2017). "Don't Forget Your Base"*. *Medium. Retrieved April 9, 2017.*
63. *Cox, Joseph. "They're Back: The Shadow Brokers Release More Alleged Exploits"*. *Motherboard. Vice Motherboard. Retrieved April 8, 2017.*
64. https://github.com/x0rz/EQGRP
65. *"Lost in Translation"*. *Steemit. April 14, 2017. Retrieved April 14, 2017.*
66. *"Share"*. *Yandex.Disk. Retrieved 2017-04-15.*
67. *"NSA-leaking Shadow Brokers just dumped its most damaging release yet"*. *Ars Technica. Retrieved 2017-04-15.*
68. *Larson, Selena (2017-04-14). "NSA's powerful Windows hacking tools leaked online"*. *CNNMoney. Retrieved 2017-04-15.*
69. *"Latest Shadow Brokers dump — owning SWIFT Alliance Access, Cisco and Windows"*. *Medium. 2017-04-14. Retrieved 2017-04-15.*
70. *"misterch0c"*. *GitHub. Retrieved 2017-04-15.*
71. *"Microsoft says users are protected from alleged NSA malware"*. *AP News. Retrieved April 15, 2017.*
72. *"Protecting customers and evaluating risk"*. *MSRC. Retrieved 2017-04-15.*
73. *"Microsoft says it already patched 'Shadow Brokers' NSA leaks"*. *Engadget. Retrieved April 15, 2017.*
74. *"Leaked NSA tools, now infecting over 200,000 machines, will be weaponized for years"*. *CyberScoop. Retrieved April 24, 2017.*
75. *"An NSA-derived ransomware worm is shutting down computers worldwide"*.
76. *Perlroth, Nicole; Scott, Mark; Frenkel, Sheera (June 27, 2017). "Cyberattack Hits Ukraine Then Spreads Internationally"*. *The New York Times*. *Arthur Ochs Sulzberger Jr. p. 1. Retrieved June 27, 2017.*

77. *Sum, Zero (2017-04-21). "zerosum0x0: DoublePulsar Initial SMB Backdoor Ring 0 Shellcode Analysis". zerosum0x0. Retrieved 2017-11-15.*
78. *"Shining Light on The Shadow Brokers". The State of Security. 2017-05-18. Retrieved 2017-11-15.*
79. *"DanderSpritz/PeddleCheap Traffic Analysis" (PDF). Forcepoint. 2018-02-06. Retrieved 2018-02-07.*
80. *"Shadow Brokers: The insider theory". August 17, 2016.*
81. *"Commentary: Evidence points to another Snowden at the NSA". Reuters. August 23, 2016.*
82. *"Hints suggest an insider helped the NSA "Equation Group" hacking tools leak". Ars Technica. August 22, 2016.*
83. *Cox, Joseph (January 12, 2017). "NSA Exploit Peddlers The Shadow Brokers Call It Quits". Motherboard.*
84. *"Circumstantial evidence and conventional wisdom indicates Russian responsibility. Here's why that is significant". Twitter. August 16, 2016. Retrieved August 22, 2016.*
85. *"This leak is likely a warning that someone can prove US responsibility for any attacks that originated from this malware server". August 16, 2016. Retrieved August 22, 2016.*
86. *"TL;DR: This leak looks like a somebody sending a message that an escalation in the attribution game could get messy fast". twitter.com. Retrieved 22 August 2016.*
87. *Price, Rob. "Edward Snowden: Russia might have leaked alleged NSA cyberweapons as a 'warning'". Business Insider. Retrieved August 22, 2016.*
88. *Eric Lipton, David E. Sanger and Scott Shane (December 13, 2016). "The Perfect Weapon: How Russian Cyberpower Invaded the U.S." New York Times. Retrieved April 15, 2017. Fox-Brewster, Thomas (February 16, 2015). "Equation = NSA? Researchers Uncloak Huge 'American Cyber Arsenal'". Forbes. Retrieved November 24, 2015.*
89. *Menn, Joseph (February 17, 2015). "Russian researchers expose breakthrough U.S. spying program". Reuters. Retrieved November 24, 2015.*
90. *"The nsa was hacked snowden documents confirm". The Intercept. 19 August 2016. Retrieved 19 August 2016.*
91. *"Who Was the NSA Contractor Arrested for Leaking the 'Shadow Brokers' Hacking Tools? — Krebs on Security". krebsonsecurity.com. Retrieved 2017-11-28.*
92. *GReAT (February 16, 2015). "Equation: The Death Star of Malware Galaxy". securelist.com. Kaspersky Lab.*
93. *Goodin, Dan (February 16, 2015). "How "omnipotent" hackers tied to NSA hid for 14 years—and were found at last". Ars Technica. Retrieved November 24, 2015.*
94. *Kirk, Jeremy (17 February 2015). "Destroying your hard drive is the only way to stop this super-advanced malware". PCWorld. Retrieved November 24, 2015.*
95. *Goodin, Dan. "After NSA hacking exposé, CIA staffers asked where Equation Group went wrong". Ars Technica. Retrieved 21 March 2017.*

96. *"What did Equation do wrong, and how can we avoid doing the same?"*. *Vault 7*. *WikiLeaks*. *Retrieved 21 March 2017.*
97. *"Equation Group: The Crown Creator of Cyber-Espionage"*. *Kaspersky Lab. February 16, 2015. Retrieved November 24, 2015.*
98. *"Equation Group: Questions and Answers (Version: 1.5)" (PDF). Kaspersky Lab. February 2015. Retrieved November 24, 2015.*
99. *Goodin, Dan (March 11, 2015). "New smoking gun further ties NSA to omnipotent "Equation Group" hackers". Ars Technica. Retrieved November 24, 2015.*
100. *"A Fanny Equation: "I am your father, Stuxnet"". Kaspersky Lab. February 17, 2015. Retrieved November 24, 2015.*
101. *"The Equation Group Equals NSA / IRATEMONK". F-Secure Weblog : News from the Lab. February 17, 2015. Retrieved November 24, 2015.*
102. *Schneier, Bruce (January 31, 2014). "IRATEMONK: NSA Exploit of the Day". Schneier on Security. Retrieved November 24, 2015.*
103. *Goodin, Dan (August 15, 2016). "Group claims to hack NSA-tied hackers, posts exploits as proof". Ars Technica. Retrieved August 19, 2016.*
104. *Goodin, Dan (August 16, 2016). "Confirmed: hacking tool leak came from "omnipotent" NSA-tied group". Ars Technica. Retrieved August 19, 2016.*
105. *Thomson, Iain (August 17, 2016). "Cisco confirms two of the Shadow Brokers' 'NSA' vulns are real". The Register. Retrieved August 19, 2016.*
106. *Pauli, Darren (August 24, 2016). "Equation Group exploit hits newer Cisco ASA, Juniper Netscreen". The Register. Retrieved August 30, 2016.*
107. *Goodin, Dan (April 14, 2017). "NSA-leaking Shadow Brokers just dumped its most damaging release yet". Ars Technica. p. 1. Retrieved May 13, 2017.*
108. *Nakashima, Ellen; Timberg, Craig (2017-05-16). "NSA officials worried about the day its potent hacking tool would get loose. Then it did". Washington Post. ISSN 0190-8286. Retrieved 2017-12-19.*
109. *Fox-Brewster, Thomas (May 12, 2017). "An NSA Cyber Weapon Might Be Behind A Massive Global Ransomware Outbreak". Forbes. p. 1. Retrieved May 13, 2017.*
110. *Goodin, Dan (May 12, 2017). "An NSA-derived ransomware worm is shutting down computers worldwide". Ars Technica. p. 1. Retrieved May 13, 2017.*
111. *Ghosh, Agamoni (April 9, 2017). "'President Trump what the f**k are you doing' say Shadow Brokers and dump more NSA hacking tools". International Business Times UK. Retrieved April 10, 2017.*
112. *"'NSA malware' released by Shadow Brokers hacker group". BBC News. April 10, 2017. Retrieved April 10, 2017.*
113. *Perlroth, Nicole; Scott, Mark; Frenkel, Sheera (June 27, 2017). "Cyberattack Hits Ukraine Then Spreads Internationally". The New York Times. Arthur Ochs Sulzberger Jr. p. 1. Retrieved June 27, 2017.*
114. *"EternalBlue Exploit Used in Retefe Banking Trojan Campaign". Threatpost. Retrieved 2017-09-26.*

115. *"CVE-2017-0144". CVE - Common Vulnerabilities and Exposures. The MITRE Corporation. September 9, 2016. p. 1. Retrieved June 28, 2017.*
116. *"Microsoft Windows SMB Server CVE-2017-0144 Remote Code Execution Vulnerability". SecurityFocus. Symantec. March 14, 2017. p. 1. Retrieved June 28, 2017.*
117. *"Vulnerability CVE-2017-0144 in SMB exploited by WannaCryptor ransomware to spread over LAN". ESET North America. Archived from the original on May 16, 2017. Retrieved May 16, 2017.*
118. *"NSA officials worried about the day its potent hacking tool would get loose. Then it did". Retrieved 25 September 2017.*
119. *"Microsoft Security Bulletin MS17-010 – Critical". technet.microsoft.com. Retrieved May 13, 2017.*
120. *Warren, Tom (May 13, 2017). "Microsoft issues 'highly unusual' Windows XP patch to prevent massive ransomware attack". The Verge. Vox Media. Retrieved May 13, 2017.*
121. *Newman, Lily Hay (March 12, 2017). "The Ransomware Meltdown Experts Warned About Is Here". wired.com. p. 1. Retrieved May 13, 2017.*
122. *Goodin, Dan (May 15, 2017). "Wanna Decryptor: The NSA-derived ransomware worm shutting down computers worldwide". Ars Technica UK. p. 1. Retrieved May 15, 2017.*
123. *Warren, Tom (April 15, 2017). "Microsoft has already patched the NSA's leaked Windows hacks". The Verge. Vox Media. p. 1. Retrieved May 30, 2017.*
124. *"NSA Exploits Ported to Work on All Windows Versions Released Since Windows 2000". www.bleepingcomputer.com. Retrieved 2018-02-05.*
125. *"The need for urgent collective action to keep people safe online: Lessons from last week's cyberattack - Microsoft on the Issues". Microsoft on the Issues. 2017-05-14. Retrieved 2017-06-28.*
126. *Titcomb, James (May 15, 2017). "Microsoft slams US government over global cyber attack". The Telegraph. p. 1. Retrieved June 28, 2017.*
127. *"New SMB Worm Uses Seven NSA Hacking Tools. WannaCry Used Just Two)".*
128. *"Newly identified ransomware 'EternalRocks' is more dangerous than 'WannaCry' - Tech2". Tech2. 2017-05-22. Retrieved 2017-05-25.*
129. *"Miroslav Stampar on Twitter". Twitter. Retrieved 2017-05-30.*
130. *"stamparm/EternalRocks". GitHub. Retrieved 2017-05-25.*