



# The Need for Proactive Incident Response

Q1 2018 Trends in the North American Threat Landscape

#### **TREND MICRO LEGAL DISCLAIMER**

The information provided herein is for general information and educational purposes only. It is not intended and should not be construed to constitute legal advice. The information contained herein may not be applicable to all situations and may not reflect the most current situation. Nothing contained herein should be relied on or acted upon without the benefit of legal advice based on the particular facts and circumstances presented and nothing herein should be construed otherwise. Trend Micro reserves the right to modify the contents of this document at any time without prior notice.

Translations of any material into other languages are intended solely as a convenience. Translation accuracy is not guaranteed nor implied. If any questions arise related to the accuracy of a translation, please refer to the original language official version of the document. Any discrepancies or differences created in the translation are not binding and have no legal effect for compliance or enforcement purposes.

Although Trend Micro uses reasonable efforts to include accurate and up-to-date information herein, Trend Micro makes no warranties or representations of any kind as to its accuracy, currency, or completeness. You agree that access to and use of and reliance on this document and the content thereof is at your own risk. Trend Micro disclaims all warranties of any kind, express or implied. Neither Trend Micro nor any party involved in creating, producing, or delivering this document shall be liable for any consequence, loss, or damage, including direct, indirect, special, consequential, loss of business profits, or special damages, whatsoever arising out of access to, use of, or inability to use, or in connection with the use of this document, or any errors or omissions in the content thereof. Use of this information constitutes acceptance for use in an "as is" condition.

# Contents

## 04

Security challenges and the nature of threats

## 05

Significant threats and trends

## 13

Most common infection vectors


## 14

Proactive incident response

## 16

Trend Micro solutions





Living in the digital age, while mostly beneficial, is not without its fair share of drawbacks, especially when it comes to security. Our increasing reliance on networks and devices means that threat actors are also evolving their techniques accordingly for maximum effectivity. As a result, today's cybercriminals have become adept at carrying out attacks from remote and often untraceable locations — to steal money, disrupt systems, or damage reputations — with just a few keystrokes.

To better understand the modern security landscape and to help organizations deal with the increasingly complex malware in the wild, we analyzed data based on the Trend Micro™ Smart Protection Network™ security infrastructure in North America in the first quarter of 2018. We saw several emerging threats and trends. Older malware appeared at the top, while cryptocurrency miners emerged as one of the region's top threats, possibly as a viable alternative to ransomware. Sophisticated threats continued to be delivered via email, which remained the prime entry point for most malware. URL links redirecting to malicious websites also remained a popular technique among attackers.

This report highlights the threats, trends, and key takeaways we see within both our large customer base and the wider threat landscape in North America in the first quarter of 2018. It gives us a unique vantage point from which we can examine and analyze the tactics, targets, and defense of today's cyberattacks. From there, we can recommend that organizations take a proactive stance with their security posture, either through their in-house security team or through a third-party security provider that offers security services such as [managed detection and response \(MDR\)](#).

## Security challenges and the nature of threats

Cybersecurity is like a chess game between security providers and cybercriminals, with each side trying to stay one step ahead of the other. The more advanced the threat, the more sophisticated the technology becomes to counter it. At the same time, threats are rarely static: They constantly evolve and gain new capabilities that make them more effective.

If there's one overarching theme that can be found in our analysis, it's that the threats found in our data are not only varied, but they also present different kinds of security challenges. Old and ever-evolving threats designed for information theft still plague a large number of organizations as well as individuals. The abundance of ransomware is such that two variants are unlikely to exhibit the same characteristics — everything from the infection vector to the evasion mechanisms and even the encryption methods might be different. There is also the relatively new [issue of cryptocurrency miners](#), the malicious type of which uses the resources of victimized systems to mine cryptocurrencies on behalf of the attackers. These usually work in the background and can be difficult to detect, especially in the case of fileless miners. They can also exploit vulnerabilities to infiltrate systems, posing a problem for organizations that lack the kind of tools that can prevent this intrusion.

Traditional security technologies may not be able to address all the threats that we lay out in this report. While they can certainly help against more common malware variants that do not display too much sophistication, they may not perform as well against threats that have more advanced capabilities such as deploying remote access tools, entering systems without leaving traces, and silently moving laterally within the network. Thus, there is a need for a more involved security strategy. This can be achieved either through a proactive approach for enterprises with an in-house security team or via third-party support for organizations that cannot afford to train their IT staff to handle more advanced threats.

Before we go further into how to address these threats, let us take a look at the emerging threats and trends in North America in Q1 2018.

# Significant threats and trends

The first quarter of 2018 saw information theft malware being the most detected event in end user's devices, with cryptocurrency mining close behind. Ransomware detections were higher during the start of the quarter, but declined in the succeeding months. The volume of threats increased as attackers used a variety of tools to keep a low profile and deter detection by law enforcement and cybersecurity analysts.

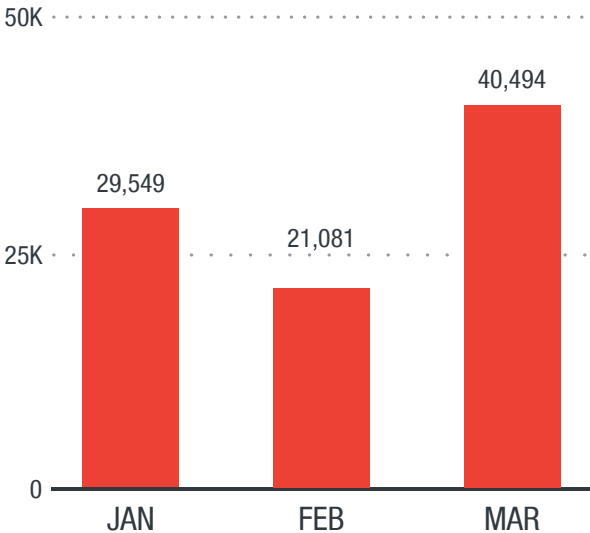


Figure 1. Total malware detections in North America in Q1 2018

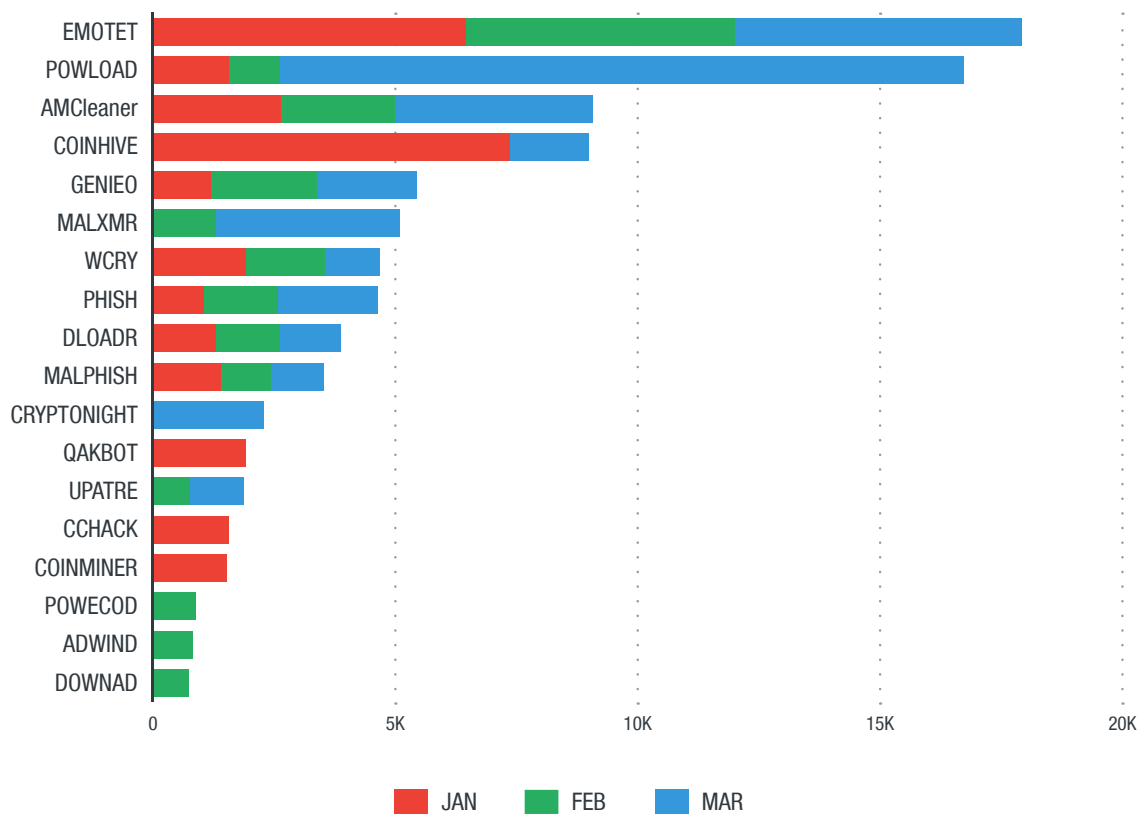


Figure 2. Top 15 malware threats in North America in Q1 2018

Threat	Type	First detection	Movement	Point of entry	Motive
EMOTET	Banking trojan	2014	▲	Emails with URL links, Word documents, or PDF files	Obtain financial information by injecting code into the networking stack of an infected computer, allowing sensitive data to be stolen via transmission
POWLOAD	Trojan	2017	▲	Spam emails with file attachments	Collect system information which may be used by cybercriminals to launch other attacks
AMCleaner	Spyware	2015	▲	Web link to download a fake utility	Generate revenue for developers through a program that pretends to have a valid use, but in fact modifies the user's computer in malicious ways

Threat	Type	First detection	Movement	Point of entry	Motive
COINHIVE	Cryptocurrency-mining tool	2017	▼	Website visit	Mine for Monero for the site owner, but using the user's CPU resources
GENIEO	Adware/Spyware	2014	◀ ▶	Unwanted application	Hijack the user's browser and track browser usage with the intention of mining information

Table 1. Details of the top 5 malware threats in North America in Q1 2018

### Information theft malware on top

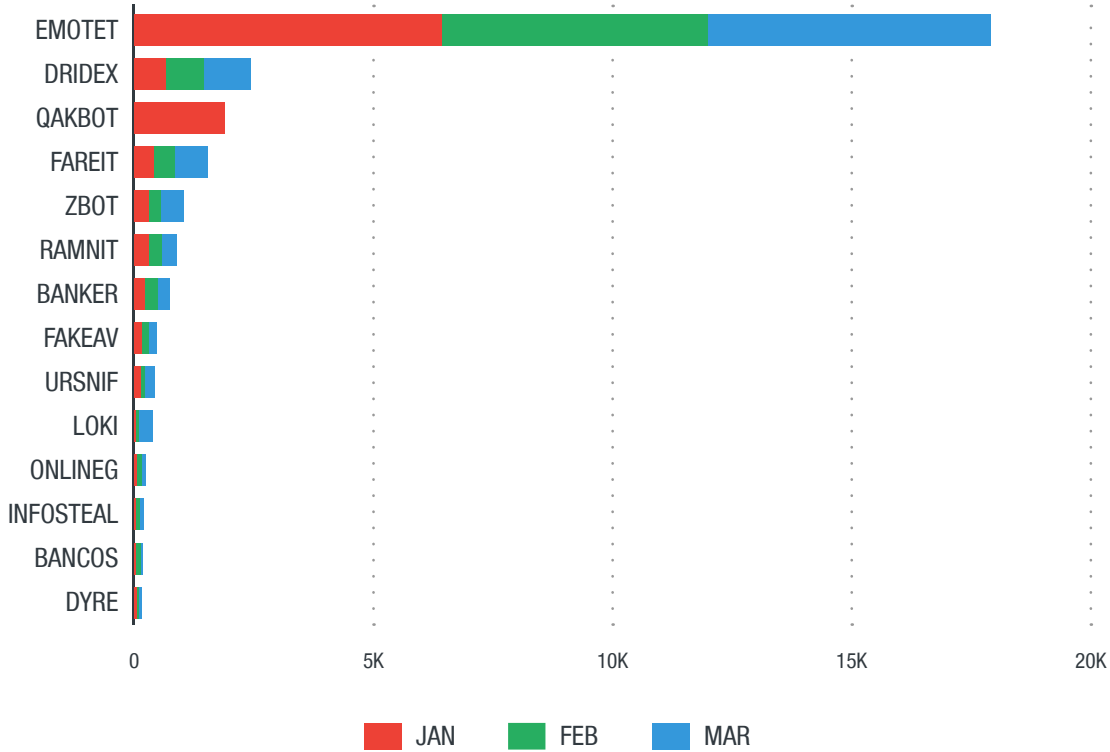


Figure 3. Information-stealing malware detections in North America in Q1 2018

Older malware families such as [EMOTET](#), [DRIDEX](#), and [QAKBOT](#) had high rates of detections in the first quarter of 2018. EMOTET and QAKBOT are both information stealers that have been showing renewed activity in recent months, with EMOTET in particular seeing a heavy spike in detections. These malware families are technically different, but they share many similarities in behavior. Both arrive via spam emails that contain malicious download links, PDF files with embedded links, or macro-enabled Microsoft Word

attachments. They share the same goal of stealing online banking credentials, which can then be abused in a variety of ways, such as targeting online banking accounts.

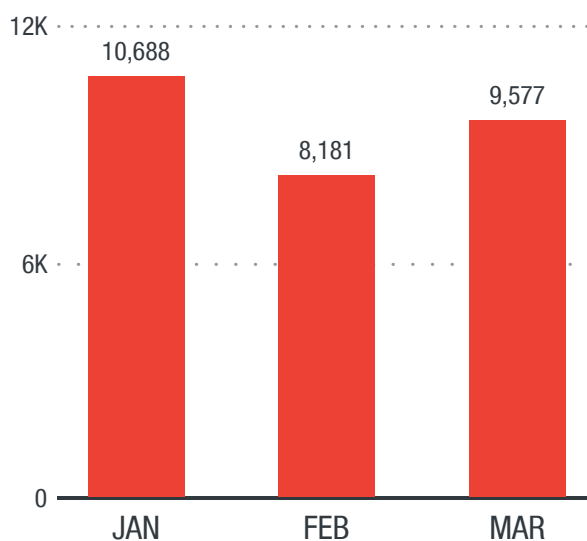


Figure 4. Total information theft malware detections in North America in Q1 2018

As previously noted, many of the most prevalent information-stealing malware families are not new, so it might be surprising to find that they are still at the top of our detection data. The simple answer as to why this is so is because they are still effective. In EMOTET's case, it's a piece of malware with email-spamming and lateral-movement capabilities, allowing it to infect business systems and acquire corporate emails, which in turn translates to more effective spam targeting and a higher chance of gaining information. It can also spread via network propagation and compromised URLs for command-and-control (C&C) purposes, and turn the infected systems into parts of a botnet intended to spread the malware even further. In addition, it's capable of harvesting email information and stealing username and password pairs found in installed browsers. These unique characteristics and its continued evolution make the malware extremely effective and versatile. Given that the reason for cybercrime is almost always about money, the use of an effective and proven information theft malware should come as no surprise.

Fraudsters are also getting more sophisticated in their attacks and using more complex monetization schemes such as person-to-person (P2P) payment accounts to facilitate money movement out of the victims' accounts. The significant shift in tactics may be attributed to the growth of intermediary new-account fraud, which involves the [monetization of compromised existing accounts](#) by opening one or more fraudulent accounts. Account takeover has grown significantly: Cybercriminals use another person's personal information to open an account and cause fraud. It is likely that the rise in information theft malware is related to these schemes.



## Decline of ransomware attacks

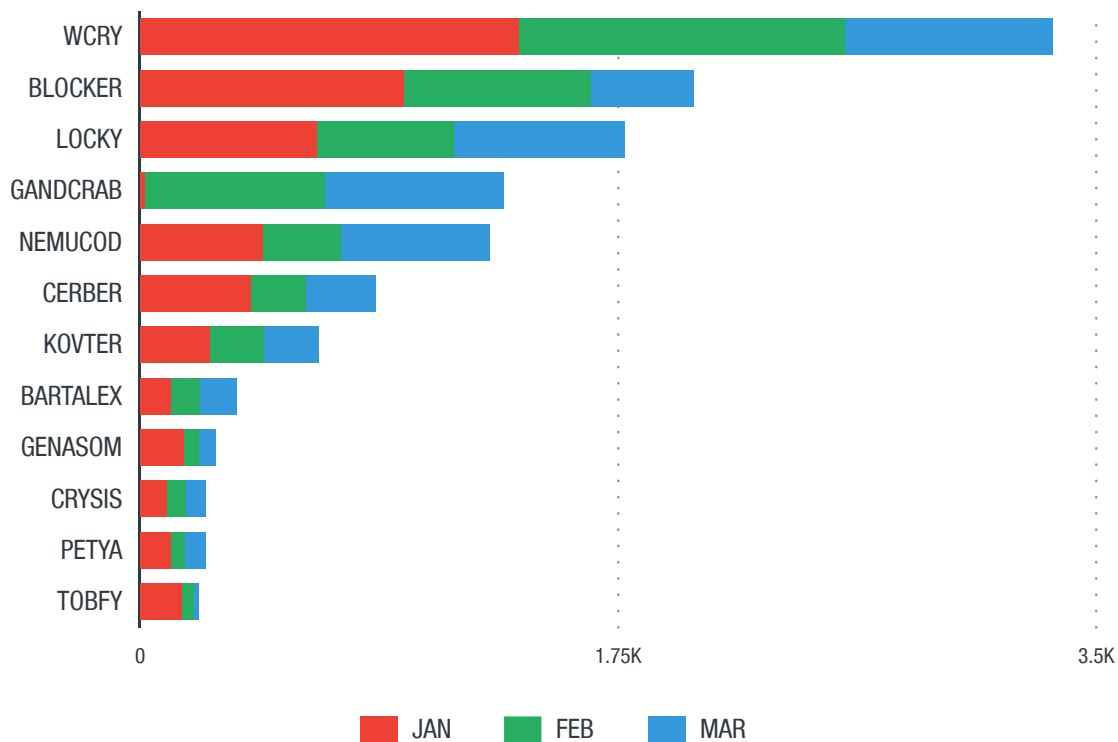


Figure 5. Top ransomware detections in North America in Q1 2018

**WCRY** (aka WannaCrypt or WannaCry), which made global headlines in 2017 for its disruptive abuse of the leaked EternalBlue and DoublePulsar exploits, still topped the chart among ransomware hits in Q1 2018. March saw further action, with a [multinational aerospace corporation](#) reportedly being hit by the same WannaCry ransomware that struck thousands of computer systems in a number of countries around the world last year.

**LOCKY** emerged as the most common variant of ransomware found in malicious emails, typically taking the form of attachments. For most of 2017 and for the first quarter of 2018, it accounted for the majority of malicious email traffic.

Other notable malware families seen in our data include BLOCKER and GANDCRAB. BLOCKER adds itself to the auto-start mechanism of the victim computer and blocks the operating system from loading normally, after which it displays a window asking the user to send an SMS message with a special text to a specified number. In the case of GANDCRAB, the trojan makes copies of itself as soon as it is executed and creates an autorun registry entry so that it starts every time Windows starts. It then connects to remote locations and encrypts files on the compromised computer. It displays a ransom note informing the user that the files have been encrypted and providing instructions on how payment can be made to have the files decrypted.

Our data showed that ransomware declined from the start of the year, with 4,756 detections in January, dropping to 4,054 in February and 3,794 in March. One thing to take note is that the decline does not necessarily mean that ransomware itself is being replaced by cryptocurrency miners. Rather, it is more likely that both ransomware and cryptocurrency miners are being deployed at the same time as cybercriminals look to maximize their revenue streams.

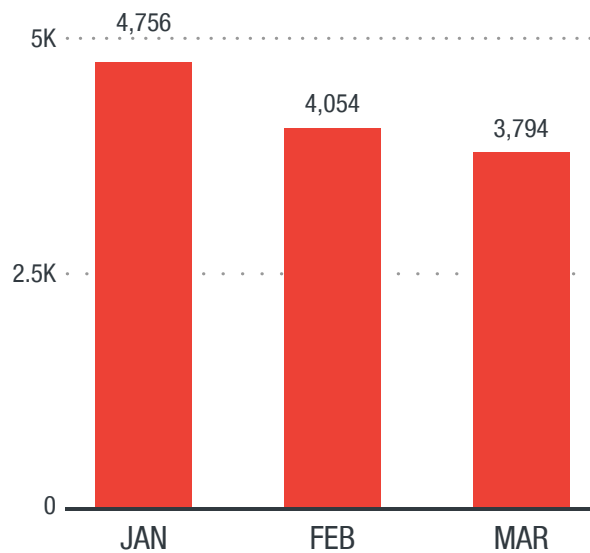


Figure 6. Total ransomware detections in North America in Q1 2018, with steady month-on-month decline

## Cryptocurrency miners as alternative to ransomware

Unsurprisingly, [the rise of cryptocurrency mining malware](#) over the past year seems to have a correlation with the rise of cryptocurrency itself. Bitcoin, in particular, underwent a [meteoric ascent in value](#), from just under US\$1,000 in January 2017 to almost US\$20,000 in December 2017. This explosive growth has attracted many cybercriminals looking to profit from the hype.

Our data shows that cryptocurrency miners have overtaken ransomware in North America. Cryptocurrency mining presents a more furtive and passive alternative to ransomware. Due to the nature of cryptocurrency mining, a single infection might not provide cybercriminals as much profit as they would from other types of malware. However, a cryptocurrency miner's stealth and longer infection time mean less work on the attacker's end.

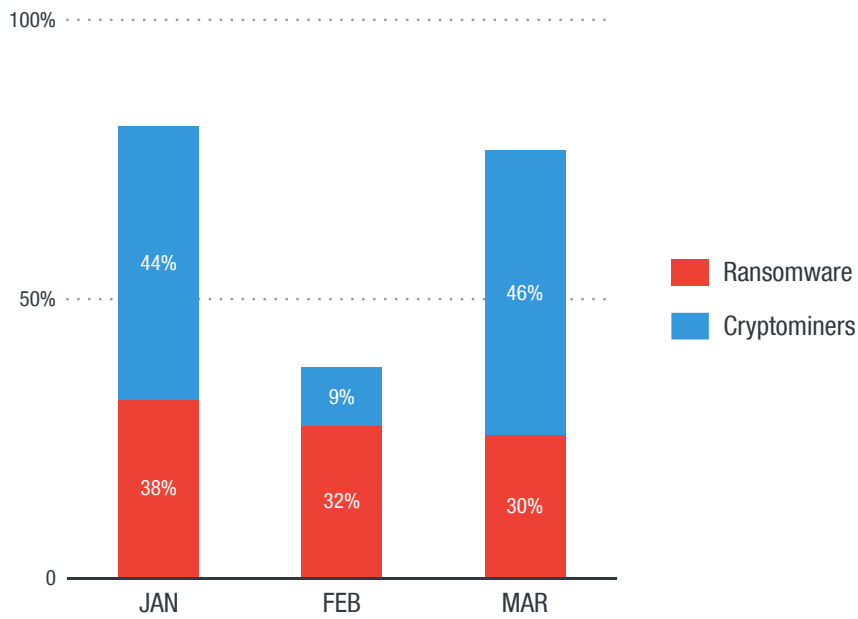


Figure 7. Percentage of ransomware and cryptocurrency miners in malware detections in North America in Q1 2018

The cryptocurrency miners **COINHIVE** and **COINMINER** were infecting more users early in the first quarter of this year, while **MALXMR** and **CRYPTONIGHT** dominated in the latter part.

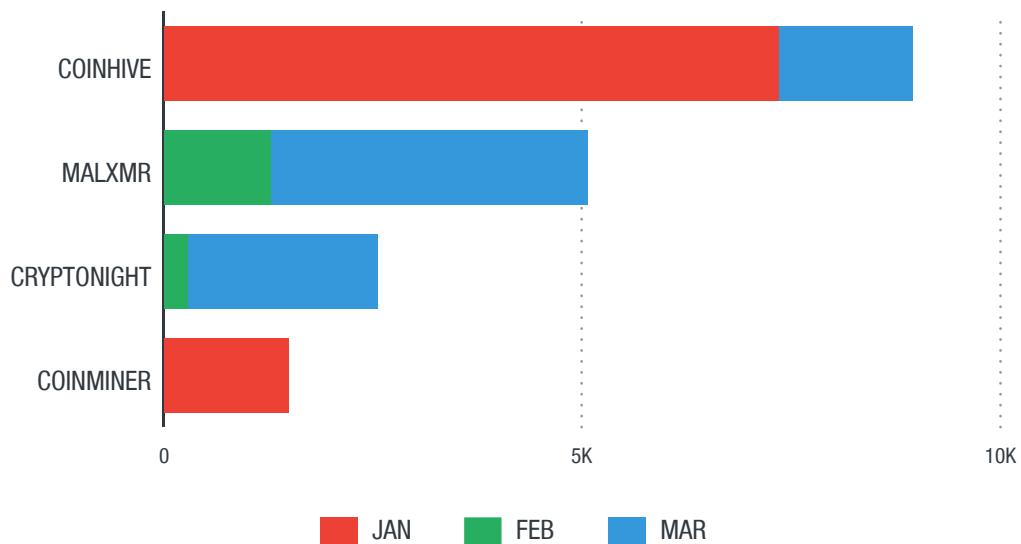


Figure 8. Top cryptocurrency miner detections in North America in Q1 2018

MALXMR uses social media messaging apps to reach the target's computer, dropping two discrete cryptocurrency miners. It will check the infected computer to see if the device is running a 32-bit or 64-bit platform and execute the corresponding coin-mining component, either a 32-bit variant or a 64-bit variant of an XMRig Monero miner. Once this is executed, it will download three files to the machine, the first one being an auto-start component, *startup.cmd*, and the other two being the mining component, *javaupd.exe*, and another malicious file, *3.exe*.

COINHIVE is a web-based cryptocurrency miner that has become one of the most popular miners because of its ease of use. By signing up with an email address, a potential user can gain access to its JavaScript code, which can then be embedded into a website. Visitors of the website, in turn, agree to run the miner in their browsers for an incentive, typically an ad-free experience. As for CRYPTONIGHT, it's a proof-of-work algorithm that runs on JavaScript code and mines for the cryptocurrency Monero. Once it infects a computer, this malware may slow the device down by heavily using the resources of the central and graphics processing units (CPU and GPU) in order to generate Monero.

Malicious actors are using web-based cryptocurrency mining scripts to process cryptocurrency transactions in affected systems, resulting in decreased speed and efficiency. Although legitimate tools and platforms exist to mine cryptocurrencies, coin miners use the resources of targeted systems to avoid paying for services. Using the resources of targeted systems is cost-effective because buying the hardware and setting it up can be costly.

The effects of the malware are visible to the end user and can even extend to enterprises. While the average user may experience slow network connectivity and consequently a loss in productivity, enterprises whose networks have been exploited by coin miners can suffer high CPU usage and added expenses. There have also been cases where cryptocurrency miners have been found embedded in legitimate websites without authorization, allowing them to avoid easy detection by users.

# Most common infection vectors

## Email-based threats

Email-based threats still make up a large number of detections in North America. The banking trojan EMOTET and the fake utility software AMCleaner, which are both delivered via email, showed a steep rise in activity. AMCleaner is an interesting malware that is similar to a fake antivirus (AV), whose evolution [we've documented in the past](#). In many ways, fake AVs are the precursor to ransomware, and in fact, many of them also feature encryption capabilities.

Another macro malware downloader, POWLOAD, has been seen picking up steam since March as well. POWLOAD is known to arrive through spam emails or be bundled with other malware in order to collect system information, which can then be used by cybercriminals to launch other attacks. It uses malicious PowerShell scripts to deliver the payload to the affected system, hiding all its malicious codes in the Windows Registry.

Phishing was also popular during the first quarter of 2018. In this social engineering tactic, an attacker, masquerading as a trusted entity, dupes a victim into opening an email, instant message, or text message. The opened item usually includes a malicious link that redirects to a website displaying certain fields and tricking the victim into entering valid information. The main purpose of this scheme is to steal personal information, such as login credentials, banking details, and credit card data.

Email-based threats have been very effective because they simply require some social engineering, a convincing decoy document, and a known exploit to do the job. Due to their effectiveness and ease of use, we expect email-based threats to remain popular for the foreseeable future.

## Web-based threats

The main web-based threats that we detected include cryptocurrency miners such as COINHIVE, which are embedded — whether knowingly or unknowingly by users — in websites in order to harvest cryptocurrencies using the resources of the victims' computers.

Another interesting web-based threat we discovered is the potentially unwanted application (PUA) GENIEO, which acts similarly to a content recommendation engine. Disguising itself as a necessary update to an existing extension, GENIEO hijacks a user's browser and tracks usage to mine information.

## Proactive incident response

The first quarter of 2018 presented an interesting mix of threats in North America. Older malware families continued their persistent evolution, adding more capabilities to what had already been proven, effective threats. Ransomware, despite its decline over the months of Q1, remained a top threat that should not be taken lightly, especially in light of some of the most devastating ransomware attacks in recent memory, including WannaCry and [Petya](#). Cryptocurrency miners also made their mark at the start of the year, as cybercriminals continued to go where money could be found.

All of these threats pose a problem for everyone, hence the need for vigilance, whether the one is a single user or an entire organization. Individual users, in particular, are prone to being targeted for social engineering, especially when it comes to ransomware. Therefore, they need to know how to [spot this technique](#) before it gets the better of them. Concerning [cryptocurrency miners](#), users also have to be vigilant with the websites they visit, and weigh each decision when it comes to the usage of resources: *Is an ad-free experience worth the trouble of computer slowdowns and inefficiency?*

For organizations, the key to dealing with these kinds of threats is continuous proactive monitoring and threat response. Many of the attacks discussed here feature multiple components and a wide array of capabilities that make them difficult for even advanced security technologies to detect and mitigate without a proactive security stance. Given the persistence of the threats, it is important that each event should be analyzed to identify the gap in the security implementation and determine the entry point of a threat, quickly respond to the threat activity, learn from it, and repeat.

[Strategies](#) such as log analysis and endpoint detection and response (EDR) tools can allow security personnel to pinpoint where and when an attack happened, and can also help prevent similar attacks from happening. What may seem to be ordinary ransomware at first glance may actually turn out to be a targeted attack once logs are examined and suspicious activity is noted. Network segmentation can also minimize the potential damage of an attack by confining it to a single part of the organization's network. This is especially important with regard to information theft malware, since access to all parts of the network also means access to all the data stored within.

## Considering managed detection and response (MDR)

A further option for organizations that do not have dedicated threat researchers is [managed detection and response \(MDR\)](#).

Building an effective threat response team requires a considerable amount of time and skilled resources, and may not be feasible for some organizations. If organizations do have the know-how to react to events, the sheer volume and the time-consuming tasks of prioritizing and analyzing events, coupled with the daily tasks associated with keeping the business up and running, may be too much to handle. If treated as just a part of the broader job of regular IT staff, threat management can prove overwhelming as it includes vulnerability assessment, patching, firmware upgrades, vendor management, intrusion detection and prevention systems (IDS/IPS) monitoring, firewall monitoring, and other specialized focus areas. Thus, it could be handled better by security professionals who are specially focused on threats.

Organizations should consider third-party security services staffed by skilled professionals who can provide advanced threat hunting services. Subscribing to a service like MDR provides faster alert prioritization, root cause analysis, detailed research, and a remediation plan that gives organizations a better ability to respond to sophisticated attacks. Many organizations have technologies, such as EDR, that provide advanced threat research and analysis, but lack the significant time or specialized skills to effectively use them. MDR affords organizations the benefit of knowledgeable professionals with years of experience along with powerful technology that can service both endpoints and the network.

## Trend Micro solutions

Trend Micro endpoint solutions such as the [Smart Protection Suites](#) and [Worry-Free Business Security](#) solutions can protect users and businesses from threats by detecting malicious files and messages as well as blocking all related malicious URLs. The [Trend Micro™ Deep Discovery™](#) solution has an email inspection layer that can protect enterprises by detecting malicious attachments and URLs.

Trend Micro [XGen™ security](#) provides a cross-generational blend of threat defense techniques to protect systems from all types of threats, including ransomware and cryptocurrency-mining malware. It features high-fidelity machine learning on [gateways](#) and [endpoints](#), and protects physical, virtual, and cloud workloads. With capabilities like web/URL filtering, behavioral analysis, and custom sandboxing, XGen™ security protects against today's threats that bypass traditional controls; exploit known, unknown, or undisclosed vulnerabilities; either steal or encrypt personally identifiable data; or conduct malicious cryptocurrency mining. Smart, optimized, and connected, XGen™ security powers Trend Micro's suite of security solutions: [Hybrid Cloud Security](#), [User Protection](#), and [Network Defense](#).

Backed by 30 years of experience in threat research, Trend Micro's MDR service provides access to experts who are proficient with live response and are familiar with products that can provide meaning to security incidents that happen to organizations and their industry. Our experts have the necessary tools and technologies to analyze threats and assist organizations in maintaining a good security posture.



Created by:

**TrendLabs**

The Global Technical Support and R&D Center of TREND MICRO

**TREND MICRO™**

Trend Micro Incorporated, a global leader in cybersecurity solutions, helps to make the world safe for exchanging digital information. Our innovative solutions for consumers, businesses, and governments provide layered security for data centers, cloud environments, networks, and endpoints. Optimized for leading environments, including Amazon Web Services, Microsoft®, VMware®, and more, our solutions enable organizations to automate the protection of valuable information from today's threats. All our products work together to seamlessly share threat intelligence and provide a connected threat defense with centralized visibility and investigation, enabling better, faster protection. With almost 6,000 employees in over 50 countries and the world's most advanced global threat intelligence, Trend Micro enables organizations to secure their connected world. For more information, visit [www.trendmicro.com](http://www.trendmicro.com).



**TREND  
MICRO™**

Securing Your  
Connected World