Defending against today's critical threats

A 2019 Threat Report

CISCO

Contents

Look back, move forward

When it comes to the threat landscape, it's important to take a look in the rearview mirror once in a while.

As with driving, not only do you get a good look at what's behind you, but you can often spot what's coming up quick, set to overtake you.

That's the spirit of this threat report. We've picked out five key stories from the last year or so, not just because they were big events, but because we think these threats, or similar ones, could very well appear in the near future.

Take modular threats like Emotet and VPNFilter, for example. These are threats that can deliver an on-demand menu of attacks and threats, depending on which device is infected or the intended goal of the attacker. We saw plenty of such modular threats in recent history, and wouldn't be surprised if we see more in the future.

Email remains the darling delivery method of attackers, with threats from cryptomining to Emotet using it to spread. It's also highly likely that other threats, such as unauthorized MDM profile, used it too. This highlights how critical it is to keep a close eye on what is coming in through your mailbox.

Modus operandi

Revenue generation continues to be a primary motivation for attackers: malware follows the money. Cryptomining threats, for instance, are laser-focused on this goal. Meanwhile, Emotet has pivoted to a threat distribution network, capitalizing on a variety of options to make money.

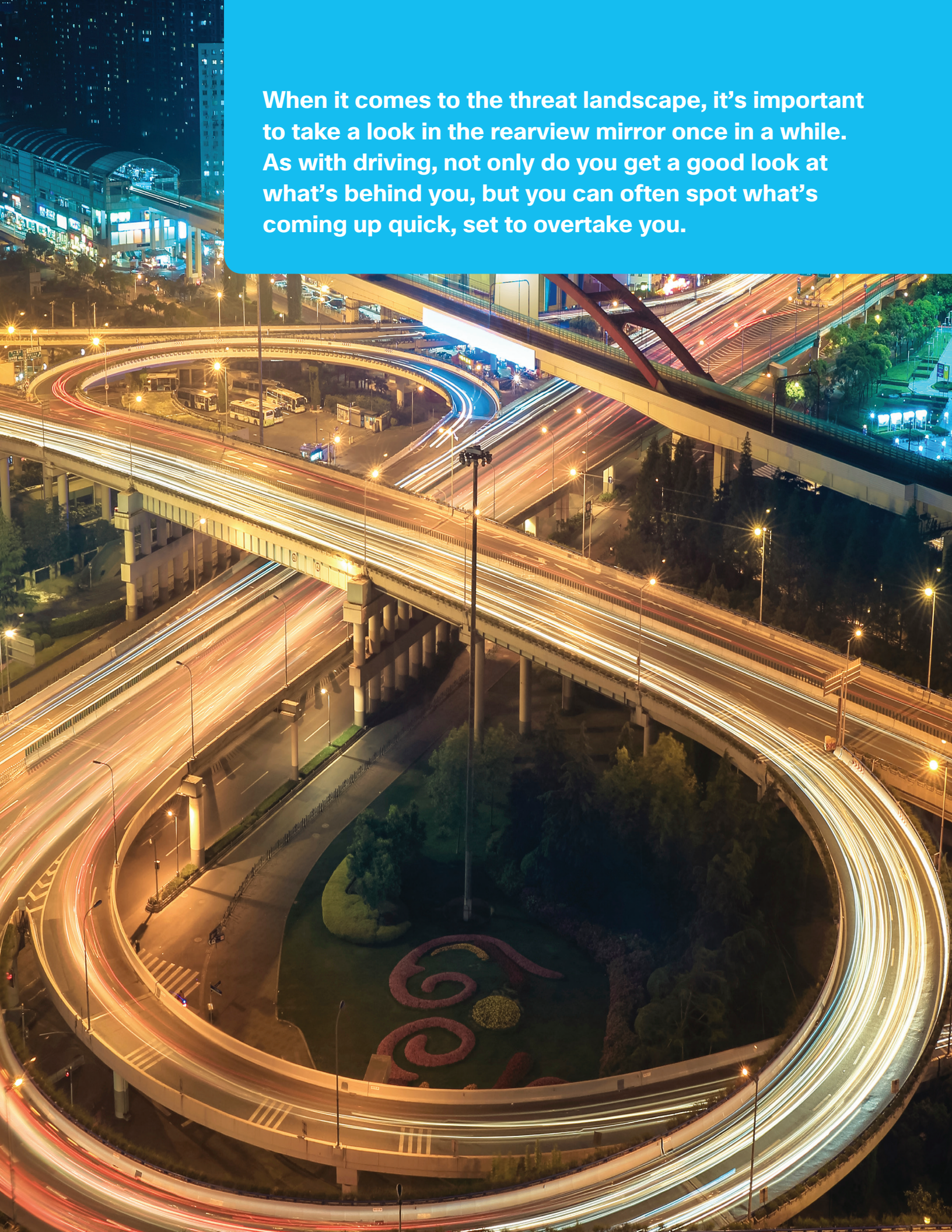
Data exfiltration has also taken its time in the spotlight. VPNFilter included the ability to exfiltrate data, among its many features. Emotet, beyond stealing network credentials to help it spread, was also seen spreading Trickbot, another popular infostealing banking trojan.

We've picked out five key stories because we think these threats, or similar ones, could appear again.

Finally, some threats just want to watch the world burn, as is the case with Olympic Destroyer. We saw a number of threats like this in the last year, but none grabbed the headlines like an attack whose sole purpose appears to have been to disrupt the Winter Olympics.

So while we look back at some of the most impactful threats of 2018, it's important to be mindful of what made these threats so successful. Many of them may be in the rearview mirror for now, but have you passed them, or are they speeding up to pass you and your security strategy?

When it comes to the threat landscape, it's important to take a look in the rearview mirror once in a while. As with driving, not only do you get a good look at what's behind you, but you can often spot what's coming up quick, set to overtake you.



Attack types and protection

A layered approach to security is always advised. We've included icons at the end of each story to indicate key threat vectors used (or suspected to be used) and tools that can help protect against them in each case. Below we decode the icons and discuss advantages of deploying the various protections as part of an integrated security architecture.

Advanced malware detection and protection technology (such as Cisco Advanced Malware Protection, or AMP) can track unknown files, block known malicious files, and prevent the execution of malware on endpoints and network appliances.

Network Security such as the Cisco Next-Generation Firewall (NGFW) and Next-Generation Intrusion Prevention System (NGIPS) can detect malicious files attempting to enter a network from the Internet or move within a network. Network visibility and security analytics platforms such as Cisco Stealthwatch can detect internal network anomalies that could signify malware activating its payload. Finally, segmentation can prevent the lateral movement of threats within a network and contain the spread of an attack.

Web scanning at a Secure Web Gateway (SWG) or **Secure Internet Gateway (SIG)** such as Cisco Umbrella, means you can block users from connecting to malicious domains, IPs, and URLs, whether users are on or off the enterprise network. This can prevent people from inadvertently allowing malware to access the network, and can stop malware that makes it through from connecting back out to a command and control (C2) server.

Email security technology (such as Cisco Email Security), deployed on premises or in the cloud, blocks malicious emails sent by threat actors as part of their campaigns. This reduces the overall amount of spam, removes malicious spam, and scans all components of an email (such as sender, subject, attachments, and embedded URLs) to find messages that contain a threat. These capabilities are critical since email is still the number one vector used by threat actors to launch attacks.

Advanced malware detection and protection technology, such as Cisco AMP for Endpoints, can prevent the execution of malware on the endpoint. It can also help isolate, investigate, and remediate infected endpoints for the one percent of attacks that get through even the strongest defenses.

Emotet's pivot: From banking to distribution

Emotet has sat in the background for years. This tactic has served it well.

Quite often in the threat landscape, the stories that grab the headlines are the ones that do something new or novel: a vulnerability is discovered that impacts a large quantity of devices, or an attack against a major organization comes to light.

However, **some of the most prevalent threats aren't the ones that steal the limelight. They may rely on tried and tested methods, rather than the latest and greatest techniques.** And this plays into the hands of attackers. Something that can fly under the radar has the potential to grow, where a more attention-grabbing counterpart may not.

Emotet is a perfect example of this. While the headlines have been filled with discussions of threats like WannaCry and NotPetya, Emotet has sat in the background for years. This tactic has served it well as it has grown to become one of today's most successful threat families.

Emotet's success lies in the way it has evolved. From "humble" beginnings as a banking trojan, the threat actors quickly pivoted into making the threat a modular platform capable of carrying out a variety of different attacks. Fast forward to today, and other threat families once seen as competitors now use it to spread their wares. And as the threat landscape shifts once again, Emotet appears to be rising to the top of everyone's radar.

From modest to modular

When Emotet first arrived on the scene, it was one of several banking trojans. The threat was delivered through spam campaigns, generally using invoice- or payment-themed spam emails. It was often attached as macro-enabled Office documents, JavaScript files, or included as a malicious link. The distribution techniques varied, though many of the campaigns targeted banks in specific regions — in particular, German-speaking countries in Europe and the US.

At first the threat was chiefly focused on stealing banking information: user names, passwords, email addresses, and other financial details. As time went on, Emotet began to spread to a more general

Email: The most common threat vector

One theme we see woven throughout most of today's major threats is email. It remains the most popular infection vector for threat actors to spread their wares, and it will likely remain that way in the near future.

Take a look at Emotet, for instance. Week after week, the attackers behind this threat crank out new phishing campaigns.

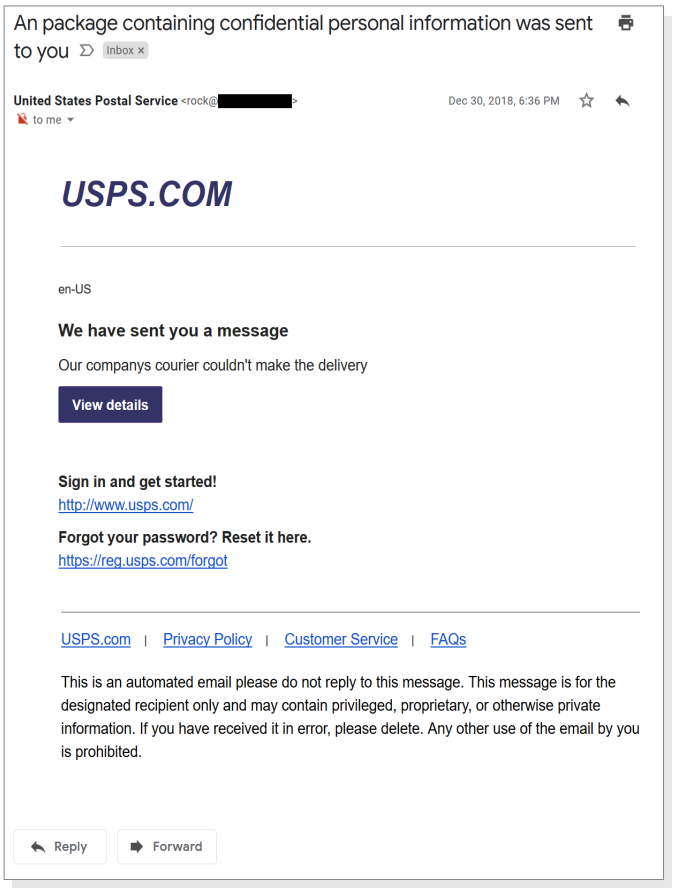
The same applies to malicious cryptomining, where spam campaigns consistently trick users into downloading the miners onto their computers.

And in terms of mobile device management (MDM) threats, it seems plausible that the attacks began through socially engineered email.

(cont'd)

audience. A new version of the threat laid the groundwork for the modular configuration we see today, containing different tools for different functions. Some modules steal email credentials, while others focus on user names and passwords stored in the browser. Some provide distributed denial-of-service (DDoS) capabilities, while others can distribute ransomware.

Figure 1 A sample spam email from Emotet



It's not surprising either, given the convincing design of many phishing emails, especially viewed on a mobile phone. And to a busy user, the risk and urgency conveyed by the mail could lead the recipient to take immediate action, overlooking the telltale signs of a threat in waiting.

It's no wonder attackers continue to turn to email to help spread their malware.

Show me the money

The primary purpose of Emotet is to discover a way to monetize the compromised computer, which is where the modules come in. It appears as though the modules installed on a particular device depend on how they can best monetize the infected device. Consider the following scenarios:

- Does the computer browser history show frequent visits to banking websites? Deploy banking modules to steal credentials and transfer money.
- Is the device a top-of-the-line laptop, more than likely indicating the target has disposable income? Deploy malware distribution modules and install ransomware or cryptomining software.
- Is the machine a server on a high-bandwidth network? Install modules for email and network distribution and spread Emotet further.

Honor among thieves

What really sets Emotet apart from many threats in today's threat landscape is not just its reach and modularity, but that the actors behind the threat appear to be shopping it around as a distribution channel for other attack groups.

For instance, we've observed situations where Emotet infects a computer only to drop Trickbot onto the system as the payload. In this seemingly contradictory case, Emotet, which has a well-known reputation as a banking trojan, is actually dropping another banking trojan instead of utilizing its own information-stealing modules. Even more interesting is that Trickbot, after being dropped by Emotet, sometimes drops the Ryuk ransomware.

As strange as this may seem, it appears that cooperation between groups could simply come down to the fact that working together leads to the largest paychecks. If Emotet can't utilize a device to spread further, Trickbot can steal the banking records. If no banking records are found, Ryuk can encrypt the device and demand a ransom. Of course, how long this unholy alliance lasts is anybody's guess.

What the future holds

Of course, a threat that grows rarely stays under the radar. In the last couple months of 2018, the security industry began to sit up and take notice of the size of Emotet. What has raised its profile is that email spam distributors appear to have shifted from cryptomining payloads to distributing Emotet and remote access trojans (RATs). And its impact is being felt. In fact, some Emotet infections have cost up to $1 million to clean up, according to US-CERT.

The actors behind Emotet appear to be shopping it around as a distribution channel for other attack groups.

Emotet is unlikely to fade away and may very well dominate the threat landscape for the foreseeable future. And if the past is any predictor of the future, Emotet will eventually subside, only to be replaced by another dominant player in the threat landscape.

For a deeper look into this topic:

https://blog.talosintelligence.com/2019/01/return-of-emotet.html

https://www.us-cert.gov/ncas/alerts/TA18-201A

https://duo.com/decipher/the-unholy-alliance-of-emotet-trickbot-and-the-ryuk-ransomware

https://blog.talosintelligence.com/2018/12/cryptocurrency-future-2018.html

IoT Machinations: The case of VPNFilter

Image: Talos

VPNFilter stands as a harbinger of what is almost inevitably yet to come.

There have been a number of notable internet-of-things (IoT) related threats in the last decade. There was the Mirai botnet, which infected IP cameras and routers to carry out DDoS attacks. And who can forget baby monitor hacks, where parents walk into the nursery to hear hackers talking to their children after breaking into the device?

Like it or not, from smart assistants to internet-connected hospital devices, IoT has entered our homes and businesses. Unfortunately in many cases, proper security practices have been overlooked in the process. As a result, we've seen such devices targeted by malicious actors.

However, nothing has been quite as pernicious as VPNFilter. This threat targeted a wide swath of routers from a variety of manufacturers, likely preying upon unpatched vulnerabilities to compromise them. One of its purposes appeared to be the exfiltration of sensitive data from the networks it compromised, but it also contained a modular system that allowed it to do so much more, making it of particular concern.

All told, the threat infected at least half a million devices across 54 countries. Luckily, researchers in the Cisco Talos group became aware of the threat early on. When infections ramped up, they were ready to stop it in its tracks. Today, the threat posed by VPNFilter has largely subsided, thanks to the work of public- and private-sector threat intelligence partners and law enforcement. Still, VPNFilter stands as a harbinger of what is almost inevitably yet to come.

How it's made

Stage one – VPNFilter has three primary components, or "stages," that comprise the threat. The primary goal of stage one is to establish a persistent hold on a device. Up until VPNFilter, malware targeting IoT devices could normally be cleared by simply rebooting the device. In the case of VPNFilter's stage one component, the malware survives such an attempt. Stage one also includes multiple options for connecting to the command and control (C2) server, which tells the malware what it should do.

Stage two – Stage two, which is the core component used to carry out VPNFilter's malicious goals, possesses capabilities such as file collection, command execution, data exfiltration, and device management. Some versions of stage two even included a "kill switch," which if activated, could render the infected device permanently unusable.

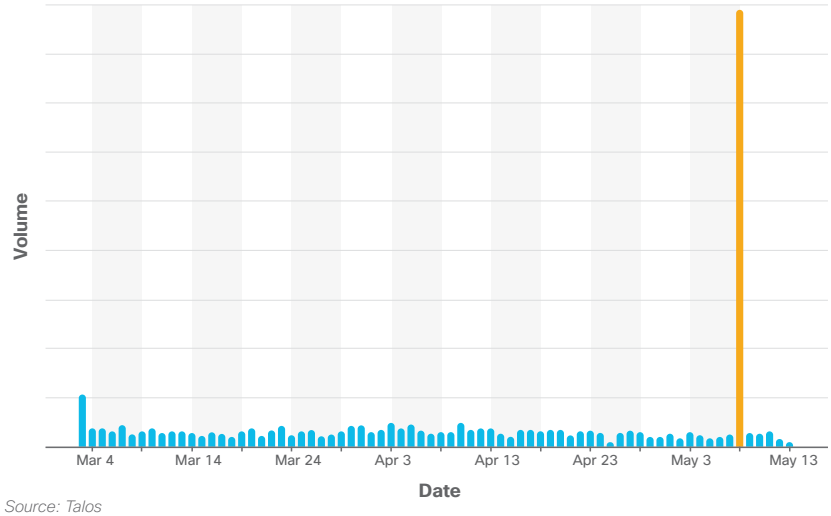
Stage three – The third stage extends the functionality of stage two, delivering plugins to help facilitate further malicious actions. Some of the notable plugins include functionality to:

- Monitor network traffic
- Steal various credentials
- Monitor specific industrial IoT device traffic
- Encrypt communication with the C2 server
- Map networks
- Exploit endpoint systems
- Spread to other networks
- Carry out DDoS attacks
- Build a proxy network that could be used to hide the source of future attacks

VPNFilter (almost) kicks off

Talos had been researching VPNFilter for several months, and the infection rate had been fairly stable. The team had been monitoring and scanning infected devices to get a better understanding of the threat and the capabilities contained in the malware.

Figure 2 New VNPFilter infections by day



Source: Talos

That is until May 8, 2018, when there was a sharp spike in infection activity. Not only that, but the majority of infections were based in Ukraine. A second spike in VPNFilter infections in Ukraine followed on May 17th, close to the one-year anniversary of NotPetya. Given that there was a history of destructive attacks in Ukraine, Talos felt it was best to address this infrastructure attack as soon as possible, even though research remained ongoing.

Talos would continued to research and release information on the botnet until, in September 2018, it was able to declare the threat neutralized.

Gone, but not forgotten

Unfortunately, while VPNFilter may be a threat of the past, vulnerabilities continue to be discovered in IoT devices. It's all but inevitable that another threat targeting IoT will appear in the future.

Defending against threats like this is difficult. IoT devices such as routers are generally connected directly to the Internet. Couple this with the fact that many users either do not have the technical expertise to patch them, or do not consider them a threat, and the situation becomes very dangerous.

At the end of the day, **IoT as part of the network will only grow. VPNFilter shows us what can happen if we don't take proper steps to secure these devices in the future.**

For a deeper look into this topic:

https://blog.talosintelligence.com/2018/05/VPNFilter.html

https://blog.talosintelligence.com/2018/06/vpnfilter-update.html

https://blog.talosintelligence.com/2018/09/vpnfilter-part-3.html

https://blog.talosintelligence.com/2018/12/year-in-malware-2018-most-prominent.html

Unfortunately, while VPNFilter may be a threat of the past, vulnerabilities continue to be discovered in IoT devices. It's all but inevitable that another threat targeting IoT will appear in the future.

Mobile Device Management: The blessing and the curse

Talos discovered that malicious actors have figured out how to use MDM for malicious purposes.

Mobile Device Management (MDM) functionality has been a boon for the enterprise. It allows an organization much more control over the devices on their network. However, as we discovered in 2018, it has also opened the door to well-funded malicious actors.

When it comes to mobile malware, mobile operating systems can be a hard nut to crack. The walled garden that has been created around the mobile operating system has, for the most part, protected it against malicious apps.

That is not to say that malicious actors haven't tried to attack mobile phones. There have been malicious apps discovered in the official app stores, but in most cases attackers have been confined to compromising devices that have been unlocked or "jailbroken," or if available, allow third-party apps.

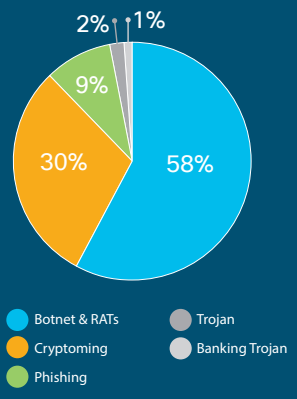
So while the walled garden can be secure, it can also be a prison. The downside to this level of restriction, and the security it provides, is that you can only install apps from an official app store, or if available, leave your device open to all third-party apps. This becomes a problem for businesses that create proprietary applications that they only want their employees to access, but also want to keep their devices secure.

The introduction of MDM

To address this need, MDM systems were introduced. This allows a business to take company mobile phones, install profiles registered to their company, and ultimately install apps of their choosing. MDM often provides other enterprise-friendly features as well, such as the ability to control device settings, prevent access to unwanted web sites, or find lost devices.

A snapshot of security incidents

What are the most common security incidents organizations are facing? Our colleagues in the Cisco Cognitive Intelligence group ran the numbers for us. Here's a snapshot of the top five categories, taken from July 2018.



By and large, botnets and RATs dominate the security incidents. Included in this category are threats such as Andromeda and Xtrat.

The second largest threat category is cryptomining, which contains incidents that unveiled unauthorized Monero and Coinhive miners, among others.

What's most noticeable about this snapshot is how small a proportion banking trojans make up. This will no doubt change as Emotet activity picks up.

We will revisit this metric in future reports to see how it changes.

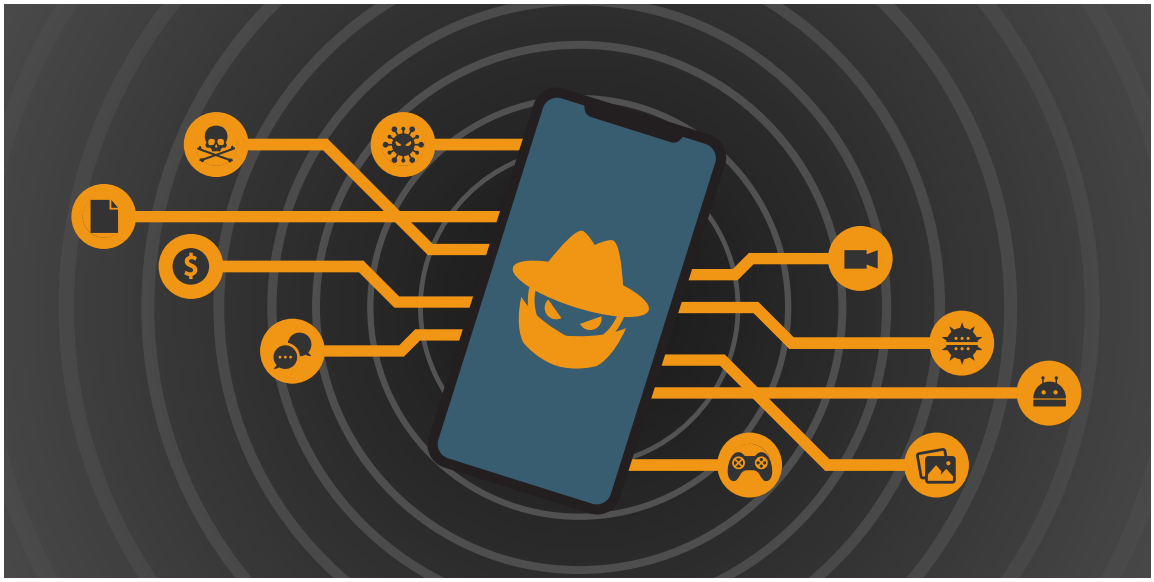


Image: Talos

There's no doubt that MDM is a powerful tool. Powerful enough that Cisco Talos has discovered malicious actors have figured out how to use it for malicious purposes.

It began in India

Our researchers at Talos discovered devices in India that had been compromised using an open source MDM system. The attackers had managed to get malicious profiles onto the devices and push out apps with the purpose of intercepting data, stealing SMS messages, downloading photos and contacts, and tracking the location of the devices, among other things.

The apps included modified versions of popular apps such as WhatsApp and Telegram that had extra features added — or "sideloaded" — onto them, allowing the attackers to monitor conversations on each compromised device.

How these devices fell prey to this attack remains a mystery. It's possible that the attackers had physical access to the devices, allowing them to install a profile that gave them control. However, it's also possible that the attackers used social engineering to trick the users into installing the profile.

This malicious alert may have arrived by email or text message, attempting to fool the user into thinking that they were required to install the malicious profile. Even so, the user would be required to follow a series of instructions and click through a number of prompts before the device was fully compromised.

Tending to your garden

There's no doubt that this is a potent and concerning attack method. Luckily it's also rare. The attack campaign uncovered by Talos is the only publicly known campaign of this particular type. It is also difficult to carry out, considering the number of steps a user is

Given the potential rewards, we're likely to see more of these attacks in the future, carried out by well-funded threat actors.

required to go through in order to configure a device for malicious activity. But given the potential rewards, Talos is already seeing more mobile device attacks, carried out by well-funded threat actors.

Ironically, the best protection against a malicious MDM is...MDM.

Organizations should ensure that company devices have profiles rolled out to them that can monitor and prevent the installation of malicious profiles or apps from third-party app stores.

It's also important that users are made aware of the MDM installation process, and that they are educated about these attacks to avoid them installing a malicious MDM.

For a deeper look into this topic:

https://blog.talosintelligence.com/2018/07/Mobile-Malware-Campaign-uses-Malicious-MDM.html

https://blog.talosintelligence.com/2018/07/Mobile-Malware-Campaign-uses-Malicious-MDM-Part2.html

What happened to ransomware?

Back in 2017, it seemed like ransomware would dominate the threat landscape for a long time to come. Threats like SamSam and Bad Rabbit had grabbed the headlines, demanding cryptocurrency payments, or else they lose all their data.

Flash forward a little more than a year, and things have certainly changed.

Ransomware has been usurped from its throne, largely by malicious cryptomining.

Why the sudden change? With ransomware, only a small percentage of victims pay the ransom. And even if they did, it was just a one-time payment, not a source of recurring revenue.

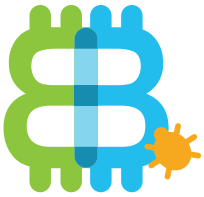
Even more risky, law enforcement agencies throughout the world began to crack down on ransomware attackers. As arrests tied to ransomware went up, adversaries were drawn to less risky attack types.

That's not to say ransomware is gone; we saw a few such threats crop up in 2018. GandCrab continued to make its presence known, and Ryuk was spread via Emotet and Trickbot infections. So while ransomware is no longer king of the hill, it still remains, requiring vigilance to avoid outbreaks.

Cryptomining: A wolf in sheep's clothing is still a wolf

By far the most prominent money-making threat scheme of 2018 was malicious cryptomining. This is a topic the Cisco Talos threat intelligence group has been researching for some time. To the mind of an attacker, it's almost the perfect crime: Miners often work in the background without the users' knowledge, stealing their computing power while generating revenue for the attacker.

As enterprises became better at dealing with ransomware, and law enforcement agencies throughout the world began to crack down on ransomware attackers, more and more adversaries were drawn to the less risky prospect of peddling malicious cryptomining software.



There is little difference between cryptomining software a user installs, and the cryptomining software installed by a malicious actor.

Sheep meets wolf

There is often little to no difference between cryptomining software that a user installs on their own and cryptomining software installed by a malicious actor. The nuance lies in consent; malicious cryptomining software is running without the owner's knowledge. There is an obvious appeal to attackers in this case – where they can reap the benefits without the victims' knowledge.

In the game of risk and reward, cryptomining is less likely to draw the attention of law enforcement. Conversely, any software that runs on a device without the owner's knowledge is a cause for concern.

And cryptomining – malicious or otherwise – can pay well. Over the past couple of years, and into the first half of 2018, the value of cryptocurrency skyrocketed. As with anything software-related and valuable, malicious actors took notice, especially as it coincided with a decline in ransomware. And cryptomining yields recurring revenue, whereas ransomware usually results in a one-time payment from the victim.

The dangers of malicious cryptomining

From the perspective of the defender, there are plenty of reasons to be concerned about malicious cryptomining. Like any piece of software on a computer, cryptomining will have a negative impact on overall system performance, and will require extra power. It may not add up to much on one system, but multiplying the cost over the number of endpoints in an organization, you could see a noticeable rise in power costs.

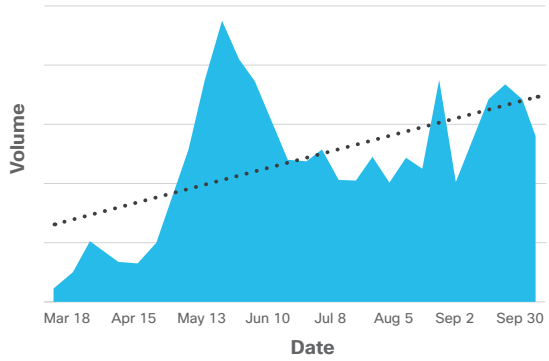
Furthermore, there may be regulatory compliance implications when cryptominers are earning revenue on corporate networks. This holds especially true for those in the financial sector, where strict rules could apply to revenue generated using corporate resources, whether or not those in charge are aware of the practice.

But perhaps most worrying is that the presence of a malicious cryptomining infection, unbeknownst to those running a network, could point to security holes in the network configuration or overall security policies. Such holes could just as easily be exploited by attackers for other means. In essence, if a cryptomining infection is found on a network, what's to stop other malicious threats from exploiting those same vulnerabilities to carry out further malicious activity?

What's happening now?

While there have been sharp peaks and valleys, in the overall volume of cryptomining-related traffic that Cisco has witnessed on the DNS layer, the takeaway is that cryptomining is trending up as time goes on.

Figure 3 Corporate DNS cryptomining traffic volume



Source: Cisco Umbrella

What is interesting is that the values of many popular cryptocurrencies have declined during the same time frame, trending downwards. Take Monero for instance, a popular coin used in malicious cryptomining.

Figure 4 Monero closing values

Source: coinmarketcap.com

Malicious actors are continuing to push malicious cryptomining out because of the ease of deployment and the low risk if discovered. The fact is, once it's installed on a device, it continues to earn the malicious actor money so long as it remains.

How does malicious cryptomining get on a system?

There are various ways that malicious cryptomining can find its way into your environment, such as:

- Exploiting vulnerabilities
- Sending emails with malicious attachments
- Employing botnets
- Leveraging cryptomining in the web browser
- Utilizing adware threats that install browser plugins
- An internal malicious actor

Unfortunately, malicious cryptomining is here to stay for the foreseeable future. Distributors of spam will likely continue to send cryptomining threats.

The presence of cryptomining, unbeknownst to network adminstrators, could point to other security holes in the network.

Money is and likely always will be one of the chief motivators for malicious actors. In many ways, malicious cryptomining can be seen as a way for attackers to make a fast profit with little overhead. This is especially true since targets are less worried about the implications of cryptomining on their devices as compared to other threats. It's a perfect situation for wolves to dress as sheep and watch the profits roll in.

For a deeper look into this topic:

https://blogs.cisco.com/security/cryptomining-a-sheep-or-a-wolf

https://blog.talosintelligence.com/2018/12/cryptocurrency-future-2018.html

https://blog.talosintelligence.com/2018/12/cryptomining-campaigns-2018.html

On the radar

For this report, we looked at a wide variety of threats to include. While not everything made it into the report, we plan to visit the following topics in the coming months through our Threat of the Month blog series. Here's a taste of what's to come:

Digital extortion. One of the more insidious phishing campaigns of late has preyed upon recipients' fears in order to extort Bitcoin payments. Some campaigns claim that they caught the recipient on camera looking at pornographic web sites. Others include fake bomb threats. Ultimately, the threats are completely fabricated, all in the hopes of tricking enough recipients into filling the attackers' Bitcoin wallets.

Office 365 phishing. Another significant phishing campaign centers around stealing credentials from Microsoft Office 365 accounts. Attackers have used a number of methods to do so. We'll outline different campaigns and how to recognize them in our upcoming blog post.

To stay abreast of our Threat of the Month blog series, be sure to subscribe to our mailing list and visit the Threat of the Month page.

Subscribe: http://cs.co/9002ERAWM

Threat of the Month: http://cisco.com/go/threatofthemonth

Winter was coming: Olympic Destroyer

Image: Talos

While the Olympics attack might have been a one-off, the group behind it is not going to rest.

Last year started out with a bang. Cybersecurity experts were still feeling the effects of the one-two punch of WannaCry and NotPetya, and were hoping for a quieter start to the year. These aspirations were quickly shattered when Talos discovered that the disruptions to the opening ceremony of the 2018 Winter Olympics in Pyeongchang, South Korea were caused by malware.

The malware was highly destructive and tailored for the environment it was in. Its name may be linked with a historic occasion, but the threat from Olympic Destroyer lives on.

During the opening ceremonies, Wi-Fi stopped working in the stadium and media areas of the Winter Olympics, and the official web site of the games was taken down. A large-scale interruption like this poses myriad challenges including data privacy risks, tarnished brand reputation, and a drop in customer satisfaction.

Eventually, it became clear that this disruption was a cyberattack, and longer-term investigation would show that the malware displayed two traits: 1) it was wiper malware designed to destroy assets (rather than execute as ransomware, for example), and 2) more interestingly, it was crafted to hide its origin and trick researchers. This was an advanced attack blending sophisticated malware techniques with devious strategy.

How exactly does Olympic Destroyer destroy?

The delivery method of Olympic Destroyer is up for speculation. What's clear is that, once inside a target network, it moves within that network, and it moves fast.

Our best analysis in the aftermath of the Pyeongchang attack is that it moved like a worm: quick and highly destructive. The file steals passwords, erases backup data, and targets data stored on servers, causing maximum devastation in the shortest possible time.

Olympic Destroyer was highly destructive and designed to demolish information.

The attackers used legitimate tools to perform lateral movement, in this case PsExec (a Windows protocol that allows you to run programs on remote computers). Given the very specific timing of the attack to coincide with the opening ceremony of the Olympics, the attack was remotely triggered.

Olympic Destroyer likely wanted to create plausible deniability for its authors by using pieces of old code that's been attached to other threat actors. Some security researchers were thrown off by this as well, as some of them rushed to attribute the attack.

There's more winter coming...

Whatever the actual motives, Cisco Talos found the markers of a sophisticated actor in the Olympic Destroyer malware. This tells us that, while Olympic Destroyer was a tailored attack, the group behind it is not going to rest. They will likely use this highly effective method again for stirring up further chaos, or for carrying out theft or other nefarious actions. We therefore need to be vigilant when looking for malware of this nature.

And that is how 2018 started. Let's hope 2019 has nothing as malicious and sophisticated in store for any other major event.

For a deeper look into this topic:

https://blog.talosintelligence.com/2018/02/olympic-destroyer.html

https://blog.talosintelligence.com/2018/02/who-wasnt-responsible-for-olympic.html

https://blog.talosintelligence.com/2018/12/year-in-malware-2018-most-prominent.html

About the Cisco Cybersecurity Series

Throughout the past decade, Cisco has published a wealth of definitive security and threat intelligence information for security professionals interested in the state of global cybersecurity. These comprehensive reports provided detailed accounts of threat landscapes and their organizational implications, as well as best practices to defend against the adverse impacts of data breaches.

In our new approach to our thought leadership, Cisco Security is publishing a series of research-based, data-driven publications under the banner **Cisco Cybersecurity Series**. We've expanded the number of titles to include different reports for security professionals with different interests. Calling on the depth and breadth of expertise in threat researchers and innovators in the security industry, the collection of reports in the 2019 series include the Data Privacy Benchmark Study, the Threat Report, and the CISO Benchmark Study, with others to come throughout the year.

For more information, visit www.cisco.com/go/securityreports.

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA), Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.

Published February 2019 THRT_01_0219_r3