Case Study – Maersk // NotPetya

Maersk has revealed that a devastating ransomware attack which struck businesses across Europe in 2017 required close to a "complete infrastructure" overhaul and the reinstallation of thousands of machines.

The Danish transport and logistics conglomerate fell prey to a campaign which used a modified version of the Petya ransomware, NonPetya, bringing down IT systems and operational controls across the board.

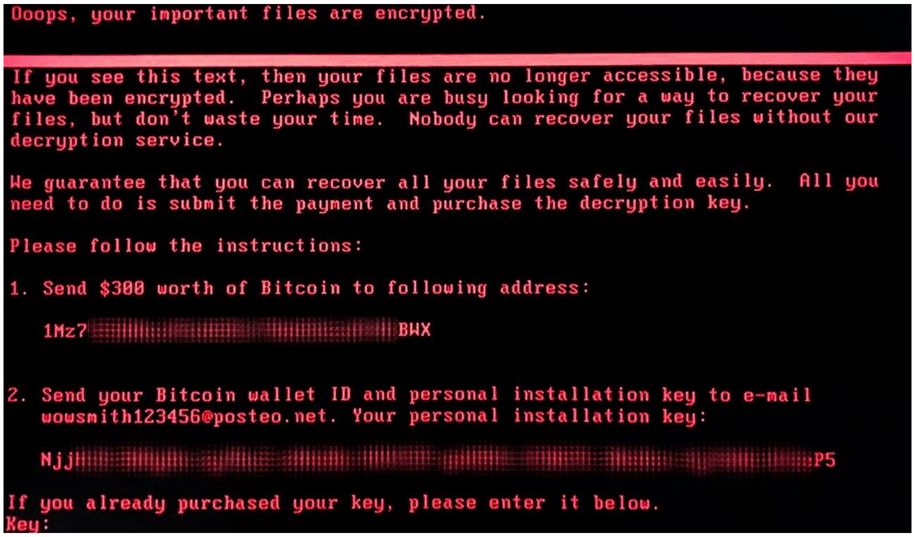
The firm, with offices in 130 countries and a workforce of close to 90,000, was one of the most high-profile victims of the Petya campaign, which spread rapidly by utilizing the leaked US National Security Agency (NSA) exploit EternalBlue, which targets Microsoft Windows systems.

In Maersk's case, while no customer or business data is believed to have been exposed, the firm endured severe disruption and was forced to halt operations as the ransomware spread through core IT systems.

Speaking at the World Economic Forum this week, Møller-Maersk Chairman Jim Hagemann Snabe shared further details on the attack, which resulted in a reinstall of "our entire infrastructure," according to the executive.

In total, Maersk reinstalled 4,000 servers, 45,000 PCs, and 2,500 applications in what the chairman called a "heroic effort" over ten days, one in which the executive said may have usually taken up to six months to implement.

"Imagine a company where a ship with 10 to 20 thousand containers is entering a port every 15 minutes, and for 10 days, you have no IT," Hagemann commented. "It's almost impossible to even imagine."



```
Ooops, your important files are encrypted.

If you see this text, then your files are no longer accessible, because they
have been encrypted.  Perhaps you are busy looking for a way to recover your
files, but don't waste your time.  Nobody can recover your files without our
decryption service.

We guarantee that you can recover all your files safely and easily.  All you
need to do is submit the payment and purchase the decryption key.

Please follow the instructions:

1. Send $300 worth of Bitcoin to following address:

   1Mz7[redacted]BWX

2. Send your Bitcoin wallet ID and personal installation key to e-mail
   wowsmith123456@posteo.net. Your personal installation key:

   Njj[redacted]P5

If you already purchased your key, please enter it below.
Key:
```

Source:

NonPetya ransomware forced Maersk to reinstall 4000 servers, 45000 PCs

By Charlie Osborne for Zero Day | January 26, 2018 -- 10:25 GMT (21:25 AEDT)

https://www.zdnet.com/article/maersk-forced-to-reinstall-4000-servers-45000-pcs-due-to-notpetya-attack/

Case Study – Norsk Hydro // LockerGoga

Researchers are still looking for answers when it comes to LockerGoga's initial infection method – and what the attackers behind the ransomware really want.

LockerGoga, the malware that took down Norsk Hydro last week, has taken the industrial world by storm, as researchers race to uncover more about the mysterious ransomware that crippled several of the aluminum maker's plants.

Questions still remain about how the malware first infects the system it targets, who is behind the attacks – and what they want. But there is one thing researchers can agree on when it comes to the seemingly-unsophisticated LockerGoga: Its developers are actively adding capabilities and targeting operations with attacks bent on destruction and costing companies millions.

"We do know that this ransomware has caused significant harm," said Palo Alto Networks Unit 42 researcher Mike Harbison in a Tuesday post. "The damage could increase significantly if the attackers continue to refine this ransomware."

A (Short) History

LockerGoga made headlines last week after targeting Norsk Hydro, forcing the company to shut down or isolate several plants and send several more into manual mode. According to an update by the company, that incident has so far cost Norsk Hydro at least $40 million in the last week.

But the ransomware was around well before this incident, spotted as early as Jan. 24 in an attack against engineering consultancy Altran, which said in a statement it was hit by a cyberattack that impacted operations in "some European countries."

Two other manufacturing companies, Hexion and Momentive, have also been hit by the ransomware, according to reports. So far, researchers with Palo Alto Networks said they have identified 31 ransomware samples that are similar in behavior and code to the initial variant.

Characteristics

The initial infection of LockerGoga remains a mystery, researchers said: "The initial infection was thought to be a phishing attack, but seems like a less likely scenario as no phishing emails have been reported," Allan Liska, threat intel analyst with Recorded Future, told Threatpost. "It is likely some form of remote access, such as an open RDP server."

Once downloaded onto the system, the malware relocates itself into a "temp" folder and renames itself using the command line (cmd).

From there, LockerGoga encrypts files stored on systems such as desktops, laptops and servers, researchers with Trend Micro said in a post last week.

Interestingly, LockerGoga appears to have both ransomware and wiper capabilities: While the malware leverages an encryption process that removes the victim’s ability to access files and other data on infected systems, various later versions of LockerGoga were also observed forcibly logging the victim off of the infected systems by changing their passwords, and removing their ability to even log back in to the system, according to Talos researchers.

Source:

Ransomware Behind Norsk Hydro Attack Takes On Wiper-Like Capabilities

Author: Lindsey O'Donnell, March 27, 2019 8:48 am

https://threatpost.com/lockergoga-ransomware-norsk-hydro-wiper/143181/

OSLO (Reuters) - Production at Norwegian aluminum maker Norsk Hydro was back to near normal after a cyber attack last month, the company said on Friday.

The group halted some of its production on March 19 and switched other units to manual operation after hackers blocked its systems with ransomware.

It has said it would not pay hackers to unlock its files, but has not said if it actually received any ransom demand.

“In terms of production output, most operations are back to normal or near normal levels,” it said. “The cyber attack has, however, caused delays to certain administrative processes, including systems for reporting, billing and invoicing.”

The company said it would take time to get IT operations fully back to normal after what it dubbed a sophisticated attack. It didn’t give a timeframe for this.

Despite the attack, Hydro’s primary metals business and most other units were able to carry on production with workarounds and manual solutions, though output of its extrusion business, which makes components for carmakers, builders and other industries, was reduced by 50 percent.

Source:

Norsk Hydro's production near normal after cyber attack

Reuters, APRIL 5, 2019 / 2:29 PM / 22 DAYS AGO

https://www.reuters.com/article/us-norsk-hydro-cyber-output/norsk-hydros-production-near-normal-after-cyber-attack-idUSKCN1RH1O3

Case Study – ASUS // Operation ShadowHammer

In January 2019, we discovered a sophisticated supply chain attack involving the ASUS Live Update Utility. The attack took place between June and November 2018 and according to our telemetry, it affected a large number of users.

ASUS Live Update is a utility that is pre-installed on most ASUS computers and is used to automatically update certain components such as BIOS, UEFI, drivers and applications. According to Gartner, ASUS is the world’s 5th-largest PC vendor by 2017 unit sales. This makes it an extremely attractive target for APT groups that might want to take advantage of their userbase.

Based on our statistics, over 57,000 Kaspersky users have downloaded and installed the backdoored version of ASUS Live Update at some point in time. We are not able to calculate the total count of affected users based only on our data; however, we estimate that the real scale of the problem is much bigger and is possibly affecting over a million users worldwide.

The goal of the attack was to surgically target an unknown pool of users, which were identified by their network adapters’ MAC addresses. To achieve this, the attackers had hardcoded a list of MAC addresses in the trojanized samples and this list was used to identify the actual intended targets of this massive operation. We were able to extract more than 600 unique MAC addresses from over 200 samples used in this attack. Of course, there might be other samples out there with different MAC addresses in their list.

We believe this to be a very sophisticated supply chain attack, which matches or even surpasses the Shadowpad and the CCleaner incidents in complexity and techniques. The reason that it stayed undetected for so long is partly due to the fact that the trojanized updaters were signed with legitimate certificates (eg: “ASUSTeK Computer Inc.”). The malicious updaters were hosted on the official liveupdate01s.asus[.]com and liveupdate01.asus[.]com ASUS update servers.

Although precise attribution is not available at the moment, certain evidence we have collected allows us to link this attack to the ShadowPad incident from 2017. The actor behind the ShadowPad incident has been publicly identified by Microsoft in court documents as BARIUM. BARIUM is an APT actor known to be using the Winnti backdoor. Recently, our colleagues from ESET wrote about another supply chain attack in which BARIUM was also involved, that we believe is connected to this case as well.

Source:

Operation ShadowHammer

By GReAT, AMR on March 25, 2019. 1:01 pm

https://securelist.com/operation-shadowhammer/89992/

Case Study – Petro Rabigh // TRITON/TRISIS

On Aug. 4, 2017, at 7:43 p.m., two emergency shutdown systems sprang into action as darkness settled over the sprawling refinery along Saudi Arabia's Red Sea coast.

The systems brought part of the Petro Rabigh complex offline in a last-gasp effort to prevent a gas release and deadly explosion. But as safety devices took extraordinary steps, control room engineers working the weekend shift spotted nothing out of the ordinary, either on their computer screens or out on the plant floor.

The reasons for the sudden shutdown were still buried under zeros and ones, nestled deep within the code of the compromised Schneider Electric safety equipment.

Investigators soon discovered a dangerous hacking tool that would usher in a new chapter in the global cyber arms race, much like the Stuxnet worm that damaged Iranian nuclear centrifuges at the start of the decade. The discovery of the Triton malware, named for the Triconex line of safety systems it triggered, echoed from the ancient Saudi city of Rabigh to a research institute in Moscow, and from California to Tokyo.

"Worst-case scenario here, you're dealing with a potential release of toxic hydrogen sulfide gases, a potential for explosions from high pressure, high temperature," said Julian Gutmanis, a cybersecurity contractor who sources say led the Saudi Arabian Oil Co.'s investigation of the Triton intrusion.

"We considered the entire organization to be compromised," Gutmanis said at the S4 cybersecurity conference in Miami earlier this year, where he declined to name the target facility or even identify his employer. "We had a very sophisticated attacker. We knew that the systems, and the integrity of these systems, can no longer be trusted."

Petro Rabigh is a 3,000-acre maze of steel pipes, hulking distillation towers and catalytic reformers, their distinctive, red-and-white caps poking up like toxic candy canes. It is one of the biggest facilities of its kind in the world.

The integrated chemical and refining complex produces more than 5 million tons of petrochemicals a year, from antifreeze to common plastics like polypropylene. It also churns out millions of barrels of refined products annually, including kerosene and gasoline. Situated along the Red Sea, Petro Rabigh has emerged as a major supplier to African, Asian and European markets. The company was launched as a joint venture between the Saudi Arabian Oil Co., the world's biggest oil company — known as Saudi Aramco — and Tokyo-based Sumitomo Chemical.

The facility stands as a poster child for Schneider Electric, one of the world's top suppliers of industrial control equipment. The French company won an operations management contract with Petro Rabigh as it expanded in the late 2000s.

In June 2017, on a Saturday during the Islamic holy month of Ramadan, Schneider Electric product specialists were called in to assess an apparently malfunctioning Triconex unit. The safety device had tripped part of Petro Rabigh offline, but it wasn't clear why. Everything seemed to be working normally.

Triconex equipment is designed to act, not to warn, like a home circuit breaker that trips automatically when outlets are dangerously overloaded. Triconex devices come loaded with a digital road map that allows them to constantly scan for unsafe conditions. If enough devices agree something's wrong, they won't wait for a human go-ahead. They'll simply grind industrial processes to a halt.

Key Take-Aways

- The malware targets Schneider Electric’s Triconex safety instrumented system (SIS) thus the name choice of TRISIS for the malware.
- TRISIS has been deployed against at least one victim.
- The victim identified so far is in the Middle East, and currently, there is no intelligence to support that there are victims outside of the Middle East.
- The Triconex line of safety systems are leveraged in numerous industries - however, each SIS is unique and to understand process implications would require specific knowledge of the process. This means that this is not a highly scalable attack that could be easily deployed across numerous victims without significant additional work.
- The Triconex SIS Controller was configured with the physical keyswitch in ‘program mode’ during operation. If the controller is placed in Run mode (program changes not permitted), arbitrary changes in logic are not possible substantially reducing the likelihood of manipulation.
- Although the attack is not highly scalable, the tradecraft displayed is now available as a blueprint to other adversaries looking to target SIS and represents an escalation in the type of attacks seen to date as it is specifically designed to target the safety function of the process.
- Compromising the security of an SIS does not necessarily compromise the safety of the system. Safety engineering is a highly specific skill set and adheres to numerous standards and approaches to ensure that a process has a specific safety level. As long as the SIS performs its safety function the compromising of its security does not represent a danger as long as it fails safe.
- It is not currently known what exactly the safety implications of TRISIS would be. Logic changes on the final control element implies that there could be risk to the safety as set points could be changed for when the safety system would or would not take control of the process in an unsafe condition

Sources:

The inside story of the world's most dangerous malware

Blake Sobczak, E&E News reporter Energywire: Thursday, March 7, 2019

https://www.eenews.net/stories/1060123327

TRISIS Malware - Analysis of Safety System Targeted Malware

Dragos

https://dragos.com/wp-content/uploads/TRISIS-01.pdf

RESOURCES

CIS Center for Internet Security®

CIS Controls

https://www.cisecurity.org/controls/

Cybersecurity Framework

https://www.nist.gov/cyberframework

NIST
National Institute of
Standards and Technology
U.S. Department of Commerce

Special Publication 800 Series

https://csrc.nist.gov/publications/sp800

Special Publication 1800 Series

https://csrc.nist.gov/publications/sp1800

Australian Government
Australian Signals Directorate

ACSC
Australian
Cyber Security
Centre

Essential 8

https://www.cyber.gov.au/publications/essential-eight-explained

Strategies to Mitigate Cyber Security Incidents

https://www.cyber.gov.au/publications/strategies-to-mitigate-cyber-security-incidents