Cybercrime tactics and techniques: Q2 2018

Provided by

Malwarebytes LABS

Contents

Executive summary

A generally slow quarter reflects an overall lull in cybercrime, picking up where Q1 left off with cryptominers continuing to dominate, ransomware continuing to evolve through experimentation, and exploits making a small but significant comeback.

In nearly every malware category for both business and consumer detections, we saw a decrease in volume, corroborating our general "Dang, it's been quiet in here" sentiments since starting the new year. Our relative malaise was punctuated, however, with some interesting developments moving from Q1 to Q2. What threat actors lacked in quantity they made up for in quality.

Malwarebytes' top two consumer detections continue to be adware and cryptomining, respectively, while miners took over the number one spot for business detections in Q2. Spyware, which had a strong Q1 for business, dipped down by 40 percent to number five, while banking Trojans held steady in the number two position, despite dropping in detections by nearly 50 percent. Meanwhile, backdoors shot up on both the consumer and business side, with consumer detections increasing by 442 percent.

New developments in ransomware and cryptomining drove the market, as Q2 attacks generally showed more sophistication than their Q1 counterparts. The introduction of complex VPNFilter malware, which dropped multi-stage attacks on hundreds of thousands of unsuspecting small office and consumer users, shook the sleepy cybersecurity industry awake. While 2017 outbreaks such as WannaCry and NotPetya have been as yet unmatched in terms of distribution volume and impact, VPNFilter, SamSam, and other such complicated campaigns show that 2018 may just be the year of higher-level, targeted attacks.

So how did we draw these conclusions? As we've done for the last several quarterly reports, we combined intel and statistics gathered from April through June 2018 from our Intelligence, Research, and Data Science teams with telemetry from both our consumer and business products, which are deployed on millions of machines. Here's what we learned about cybercrime in the second quarter of 2018.

QUICK FACTS

- Cryptomining still hot, but starting to decline
- GrandCrab is the top ransomware variant of Q2
- Adware **up 19%** over last quarter for consumers
- VPNFilter debuts with **500,000** consumer and business infections
- Exploits on the rise
- Scammers increasingly targeting PI

Key takeaways

Cryptominers plateau

Cryptomining detections are slowly declining; however, as one of the top two detections for both businesses and consumers, they still dominate the threat landscape. With new Windows and Mac malware variants, diversification into other browser-based mining APIs, and new server-side attacks, cybercriminals are continuing to experiment with this fairly new attack vector.

Ultimately, many criminals aren't getting the return on investment from cryptomining they were expecting. The cryptojacking craze will likely stabilize as it follows market trends in cryptocurrency; however, a massive spike or downturn in the currency market could quickly impact those numbers one way or the other.

GandCrab now king of ransomware

GandCrab is now the top ransomware variant being used in the wild. This incredibly popular payload of multiple spam campaigns was dropped via email in Q1. In Q2, Gandcrab moved over to the Magnitude exploit kit for distribution. While Gandcrab led the way in ransomware, other families also made appearances in Q2, such as SamSam and Spartacus, continuing the trend of smaller, experimental campaigns over global-scale outbreaks.

Adware detections hold steady

Adware is still a top consumer detection (in sheer volume), increasing by 19 percent quarter over quarter. It remains a top business detection as well, just behind cryptominers and banking Trojans. However, new developments of this malware category remained few and far between in Q2. A notable exception: Kwik, a Mac adware campaign, used system configuration profiles as a means of attack, a rather novel and sneaky approach.

VPNFilter malware makes splashy debut

A new malware called VPNFilter made news this quarter with advanced, multi-staged attacks that reportedly infected over 500,000 small office and consumer-grade routers and NAS devices. The attack spanned more than 50 countries and affected major brands such as Asus, D-Link, Linksys, and Netgear.

VPNFilter is capable of covertly monitoring all traffic on the network in order to exfiltrate data, serve up man-in-the-middle attacks, or even destroy infected devices. This malware is not only able to harvest usernames and passwords, but it can also change webpages and insert artificial data to deceive users while, at the same time, draining accounts in the shadows. VPNFilter could also be used to perform DDoS attacks or as a catalyst to install other software, such as coin miners.

Exploits enjoy a renaissance

Don't call it a comeback: Zero-days have experienced a resurgence this quarter thanks in part to exploits that capitalize on four critical flaws identified in popular software. While vendors have been quick to issue fixes, many consumer and enterprise users do not patch promptly and therefore remain exposed.

The exploits in Adobe Flash Player, VBScript engine (Office, IE), and Adobe Reader were first used in either MS Office or Adobe documents, a sign that the threat landscape has shifted from drive-by attacks to social engineering schemes. Indeed, malicious spam—either targeted or via larger campaigns—is one of their main distribution vectors.

Scammers target PII

Scammers are increasingly targeting Personally Identifiable Information (PII) in Q2. We first observed scammers blatantly stealing PII from victims with Bitcoin scams. Light regulation, limited fraud protection, and poor support on exchanges contributed to making social engineering attacks against Bitcoin wallets highly lucrative. But as the victim pool for traditional tech support scams has contracted in the face of user awareness and increased enforcement, scammers have been stealing passwords, bank account information, and email accounts with increasing frequency. New GDPR regulations are likely adding fuel to the PII theft fire, as that type of information snatches a healthy paycheck on the black market.

Cryptomining

Six months into the year and eight months since the flood of cryptominers began, we see the beginning of another shift in the cybercrime landscape. We are not certain which threat is going to take over as the top detection next quarter, but it's unlikely to be cryptominers.

Windows cryptomining malware detections have dropped in Q2, despite rating highly on overall detections for the quarter. Data collected from late June, however, show a plateau starting to form from the slope.

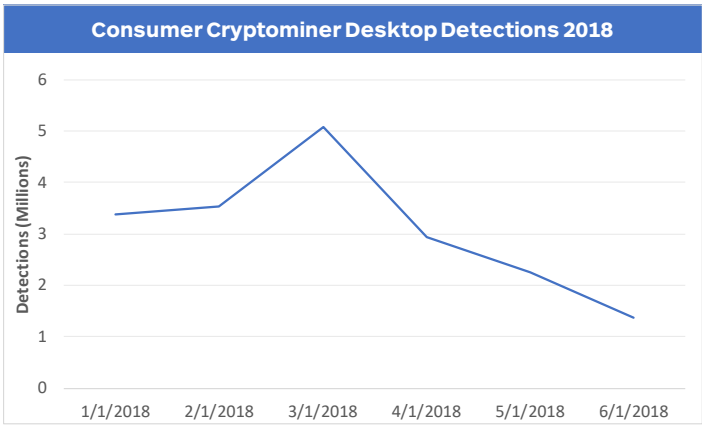


Figure 1. Consumer cryptomining malware detections, January – June 2018

Miners found on enterprise systems have fluctuated in the number of detections every month since the crypto craze began. So far in 2018, each quarter has had some form of spike in detections, the first being in January and the second in May. By Q3, we may be able to identify an ongoing trend and/or campaign trying to spread these tools. More than likely, though, we'll see a decline in business detections as we head into Q3, which has already been observed on the consumer side.

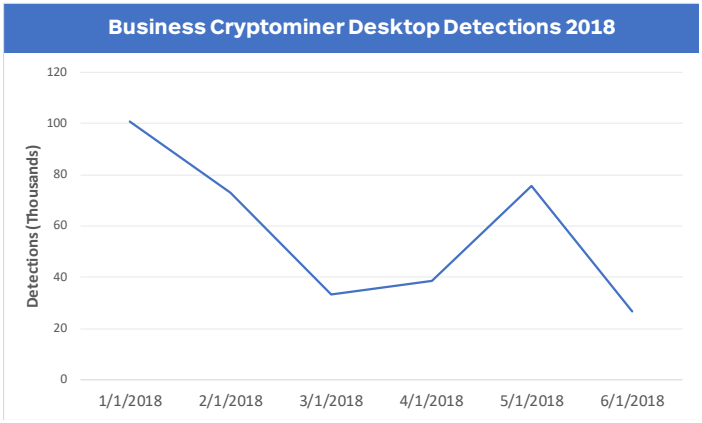


Figure 2. Business cryptomining malware detections, January – June 2018

The end of Q1 2018 showed a massive spike in detections of Android cryptominers, leading us to believe that we would see tidal waves of mobile miners in Q2. Luckily, we were wrong.

In fact, in May, the number of Android miner detections dropped by 16 percent from the previous month. However, despite these inconsistencies, Q2 still managed to come in with 244 percent more miner detections than Q1. The Android landscape is likely where we'll see an overall increase in the use of miners.

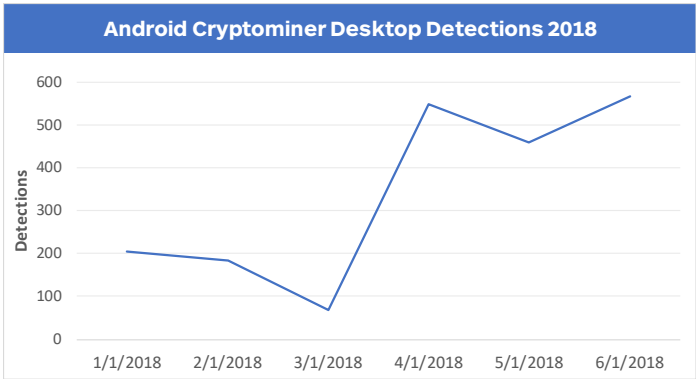


Figure 3. Android cryptomining detections, January – June 2018

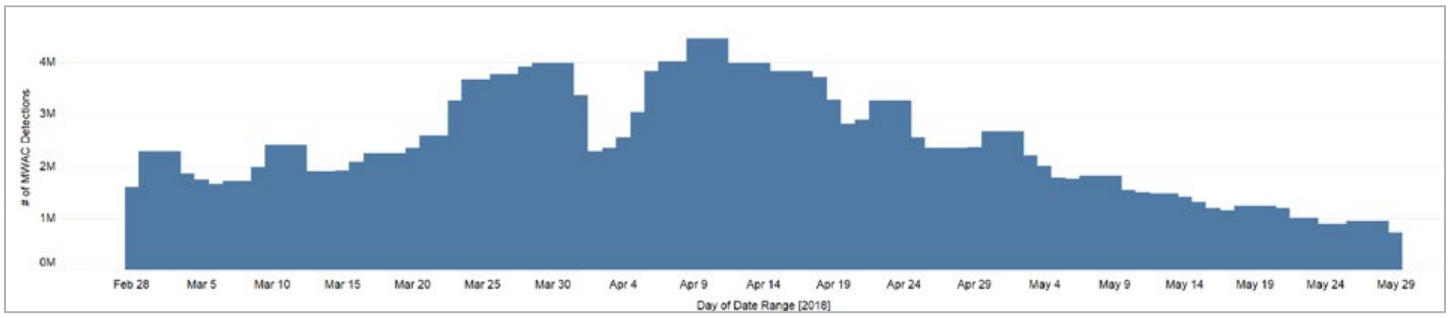


Figure 4. Blocked drive-by mining events, February – May 2018

Despite decreases in detections across the board, cryptominers are still one of the most common payloads this quarter, both in malware (Windows, Mac, Android) and browser-based versions (Coinhive.com). Being a less noisy payload has its advantages, as these threats can stay on systems for much longer, eventually generating larger profits. At the same time, their development and spread are closely tied to what is happening in the cryptocurrencies market.

The trend in detections closely mirrors the ebb and flow of cryptocurrency market prices, including Bitcoin, Ethereum, and Monero.

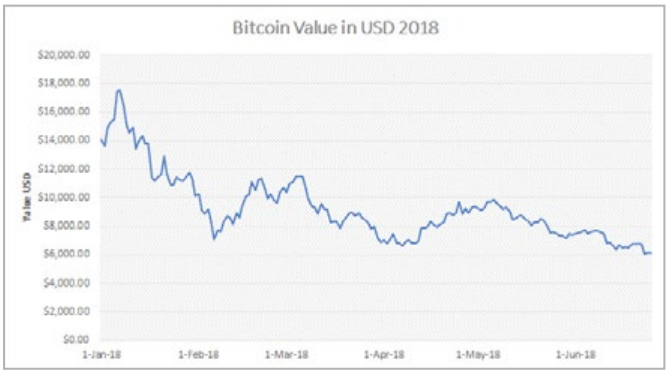


Figure 5. Bitcoin market price changes, January – June 2018

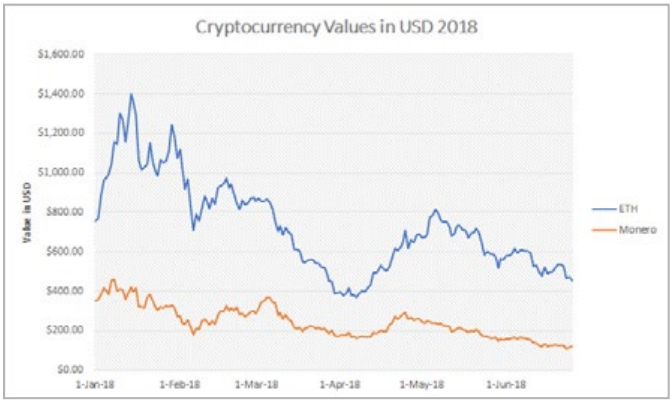


Figure 6. Ethereum and Monero market price changes, January – June 2018

The drop in cryptomining infections is a sign of decreased interest by people and criminals trying to make a quick buck from the popular cryptocurrency market, which is likely not making as many people rich overnight as it did in late 2017. Until changes in the cryptocurrency market cause a spike or swift downturn, expect to see cryptomining hum along at its current slower pace into Q3.

Windows cryptominer malware

On the Windows side, we have Smoke Loader, a popular payload among exploit kits, dropping cryptominers in several campaigns. Smoke Loader, aka Dofoil, has been around for years and is a sophisticated Trojan that uses several methods to avoid detection and analysis, such as process hollowing and actively blocking analysts' tools.

Process hollowing is a technique that runs a legitimate process and then replaces the code inside that process with malicious code. In one of the largest recent campaigns, the hollowed process was explorer.exe, which downloaded and ran a cryptominer, giving it the process name of wuauclt.exe (to mimic the legitimate Windows Update AutoUpdate Client). The cryptominer has gained persistence by hijacking the OneDrive Run key in the Windows registry and pointing it to a copy of the cryptominer in a subfolder in the Windows AppData folder.

Besides being dropped by exploit kits, Smoke Loader has also been seen posing as fake Spectre and Meltdown patches and as updates for other popular software.

Server-side attacks

Server- and client-side cryptomining has continued unabated in large part due to major vulnerabilities identified within Content Management Systems (CMSes), such as Drupal. Indeed, the Drupalgeddon attacks (CVE-2018-7600 and CVE-2018-7602) were almost immediately weaponized in the wild.

Upgrading a CMS is not always an easy task due to various dependencies (e.g., themes, plugins) that might stop working after the core has been updated. It is also a cost and, for some people, a technical hurdle, which means hundreds of thousands of sites will remain vulnerable to automated attacks.

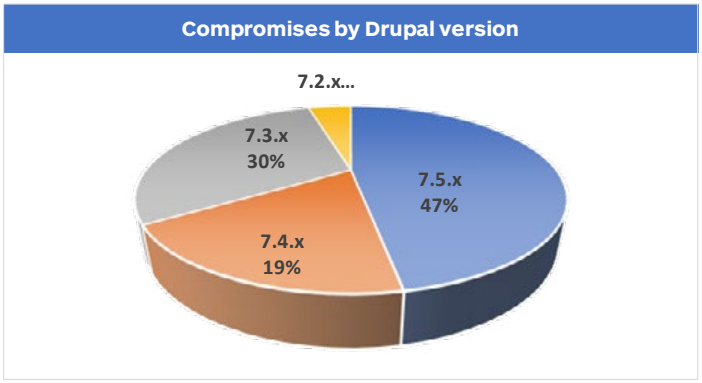


Figure 7. Compromises by Drupal version

Threat actors can repurpose hacked websites for a variety of uses, but according to a recent study we performed, the most common client-side payload is injection of in-browser mining code. This follows on the trend we have been monitoring since September 2017, with the emergence of a new threat we call drive-by cryptomining, which is made possible by silent APIs that use the browser of visitors to a website to mine for cryptocurrencies.

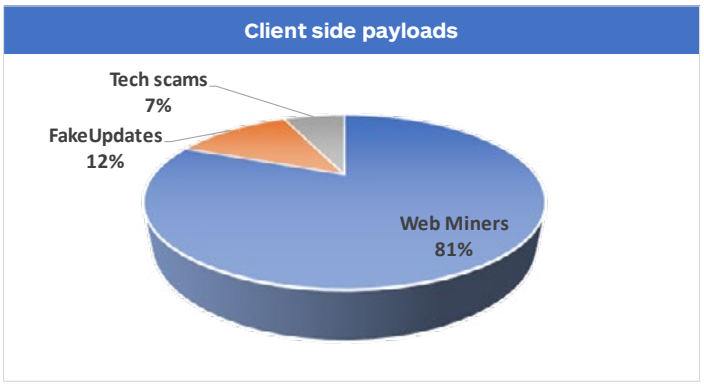


Figure 8. Type of injected payload

In the past few months, we have noted an increase in obfuscated scripts, making identification and blocking of web miners more difficult. These evasion techniques were to be expected and are a natural evolution of a still young and volatile threat.

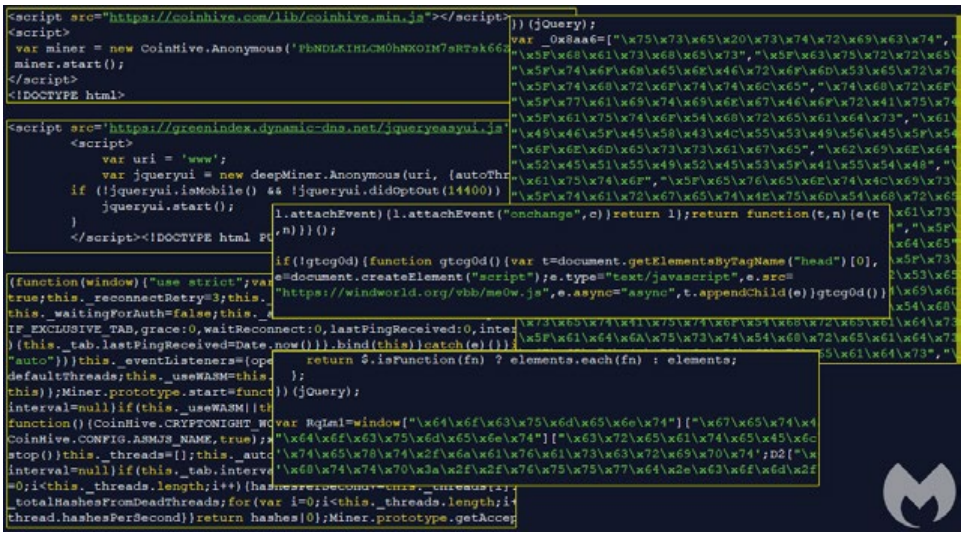


Figure 9. Various obfuscated scripts injected in the browser

Diversification into other mining APIs

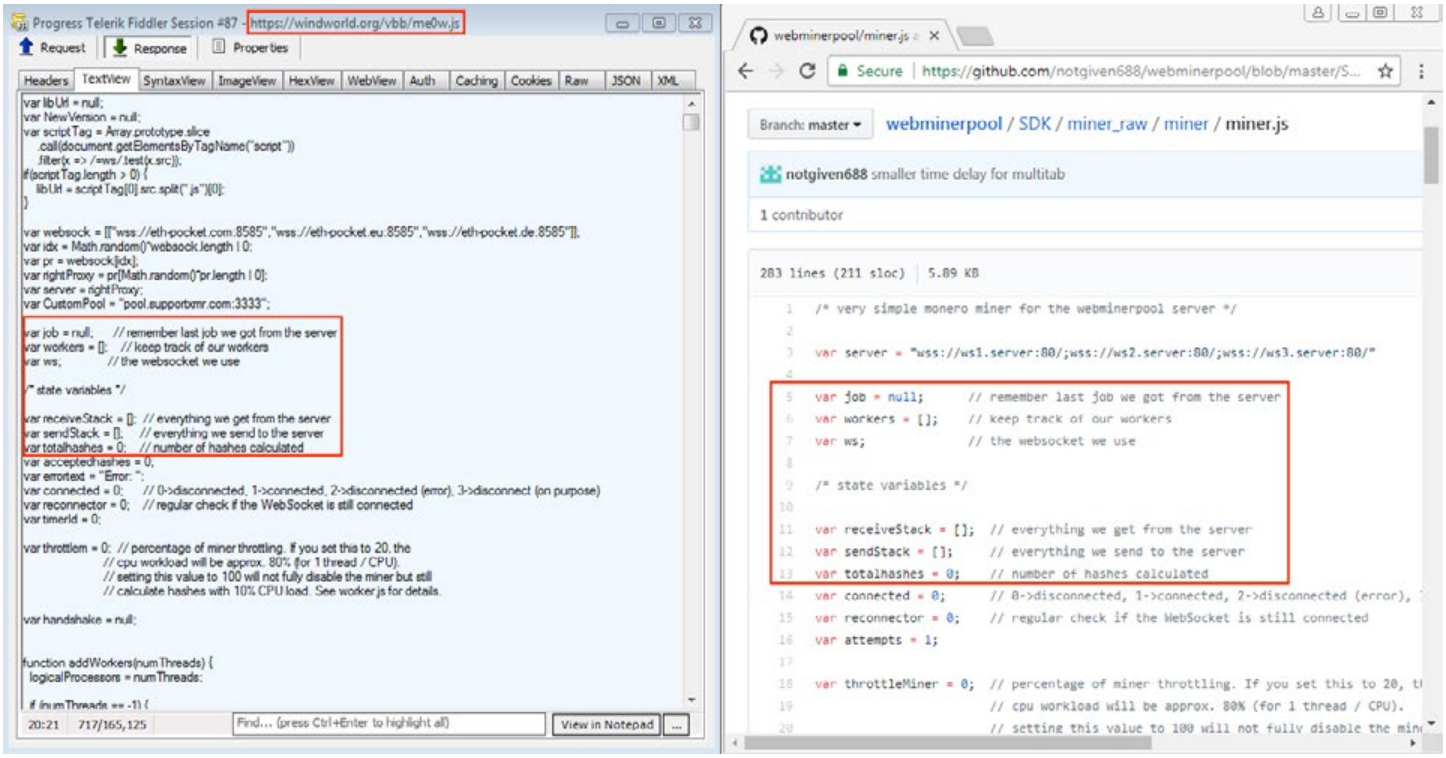


Figure 10. Left: a malicious web miner used in a campaign. Right: the open source version.

While we are still recording high levels of Coinhive-related activity, we are also seeing an increase in other in-browser "services," such as Cryptoloot.

Threat actors are paying close attention to developments with in-browser mining and are naturally driven by the prospect of making larger profits. They can do so by switching to services that offer them complete control of the mining script, bigger payouts, and lower detection rates from security products and ad blockers. Attackers are also leveraging open source web mining code and adapting it to their needs.

While Monero is still the de facto coin for cryptomining—legitimate or otherwise—there are many other up-and-coming currencies tailored for different needs. We expect to see matching trends between legitimate cryptomining and its criminal counterpart for a long time to come.

Malware

	Business	Q/Q		Consumer	Q/Q
1	RiskWareTool	5%	1	Adware	19%
2	Banking Trojan	-49%	2	Riskware Tool	-36%
3	Adware	-7%	3	Backdoor	442%
4	Backdoor	109%	4	HackTool	-16%
5	Spyware	-41%	5	Ransom	-12%
6	Ransom	-35%	6	Spyware	32%
7	Rogue	23%	7	CrackTool	-10%
8	HackTool	-41%	8	Rogue	-22%
9	Rootkit	-22%	9	Banking Trojan	-47%
10	CrackTool	-29%	10	Rootkit	-18%

Figure 11. Top 10 malware detections, consumer and business, Q2 2018

Our top malware categories of Q2 2018 show an overall dip in detection volume quarter over quarter for nearly every category on both the business and consumer sides. Banking Trojans took an especially hard hit, decreasing by 49 and 47 percent for business and consumer detections, respectively. In addition, spyware, which had a strong Q1 for business detections, fell by 41 percent, dragging the nosy malware down to the number five spot from number one.

Surprisingly, cryptominers (RiskWareTool), which have traditionally gone after consumer targets, took the number one spot for business detections. Meanwhile, adware hung onto its title as the top consumer detection—mostly because of a 36 percent decrease in cryptomining. Despite this drop, cryptomining still maintained a top position as the second-most detected malware for consumers. Backdoors also had a healthy increase in detections, jumping up by more than 440 percent on the consumer side.

Banking Trojans

When talking about banking Trojans this quarter, we are only referring to one family: Emotet. The first quarter of 2018 ended with a massive campaign effort to infect thousands of users with the Emotet banking Trojan.

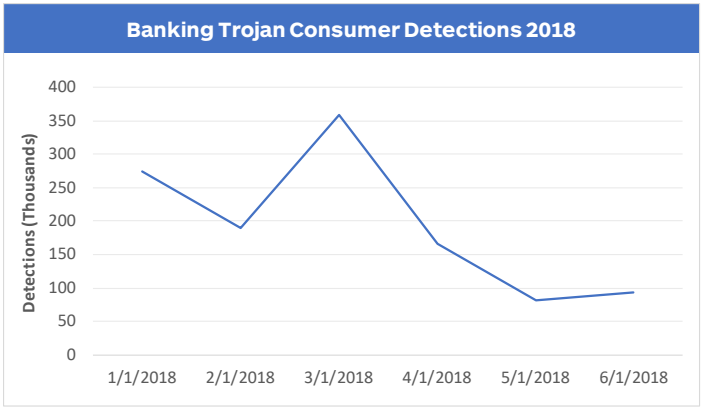


Figure 12. Consumer banking Trojan detections, January – June 2018

Detection for this campaign, both for business and consumer customers, continued through April and May.

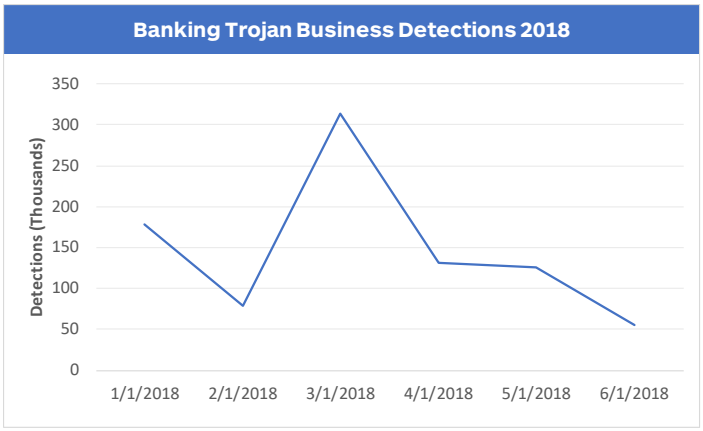


Figure 13. Business banking Trojan detections, January – June 2018

Banking Trojans have not been used as a primary payload for a few years. The likely reason behind the Emotet campaign at the end of Q1 lies in modifications made to banking Trojans that identify credentials and offline wallets for cryptocurrency, using the infection to steal coins. As the value of cryptocurrency decreases, we see less and less of this malware.

Backdoors

The second quarter of 2018 had a huge spike in backdoor malware detections, which seemingly came out of nowhere. However, the spike is due to a particular campaign spreading malware we refer to as Backdoor.Vools.

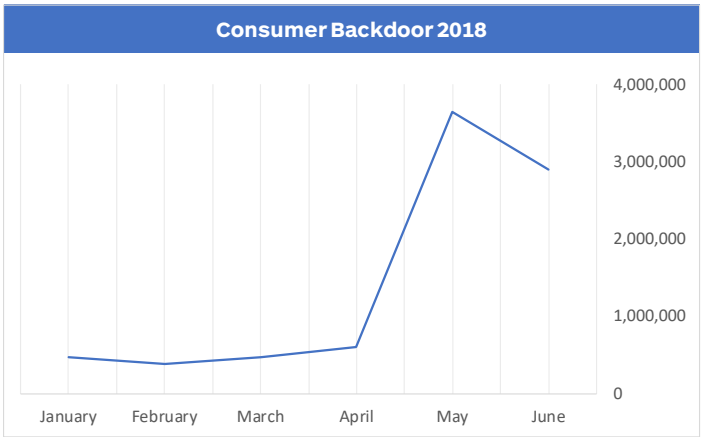


Figure 14. Consumer backdoor detections, January – June 2018

The Vools backdoor malware has been primarily observed installing cryptocurrency miners on the affected system after it communicates with a command and control server. In addition, Vools utilizes some of the exploits used in the WannaCry attack, namely the ETERNALBLUE SMB vulnerability.

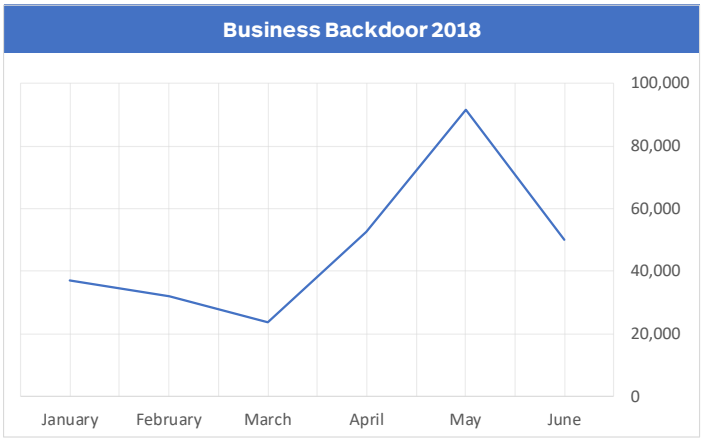


Figure 15. Business backdoor detections, January – June 2018

The campaign started in May, and it is likely that statistics for the next few months will continue to show Vools as a top backdoor detection. Users infected with Vools may want to investigate any servers running on their networks with vulnerable SMB protocols. Since this malware uses exploit technology, a system or network may become infected with little-to-no interaction from users.

The primary fear of Vools' capabilities is not due to its mining component or even its use of ETERNALBLUE, but the additional threats that this malware can and will install on the system once cryptomining goes out of fashion. Based on plummeting cryptocurrency values over the last few months, that time is going to come sooner than later.

Spyware

The biggest shake-up from Q1 to Q2 is the dramatic drop of spyware from the top business detection to the fifth-most detected malware type this quarter.

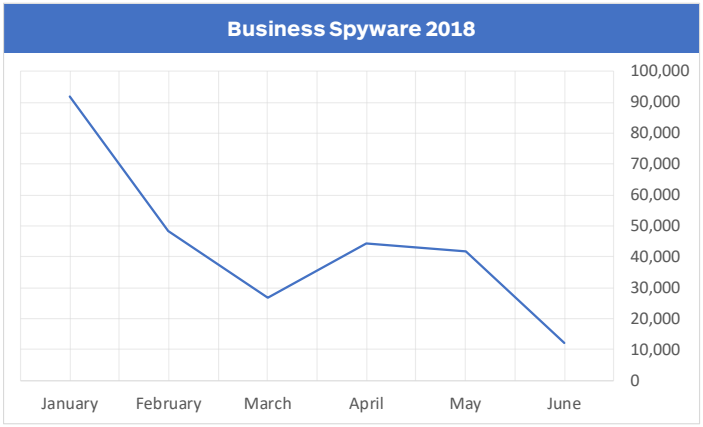


Figure 16. Business spyware detections, January – June 2018

Spyware started the year strong, however, the exact family responsible for this is unknown, with the majority of our Q1 spyware detections falling under a generic spyware category. However, the top spyware for Q2 was the notorious TrickBot, which added functionality to steal cryptocurrency wallets from its victims (something we talk about in the Q1 2018 Cybercrime Tactics and Techniques report).

As we head into Q3, and with the drop in detections for miners, we may not see spyware breaching the top 10 detections next quarter.

Ransomware

Ransomware detections dropped this quarter on both the consumer and business sides by 12 and 35 percent, respectively. It now ranks as the fifth-highest detection for consumers and the sixth-highest for businesses.

Similar to last quarter, ransomware authors have aimed their campaigns at businesses in Q2, with a serious increase in May following a slight drop in February. This follows the trend of repurposing most ransomware attacks to the more successful target: companies and organizations.

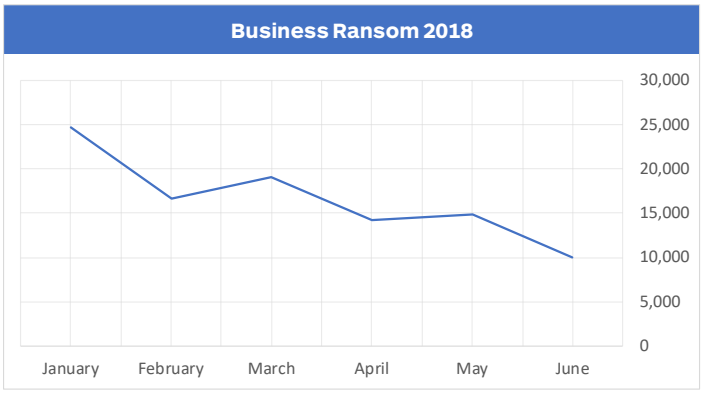


Figure 17. Business ransomware detections, January – June 2018

Consumer ransomware, however, experienced a spike in detections during March, but quickly dropped heading into Q2. Following the current trajectory, it looks like consumers are less likely to be hit by ransomware in Q3 than they were at the beginning of the year.

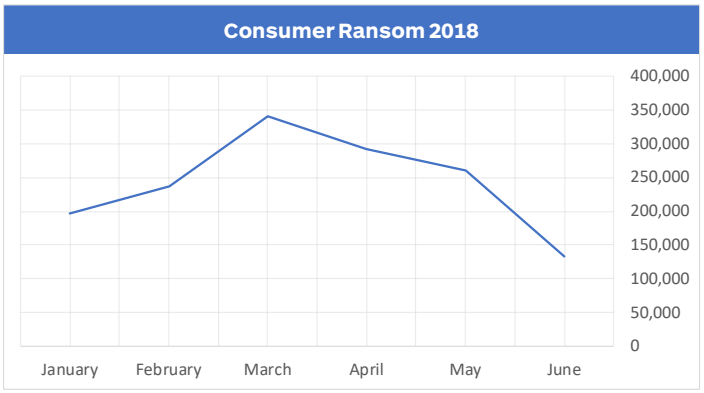


Figure 18. Consumer ransomware detections, January – June 2018

Meanwhile, Android ransomware started off the quarter with a strong push of SLocker Android ransomware, but since mid-April, there has been little significant activity—another sign of ransomware actors diverting targets and changing strategies.

New ransomware campaigns

The last quarter has seen some interesting developments in ransomware authoring. GandCrab is still making waves, laying claim to being the biggest player in town. We're also seeing new ransomware variants delivering attacks on opposite sides of the spectrum, from the sophistication of SamSam to the relatively new infection file known as Spartacus, which is as basic as it gets.

All three variants saw some action in Q2, proving that ransomware is nowhere near being dethroned as an effective attack vector. Threat actors are likely treading water, waiting for the appropriate moment to strike big. In the meantime, here's what we saw.

Spartacus

Although there are some files that perform sophisticated tasks, much of the ransomware plague today is made up of basic files conducting basic tasks to compromise a PC. Spartacus, making itself visible in April, is one such example. Sharing similarities in coding with Blackheart, Satyr, and ShiOne, Spartacus is written in C#, something a criminal could code in no time.

Spartacus—just like any other form of ransomware, regardless of how sophisticated—will compromise a PC and encrypt all its files. If you realize that this ransomware has hit your system, you can potentially save yourself by performing a process memory dump, in which case the keys could be extracted from memory.

Spartacus is the kind of software one expects to find offered on a script kiddie forum. There's no online functionality whatsoever, no C&C to call back to, and no additional files to download. There's also at least one possible mistake in its code: the RSA key is embedded in the ransomware, implying that the private key exists on the server side of the ransomware author's system. Decryption for all victims is possible, should this key ever be leaked.

The only way the ransomware author knows if someone is infected is if the victim emails their personal key to the creator, at which point they can begin extorting money. Without victims voluntarily sending a message back to base, the author won't be able to work out how successful their campaign is in terms of pure infection numbers.

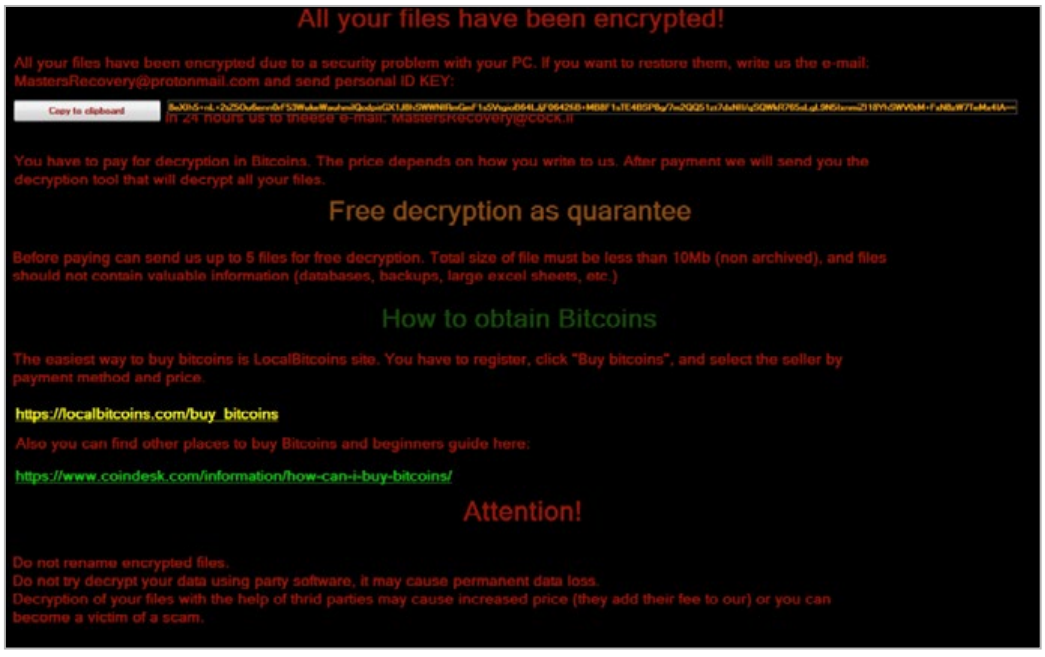


Figure 19. Spartacus ransomware encryption message

Even so, Spartacus displays a few of the more popular tricks used by big players. In the same way that some well-known infections try to gain the victim's trust by offering "free" file decryption before payment, Spartacus offers up to five files victims can claim back. This is reasonably generous, by ransomware terms. There's also no decryptor available to decrypt hijacked files, so victims will be in a lot of trouble if they don't have a good backup system.

Some newer versions of Spartacus are now targeting specific file types to encrypt, rather than attacking everything in sight. The encrypted files have the .SF extension instead of .spartacus, possibly as a way to avoid tracking across versions. It's also possible that someone else entirely has made the newer versions, in which case, we really would have an "I'm Spartacus!" situation.

GandCrab

GandCrab, the incredibly popular payload of multiple spam campaigns waged via email in the first quarter of the year, has moved over to the Magnitude exploit kit for distribution. Previously, Magnitude was extremely loyal to its Magniber ransomware files. And although it still focuses on South Korea, Magnitude has now added GandCrab into the overall mix.

Magnitude has always experimented with unconventional ways to load its malware, for example via binary padding (where additional data is added to the file to bypass scanners looking at static signatures). To make things worse, Magnitude is now also using a fileless technique to load the ransomware payload, making it somewhat harder to intercept and detect.

The variations of this technique have been known for several years and used by other malware families like Poweliks, giving the creators of this new blended attack an added edge over less sophisticated forms of ransomware.

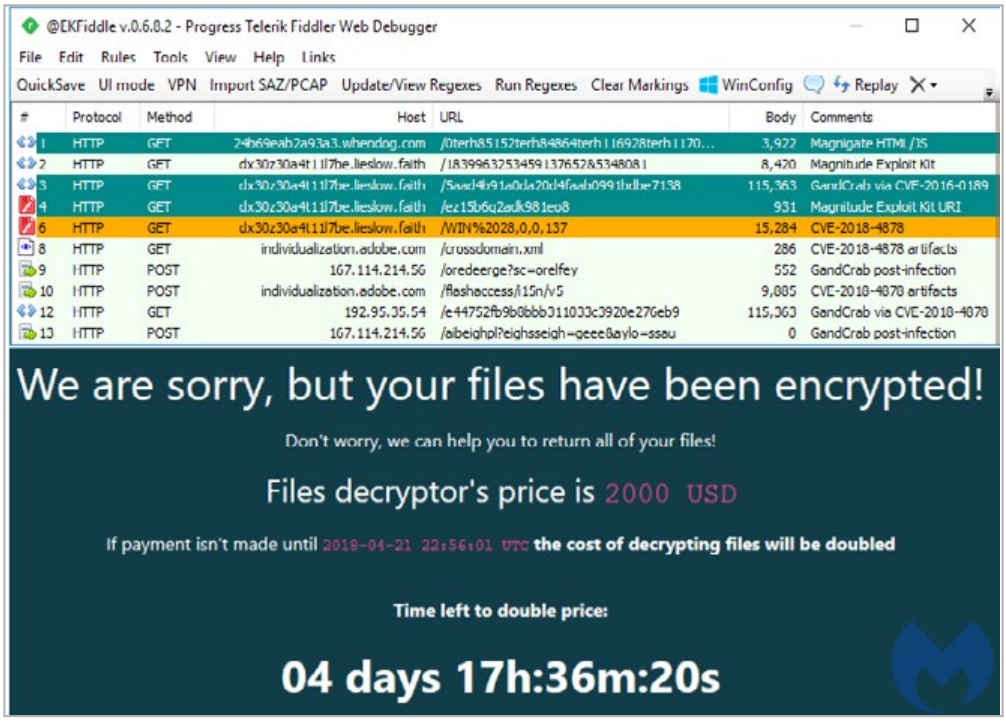


Figure 20. Magnitude EK traffic capture with the GandCrab payload

The encoded payload embedded in a scriplet is later decoded in memory and executed. After the payload is injected into explorer.exe, it immediately attempts to reboot the machine. Upon successful infection, files are encrypted with the .CRAB extension while a ransom note is left with instructions on the next steps required to recover those files.

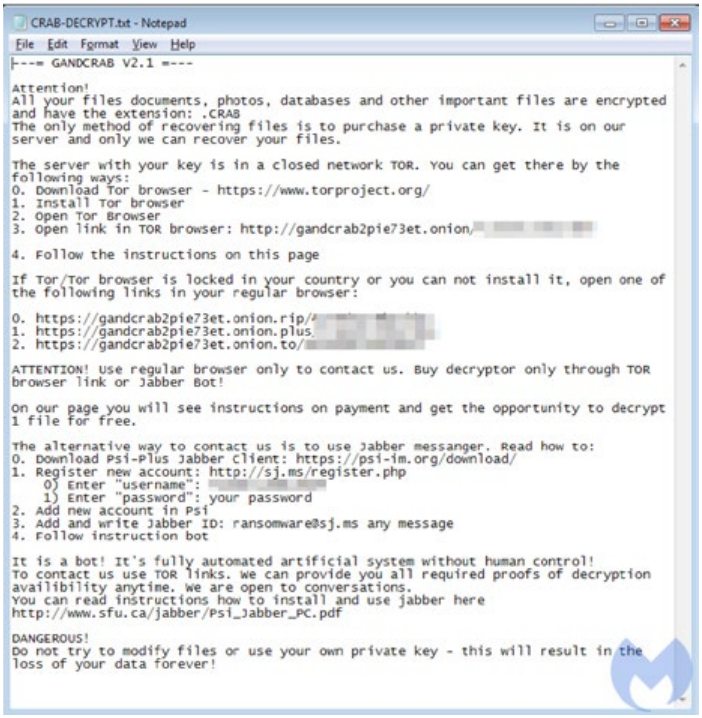


Figure 21. GandCrab's ransom note

While law enforcement operations resulted in earlier GandCrab infections having the opportunity to be decrypted without payment, there's always a risk that the latest versions being distributed by various exploit kits have no solution in place. Whether a ransomware file is advanced or basic by comparison, the threat to your files remains the same if deployed on your PC.

SamSam

While it may be lacking in size and distribution of the GandCrab family, the SamSam ransomware family packs a powerful punch. SamSam made headlines with the infiltration and destruction of files on systems maintained by the City of Atlanta and attacks against Hancock Health. Despite large-scale media coverage, this malware remains elusive due to the targeted nature by which cybercriminals are delivering the ransomware itself, ensuring that only profiled targets receive the encrypting payload.

While SamSam has been around for some time, recent evolutions in the attack vector and methodology have proven novel in their approach and successful for the attackers—raking in over $1 million this year for their efforts (largely depending on the value of Bitcoin). Instead of sending the malware payload to large numbers of potential victims through the use of malspam or exploit kits, the group responsible for SamSam chose to surveil potential targets to determine the value of the compromised information. Then they priced the recovery of the information at a rate that is more economical than alternative recovery efforts.

When the Hancock Health network was compromised by SamSam earlier this year, CEO Steve Long said, "From a business standpoint, paying a small ransom made more sense. They made it just easy enough to pay the ransom. They priced it right."

In a field dominated by easy-to-create ransomware construction kits and ransomware-as-a-service (RaaS) packages, SamSam attackers have taken a different approach. Recent attacks have shown a willingness of the criminals to seek out vulnerable systems using known exploit vectors within the RDP and SMB protocols. After compromising victim machines, attackers traverse laterally within the network, creating backdoors and performing reconnaissance to better understand the value of the data.

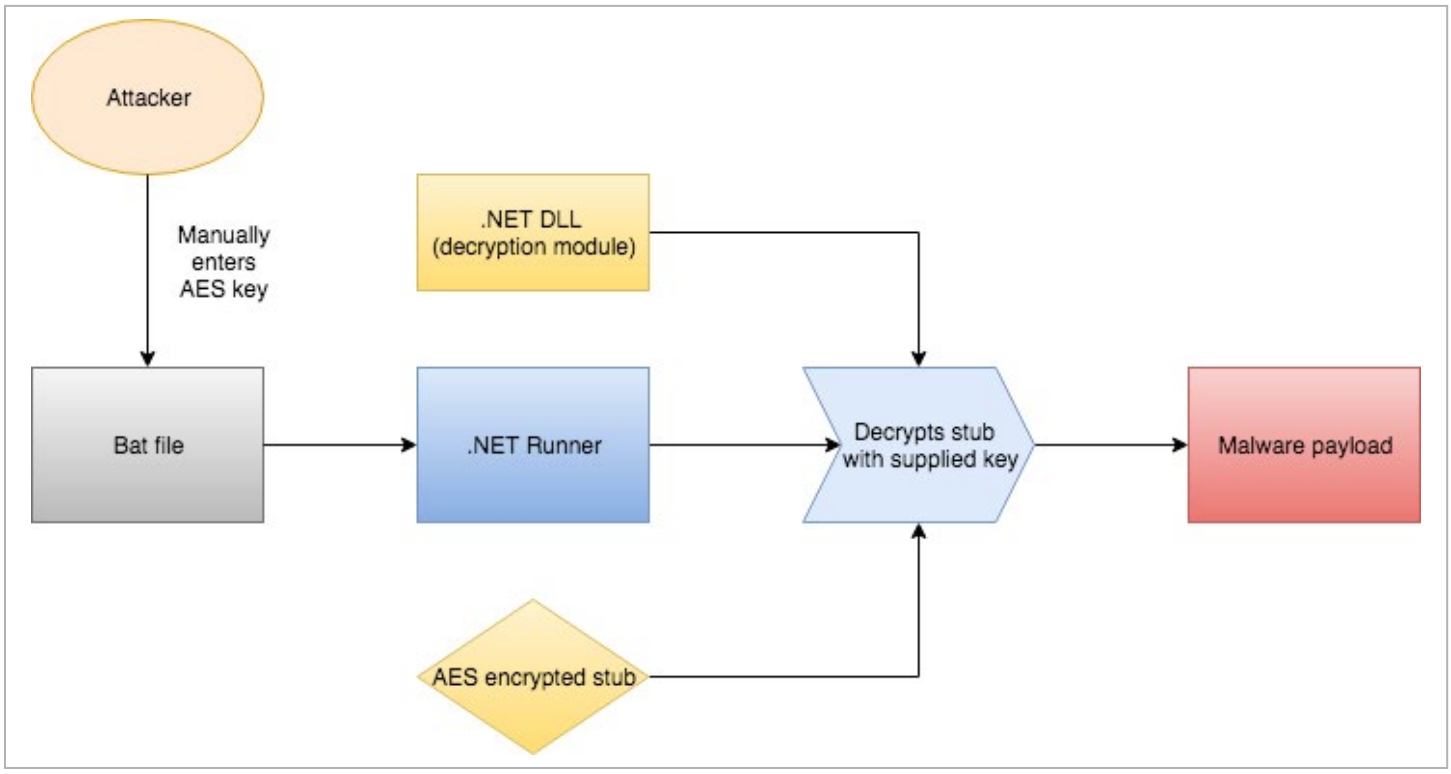


Figure 22. SamSam installation mechanism

After the group successfully compromises a victim network, they then decide on a reasonable ransom and use a custom install procedure to install the ransomware to machines on the network. Rather than using a simple executable to launch the encryption instructions, the attackers utilize direct human involvement to pass a specially-crafted password, which is in turn used to decrypt the malware payload. This means that there is a physical person sitting behind a keyboard during this phase of the attack. This not only makes it difficult for Incident Responders to reconstruct the attack but also makes analysis by malware researchers difficult, if not impossible.

The sort of attack methodology employed by the SamSam group is unique and has proven successful. Calculations of the various Bitcoin wallets being used have shown the group has collected nearly 100 bitcoins [1, 2] since December 2017, and attacks against vulnerable networks continue to line the pockets of the attackers to this day.

We are certain to see more attacks from the SamSam group, and considering the successful nature of the campaign, it's only a matter of time before other criminal groups begin to use the same distribution methodologies.

Adware

Being one of the easier forms of malware to distribute, and more often ignored by users, it is no wonder we see a significant number of consumer and business detections for adware. Despite this, it's important to note that adware, like any other malicious software, can easily infect systems with additional threats. The best outcome of allowing adware to run on your system is an additional infection of cryptominers. But the worst is nothing to sniff at: fileless rootkit malware that spies on everything you do.

Coming in as our third-highest detection this quarter, adware infections for businesses remain one of the more common threat types an organization might face. Adware detections include not only overly-aggressive advertising methods but also a wide variety of potentially unwanted programs such as sketchy third-party software, questionable toolbars, and even system modifications created by adware to reduce your system's security.

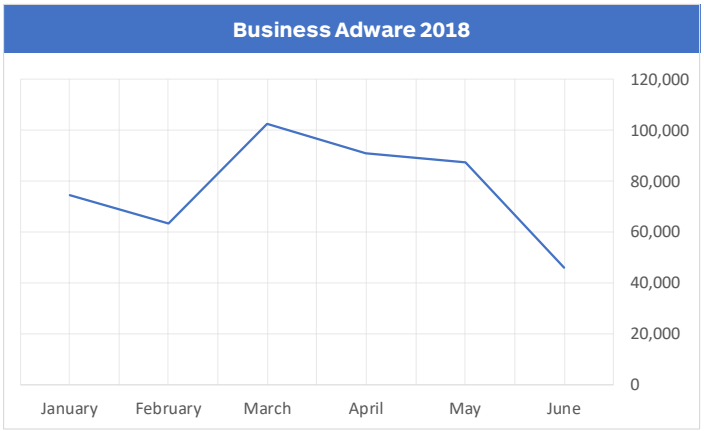


Figure 22. Business adware detections, January – June 2018

April was an eventful month for consumer adware in Q2, with a 184 percent increase over March. This spike usually designates an active campaign pushing some form of adware persistently. With the numbers returning to what we saw before April, it's uncertain whether more of these adware campaigns are in store for us this year.

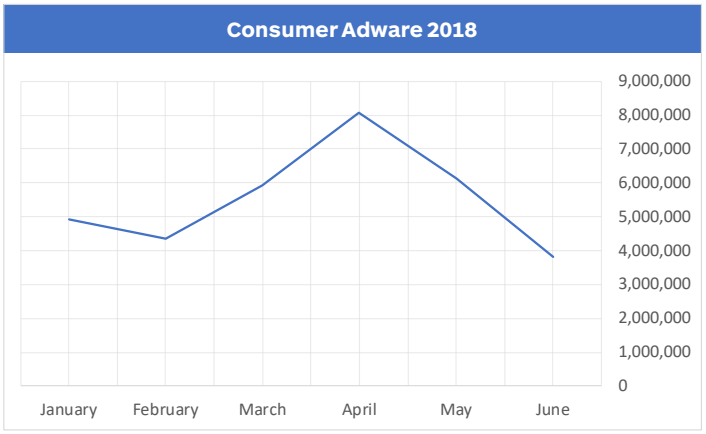


Figure 23. Consumer adware detections, January – June 2018

Notable Mac adware campaign

Some malware can be so simple—and yet such a pain to get rid of—especially when it starts interfering with system configuration. This much is true for Kuik, a Mac adware campaign that debuted in early May, surprising us all by forcing affected machines to join a domain controller.

Kuik Mac adware uses a sys config profile (sneaky) to set a specific homepage in Safari or Chrome, and then prevents users from changing it. It points the browser to chumsearch.com, which is a domain we've seen with a number of browser extensions and other pieces of adware associated with Crossrider.

Figure 24. Stage one of the Kuik attack

The perpetrators used this unusual technique to push Google Chrome extensions and coin miner applications to their victims.

VPN/IT router malware

Another attack that garnered a lot of media coverage over the last quarter was the VPNFilter malware that reportedly infected over 500,000 small-office and consumer-grade routers and NAS devices. The attack, spanning more than 50 countries and affecting major brands such as Asus, D-Link, Linksys, MicroTek, Netgear, and TP-Link, is capable of covertly monitoring all traffic on the network and serves the purpose of data-exfiltration, man-in-the-middle attacks, and even the destruction of infected devices.

The FBI announced the sophisticated, multi-stage attack in late May and warned all consumers to power-cycle routers in an attempt to wipe potential infections, and then to apply firmware updates to the devices.

While much of the attack is still being uncovered, the United States Justice Department linked the attack to Fancy Bear (APT 28), which is believed to be directed by Russia's military intelligence agency and is linked to attacks against the German Parliament, Democratic National Convention (DNC), and the International Olympic Committee (IOC).

The attack

Though the initial infection vector is still unknown, researchers have started to analyze the malware payloads to understand the capabilities.

After successfully compromising vulnerable devices, the first stage payload, compiled as a Linux executable, is written to the device. The file modifies the cron table (or crontab, a file that allows for scheduled tasks) of the router to run a job every five minutes. The purpose of this job is to download a list of parameters to be used to extract a second stage payload.

The second stage payload is responsible for installing a backdoor, which allows for the installation of additional software and to configure the communication channels that will be set up in stage three. Decompiled commands from the stage two payload indicate that the malware is capable of the following abilities: download files, restart devices, copy data, execute programs, kill processes, and set proxies and other configuration parameters.

The third and final stage payload is responsible for setting up a Tor client on affected devices for the exfiltration of data back to the attackers. Functionality within this third stage provides sniffing capabilities that look for matching strings that may pass across the network device. This may include usernames and passwords, and credentials for popular websites.

VPNFilter poses a great danger to affected users due to its ability to remain hidden and undetected by modern security solutions. This malware is not only capable of harvesting usernames and passwords, but can also change webpages and insert artificial data to deceive users while, at the same time, draining accounts in the shadows. VPNFilter could also be used to perform DDoS attacks or as a catalyst to install other software like coin miners.

The FBI urges all owners of routers to power-cycle the devices in an attempt to clear malicious code, disable remote management settings, secure the device with a strong, unique, and new password, consider enabling encryption, and to install firmware updates provided from manufacturer websites.

Exploits

CVE ID	Software	Date	Affected versions
CVE-2018-4878	Adobe Flash Player	2/2/2018	28.0.0.137 and earlier
CVE-2018-8174	VBScript engine (Office, IE)	4/18/2018	Windows 7 to 10 & Server 2008 to 2016.
CVE-2018-4990	Adobe Reader	5/15/2018	2018.011.20038, 2017.011.30079, 2015.006.30417
CVE-2018-5002	Adobe Flash Player	6/1/2018	29.0.0.171 and earlier

Figure 25. High profile zero-days in 2018

It has been a few years since we last saw back-to-back zero-days in popular client-side software, such as Adobe Flash Player or Internet Explorer. This is due in large part to the decline in exploit kit activity but also better protections in modern browsers, the two being correlated.

However, 2018 has brought zero-days back to life, with critical flaws identified in popular software. While vendors have been quick to issue fixes, both consumer and business users may not have remembered to or been able to patch promptly; therefore, they remained exposed during the zero-day window and after patches had become available.

The fact that all these exploits were first used in either MS Office or Adobe documents is a sign that the threat landscape has shifted from drive-by attacks to social engineering schemes. Indeed, malicious spam—either targeted or via larger campaigns—is one of their main distribution vectors.

Due to better sandboxing capabilities rolled out in recent years, attackers should be able to exploit a vulnerability in one piece of software and the underlying operating system to completely break out of the sandbox.

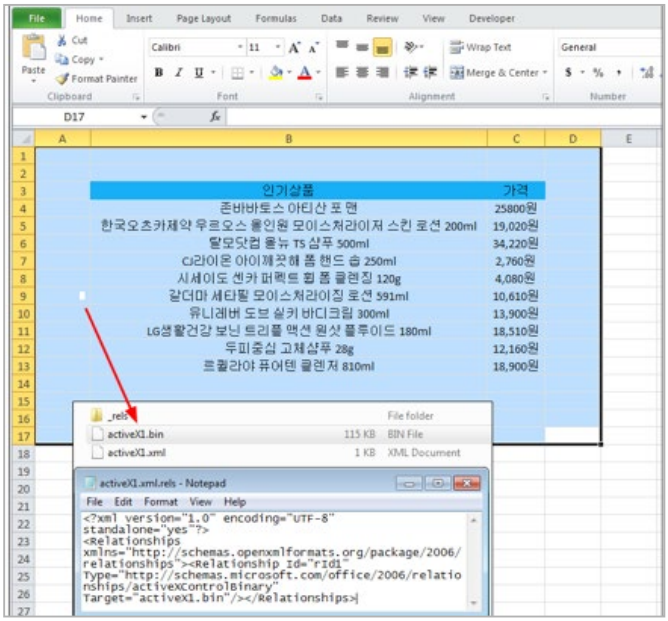


Figure 26. CVE-2018-4878 embedded into an Excel spreadsheet

This was the case with Adobe Reader's zero-day exploit that required a privilege escalation vulnerability in Windows —particularly, CVE-2018-8120—to fully compromise systems.

Exploit kits are being packaged with these high-profile vulnerabilities, often facilitated by the availability of proof of concepts. To date, both the RIG and Magnitude exploit kits have integrated CVE-2018-8174 (Internet Explorer), and CVE-2018-4878 (Adobe Flash).

It is possible that, because of a boost with these new exploits, we have observed a slight increase in drive-by download campaigns that are mostly related to the RIG EK. These are driven by malvertising as well as the presence of traffic distribution systems (TDS), such as BlackTDS.

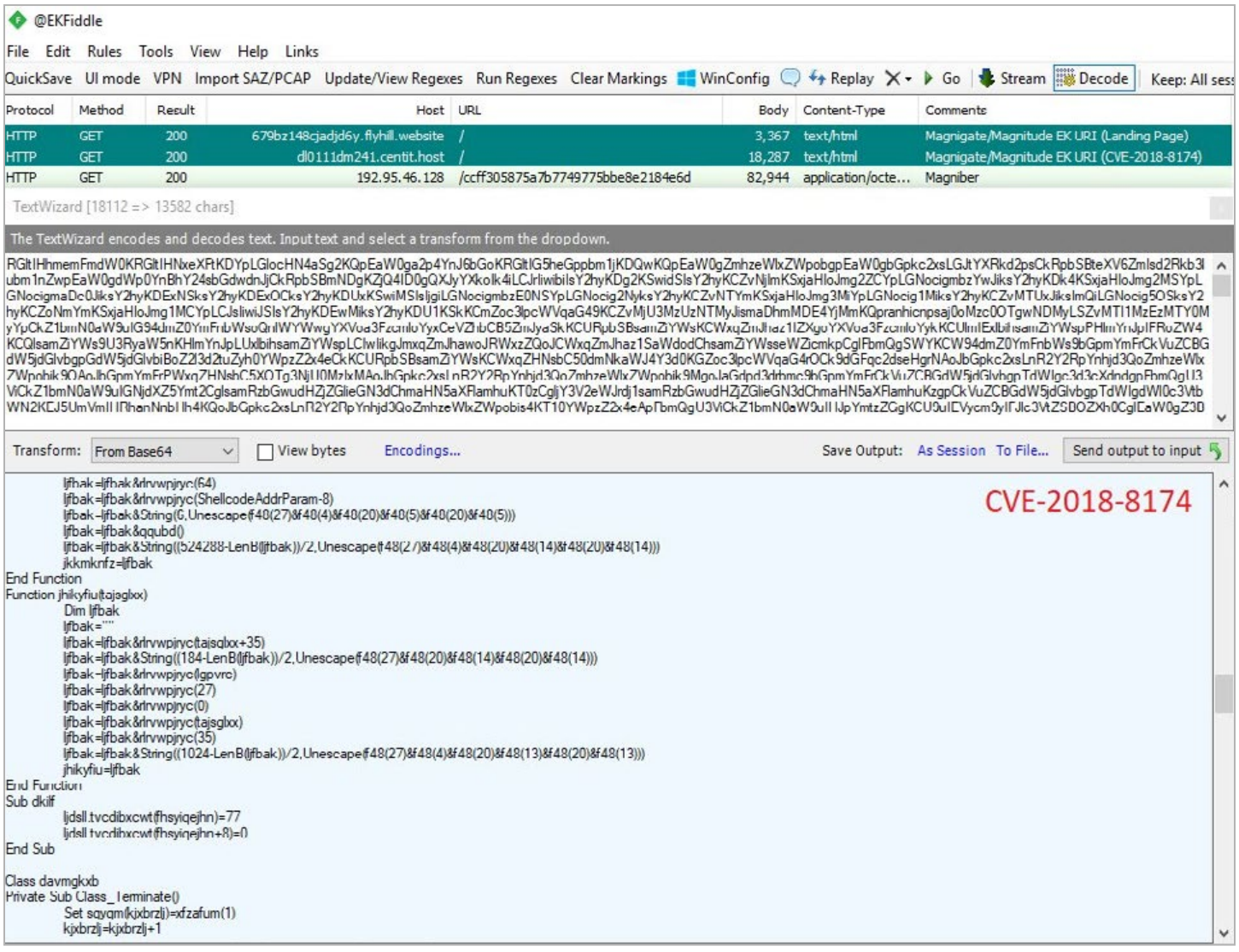


Figure 27. Magnitude EK using CVE-2018-8174

We can expect to see more zero-days through the rest of the year. And while the drive-by vector is weaker than it used to be, threat actors will most likely still rely on social engineering tricks where they can—at least to have victims do some of the work. As more businesses become aware of macros and script-based attacks that they can disable company-wide via group policies, attackers will resort to techniques such as exploits, which cannot be disabled in the same way.

Protocol	Host	URL	Body	Comments
HTTP	[redacted]	/hodxg679/index.php?s=[redacted]	5,187	Fobos Campaign URI
HTTP	95.142.40.194	/?MjcyMjM0&phDGKhWE&GxrLgEuuCH=c3BvcnQ=&TRQ...	141,073	RIG Exploit Kit URI
HTTP	95.142.40.194	/?NDAxMjQ1&mRWeysBstSg&StvdxdCzzPfJT=bW9uZXk...	34,284	RIG Exploit Kit URI (Flash Exploit)
HTTP	95.142.40.194	/?NTk4NzA2&hQmCPhoDNNXGz&fdgfgh2f=xHrQMrLYbRv...	287,744	RIG Exploit Kit URI (Bunitu)
HTTP	youtubeconverter.slyip.net	/WpLTQb?browser[redacted]	0	Slyip Campaign URI
HTTP	95.142.39.202	/?NTg5MDMx&fxfUbAGRKcLYzW&hHDHUhHLTprms=c2hh...	96,058	RIG Exploit Kit URI
HTTP	95.142.39.202	/?NTMwNjYw&gsIKWzadzr&KnlzoMKHBrv=cmVzb3J0&qgZ...	34,522	RIG Exploit Kit URI (Flash Exploit)
HTTP	95.142.39.202	/?NDE3NDYw&VoqbEmjP&fpVhko=c3BvcnQ=&fdfsdf3gf=...	573,952	RIG Exploit Kit URI (Ursnif)
HTTP	haimuoitu.gq	/camps	24,719	ngay Campaign URI
HTTP	188.166.215.114	/	11,296	Seamless Gate HTML/JS
HTTP	46.30.41.179	/?NTM3Njgw&OsieSGwFC&rNVQrzbPKm=cmVzb3J0&rXpRl...	90,380	RIG Exploit Kit URI
HTTP	46.30.41.179	/?NjA2MjY3&LpuuRuGF&WzoDXkL=c3BvcnQ=&ZmOWDGi...	142,974	RIG Exploit Kit URI (SmokeLoader)
HTTP	[redacted]	/[redacted].js	336	BlackTDS Campaign URI
HTTP	[redacted]	/js.php	507	BlackTDS Campaign URI
HTTP	46.30.41.179	/?MTIxNDA4&dpWIWEnisM&yiZEgUaXu=c3BvcnQ=&qbfiL...	90,411	RIG Exploit Kit URI
HTTP	46.30.41.179	/?NzM4OTc=&XSgkmxfKVjp&yMtrccaLrqOmr=Y2F0cw==...	34,334	RIG Exploit Kit URI (Flash Exploit)
HTTP	46.30.41.179	/?MzAwNDM2&HYsDAWCROQdIK&sRnTqUbVPPkVf=c2hh...	257,536	RIG Exploit Kit URI (SmokeLoader)

Figure 28. Four different RIG exploit kit campaigns: Fobos, Slyip, ngay, BlackTDS

Scams

Second quarter trends in scams were marked by an increase in PII theft, coordinated spam attacks using Twitter, and an increase in victim filtering to assure that a scammer is only connecting to the most vulnerable targets.

Social media spam campaigns

Due to uneven enforcement and somewhat vague policies on IP infringement and scams, Twitter is used by scammers to coordinate spam campaigns promoting their fake tech support.

Figure 29. Fake Malwarebytes customer support number on Twitter

In-platform spam like the above is extremely common and covers every conceivable tech product. Offending accounts are typically left to operate untouched for years. But more recently, Malwarebytes has observed a more novel use case where Twitter accounts were used to coordinate spam attacks on other platforms. In theory, the offsite spam is linked by the Twitter account to offer a veneer of legitimacy by referencing a legitimate property rather than the scammer's own infrastructure.

Given that accounts like these generally operate with impunity for long stretches of time, we expect the technique to continue amongst those scammers who have the resources to acquire spam bots.

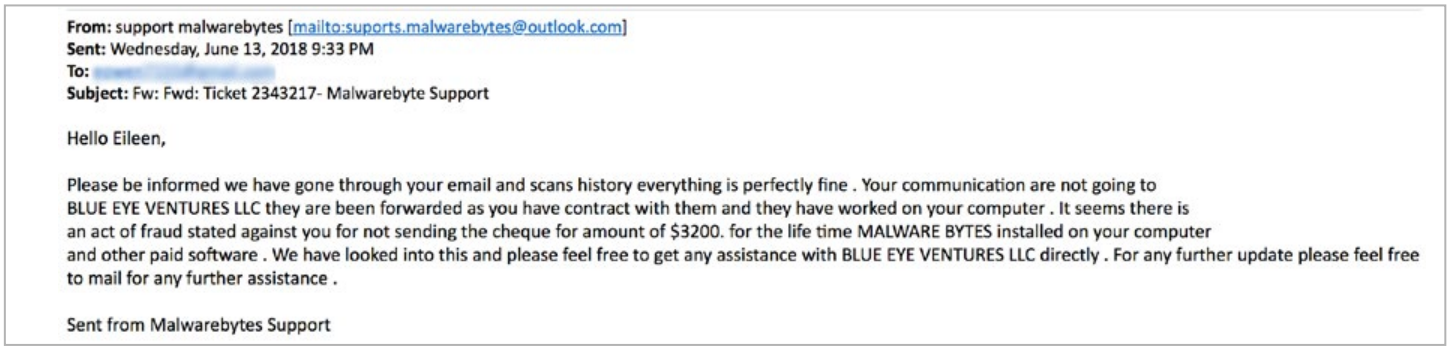
Figure 30. Fake Malwarebytes support account references real forums link

PII theft

We first observed scammers blatantly stealing PII from victims with Bitcoin scams. Light regulation, limited fraud protection, and poor support on exchanges contributed to making social engineering attacks against Bitcoin wallets highly lucrative. But as the victim pool for traditional tech support scams has contracted in the face of user awareness and increased enforcement, scammers have been stealing passwords, bank account information, and email accounts with increasing frequency.

In one instance, a victim allowed the scammer entry into their computer, and the threat actor promptly stole email credentials. The actor had visibility when the victim communicated with the Malwarebytes help desk, and after the victim was informed that they had not been talking to a legitimate company, the scammer promptly set up an email masquerading as Malwarebytes to assure them that all was well.

Limited English skills and professional experience make these types of secondary attacks largely ineffective, but low barriers to entry also make it likely to continue over time.



From: support malwarebytes [mailto:suports.malwarebytes@outlook.com]
Sent: Wednesday, June 13, 2018 9:33 PM
To:
Subject: Fw: Fwd: Ticket 2343217- Malwarebyte Support

Hello Eileen,

Please be informed we have gone through your email and scans history everything is perfectly fine . Your communication are not going to BLUE EYE VENTURES LLC they are been forwarded as you have contract with them and they have worked on your computer . It seems there is an act of fraud stated against you for not sending the cheque for amount of $3200. for the life time MALWARE BYTES installed on your computer and other paid software . We have looked into this and please feel free to get any assistance with BLUE EYE VENTURES LLC directly . For any further update please feel free to mail for any further assistance .

Sent from Malwarebytes Support

Figure 31. Scammer sends spoofed Malwarebytes email

Victim filtering

As phone scamming has risen in awareness with the general public, so has skepticism with potential victims. Scambaiters, time wasters, and general resistance to being scammed costs threat actors money. In response, some tech support scammers have followed the lead of 419 scams and use various methods of filtering for the most vulnerable victims before ever launching a pitch.

Common filter methods we've observed include double calling to route straight to voicemail and requesting a callback, hanging up on victims who aren't entirely convinced, and requiring a small upfront payment before the scam. The intention behind these methods is to preselect victims who are unable or unwilling to exercise skepticism regarding bogus technical claims, thereby maintaining a high-value pool that can be scammed, manipulated, and sold off to the next scammer when no longer profitable. Since skeptical victims frequently make reports to law enforcement and legitimate tech companies, victim filtering for gullibility can also serve as an effective OPSEC measure.

Predictions

Expect big changes next quarter.

We are on the cusp of another significant change in the cybercrime world. Between the second and third quarters of 2017, we started seeing significant changes in distribution, families disappearing, and new technologies being adopted. We expect our Q3 2018 report to be quite different from this one. It's also wise to be alert for whatever new threat that is likely to arise over the next three months.

Cryptocurrency miners will be going out of style.

Cryptominer detections are declining across the board. This is in direct parallel with the interest the public at large has for legitimate cryptocurrency mining. Of course, we are still going to see plenty of miners being distributed and detected. However, it looks like we are at the tail end of the "craze" and moving into a new era of a more stable cryptocoin.

Exploit kits will still be a threat.

With the increase in exploit kit activity in South Korea and multiple new exploits being discovered, we still expect to see more exploit kit activity throughout the rest of the year. However, unless a lot MORE exploits are being released, EKs will still not be a primary method of malware distribution.

Ransomware will ramp up again.

Detections of ransomware against consumers are down, which is great. However, businesses still face an ever-increasing amount of cases where ransomware is used against their systems. Combine that with new evolution of threats like GandCrab, Satan, and SamSam, and we might be seeing the "reboot" of ransomware.

PII will become an even juicier target.

Because of the new policies ushered in by the EU's General Data Protection Regulation (GDPR) in late May, organizations will only have a limited time to hold onto PIIs of their customers, making it more valuable to criminals. This means we may see an uptick in data-stealing threats, from spyware and info stealers to keyloggers and good old-fashioned phishing scams.

VPNFilter malware will spawn copycats.

The creation and distribution of VPNFilter to specific network devices this year has shown the value of investing in this form of cybercrime. Therefore, we expect to see copycats that are going to target widely-used devices as the primary focus for new malware. A new age of IoT malware, long predicted, may finally come to pass.

Conclusion

Once again, we are seeing obvious connections between real-world trends (decreasing cryptocurrency values) and evolutions in the threat landscape in the second quarter of 2018. Malware authors are squeezing the last viable juices out of the cryptomining craze, adding miner payloads to new and old attack vectors, and modifying traditional malware in order to funnel more coin into their cryptowallets. While malicious cryptomining appears to be on the downslide, we don't think it'll ever fully disappear. Instead, it'll take its place in malware authors' arsenal next to other malware categories, biding its time until the next bump in market price heralds another cryptocoin rush.

While overall volume of malware detections dropped in Q2, we're not exactly breathing a sigh of relief. Experimentation with more sophisticated forms of malware, including new ransomware families and router-based threats, shows that cybercriminals are likely getting ready to redirect their energy to other, potentially more dangerous attacks. If and when that happens, Malwarebytes will be ready to protect our customers—on all platforms.

Contributors

Adam Kujawa // Director of Malwarebytes Labs

Wendy Zamora // Head of Content, Malwarebytes Labs (Editor-in-Chief)

Jovi Umawing // Malware Intelligence Analyst (Senior Editor)

Jérôme Segura // Head of Investigations, Malwarebytes Labs

William Tsing // Head of Operations, Malwarebytes Labs

Adam McNeil // Senior Malware Intelligence Analyst

Chris Boyd // Senior Malware Intelligence Analyst

Pieter Arntz // Malware Intelligence Analyst