MINERVA

Minerva Labs Research Report:
2017 Year in Review

CONTENTS

Executive Summary

End of the year offers an opportunity to reflect upon the key events that have shaped 2017 and set the direction for 2018. At Minerva, we are focused on understanding the nature of threats that succeed at bypassing security tools, so we may enhance the security architecture without overlapping with other approaches. From this perspective, in 2017 we saw both the deployment of defensive measures that have been unavailable to the community at large until recently, as well as the ability among the attackers to breach our defenses despite these measures.

Endpoint security discussions in 2017 often included conversations about the use of machine learning in anti-malware products. It's encouraging to see advancements such as artificial intelligence being incorporated into traditional and "next-gen" endpoint security solutions; however, 2017 has shown that the adversaries continue to find ways around such defensive measures. Minerva's research into the malware families that were prevalent in 2017, including popular exploit kits and ransomware, has shown that such malicious programs employ at least one evasion technique to penetrate defenses.

Sophisticated exploits and anti-malware evasion will continue to grow in popularity, in part in response to the continued advancements in endpoint security products available to defenders.

The use of powerful techniques to bypass enterprise defenses is not limited to advanced adversaries. For instance, the methods published by Shadow Broker in 2017 made it possible to rapidly distribute malicious software even without an in-depth understanding of exploit development. Similarly, the tactics for evading detection by anti-malware products are widely-known in the criminal community, with custom and open source tools available for implementing them to increase infection rates.

In 2017, adversaries continued to monetize or otherwise benefit from the classic use of malicious software, which included holding systems at ransom, conducting industrial espionage, and stealing sensitive personal data. Closer to the end of the year, we've seen an increase in another tactic: the use of malicious software that used victims' systems to mine cryptocurrency on behalf of the intruder.

As we learn from 2017 to understand where the security industry will be in 2018, we expect the continued commoditization of the attack tactics that at some point were considered advanced. Sophisticated exploits and anti-malware evasion will continue to grow in popularity, in part in response to the continued advancements in endpoint security products available to defenders. Such techniques will be used in both classic forms of malware, such as ransomware, as well as in malware that offers adversaries new revenue streams, such as malicious cryptominers. Minerva, in turn, will continue to provide technology that "attacks" any attempt to evade security tools on the endpoint, strengthening enterprise security posture to cover the gap left by baseline anti-malware tools.

Malware Going More Evasive

Evasion in Exploit Kits

Exploit kits, which target vulnerabilities in client-side software of website visitors remained an effective attack vector in 2017. Execute Malware, a technical blog discussing malware internals, published a graph of exploit kit campaigns from 2017. The data was collected from multiple trusted sources. Minerva took this publication and used it as a basis for a different study, testing to what degree evasive exploit kits are.

The data was originally displayed as a graph – an exploit kit campaign and all the possible payloads it delivered. Our team of researchers observed the data as "infection paths", from the exploit kit via intermediate downloaders to the actual payloads. A total of 74 infection paths were tested, enumerating all possible combinations as seen in the wild.

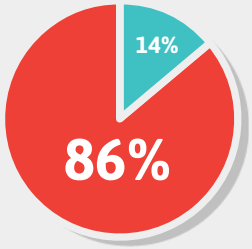
Campaign	StageOne	StageTwo	Prevented Chain
Rig EK	Rig EK	ASN1 Ransomware	✓
Rig EK	Rig EK	Banitu	✓
RoughTed Campaign	Rig EK	Banitu	✓
Unnamed Malversting Campaign	Rig EK	Banitu	✓
Magnitude EK	Magnitude EK	Cerber Ransomware	✓
RoughTed Campaign	Magnitude EK	Cerber Ransomware	✓
Unnamed Malversting Campaign	Magnitude EK	Cerber Ransomware	✓
Seamless	Rig EK	Cerber Ransomware	✓
EITset	Rig EK	Cerber Ransomware	✓
pseudoDarkleech	Rig EK	Cerber Ransomware	✓
EITset	Rig-V	Cerber Ransomware	✓
pseudoDarkleech	Rig-V	Cerber Ransomware	✓
Rig EK	Rig EK	Cthonic	✓
HookAds	Rig EK	Cthonic	✓
RoughTed Campaign	Rig EK	Cthonic	✓
Despicable Campaign	Rig EK	Cthonic	✓
Unnamed Malversting Campaign	Rig EK	Cthonic	✓
Rig EK	Rig EK	DELoader/Zloader	✓
Rig EK	Rig EK	Dreambot	✓
HookAds	Rig EK	Dreambot	✓
EITset	Rig EK	Dreambot	✓
Unnamed Malversting Campaign	Rig EK	Dreambot	✓

Partial list of the enumerated combinations, grey cell is a prevented exploit kit or payload

For each combination, we analyzed both exploit kit and payload separately, verifying whether they are evasive or not and if so – if they are prevented by Minerva's Anti-Evasion Platform.

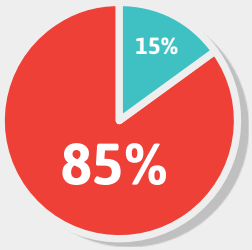
*Out of the 74 different infection paths **86%** would have been prevented during the first exploit kit phase*

This number is not a surprise, as many kits "traditionally" use exploits to detect virtual machines, anti-exploitation products and network sniffers to avoid detection and malware analysis.



Exploit Kits

- Evasive, Prevented
- Not Prevented



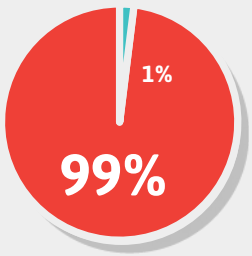
Payload

- Evasive, Prevented
- Not Prevented

Similarly, 85% of the payloads were evasive and prevented by Minerva's Anti-Evasion Platform:
This data is consistent with the results of previous researches by Qualys from 2012 and 2014, which determined that over 80% of malware in general possesses evasive characteristics.

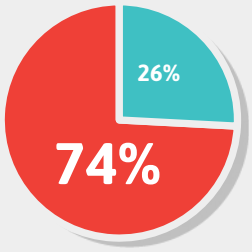
Out of the 99%, three quarters of the paths included both evasive exploit kit and a payload

When considering the entire "path" from an initial infection to a running payload, we were able to verify that 99% of the campaigns were evasive either in the exploit kit or the payload phase:



Overall

- Evasive, Prevented
- Insufficient Data



Total

- Prevented in more than one stage
- Prevented in one stage

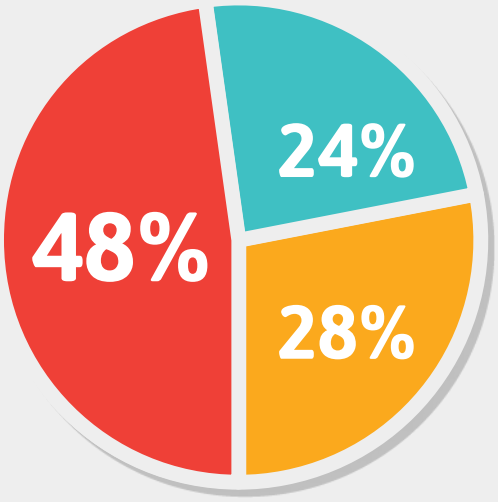
Quantifying Evasive Ransomware

Since Minerva's focus is on stopping malware that tries to get around other security tools, our research team took a close look at the evasive capabilities of popular ransomware families including Locky, Spora, TeslaCrypt, Cryptomix, JigSaw and so on. We discovered that in almost all cases, the samples employed at least one evasive tactic, which explained their ability to thrive in the wild.

The samples included executable files, malicious Microsoft Office documents, script-based downloaders based on PowerShell and many others. We verified that the samples we collected are alive by detonating them in a clean unprotected environment, proceeding only if the sample successfully encrypted the test machine.

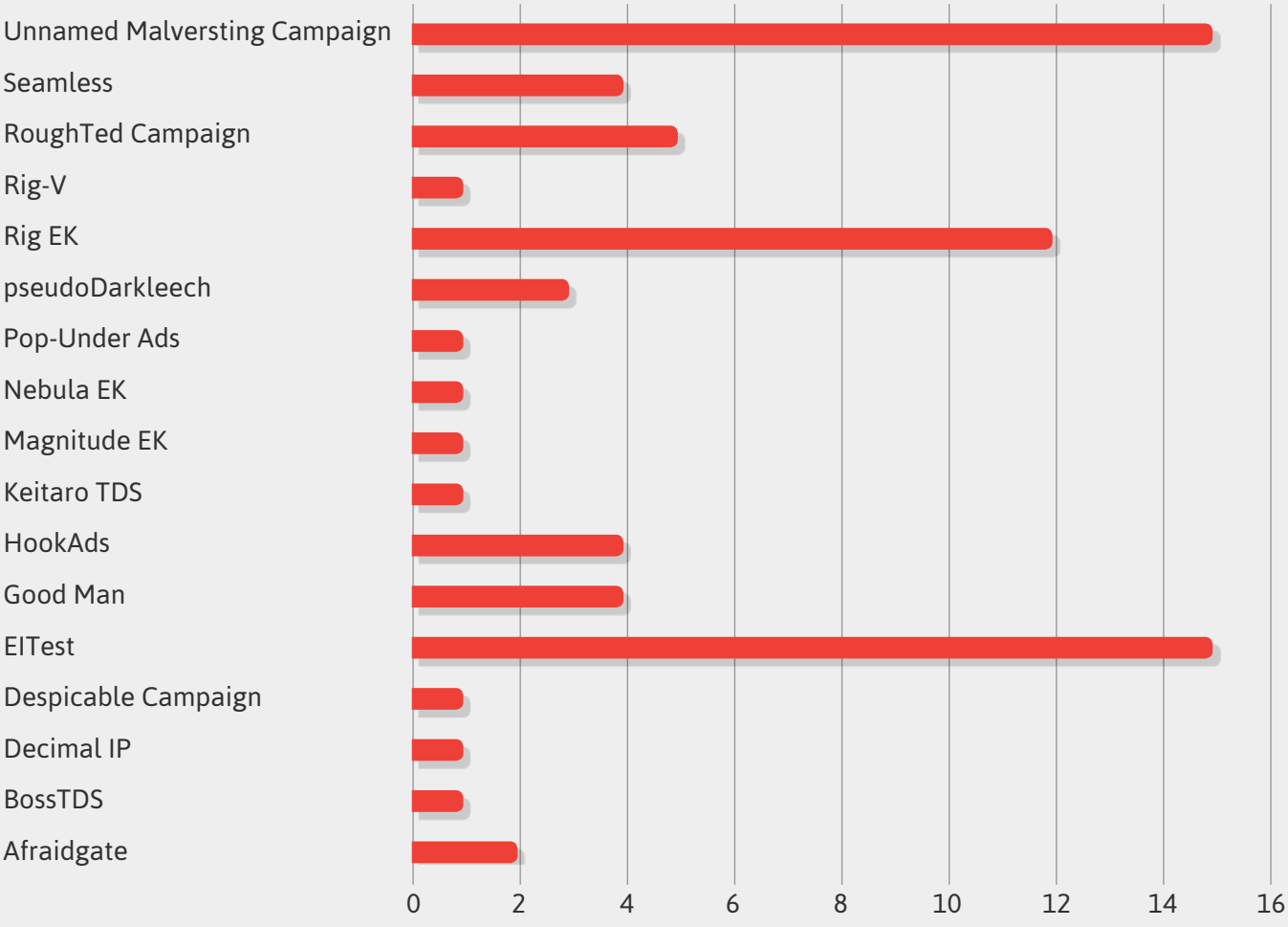
Next, we detonated the same malware on the same machine, now protected by Minerva's Anti-Evasion Platform. Minerva's team of researchers recorded the differences in the behavior of the malware, classifying each sample's evasive techniques.

Roughly half of the samples were prevented by the Memory Injection Prevention module, blocking malicious execution of code in the context of a different process. The next most potent module was Hostile Environment Simulation, closely followed by the Malicious Document Prevention module.



Exploit kits were among the most common ways to spread ransomware in 2017 with over 60% of them applying evasive techniques

Interestingly, the actual percentage of evasive ransomware is probably even higher than shown in the graph. Minerva tested only the payloads and some of the droppers, but exploit kits were also among the most common ways to spread ransomware in 2017 with over 60% of them applying evasive techniques.



Number of exploit kit campaigns delivering Ransomware

Note that as mentioned in the separate section discussing exploit kits in detail – when observing the overall chain of infection, from the malware serving website to the final ransomware payload, usually there is more than a single evasive stage. Over 60% of the tested ransomware "chains" would have been prevented in a real-life scenario more than once.

The Shadow Brokers Leak Aftermath

One of the most noteworthy events of the past year took place in June when an elusive group named The Shadow Brokers publicly released a repository of extremely potent exploits.

Since the leaked exploits were released, there was a spike in viral malware abusing ETERNALBLUE/DOUBLEPULSAR and ETERNALROMANCE. It is impossible to know exactly how many people were affected by this spike, but in the months following the exploits' release, many suffered from the damage caused by the adversaries who employed them.

Examples of malware that spread using the exploits published by The Shadow Brokers include not only the high-profile samples such as WannaCry and NotPetya, but also lesser-known malware families such as the Adylkuzz cryptominer.

Most of the exploits "casualties" so far were large enterprises. NotPetya, for example, caused damages of roughly $300 million to Maersk, Merck and FedEx. Moreover, WannaCry losses could be as high as $4 billion.

The use of the exploits leaked by The Shadow Brokers is likely to lead to more damages, as was the case with other potent attack tools released in the past.

For example, the leak of Hacking Team's exploits in 2015 showed that while only a handful of attackers successfully integrated the exploits initially, an increasing number of malware samples integrated the exploits as time went by.

Not surprisingly, we have observed how the Shadow Brokers' exploits is increasingly used by commodity malware for propagation. Retefe, a banking Trojan targeting mostly Europe, now infects endpoints utilizing ETERNALBLUE/DOUBLEPULSAR.

ETERNALBLUE/DOUBLEPULSAR exploits make Retefe much more powerful, capable of virally infecting large enterprise networks even if only a single user was successfully infected in the initial attack.

Even the common open-source framework Metasploit has a module implementing ETERNALBLUE/DOUBLEPULSAR, making us believe that we will see much more of these exploits in the near future.

Vaccination Renaissance

Many malware samples are designed to avoid infecting the endpoint more than once by relying on its infection markers to establish its presence on the system. A marker could be an artifact such as a specific registry key, a file, or a mutex object. Defenders who can generate the right infection markers can vaccinate their endpoints against corresponding malicious programs.

Defenders who can generate the right infection markers can vaccinate their endpoints against corresponding malicious programs.

While the concept of vaccination is not new, organizations are starting to pay more attention to it due to the broader availability of the tools that make it feasible to deploy vaccines in the enterprise. Minerva makes it especially practical to accomplish this by simulating the presence of the infection markers without generating an actual artifact, fooling the malware to skip the inoculated endpoint.

Spora was distributed mainly by massive malicious e-mail campaigns and infected websites.

Another reason for the increased interest in vaccination might be tied to the increasing difficulty in detecting evasive malware. In contrast, infection markers are mostly easy to spot.

Minerva observed many malware samples in the past year that can be controlled using vaccination, including the following:

Spora – Similar but Not the Same

Spora was one of the more prolific ransomware families in 2017. It was different from most ransomware because it encrypted files even when the victim's system was not connected to the Internet. Spora was distributed mainly by massive malicious e-mail campaigns and infected websites.

Spora could be controlled using vaccination. This ransomware creates a mutex-based infection marker whose name it derives on the basis of the infected computer's volume serial number. If Spora discovers that its mutex is already present on the machine, it does not infect the endpoint.

Endpoint vaccination prevented Spora, WannaCry, NotPetya and other malicious programs by simulating infection markers

WannaCry – Catastrophe Averted?

The WannaCry worm leveraged the ETERNALBLUE/DOUBLEPULSAR exploits alongside other tactics to spread itself worldwide. As with most ransomware, WannaCry encrypted the files on the victim's machine and demanded payment to decrypt them. In this case, ***the payments varied between $300 to $600 worth in Bitcoin. Within 24 hours WannaCry infected over 230,000 machines in over 150 countries.***

Early during the outbreak, the defenders were uncertain whether their security tools were effective at blocking WannaCry. However, researchers discovered two ways to control the behavior of WannaCry variants to prevent infections. The first measure involved allowing this malware to access a specific domain via a URL, which WannaCry used to detect whether it was running in an analysis environment. If the malware succeeded at connecting to this URL, it terminated itself, because it believed that it was being examined in an unwanted/hostile environment. A security researcher named Marcus Hutchins discovered this "kill switch" and registered the domain. This allowed endpoints to successfully connect to this URL, preventing the worm from infecting endpoints. Researchers also discovered that there was another way to fool WannaCry into not infecting the host. This malware checked for and created a mutex named MsWinZonesCacheCounterMutexA. If the mutex was already present on the machine, WannaCry halted its execution before damaging the system. This infection marker could be used as a vaccine against WannaCry.

NotPetya

NotPetya is another example of the devastating abilities of modern malware. At first, researchers treated this specimen as a new variant of the Petya ransomware due to the appearance of its ransom notice. Later, the researchers realized that ransomware was not the true objective of this malicious program. NotPetya hit large companies, such as the shipping company Maersk, causing a halt to operations across 76 port terminals around the world. NotPetya was built to spread rapidly across the network and made it impossible to decrypt the files – its main purpose was to cause damage, and not to earn money. A fellow malware researcher discovered that before NotPetya causes damage to the machine, it attempts to create the file "c:\windows\perfc.dat". To vaccinate an endpoint against NotPetya, organizations could create this file with read-only permissions.

Mystique – Fighting malware with Automatic Infection Markers Extraction

During the past year we saw numerous malware samples that employed infection markers and, therefore, could be controlled via vaccination. Minerva developed an open-source tool called Mystique to help organizations automatically derive mutex-based infection markers from malware for vaccination purposes.

Mystique examines how the malware reacts to the presence of the mutex artifacts the specimen generates when running in a sandbox environment. The tool then creates these artifacts after detonating the specimen in the sandbox again and reports whether the sample's execution flow has changed. Mystique makes it possible to analyze a large set of malware to derive potential vaccines. Going over Mystique shows that it's possible to automatically determine whether a malware sample is subject to vaccination even without being a malware expert.

Mystique examines how the malware reacts to the presence of the mutex artifacts the specimen generates when running in a sandbox environment. The tool then creates these artifacts after detonating the specimen in the sandbox again and reports whether the sample's execution flow has changed. Mystique makes it possible to analyze a large set of malware to derive potential vaccines. Going over Mystique shows that it's possible to automatically determine whether a malware sample is subject to vaccination even without being a malware expert.

Mystique, an open-source tool, helps organizations automatically derive mutex-based infection markers for vaccination purposes

The Rise of Cryptominers

Malware Authors Adapt to Innovations

Cryptocurrencies such as Bitcoin, Ethereum, ZCash and Monero are becoming increasingly common and malware authors are adopting them with arms wide open. Cryptomining malware (also known as malicious cryptominers) are increasing in popularity amongst cybercriminals due to multiple factors:

- Malicious cryptomining is less likely to attract the attention of law enforcement than other forms of cybercrime, such as ransomware.
- The majority of virtual coins offer high level of anonymity, making it more difficult to track down the identity of the criminals.
- The victims' funds are not diverted from a bank account or credit card monitored by professional anti-fraud departments.
- It is easier to cash out illicit gains, since the criminal only needs to exchange the cryptocurrency to another "traditional" currency or even pay directly using it.

Moreover, many organizations have countermeasures specially against ransomware, which has been criminals' favorite cash cow. Attackers are looking for new revenue sources, and are attracted by the low-hanging fruit of cryptomining malware, which enterprises often have a hard time detecting or preventing.

This section of our report describes the dangers of malicious cryptominers, provides some examples for ongoing campaigns, and offers tips to protect against such abuses. It also shares predictions about the next stage in the evolution of malicious cryptominers.

Damage caused by Cryptomining

Veterans of the ransomware explosion era might think that they should not be too worried about cryptominers as they don't cause direct data loss – but this is a dangerous misconception. There are many direct and indirect implications of this type of malware:

Slowing down machines
Some miners either by design or as a result of poor coding consume over 90% of the endpoint's CPU, making it useless, impeding productivity by effectively performing a denial-of-service attack as a side-effect of the mining.

Significant increase in cloud services payments
The same danger of slowing down physical machines applies to virtual machines provided as a cloud service. Unlike physical machines, IT teams many times prefer to "upgrade" a machine which is slugish (as a result of illicit mining activity) rather than finding the root cause. Adding more virtual resources might solve the problem in some cases but will result in higher bills for the service provider.

Impact on power consumption
Miners can triple the power consumed by PCs. This may not sound horrible but multiplying it by the number of endpoints in a large organization, working 24/7 – this adds up to a considerably higher electricity bill.

Cryptomining used alongside other malicious threats
Actors spreading traditional bots and infostealers are often the ones deploying the "higher-tier" miners. Some bots have the capability to deploy cryptomining modules but it is not farfetched to assume there are mining bots with the capability to deploy malicious bots.

When discussing the above effects, remember that there are multiple examples for cryptominers spreading themselves virally within infected organizations (e.g. Adylkuzz spreading using ETERNALBLUE/DOUBLE PULSAR). This means that when assessing the risks for an enterprise – you should assume that massive segments of the protected organization will be infected. This will turn what seems to be minor extra fees for electricity or a tiny fixable IT issue into a fully blown catastrophe.

Notable Examples

So how profitable can cryptomining be? Our team of researchers tested it via a campaign unveiled over a year ago called PhotoMiner. It had quite a unique way of spreading laterally, repeatedly collecting credentials for servers to infect files stored on it, waiting for non-infected users to access the trojanized files and be infected, collecting info about new potential pivoting servers from the new victims and so on.

The original report unveiling this campaign is from June 2016, but it seems that many instances of this malware are still up and running!

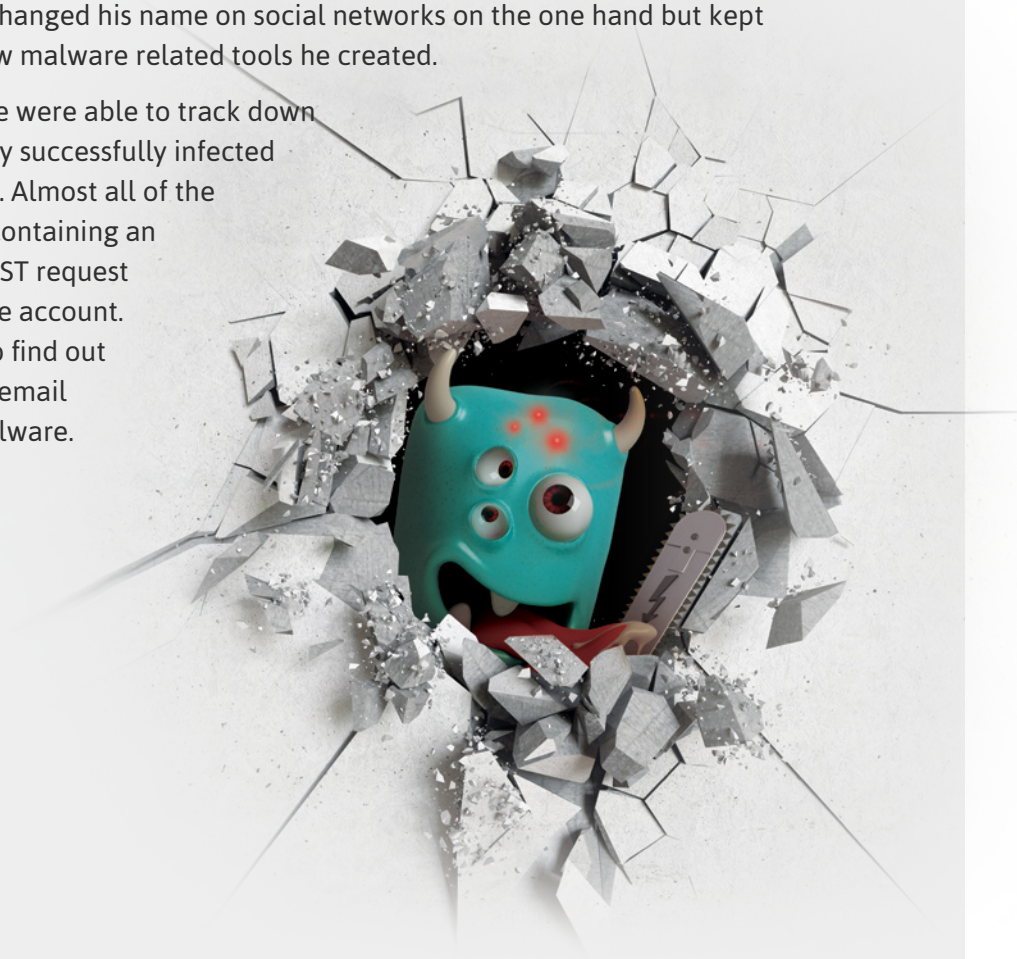
As of early December 2017 the sum of Monero accumulated in the wallets of this campaign exceeds two million dollars.

As stated above, many "traditional" cybercriminals pivoted to cryptominers or ran them in parallel to their bots. One example we've seen during the past year is SnatchLoader. It is a typical downloader, distributing all types of malware and recently it added a cryptomining optional module. We expect this trend to continue, as mining provides easy extra income at a very low price.

However, some of the more interesting cases of cryptomining campaigns are not about the most successful ones but the other way around. Just like the "real" gold rush, we observe many novice malware writers seeking fortune and glory in the lands of cryptocurrency.

We already released a detailed blog post about the WaterMiner campaign, demonstrating a case of the amateur operations security (OPSEC) failures as observed in a running campaign. Since then, the perpetrator behind the campaign changed his name on social networks on the one hand but kept uploading material about other new malware related tools he created.

Since the WaterMiner campaign, we were able to track down dozens of similar petty thieves. They successfully infected victims with cryptomining malware. Almost all of the mining pools require a parameter containing an email address associating HTTP POST request from the miner with the appropriate account. Time after time we were amazed to find out that the criminals use their private email addresses in their cryptomining malware.



Defending Against Malicious Cryptominers

Cryptominers are here to stay but luckily there are many simple countermeasures to apply against it:

- Networking:
  - Use existing network IDS/IPS tools to detect outgoing traffic to well known cryptocurrency pools.
  - Monitor ports known to be associated mining activity.
  - Block access to known sources of “server-side” miners such as Coinhive.
- Monitor unfamiliar processes consuming excessive CPU resources. This can be performed, for example with a combination of Winlogbeat and Sysmon combined with centralized log management.
- As malicious cryptominers continue to evolve, implement anti-evasion measures on endpoints to prevent infections that get past baseline antivirus tools.

Predictions for 2018

Minerva took a deep dive at the characteristics of malware that has captured people's attention and endpoints in 2017. Our report summarizes the approaches the adversaries used to evade enterprise defenses to achieve their objectives. As we learn from 2017 to understand where the security industry will be in 2018, we expect the continued commoditization of the attack tactics that at some point were considered advanced. Sophisticated exploits and anti-malware evasion will continue to grow in popularity, in part in response to the continued advancements in endpoint security products available to defenders. Such techniques will be used in both classic forms of malware, such as ransomware, as well as in malware that offers adversaries new revenue streams.

One example of new revenue sources for the adversary are malicious cryptominers. We expect the popularity of such malware continuing to increase. Established criminal groups will use malicious cryptomining to supplement their revenue stream from activities such as ransomware infections. Newcomers will see this practice as an easy way of getting into the field, in part because some might view such activities as a "victimless crime." As these adversaries gain experience, and as defenders' tools improve their ability to detect such malicious software, the authors of cryptominers will begin incorporating evasion techniques into their creations.

Enterprise defenders won't stand still when faced with continually-evolving threats. They will continue to invest into additional methods for safeguarding critical IT components, be they internal servers and workstations, IoT devices or BYOD systems. In addition, incident response teams will look for ways to more actively combat malicious presence in the enterprise, going beyond the practice of merely identifying which systems might have been compromised. Such steps might entail misdirecting or slowing down adversaries and their tools. A related example might involve vaccinating systems against specific malware families, "persuading" malware that it's already on the system to prevent the infection in the first place. Minerva will, of course, play a key role in arming the defenders with the tools they need to gain an edge over the adversaries.