2019 State of Malware

Provided by

Malwarebytes LABS

Table of contents

Executive summary

2018 came in like a lion and out like—a different lion. It's fair to say that, despite a sleepy second quarter (there's the lamb), this year was action-packed from start to finish. Fresh on the heels of a cryptomining explosion in the last quarter of 2017, 2018 began with threat actors diversifying their cryptomining tactics, broadening their reach to Android, Mac, cryptomining malware, and experimenting with new innovations in browser-based attacks.

While cryptomining died down by the second quarter, a new set of threats were eager to take its place: information stealers. These former banking Trojans—especially Emotet and TrickBot—evolved into droppers with multiple modules for spam production, lateral propagation through networks, data skimmers, and even crypto-wallet stealers. These variants of malware focused their energies on ensnaring businesses, gleaning the most profit from ultra-sensitive data that could be sold on the black market for re-targeting in future campaigns.

Speaking of business victims, other malware families soon followed in Emotet and TrickBot's footsteps, redirecting their focus toward organizations whose networks were unpatched and insecure. And they found plenty of targets. From massive data breaches to ransomware attacks that brought critical infrastructure to a halt, businesses finally experienced what consumers have been dealing with for years now, but on a much larger and more dangerous scale.

As a result, 2018 came to a close with a different set of problems for a different set of users, with the promise that we're likely to see just as much drama in 2019 as the previous year.

Methodology

In contrast to our quarterly Cybercrime Tactics and Techniques reports, which zoom in on metrics gathered over a three-month period, our annual State of Malware report compares January through November 2018 with the same period in 2017. We combine intelligence gathered by our researchers with data collected by honeypots, virtual sandboxes, and our business and consumer product telemetry in order to identify top threats for the year and trends in both volume and distribution.

In addition, our annual report examines threats by region—North America, Asia Pacific, Latin America, and Europe, the Middle East, and Africa (EMEA)—as well as top industry verticals for the most prolific forms of malware.

Without further ado, here's what we learned about the state of malware in 2018.

Top 10 takeaways

Make way for cryptominers

Ransomware was dethroned in the first half of 2018 to make way for a massive wave of cryptominers, following a meteoric spike in Bitcoin value at the tail end of 2017. Threat actors seemingly abandoned all other forms of attack for experimentation in this new technique, spanning from desktop to mobile; Mac, Windows, and Android operating systems; and software- and browser-based attacks. Cryptomining detections increased by seven percent year over year—a small percentage overall, as the second half of the year was slow for this threat.

The year of the mega breach

Unlike the ransomware plagues that were indicative of 2017, there were no major global outbreaks in 2018. Instead, it was the year of the mega breach. Major businesses, including Facebook, Marriott, Exactis, MyHeritage, and Quora were penetrated, with hundreds of millions of customers affected. The number of compromised records increased by 133 percent in 2018 over the previous year.

Ransomware gets tricky

In 2018, we saw a shift in ransomware attack techniques. Instead of the one-two punch of malvertising exploits which delivered ransomware payloads, threat actors engaged in targeted, manual attacks. The shotgun approach was replaced with brute force, as witnessed in the most successful SamSam campaigns of the year.

Businesses take a hit

Malware authors pivoted in the second half of 2018 to target organizations over consumers, recognizing that the bigger payoff was in making victims out of businesses instead of individuals. Overall business detections of malware rose significantly over the last year—79 percent to be exact—and primarily due to the increase in backdoors, miners, spyware, and information stealers.

Consumer detections fall by marginal percentage

Despite the focus on business targets, consumer malware detections only decreased by three percent year over year, thanks to increases in backdoors, Trojans, and spyware malware categories throughout 2018. While 2017 saw 775,327,346 consumer detections overall, 2018 brought with it about 25 million fewer instances of infection—a healthy decrease in number, percentages aside.

SMB vulnerabilities spread Trojans like wildfire

The fallout from the ShadowBrokers' leak of NSA exploits in 2017 continued, as cybercriminals used SMB vulnerabilities EternalBlue and EternalRomance to spread dangerous and sophisticated Trojans, such as Emotet and TrickBot. In fact, information stealers were the top consumer and business threat in 2018, as well as the top regional threat for North America, Latin America, and Europe, the Middle East, and Africa (EMEA).

Malspam replaces exploits as the favorite attack vector

The exploit landscape became a bit barren by the end of 2017, with many of the kit creators locked behind bars. As a result, threat actors returned to an old favorite—malspam—which replaced exploits as the major delivery mechanism for threats in 2018.

Rogue extensions and malicious apps appear in legitimate webstores

Browser-based security became even more important, as rogue apps and extensions fooled users and app stores alike, worming their way past security reviews in Google Play, iTunes, and the official web stores for Chrome, Firefox, Safari, and others with sneaky social engineering tactics.

Attacks on websites steal user data

The criminal group Magecart was behind a series of high-profile attacks on ecommerce websites, stripping credit card information and other Personally Identifiable Information (PII) from payment platforms in plain text and in real time.

Sextortion scams

And finally, major scams for the year capitalized on stale PII from breaches of old. Phishing emails were blasted out to millions of users in extortion (or in some cases, sextortion) attempts, flashing victims' old, but potentially still viable, passwords and warning them that they'd expose their secrets if they didn't pay up.

Top detections of 2018

Consumer detections

In our Q3 2018 Cybercrime Tactics and Techniques report, we noted a decline in the amount of threats facing consumers. Zooming out for the full year, we can see that the total amount of malware detections changed only slightly between 2017 and 2018. Surprisingly enough, the overall difference is only three percent less than the previous year, thanks to some large increases in Trojan, backdoor, and spyware detections.

Consumer detections 2017/2018		
Pos.	**Threat**	**Y/Y% Change**
1	Adware	**-39%**
2	Trojan	**19%**
3	Riskware Tool	**7%**
4	Backdoor	**34%**
5	HackTool	**-36%**
6	Hijacker	**-84%**
7	Worm	**-28%**
8	Spyware	**27%**
9	Ransom	**-29%**
10	Rogue	**-39%**
Overall Detections		
2017	**775,327,346**	**-3%**
2018	**750,296,307**	

Figure 1. Top 10 Malwarebytes consumer detections of 2018

That being said, we observed a decline in many malware types that used to exclusively target consumers. Over the year, we have seen more attacks against businesses, more detections of malware on their endpoints, and a greater focus on what cybercriminals consider a more lucrative target.

Adware dropped significantly, as well as hacktools, hijackers, worms, ransomware, and rogue malware. This decline is likely because these types of malware are often detected together, as they make similar system modifications to affected machines. For example, many adware system modifications are identified and fixed by our hijacker detection tool—and hijacker detections decreased by 84 percent.

We also saw an increase in detections of Trojans, RiskwareTools (our detection name for cryptomining), backdoors, and spyware in 2018, some by a significant amount. Backdoor.Vools, for example, our current top backdoor detection, has been seen all over the world this year, yet it was non-existent the year before. The increase in backdoor, spyware, and Trojan detections can be attributed to the current trend of exploiting vulnerabilities—EternalBlue, for example—to inject malware that can establish a foothold on a network.

On the other hand, the slight overall increase in RiskwareTool detections came from a massive influx of cryptomining malware at the beginning of the year, which trailed off by mid-2018.

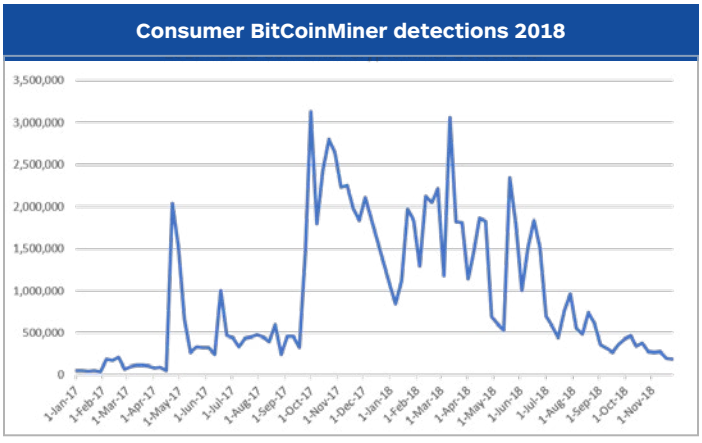

Figure 2. Consumer detections of RiskWare.BitCoinMiner in 2018

RiskWare.BitCoinMiner, our most popular miner detection, declined steadily throughout the 2018. By July, we saw a similar number of detections as what we witnessed in early 2017. However, we did note a slight spike in detections starting in mid-September.

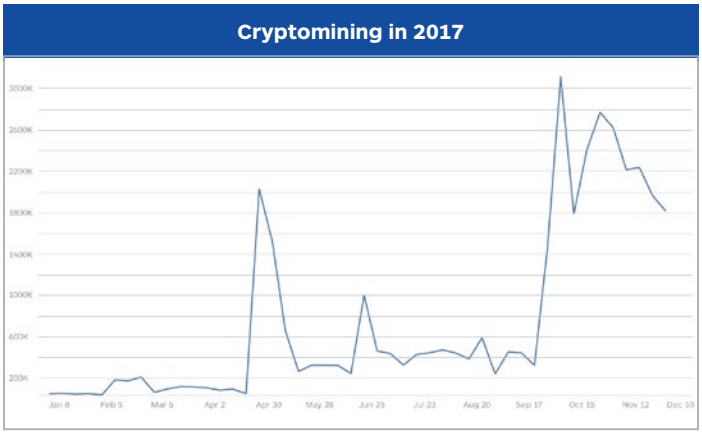

Figure 3. Cryptomining spike in fall 2017

This spike precedes the rise of Bitcoin value that took place in October 2017 by about a month. Perhaps the criminals behind these cryptomining knew something the rest of us didn't.

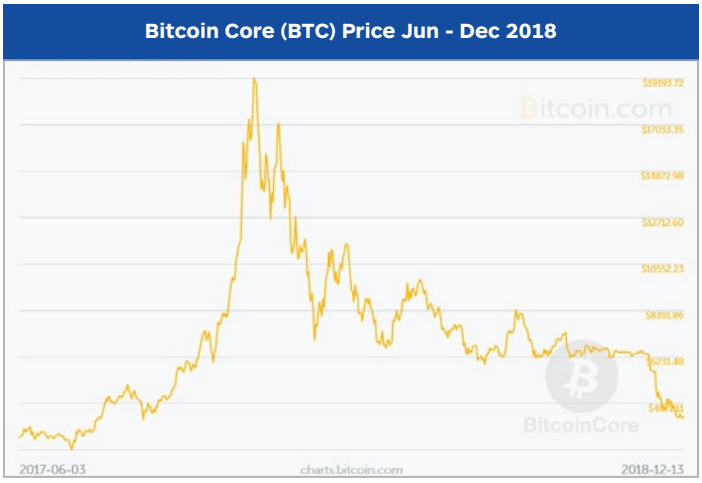

Figure 4. Spike in Bitcoin value in October 2017 Photo credit: Bitcoin 2018

A large-scale flood of cryptocurrency miners was deployed between October 2017 and March 2018. During this time, malware affecting consumers was also on the uptick. However, the cryptocurrency fever eventually broke months after, which led to a decline of criminal interest in consumers.

The majority of the threats we see in the wild today use tactics and techniques that we've mostly seen with state-sponsored malware in the past.

This means that larger targets—networks with multiple endpoints—will be disrupted far more. Unless we observe new evolutions of consumer-facing malware that specifically exploit weaknesses in the individual, then the shift in focus to businesses may move beyond a passing trend.

Business detections

With the overall detection count for consumer endpoints down by three percent year over year, one might assume that overall malware production is also down. However, this trend instead demonstrates the shift in focus by cybercriminals away from the average Joe and instead on juicier targets, such as businesses. In fact, four of our top seven business detections increased by more than 100 percent from 2017 to 2018.

Business Detections 2017/2018		
Pos.	**Threat**	**Y/Y% Change**
1	Trojan	**132%**
2	Hijacker	**43%**
3	Riskware Tool	**126%**
4	Backdoor	**173%**
5	Adware	**1%**
6	Spyware	**142%**
7	Ransom	**9%**
8	Worm	**-9%**
9	Rogue	**-52%**
10	HackTool	**-45%**
Overall Detections		
2017	**39,970,812**	**79%**
2018	**71,823,114**	

Figure 5. Top 10 Malwarebytes business detections in 2018

Overall business detections of malware rose significantly over the last year—79 percent to be exact—and primarily due to the increase in backdoors, miners, spyware, and information stealers. The "cryptocraze" wasn't only on the consumer side, as we've observed plenty of malicious cryptominers forcing their way onto corporate networks.

Our Trojan detections were topped by the Emotet family, which can move laterally throughout corporate networks using exploits and credential brute forcing. This same functionality is mirrored in other information stealing malware, such as TrickBot, but also in backdoor malware, such as Vools, our top detection among backdoor infections in 2018. Vools uses the same exploits mentioned to infect and expand on endpoints.

Ransom detections in the business world have increased only slightly this year, by nine percent, much of which is from ongoing, yet dormant WannaCry infections being flagged in our system. While we have seen advancements by ransomware families like GandCrab and SamSam, we did not see the kind of problematic outbreaks that were witnessed in 2017.

Finally, spyware detections have climbed significantly due to similar variants and families of Emotet and TrickBot being identified as spyware in the wild—a clear sign of the focus threat actors have placed on information stealing and establishing holds on corporate networks.

Regional threats

Not all malware attacks focus on a particular part of the world. In fact, many families end up spreading to numerous countries because attacks are opportunistic, and the Internet has no borders (except in China and North Korea.) However, there are campaigns that push malware to different countries and regions in the hopes that their culture, economy, or political climate would make them more likely victims.

While cybercrime is an international problem, and we like to analyze trends and events on a global scale, it's important to dig into what is happening in specific regions to understand patterns of attack, as well as what pain points customers in those regions experience. Here's what we found for the regions of North America, Asia Pacific (APAC), Europe, the Middle East, and Africa (EMEA), and Latin America (LATAM).

North America

Top North America Detections 2017/2018				
Business		Pos.	Consumer	
Y/Y	Threat		Threat	Y/Y
99%	Trojan	1	Adware	-19%
33%	Hijacker	2	Trojan	7%
121%	RiskwareTool	3	RiskwareTool	38%
29%	Adware	4	Backdoor	10%
82%	Spyware	5	Hijacker	-41%
11%	Backdoor	6	Spyware	18%
-27%	Worm	7	HackTool	-40%
-15%	Ransom	8	Rogue	-35%
-55%	Rogue	9	Rootkit	-50%
-64%	Rootkit	10	Virus	-57%

Figure 6. Top North American business and consumer detections

North America mainly dealt with an influx of business-focused, information stealing malware and cryptocurrency miners infecting businesses at higher rates than we have seen previously. On the consumer side, we saw a drop in the majority of top consumer detection categories, with the exception of cryptocurrency miners.

Asia Pacific (APAC)

Top APAC Detections 2017/2018				
Business		Pos.	Consumer	
Y/Y	Threat		Threat	Y/Y
5137%	Backdoor	1	Trojan	88%
261%	Trojan	2	Backdoor	591%
-48%	Adware	3	Adware	-36%
170%	RiskwareTool	4	RiskwareTool	-18%
148%	Ransom	5	Ransom	79%
305%	Worm	6	Worm	-26%
50%	Hijacker	7	HackTool	-25%
3690%	Exploit	8	Exploit	740%
-7%	HackTool	9	Spyware	16%
9%	Spyware	10	Hijacker	-48%

Figure 7. Top APAC detections, consumer and business

The Asia Pacific region of the world saw massive increases in backdoor malware and the use of exploits against their endpoints. Considering the primary backdoor threat in 2018 was Vools, a malware family that uses exploits to spread, seeing an increase in both threat types makes sense. However, the reason why APAC has been targeted far more than other regions is still not clear.

On the consumer side, we saw the same spikes in backdoor and exploit detections, with a drop in most other types of malware seen earlier in the year.

Europe, the Middle East, and Africa (EMEA)

Top EMEA Detections 2017/2018				
Business		Pos.	Consumer	
Y/Y	Threat		Threat	Y/Y
150%	Trojan	1	Adware	-40%
122%	Hijacker	2	Trojan	-15%
-59%	Adware	3	RiskwareTool	-23%
20%	RiskwareTool	4	HackTool	-41%
-6%	Backdoor	5	Backdoor	-15%
-41%	HackTool	6	Worm	-5%
-1%	Spyware	7	Spyware	25%
-14%	Ransom	8	Hijacker	-57%
-37%	Worm	9	Ransom	-53%
-56%	Rogue	10	Rogue	-62%

Figure 8. Top EMEA business & consumer detections

Europe, the Middle East, and Africa (EMEA) grappled with many of the same issues as North America. In fact, of the 150 percent increase in Trojan activity for businesses in EMEA, we know that the majority was Emotet (just as it was in North America). Due to the intense focus cybercriminals are now giving to certain families of malware, we see a drop in nearly all other types of threats.

Despite interesting spikes of Trojan and hijacker detections for EMEA consumers, we've otherwise observed a significant drop in nearly every type of malware, except for spyware. This is another sign that the focus of cybercriminals is moving away from consumers and taking aim at businesses.

Latin America (LATAM)

Top LATAM Detections 2017/2018				
Business		Pos.	Consumer	
Y/Y	Threat		Threat	Y/Y
176%	Trojan	1	Adware	-55%
137%	RiskwareTool	2	Trojan	-1%
-56%	Adware	3	RiskwareTool	-25%
137%	Ransom	4	HackTool	-32%
23%	Backdoor	5	Backdoor	-33%
343%	Spyware	6	Worm	-16%
101%	Worm	7	CrackTool	-35%
-47%	HackTool	8	Spyware	43%
-60%	Hijacker	9	Ransom	59%
473%	Rootkit	10	FraudTool	-97%

Figure 9. Top LATAM detections

Latin America had a fascinating year in malware development. The criminals who target this region have dropped everything to increase all types of malware on the business side, from Trojans to miners, spyware, and even rootkits. Organizations that operate out of LATAM might want to beef up their security quickly, as the next year could result in an even greater increase.

While malware distribution has been churning on the business side, it's not the same case for consumers, where the only increases in threat detections we've observed are from spyware and ransomware. Keep in mind, however, that many ransomware detections this year have been from WannaCry gone wild, identifying vulnerable systems and infecting them, but refraining from encrypting files. Instead, the infections are merely hopping from system to system, with no apparent fallout associated. Therefore, we detect large amounts of WannaCry in areas where patching against this threat hasn't been paramount.

Threats by country

Top 10 countries with most consumer detections		
	Country	**Biggest threat**
1	United States	Information theft
2	Brazil	Click fraud
3	United Kingdom	Adware
4	Vietnam	Backdoors
5	India	Backdoors
6	Indonesia	Backdoors
7	France	Adware
8	Italy	Cryptomining
9	Thailand	Backdoors
10	Russia	Backdoors

Figure 10. Top 10 countries with the most consumer detections, plus their biggest threats

Top 10 countries with most business detections		
	Country	**Biggest threat**
1	United States	Information theft
2	Indonesia	Backdoors
3	United Kingdom	Information theft
4	France	Information theft
5	Malaysia	Backdoors
6	Thailand	Backdoors
7	Australia	Cryptomining
8	Germany	Information theft
9	Brazil	Adware
10	Philippines	Information theft

Figure 11. Top 10 countries with the most business detections, plus their biggest threats

The United States came out as the country with the most consumer malware detections, with Emotet as its biggest problem this year. This should not be a surprise, since most malware targets Western countries for their strong economies, most especially the US.

Brazil had its fair share of dealings with click fraud malware in 2018, a similar issue to the previous year. The United Kingdom and France were targeted with adware more so than other categories of malware. Note that adware's capabilities should no longer be questioned, as they're capable of modifying system settings and disabling security software to install malware.

The biggest consumer threat facing many of these countries falls under the category of backdoor, a type of malware that finds its way into the system, then leaves a door open for future attackers to get back in. Vietnam, India, Indonesia, Thailand, and Russia—almost all APAC countries—have a serious issue with backdoor malware, likely due to a greater need to patch and secure endpoints.

Our top 10 countries for business detections shows a significant problem for much of the world with information-stealing malware. This malware category infects an endpoint, drops additional malware, and moves laterally through the network, infecting every connected computing device it can. From there, the malware can steal credentials, install additional threats, and spread itself further via email.

Western countries, such as the US, UK, France, and Germany, seem to have taken the brunt of the information-stealing attacks, although many other countries have also been hit. Meanwhile, in the East, countries such as Indonesia, Malaysia, and Thailand have been fending off an influx of backdoor malware in their business networks.

Countries such as Australia and Brazil, whose main threats in 2018 were adware and cryptomining, have plenty of reason to be concerned, as many miners and adware families drop additional malware, modify system settings, slow down or use up computing power, or otherwise disrupt operations.

Threats by vertical

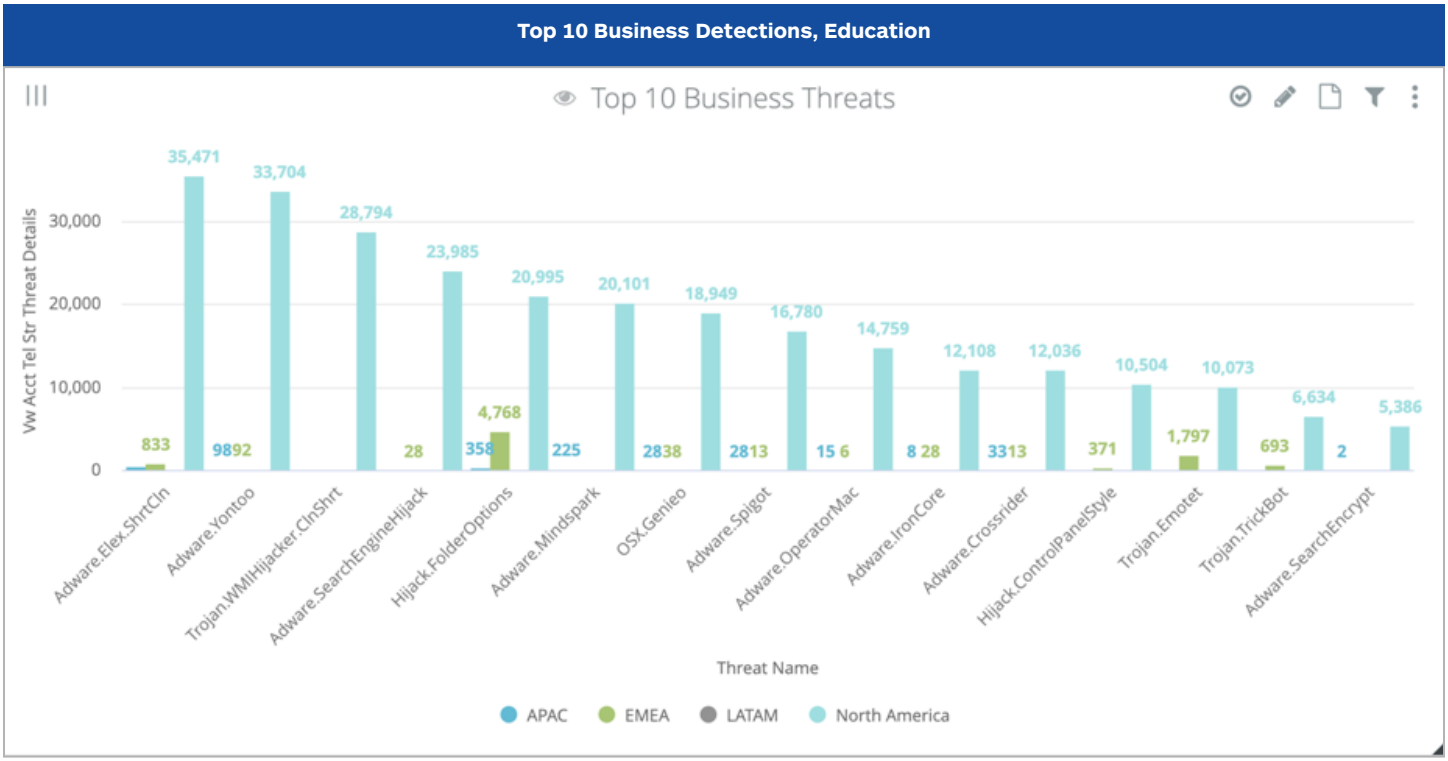

Figure 12. Top 10 business detections for education industry, 2018

Education, manufacturing, and retail were the top industries impacted by the top malware of the year—Trojans. However, when we zoom in on the Trojan category to look at its top family, Emotet, the industries shift. Consulting shoots to the top of the list and hospitality makes an appearance in fourth place.

In addition, ransomware had a few other industries in mind for targeting. Consulting was once again a top target for malware authors, with education coming in a strong second. Manufacturing, retail, and government rounded out the top five.

But what about if we turn the tables and filter our business product telemetry to look at the industry first? For example, education, which makes an appearance in nearly all of our threat categories, was hit hardest with adware in 2018.

Note that two Mac malware families—detected as OSX.Genieo and Adware.OperatorMac—made the list, demonstrating both the popularity of Macs in education and as vertical targets.

Meanwhile, consulting, which took the top spot for both the ransomware category and the Emotet family of Trojans, saw several others in the Trojan category, including bankers, downloaders, and packers. Backdoors, hijackers, and worms also set their sights on consultants in 2018.

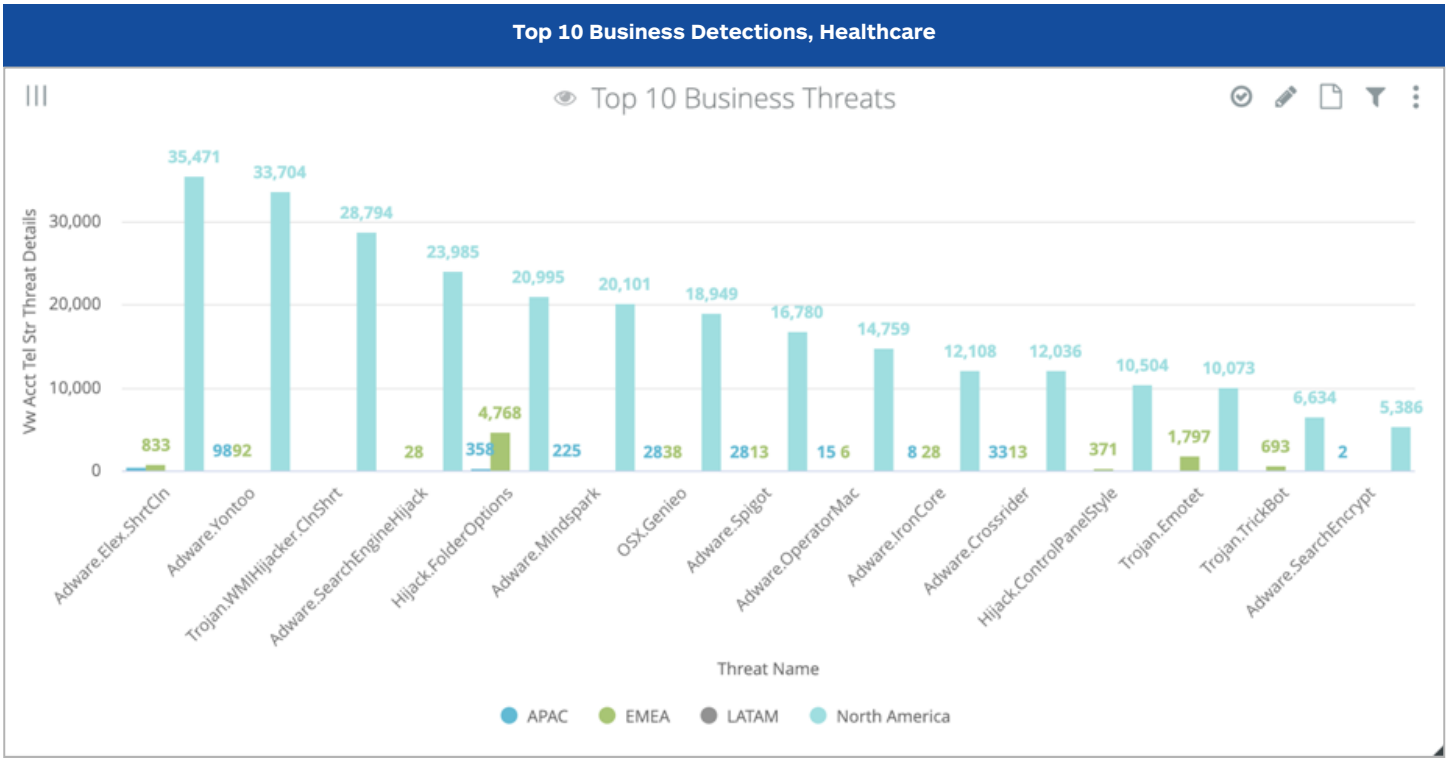

Figure 13. Top 10 threats aimed at the healthcare industry

Despite the many major stories throughout 2018 dealing with healthcare and government attacks, they remained fairly lowkey as vertical targets, sometimes not even making the top 10 industries for the most popular threats of the year. However, looking at healthcare, it's clear which forms of malware found this industry most appealing: Emotet and TrickBot, our new Bonnie and Clyde. Hijackers, rootkits, and riskware also rounded out the top healthcare threats.

Government threats were similar to those pointing toward healthcare, though hijackers took the top spot over Emotet, which came in second. In addition, more adware variants made the list, while TrickBot was not invited to the government party.

Noteworthy malware

While categories such as adware and backdoors maintained a healthy presence, it was truly Trojans (information stealers) and cryptominers who were the all-stars of the year, with ransomware making quiet, yet impactful changes in the background. Let's take a closer look at these threats and how they affected consumers and businesses in 2018.

Cryptominers

Our number one security prediction for 2018 was that the cryptomining "gold rush" would be the top priority for cybercriminals. Indeed, in riding the cryptocurrencies valuation wave, we saw a number of threat actors distributing coin miners in their classic malware binary form, as well as via drive-by mining.

Mining on infected devices

Online criminals dropped a variety of cryptominers—sometimes even loading several on the same victim—via exploit kits, including RIG. Unlike other threats, such as ransomware, this type of malware wants to remain undetected. But the need for CPU cycles is often the first telltale sign that something is going on, with machines becoming slow and their cooling fans continuing to hum.

Drive-by mining: no infection required

On the browser side, drive-by mining quickly became our most detected web threat, completely eclipsing exploit kits. Thanks to vulnerabilities in content management systems, in particular the infamous Drupalgeddon campaigns, criminals were busy injecting websites with cryptojacking scripts in Q1 and Q2.

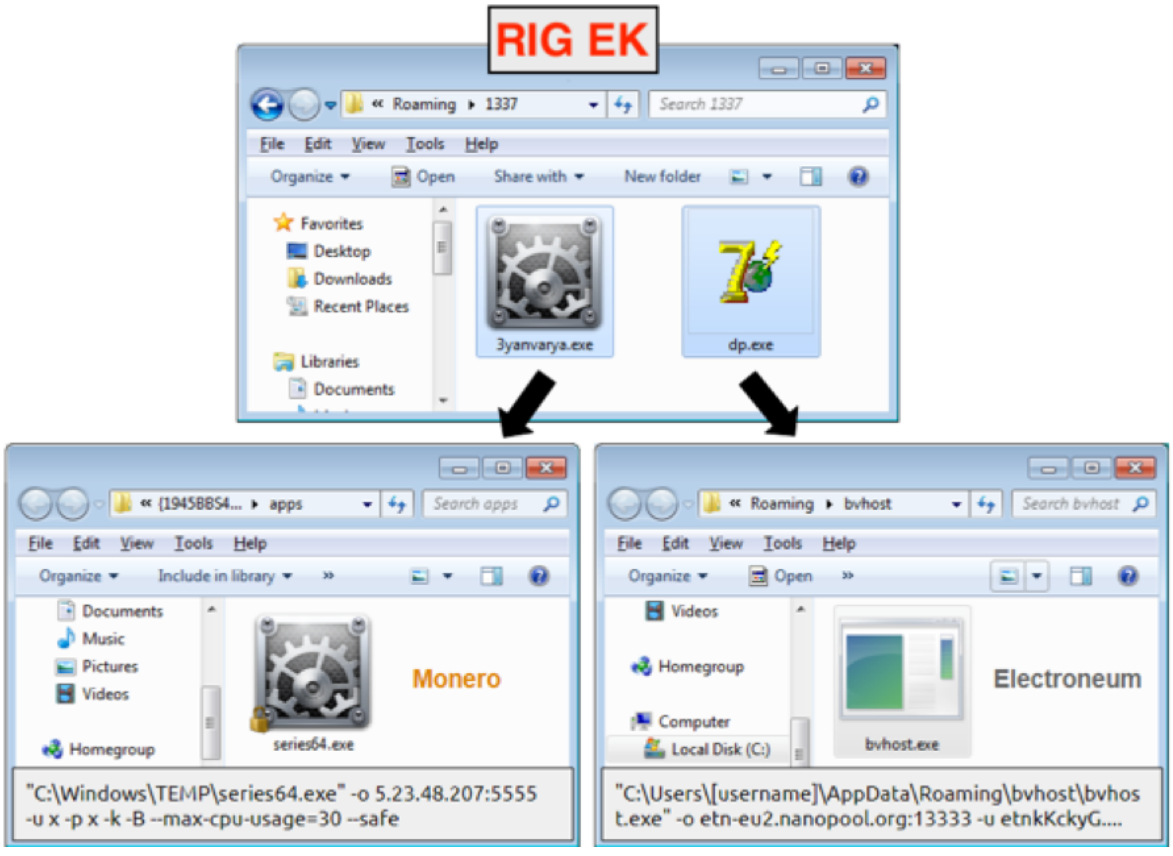

Figure 14. RIG EK dropping Monero and Electroneum miners

#	Server IP	Protocol	Host	URL	Body	Comments
882	223.165.64.100	HTTP	www.nzsap.org	/misc/jquery.once.js?v=1.2	3,641	Drupal Drive-by Mining HTML/JS
883	13.228.219.59	HTTPS	www.odysseypremier.com	/misc/jquery.once.js?v=1.2	3,670	Drupal Drive-by Mining HTML/JS
884	118.143.50.216	HTTPS	www.orbusneich.com	/misc/jquery.once.js?v=1.2	3,670	Drupal Drive-by Mining HTML/JS
885	136.243.4.40	HTTP	www.pixshock.net	/misc/jquery.once.js?v=1.2	3,641	Drupal Drive-by Mining HTML/JS
886	52.64.6.39	HTTP	www.progility.com.au	/misc/jquery.once.js?v=1.2	3,641	Drupal Drive-by Mining HTML/JS
887	143.106.32.80	HTTPS	www.prp.unicamp.br	/misc/jquery.once.js?v=1.2	3,670	Drupal Drive-by Mining HTML/JS
888	35.200.201.129	HTTPS	www.questin.co	/sites/default/files/advag...	365,227	Drupal Drive-by Mining HTML/JS
889	80.241.209.95	HTTPS	www.radiodogo.com	/misc/jquery.once.js?v=1.2	3,641	Drupal Drive-by Mining HTML/JS
890	139.162.23.226	HTTP	www.sankalpindia.net	/sites/default/files/js/js_0...	23,757	Drupal Drive-by Mining HTML/JS
891	217.218.243.197	HTTP	www.semnaniau.ac.ir	/misc/jquery.once.js?v=1.2	3,641	Drupal Drive-by Mining HTML/JS
892	81.246.25.226	HTTPS	www.sesvanderhave.com	/RU/misc/jquery.once.js?...	3,670	Drupal Drive-by Mining HTML/JS
893	173.44.46.188	HTTPS	www.sicrediuniaomsto.coop.br	/sites/default/files/js/js_-...	96,973	Drupal Drive-by Mining HTML/JS
894	202.146.214.234	HTTPS	www.silver-sewing-sisters.com.au	/misc/jquery.once.js?v=1.2	3,670	Drupal Drive-by Mining HTML/JS
895	162.144.65.226	HTTP	www.snellrealestate.com	/misc/jquery.once.js?v=1.2	3,641	Drupal Drive-by Mining HTML/JS
896	91.194.60.51	HTTP	www.spil.org	/misc/jquery.once.js?v=1.2	3,641	Drupal Drive-by Mining HTML/JS
897	104.200.18.26	HTTP	www.thebigwiki.com	/sites/default/files/js/js_...	98,825	Drupal Drive-by Mining HTML/JS
898	205.186.132.167	HTTPS	www.thenationalpastimemuseum.com	/misc/jquery.once.js?v=1.2	3,670	Drupal Drive-by Mining HTML/JS
899	104.199.98.224	HTTPS	www.thense.co.uk	/misc/jquery.once.js?v=1.2	3,670	Drupal Drive-by Mining HTML/JS
900	151.80.115.77	HTTPS	www.tmtg.org.uk	/misc/jquery.once.js?v=1.2	3,641	Drupal Drive-by Mining HTML/JS
901	184.168.231.182	HTTPS	www.umbiesoft.com	/misc/jquery.once.js?v=1.2	3,670	Drupal Drive-by Mining HTML/JS
902	83.169.6.193	HTTP	www.welayetnews.com	/misc/jquery.once.js?v=1.2	3,641	Drupal Drive-by Mining HTML/JS
903	76.72.163.154	HTTPS	www.wood-mode.com	/misc/jquery.once.js?v=1.2	3,670	Drupal Drive-by Mining HTML/JS
904	23.196.199.47	HTTPS	www.wowengage.com.au	/misc/jquery.once.js?v=1.2	3,670	Drupal Drive-by Mining HTML/JS
905	34.232.250.21	HTTPS	www.xplor.ai	/misc/jquery.once.js?v=1.2	3,641	Drupal Drive-by Mining HTML/JS
906	46.243.119.189	HTTP	www10.pmu.ro	/misc/jquery.once.js?v=1.2	3,641	Drupal Drive-by Mining HTML/JS
907	216.187.97.215	HTTP	www3.zipangcasino.com	/misc/jquery.once.js?v=1.2	3,641	Drupal Drive-by Mining HTML/JS
908	41.87.228.50	HTTP	zainbspectramedwhl01.spectramed.co.za	/misc/jquery.once.js?v=1.2	3,641	Drupal Drive-by Mining HTML/JS

Figure 15. Thousands of Drupal websites injected with cryptomining scripts

Mining is cross-platform

Other platforms such as Android or macOS haven't been immune to cryptomining. In February, we blogged about a cryptominer for the Mac that, upon further review, showed it already had 23 variants. Just a few months later, we reported on yet another miner using a malicious implementation of the XMRig program.

Our latest discovery was OSX.DarthMiner, which was installed alongside the EmPyre backdoor and came via a booby-trapped application, as is often the case with Mac malware.

Decline in mining: Is it over already?

According to our telemetry, Q3 and Q4 have started to confirm a downward trend with cryptominers. The craze generated by the high valuation of Bitcoin seems to have somewhat dissipated, and profits from mining, especially for web-based miners, are disappointingly lower than expected, according to various studies.

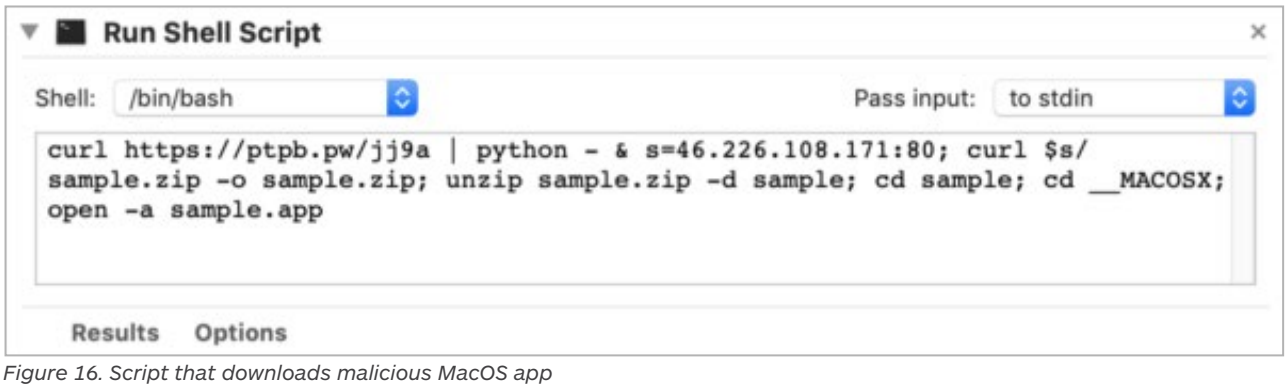

Figure 16. Script that downloads malicious MacOS app

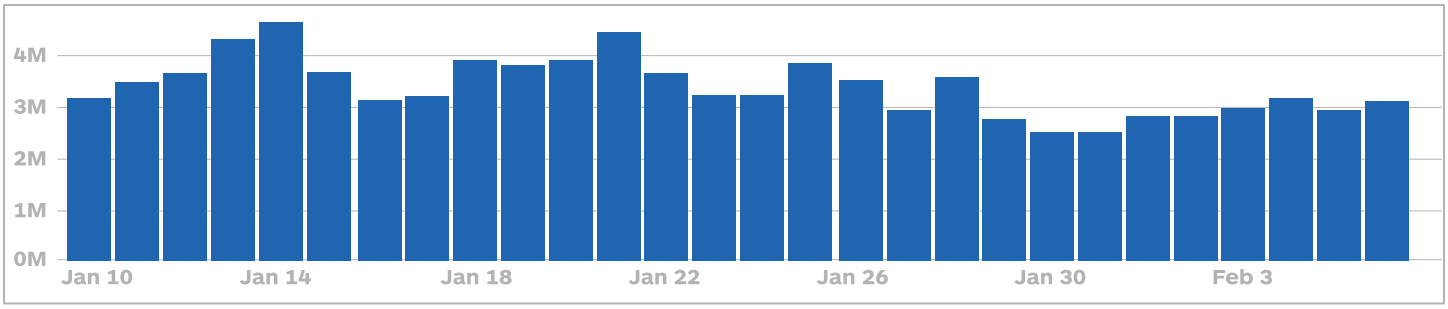

Figure 17. Coinhive detections from January–February 2018 show an average of 3 million daily hits

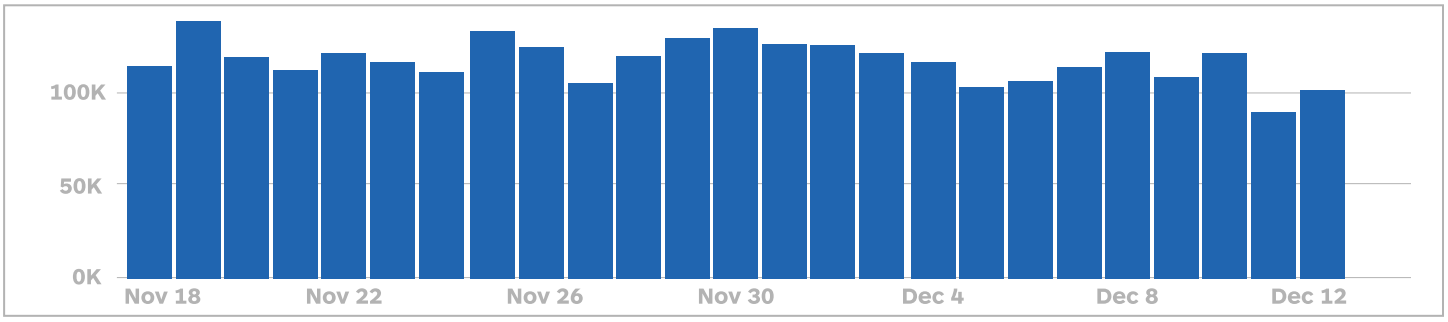

Figure 18. Coinhive detections November–December 2018 show an average of 100,000 daily hits

Despite this drop in activity from Coinhive, other services also focusing on Monero show signs that browser-based mining isn't completely over. CoinIMP in particular has gained popularity in recent months.

Overall, it seems as though criminals have reached the consensus that sometimes stealing is better than mining. In fact, a number of malware families, such as TrickBot, have added the capability to rob cryptocurrency wallets directly. In the same vein, there is also great interest from attackers to exploit vulnerabilities in the JSON-RPC protocol implementation of many cryptocurrencies.

In those cases, the simple act of browsing a malicious website could result in your wallet being emptied.

Despite a drop in their value, cryptocurrencies remain attractive to online criminals. A such, 2018 has seen large campaigns of miners distributed via many platforms with considerable success. But cryptojacking may have already had its heyday in the fall of 2017 and the first few months of 2018, especially for its in-browser model. Indeed, there are other types of payloads that are far more lucrative—as we have seen with the recent wave of web skimming attacks.

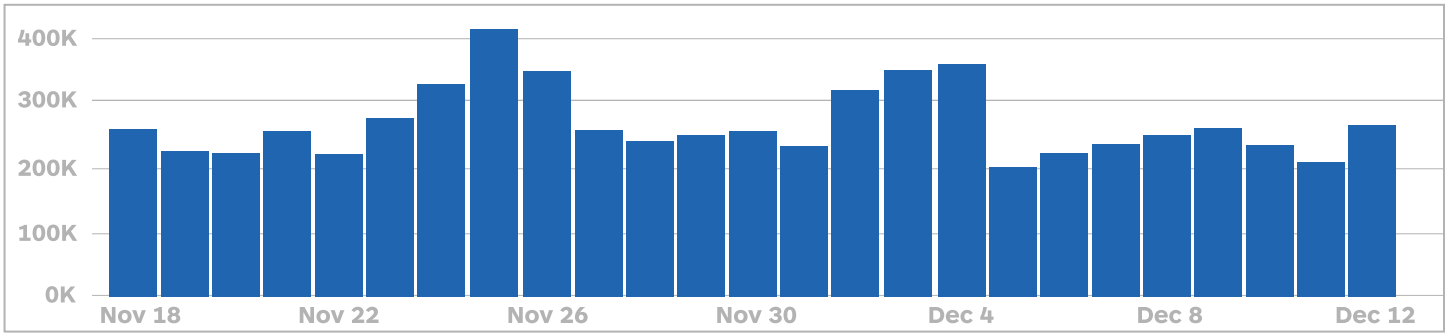

Figure 19. CoinIMP detections November–December 2018

Trojans

The term "Trojan" is broad, applying to a wide variety of malware with different targets, goals, and behaviors. While Trojan became synonymous with the legend of the Trojan horse to those in cybersecurity, specifically, it speaks to the malware's ability to sneak in undetected under the guise of a friendly gesture—how a piece of code can hide within another piece of code to get past security measures.

When the term "Trojan" was first used to describe a type of malware, there weren't many other threats that employed the same tactics for infection. Today, however, almost all malware has some kind of "Trojan" functionality, as hiding from security software is one of the pillars of modern cyberwarfare. In addition, Trojan is a useful term when referring to malware families that do not fall directly into spyware or adware or backdoor categories, but rather multiple buckets.

The Emotet family, for example, started as a run-of-the-mill banking Trojan. After infection, it looked for instances where users logged into their bank accounts or provided financial details on a website, stole that data, and then sent it back to the command-and-control (C&C) server.

As time passed, Emotet evolved in interesting ways: It is now able to use exploits to infect systems, spread additional malware, and even send emails to contacts. These capabilities, individually, would put Emotet in multiple malware categories, such as worm, spyware, backdoor, and downloader. Combined, they are a Trojan.

In this section, we are going to examine how much of a global problem Trojans have been this year compared to last year, and the trends of the biggest Trojan families we are tracking.

Business-facing Trojans

Trojan malware was less often observed on corporate endpoints in 2017, making the influx of information-stealing Trojans primarily a 2018 problem. Figure 20 expresses the low detection numbers of Trojan malware through Q1 to Q3 2017, which then spiked in September and kicked off a new base level of Trojans being detected by our corporate customers.

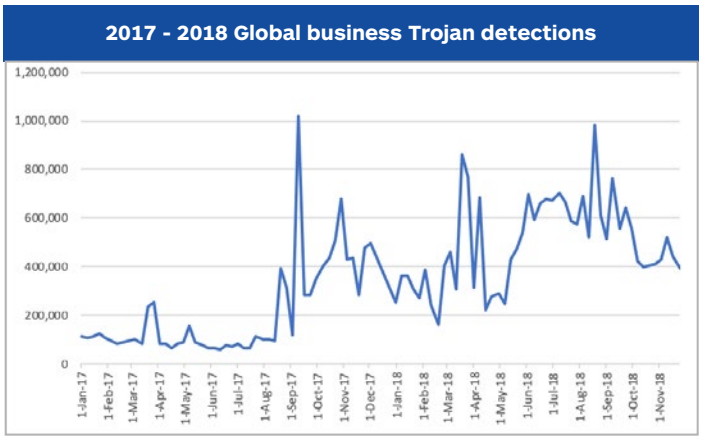

Figure 20. Global Trojan detections for businesses

Information-stealing malware is the primary cause of the number of Trojan detections observed in 2018. Possible reasons range from the fallout from policies, such as the Global Data Protection Regulation (GDPR) to the use of exploits, such as EternalBlue, and backdoors, such as DoublePulsar.

The trend in information-stealing Trojans being leveraged for business breaches does not appear to be slowing down. However, the deployment of patches, network and data segmentation, as well as user rights management configuration might keep the Trojan invasion from spreading so easily.

Consumer-facing Trojans

While Trojans have been doing a number on businesses, they've remained fairly steady on the consumer side, chugging along with only slight variation between 2017 and 2018.

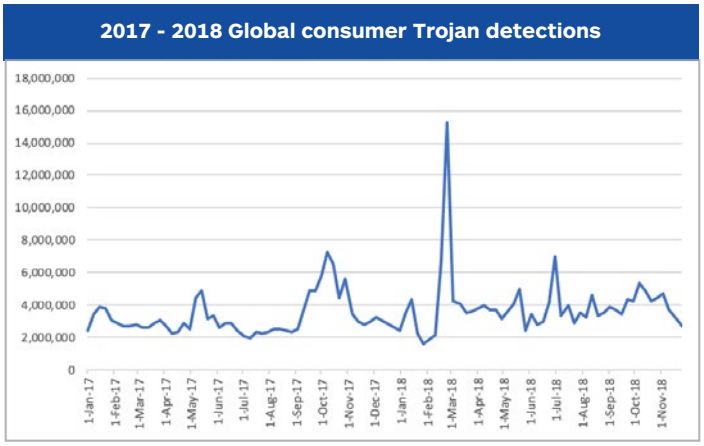

Figure 21. Global Trojan detections for consumers

The total detection variation between 2017 and 2018 was about 30 million, with 2018 coming in at 190 million Trojan detections, and 2017 registering 160 million. The majority of what we've seen has been either information stealers, malicious miners, or generic detections.

We don't expect to see meaningful change in this trend on an annual scale in 2019, however, quarterly evaluation will likely reveal interesting variations among Trojan families.

Information stealers

Two of the biggest Trojan type threats of this year were Emotet and TrickBot, information-stealing malware that enjoys infecting and spreading, then infecting again. We've covered both of these families extensively on our blog and in other reports released this year. Let's now take a look at overall detection trends for the year.

Emotet

This information-stealing spammer was a huge menace in 2018, as it's one of the breakout families to infect on a large scale, both on the business and consumer sides.

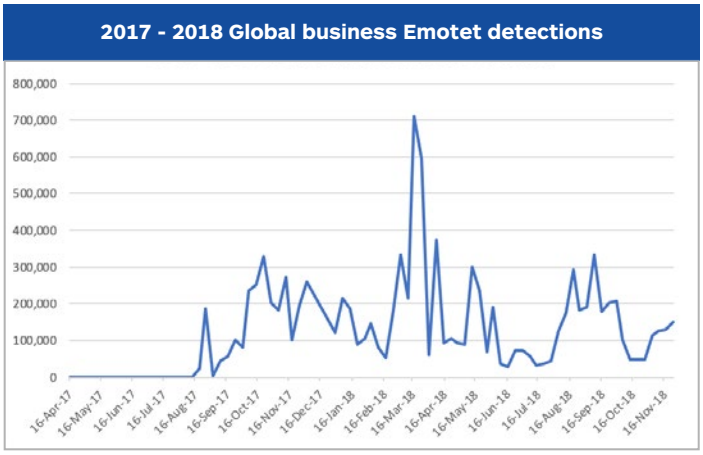

Figure 22. Emotet business detections, April 2017–November 2018

Emotet business detections are similar to detections on the consumer side; however, they are smaller in scale. Note how the detection spikes for consumer and business Emotet infections are parallel in Figure 23.

Now, observe the shape and size of the business and consumer detections line of Q3 2018—it looks like a dog's head. The difference between the two shapes is about 78,000 detections, while the first two shapes were roughly 475,000 greater on the consumer side than the business side.

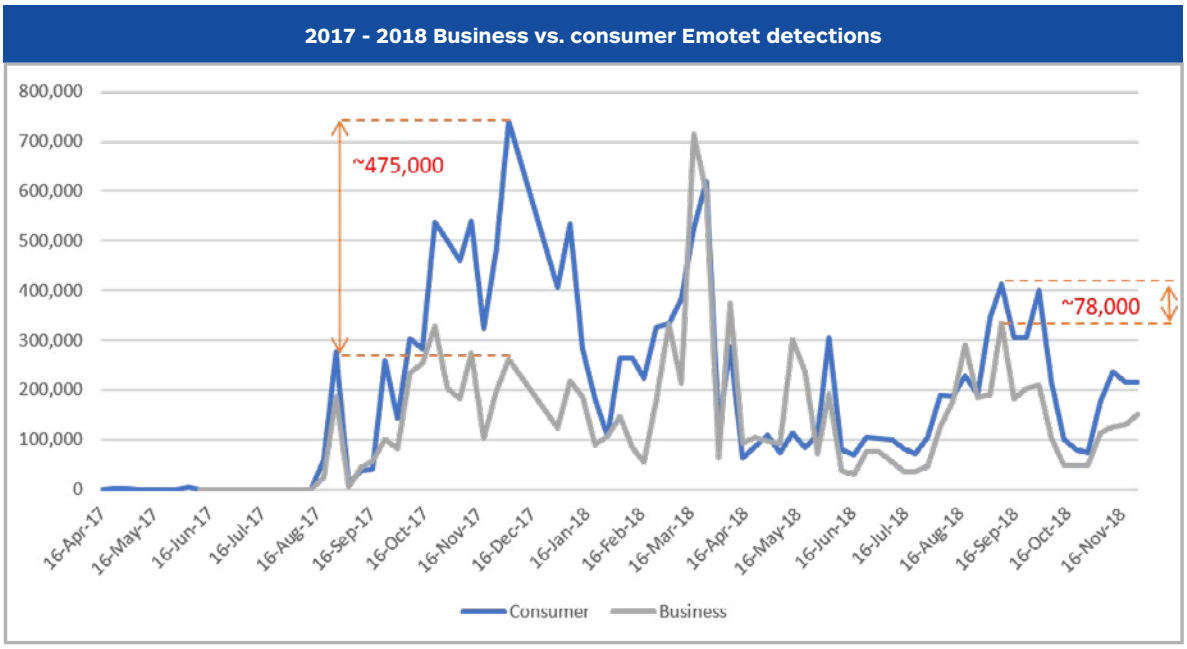

Figure 23. Business vs. consumer Emotet detections

Why is this important to point out? Because the similar shapes of the detection humps for both business and consumer during the same time period show us that Emotet campaigns cast a large net against both consumers and businesses. Historically, these nets have caught far more victims on the consumer side, however the gap between the two is shrinking.

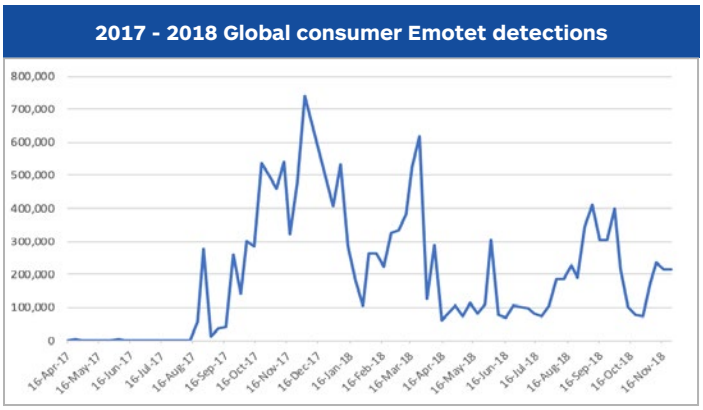

Figure 24. Emotet consumer detections, April 2017–November 2018

The attackers behind Emotet are intentionally attempting to spread their malware to business targets. Combine this with the family's upgrades in functionality, such as the ability to move laterally and spread malicious spam from the infected endpoint, and the motive of the Emotet controllers becomes evident.

TrickBot

If more business-focused Emotet attacks didn't make you think information stealers have found a better target, look no further than malware that is not only piling up business victims on its own, but is also being dropped as a secondary payload by Emotet itself.

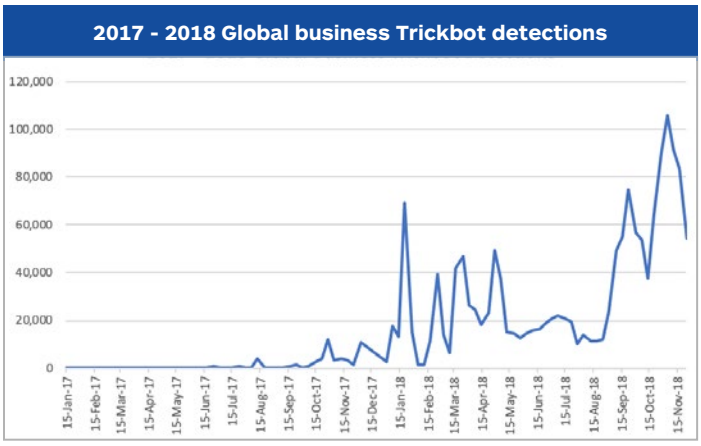

Figure 25. Global business detections of TrickBot

TrickBot is a nasty information stealer that can download components for specific malicious operations, such as keylogging and lateral movement within a network. As Figure 25 shows, this family didn't start making waves until the end of 2017 and was one of the most common payloads pushed by Emotet.

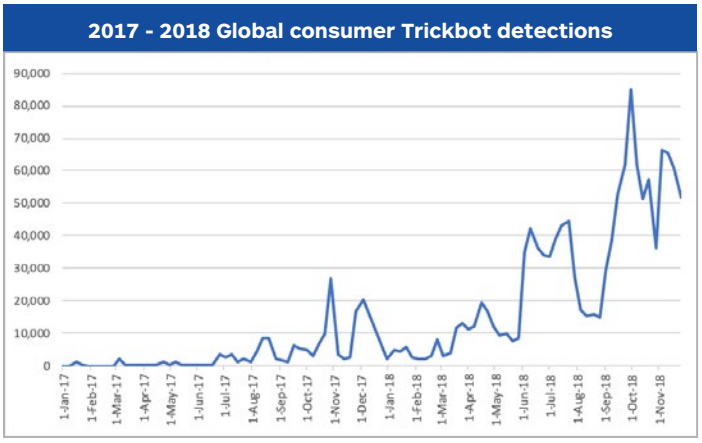

Figure 26. Global consumer detections of TrickBot

Overall detections of TrickBot on business and consumer endpoints show a 200,000 difference between the two, with businesses taking the top position. Business endpoints have detected 1.5 million TrickBot instances, while consumers detected nearly 1.3 million times.

Most malware we deal with tends to have greater detection numbers on the consumer side than on corporate endpoints. When analyzing these newfound detections on the business side, we are able to parse out cybercriminals' intent to target businesses and exploit their vulnerabilities.

Trojans by vertical

As mentioned in our Trojan introduction, Trojans can refer to multiple malware types that are either hiding their intent or don't fit neatly into one category. When we zoom out and look at the industries that Trojans target, the picture is similar to that of our global detections combined. Education, manufacturing, and retail top the chart, with consulting, government, and healthcare occupying the middle ground. Food and beverage are in last place, and hospitality, which made waves in the news with the Marriott breach, doesn't even make the list.

Top 10 industries affected by Trojan malware	
1	Education
2	Manufacturing
3	Retail
4	Consulting
5	Government
6	Telecommunications
7	Healthcare
8	Technology
9	Business services
10	Food and beverage

Figure 27. Top 10 industries impacted by Trojans

However, when we clarify the Trojan category to look at the top family of Trojans, Emotet, the industries shift. Consulting shoots to the top of the list and hospitality makes an appearance in fourth place. In addition, transportation and logistics and chemicals join the top 10, pushing out telecommunications, business services, and food and beverage industries.

Top 10 industries affected by Emotet Trojan malware	
1	Consulting
2	Education
3	Manufacturing
4	Hospitality/Leisure
5	Government
6	Retail
7	Transportation and logistics
8	Chemicals
9	Healthcare
10	Technology

Figure 28. Top 10 industries impacted by Emotet

Trojans of tomorrow

The current trends we've been observing with Trojans are likely to continue while there are opportunities for criminals to exploit weak configurations and outdated assets. However, the greater concern is the copycats and new generations of families that are likely going to dominate 2019.

At the moment, we don't see much competition for Emotet (outside of TrickBot) as it either targets organizations on its own or acts as an infection vector for another family. However, if the ransomware trends of 2012 to 2016 are any indicator of things to come, we'll see competitors pop up quickly in the next 12 months.

Ransomware

Ransomware isn't the wide-ranging threat it was in 2017, but it's still a force to be reckoned with. Overall trends show a drop in volume for the year, but an increase in focused, sophisticated attacks aimed at businesses. Indeed, the only real spike in numbers has been in the realm of the workplace, with a distinct lack of interest and innovation aimed at consumers.

While there has been some surprising reworking of older files to perform new attacks, and a few big splashes from famous variants such as WannaCry, ransomware in 2018 remained mostly dormant.

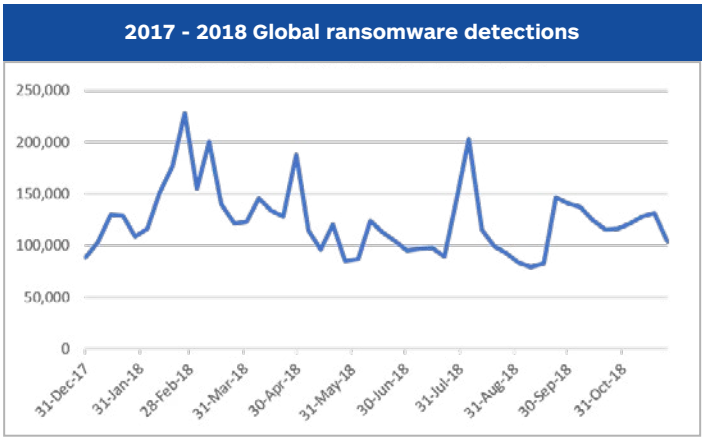

Figure 29. 2018 global ransomware detections

Consumer vs. business

The drop in overall attacks is significant: In 2017, we saw 8,016,936 attacks across business and consumer globally. Compare that to 2018, where there were 5,948,417 detections recorded—a decline of 26 percent.

The difference in interest for business targets over consumer is easy to see, with one steadily increasing while the other declines.

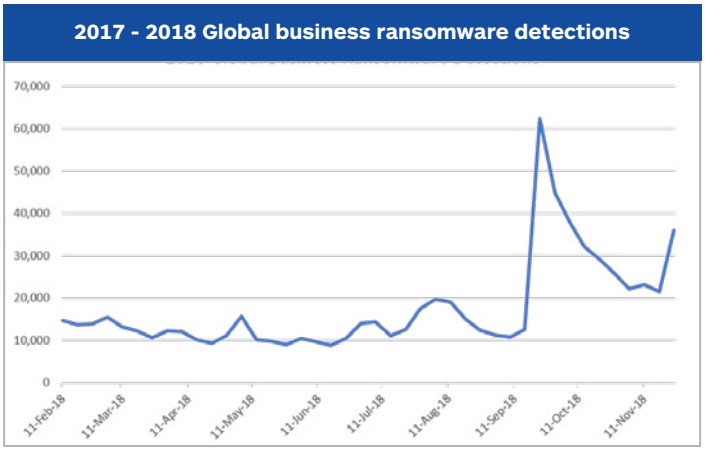

Figure 30. Global business detections of ransomware

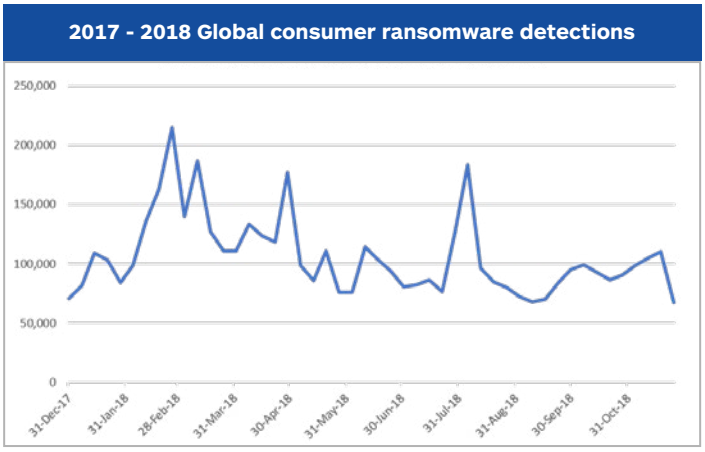

Figure 31. Global consumer detections of ransomware

Given that businesses house so much valuable data and critical systems, they are proving to be a more profitable target for criminals. Not only do they have the potential funds to pay a ransom, they're also likely to have multiple pressing reasons for wanting to get back into action. Ransomware delays can be incredibly costly, especially when an affected organization has no backup plan in place and multiple endpoints to remediate. Incident response and digital forensics all add to the cost, which is often a lot more than simply paying the ransom (a tactic we do not recommend).

Vertical business stats

You may be wondering: How popular is ransomware across various industry sectors? Which verticals took the hardest hit? Our data shows that consulting took the top spot, with education swooping up second place.

Top 10 industries affected by ransomware	
1	Consulting
2	Education
3	Manufacturing
4	Retail
5	Government
6	Transportation
7	Telecommunications
8	Electronics
9	Healthcare
10	Technology

Figure 32. Top industries affected by ransomware

Despite the many major stories throughout 2018 dealing with healthcare and government attacks, other industries felt the brunt of the ransomware menace—with government taking the middle spot on the list, and healthcare down in ninth place.

SamSam

SamSam caused chaos across medical networks in the US, exploiting and brute forcing its way into systems to make over $1 million dollars for holding systems to ransom. One of its many older variants revamped to be more appealing to criminals, charging victims a more moderate price than alternative recovery methods, making significantly more money as a result.

From January to March, SamSam took down everything from hospitals to city services, including departments of transportation and city-facing applications in Atlanta. Additional major attacks took place in September, with both the ports of San Diego and Barcelona suffering outbreaks.

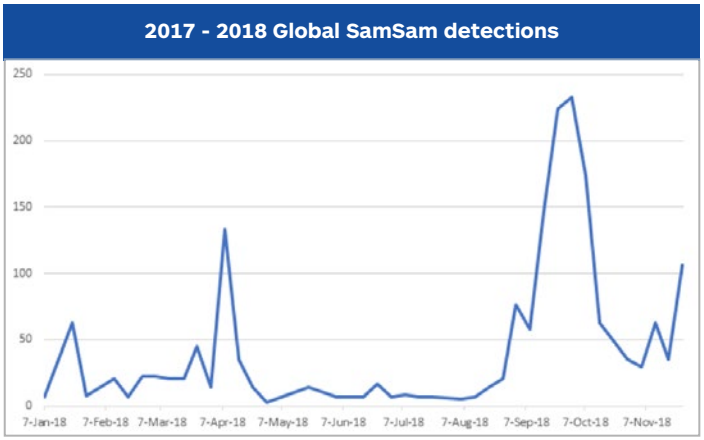

Figure 33. 2018 global SamSam detections

Although law enforcement agencies believe they know who is behind the infection, the alleged duo are still at large, and we still continue to see spikes in attacks. SamSam will continue to be a strong source of malware infections well into 2019.

GandCrab

GandCrab was also a major player in 2018, making use of various exploit kits shortly after its first appearance in January. Numbers levelled off and remained constant for most of the year, with a huge spike of activity in February, thanks to multiple spam campaigns in Q1.

Moving to the Magnitude exploit kit for distribution, GandCrab continued to cause trouble for network admins and home users. This is partly thanks to Magnitude's unconventional malware-loading methods. Everything from fileless techniques to binary padding (where extra data is added to files to bypass scanning) were used in the race to make it the biggest player in town.

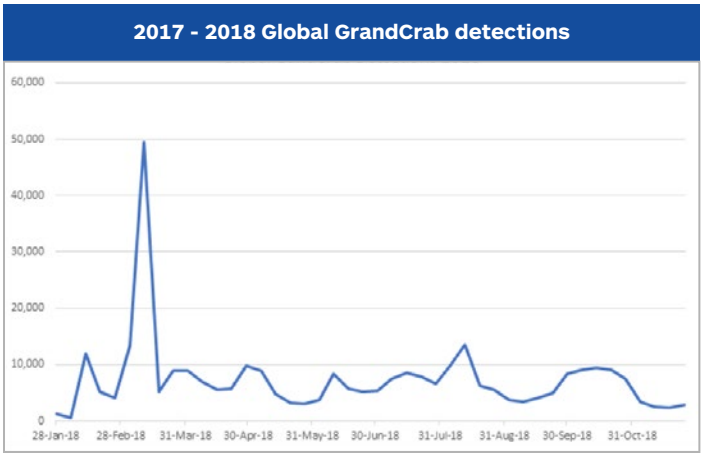

Figure 34. 2018 global GandCrab detections

GandCrab, the top ransomware variant of Q2 2018, is also notable for being the first ransomware to ask its victims for a cryptocurrency payment other than Bitcoin. At a time when business ransomware detections were up by 28 percent, but the overall volume remained low, it became one of the leading sources of malicious ransomware campaigns—to the eternal aggravation of its victims.

End of year

Although ransomware has lost ground to other players, such as cryptominers and Trojans, it still packs a punch, and 2018 has been a year of quiet experimentation and reassessment. The public at large are much more aware of such attacks now, and the same old tricks won't work forever. We expect to see more innovative reworkings of older files and strengthened ties to cutting-edge exploit kits to push ransomware further still.

Noteworthy attack vectors

2018 was a mixture of the old and new, with malware authors both falling back on traditional delivery techniques, such as malspam and social engineering, and exploring new territory with browser-based cryptomining. In addition, threat actors got even more creative at avoiding detection by injecting malicious code into online payment platforms, slipping rogue apps into legitimate webstores, and stealing information out from under users' eyes with plugins that did more harm than good. Let's have a look at the most noteworthy attack vectors of the year.

Malspam

Emotet and TrickBot, two of 2018's worst nightmares, tag-teamed for an effective attack that included distribution via malspam disguised as legitimate email—your classic phishing/spear phishing campaign. However, what made their attacks so impactful were not just how the malware was delivered, but how it spread.

Emotet is commonly spread by malspam that includes infected attachments or embedded URLs. There is a social engineering factor involved. Since Emotet takes over victim email accounts, malicious emails appear to come from trusted sources to their recipients. The infected attachment usually comes in the form of a Microsoft Word document with macros enabled.

Once Emotet has infiltrated a network, it uses EternalBlue, one of the SMB vulnerabilities leaked by the ShadowBrokers Group last year, to exploit unpatched systems. Infected machines attempt to spread Emotet laterally via brute force of domain credentials, as well as externally via its built-in spam module. As a result, the Emotet botnet is quite active and responsible for much of the malspam we encounter.

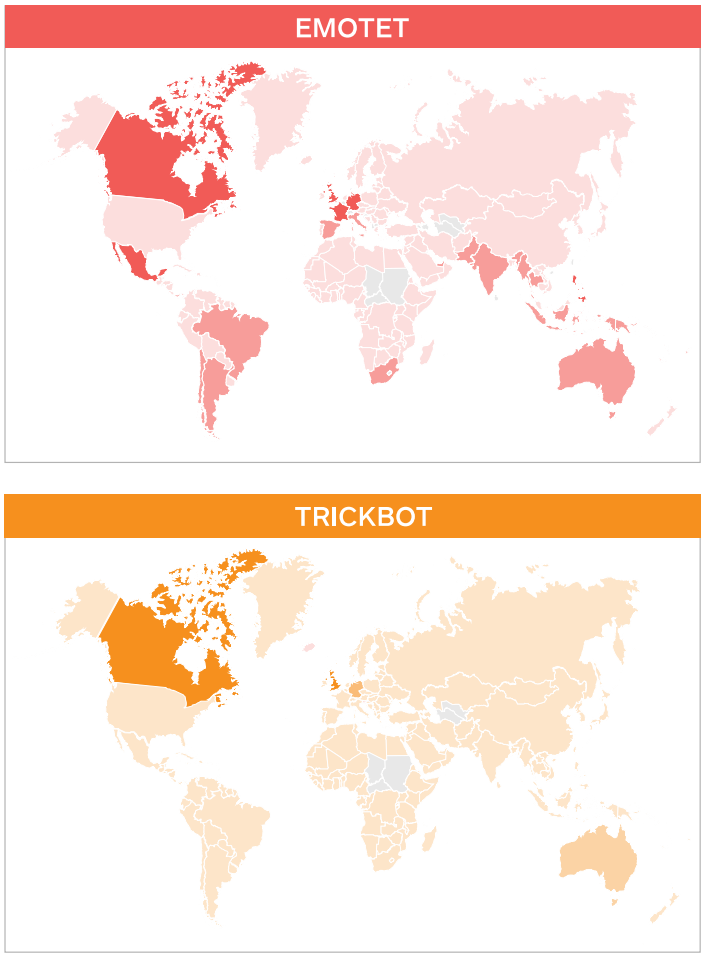

Figure 35. Emotet vs. TrickBot global detections

TrickBot is another active Trojan that uses malspam to infect systems. It primarily relies on infected Word documents, but also uses embedded URLs that lead to infected PDF files. Like Emotet, TrickBot uses one of the SMB vulnerabilities—this time, EternalRomance—for lateral movement inside a network.

Relatively new on the malspam front are Office documents that manage to escape the macOS sandbox for Office macros. The Word macro malware, currently detected as OSX.BadWord, sets up a backdoor using Python on the affected system.

Website attacks

In 2018, we saw a steady increase of high-profile attacks on trusted, legitimate ecommerce sites via third-party compromise for skimming credit card details and other PII. One such attack on British Airways impacted nearly 400,000 customers, whose names, home addresses, and financial information were stolen.

By lurking on trusted websites, the threat actor group known as Magecart stole payment and contact information that visitors entered when checking out their purchases. The Magecart attacks exploited weaknesses in the code of the payment processing pages and used cross-site scripting (XXS). Several groups using Magecart tactics sometimes compete with each other by tampering with one another's code.

The malicious code below, the work of Magecart, was appended to a legitimate and trusted script in an obfuscated format.

After decoding the script, we can see the code responsible for harvesting the data when customers hit the checkout button. At the network level, this looks like a POST request where each field (name, address, credit card number, expiry date, CVV, etc.) is sent in Base64 format to a rogue server (in this case, info-stat[.]ws) controlled by the criminals.

This kind of attack happens transparently to both the merchant and customer. In contrast to breaches that involve leaked databases where the information may be encrypted, web skimmers are able to collect data in clear text and in real-time.

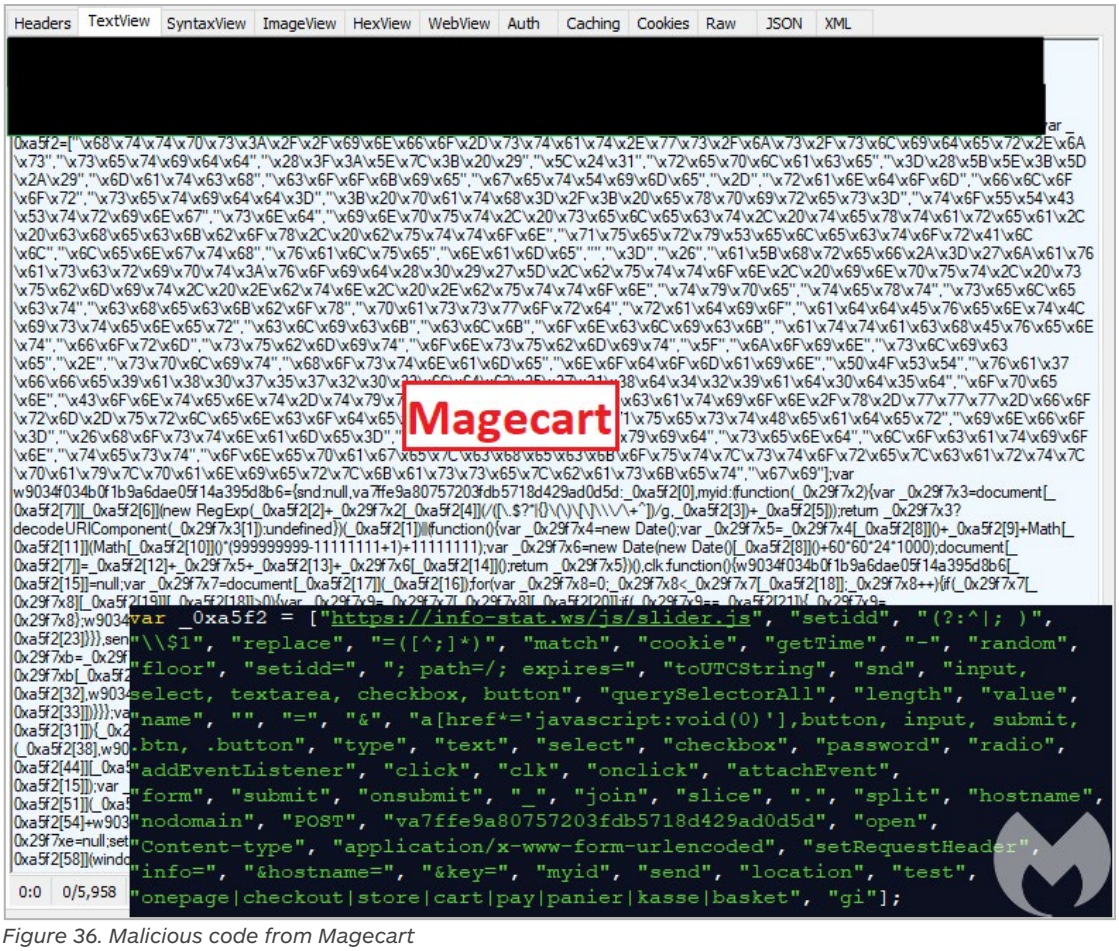

Figure 36. Malicious code from Magecart

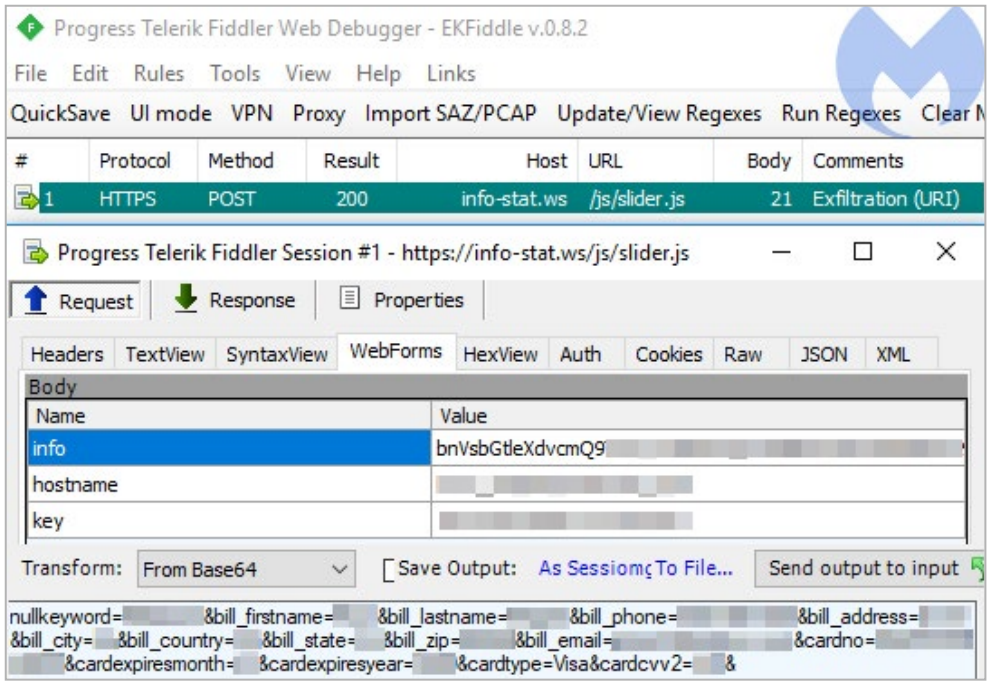

Figure 37. Magecart code sends details to a rogue server

Malicious browser extensions

In 2018, malicious browser extensions (plugins) made quite a splash. Whether legitimate extensions were compromised and used in supply-chain attacks or rogue extensions promised user privacy while tracking their movements online, there were plenty of examples to choose from. Some of the standout cases we saw were:

- Compromised legitimate extensions in a supply-chain attack, most notably filesharing MEGA.nz's Chrome extension, which stole usernames and passwords. Users could only notice the difference from the original extension because of the extra permissions the hacked version asked for.
- A slew of Firefox extensions (and also some Chrome ones) were caught red-handed spying on their users' browsing history.
- Extensions that mimicked popular plugins to trick users into installing them, including an extension that claimed it didn't track its users or store their data, but instead protected users from the prying eyes of the browsers themselves. Of course, what users really got was an extension that simply redirected their homepage to Yahoo!

On the bright side, major browsers were compelled to take action against these malicious extensions. Here are the changes they have implemented so far:

- Stopped inline installs. Everything must now go through the official web stores.
- Blocked obfuscated code in the extensions.
- Ceased support for legacy protocols like TLS 1.0 and 1.1. This was announced for 2020.

While major browsers have taken measures to shield malicious extensions from entering their stores, we still see a lot of adware and PUPs coming through. Most of these are hijackers, which can change your browser's default search provider or its Start or New Tab pages. Sometimes, they pretend to enhance your search privacy.

And while we keep telling users that they should get their apps from the official stores, popular game Fortnite decided to offer up its Android version of the game outside of Google Play. To get the game, users have to enable the "allow installs from unknown sources" option, which can lead to other unwanted installs. To make matters worse, their installer allowed man-in-the-disk attacks, a way for rogue apps to hijack the installer and install their own junkware in place of the legitimate app.

Exploits

We expected to continue seeing attacks via malicious spam and Microsoft Office documents in 2018, as this was a trend we had already observed during the previous year.

We have seen an interesting shift happening with regards to how vulnerabilities are being used in the wild, however. Because browsers have become more secure, as well as automatically updated, drive-by downloads are far fewer in between. As such, the email vector is one of the most relied upon ways threat actors have to compromise systems.

Plugin and browser exploits

To kick off the year, we saw a zero-day vulnerability in the Flash Player (CVE-2018-4878) being used in targeted attacks against South Korea, attributed by many to the Lazarus group.

The exploit was embedded within a decoy Excel spreadsheet and loaded as an ActiveX object. Soon after, a number of exploit kit authors had adopted this vulnerability as part of their web-based distribution toolkits.

Another zero-day for the VBScript engine (CVE-2018-8174) was discovered in late April and was significant because it had been two years since we had seen a fresh exploit affecting the popular Internet Explorer browser. However, it is worth noting that this zero-day was once again packaged in a document rather than as a drive-by. Following the typical zero-day ⊕ patch ⊕ Proof-of-Concept (PoC) cycle, this new exploit became mainstream among browser exploit kits, relegating its predecessor, CVE-2016-0189.

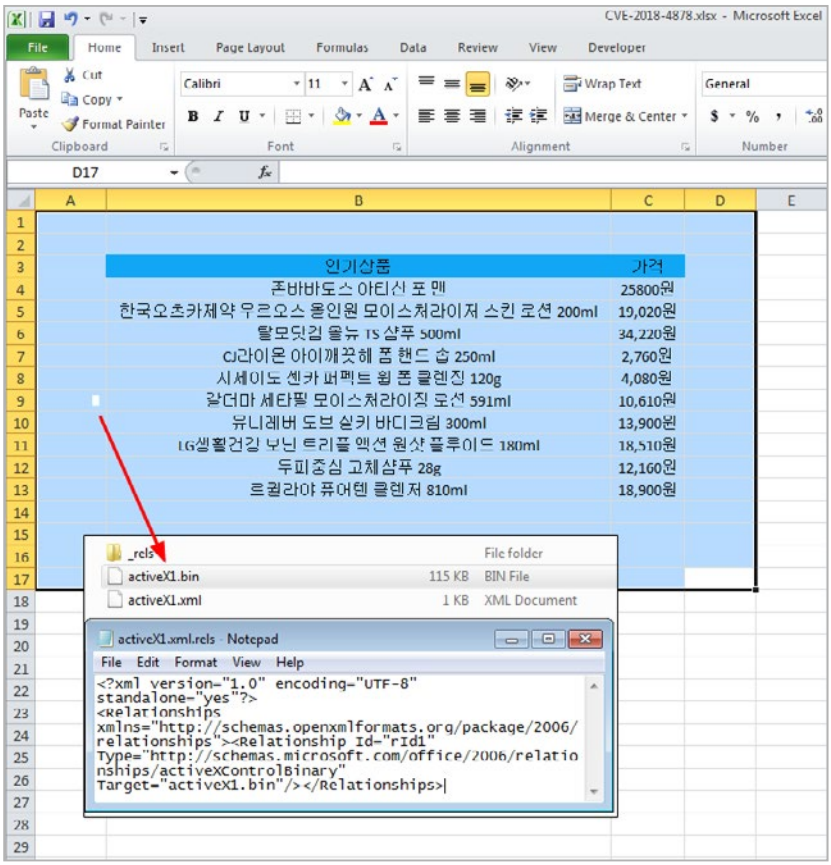

Figure 38. Hidden Flash ActiveX embedded in lure document

Mass compromises via routers

April was a busy month indeed, as a critical flaw affecting MikroTik routers (CVE-2018-14847) was found inside RouterOS, the operating system powering those devices.

Restricting access to Winbox (MikroTik's management panel) via the firewall was highly recommended to prevent intrusions. Attackers automated login attempts and even used malware to exploit the path traversal vulnerability.

Fixing the issue not only required to apply security patches but also to clean up certain configuration files. Those files were often used to inject Coinhive cryptojacking scripts, thereby making anybody connected to an infected router, regardless of the device or website they were visiting, mine for cryptocurrencies.

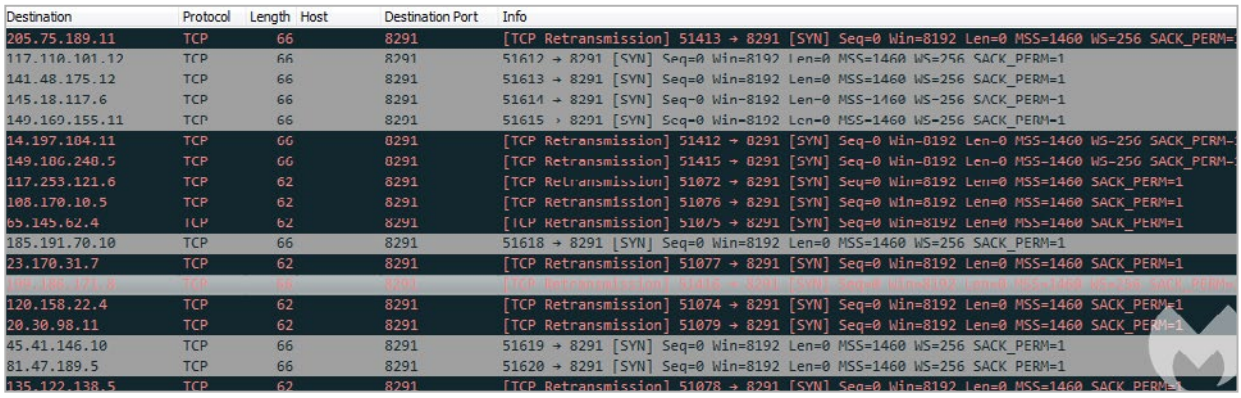

Figure 39. Malware scanning for other vulnerable devices on the default Winbox port (8291)

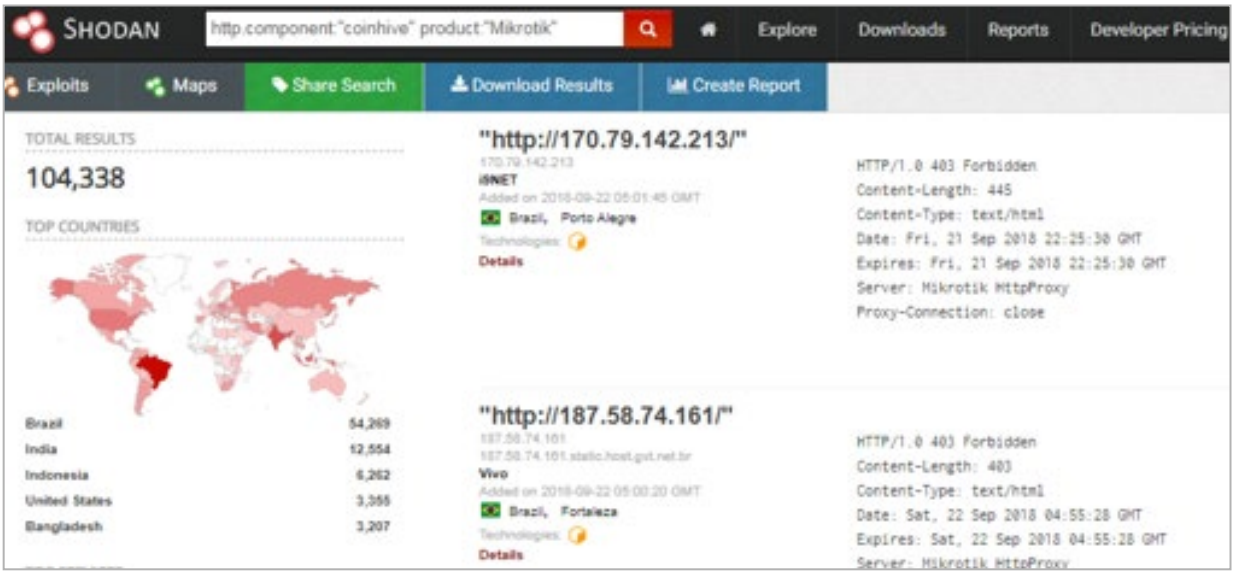

Figure 40. Shodan scan showing over 100,000 compromised MikroTik devices

CMS hacks

It would be hard not to mention Content Management Systems (CMS) and how they were affected by exploits in 2018. Attackers often discovered or exploited Remote Code Execution vulnerabilities in popular software such as WordPress, Jooma, or Drupal.

Drupal was one the most probed CMSes in the first half of 2018, in large part due to back-to-back flaws (CVE-2018-7600 and CVE-2018-7602) that led to massive compromises.

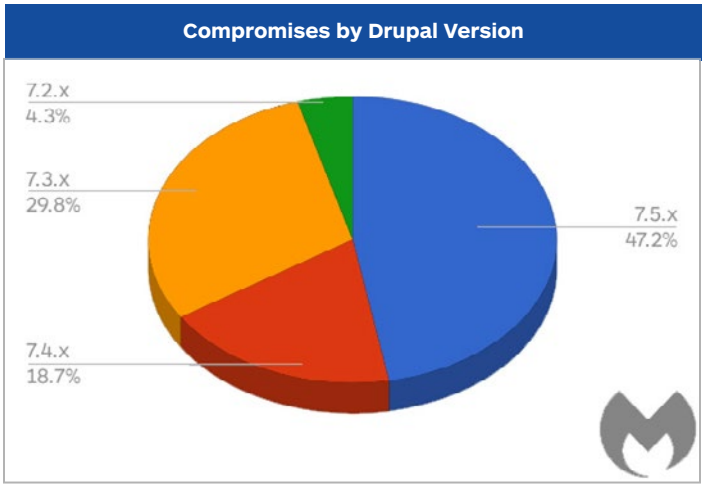

Figure 41. Most compromised sites by Drupal version (7.x branch)

A majority of website owners do not keep their CMS (or its plugins) up to date and unsurprisingly suffer compromises. The fear of breaking a site by upgrading it is often cited as a reason to remain on an older revision. Having said that, unless those sites are protected behind some kind of application firewall, they will easily be hacked.

Zero-days in browsers and plugins were high on the list in 2018, but not necessarily used in the way one would expect. Indeed, attackers have instead been combining them with spear phishing or social engineering attacks embedded within Office files.

Criminals have also been targeting hardware devices—particularly routers—to perform compromises on a large scale. As we know, those devices are often outdated and will likely never be patched until they stop working altogether. This is a perfect scenario for attackers, and one that is difficult to combat for security vendors without user awareness.

Noteworthy scams

In 2018, we experienced a wide range of scams that often mirrored developments in malware distribution and creation. In Q1, cryptomining took over just about every aspect of cybercrime—scams included. The more successful players consolidated resources

and turned to more inventive tactics, transporting themselves beyond simple tech support scams to drain cryptowallets themselves. By Q2, we noticed a shift away from cryptoscams to targeting PII—a tactic that remains active today.

Most notably, Coinbase-themed TSS achieved thefts of spectacular scale, based largely on the lack of fraud protection involved with Bitcoin and Coinbase itself. Victim reports on Twitter claiming empty wallets and losses in the five figures suggest that these threat actors found it easier to simply drain wallets at their leisure rather than provide fake tech support.

Scammers were also observed updating their lead generation tactics using API abuse to assist in freezing the victim's browser at the beginning of 2018. The primary target for this technique was Chrome, but it also impacted Firefox and Brave.

Exploitable business practices

Tech support scams primarily rely on exploitable business processes rather than specific tools. In the case of Coinbase-themed scams, scammers exploited the lack of fraud protection inherent to Bitcoin transactions to boost their profits significantly above average. With the API abuse referenced, the real exploit is the significant lag between reporting to the companies in question and an eventual patch.

Given that a particular browser function generally has a legitimate function to many users, patch lag time for tech support cases tends to be relatively long. As such, scammers can exploit that period for large gains.

We expect both Bitcoin-themed scams and browser abuse to be useful tools for scammers for quite some time.

Targeting PII

Moving into Q2, scammers increasingly began targeting PII. 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 contracted in the face of user awareness and increased enforcement, scammers started stealing passwords, bank account information, and email accounts with increasing frequency. New GDPR regulations likely added fuel to the PII theft fire, as that type of information snatches a healthy paycheck on the black market.

Sextortion

In early July, an extortion scam campaign attracted our notice due to its large scale and unique twist. Unlike traditional sex-based extortion scams, this email campaign came with a user's password as a sign that the sender had "hacked" the victim. These credentials came from a variety of past high-profile breaches, most likely drawn from one of several omnibus collections

of leaks over the past four years. The credentials were accurate, although most victims said the threat actors were using old and often outdated passwords.

Using leaked credentials as a social engineering tool is a relatively novel approach to this sort of attack, allowing an additional monetization channel for the credentials themselves, and adding a veneer of plausibility to the subsequent extortion attack. As third-party breaches show no signs of decline, we expect this technique to remain in use as an aid to phishing, extortion, and other scams.

Tightening the noose

Over the past quarter, we've observed a hard shift away from credit card processing by scammers targeting Malwarebytes customers. Credit card processors have increasingly been taking action against scammers abusing their platforms, prompting a shift to less closely monitored platforms like PayPal, as well as formats with less built-in fraud protection like Bitcoin and personal checks. While this provides the threat actors with a more stable revenue stream, it also limits the scope of their activities, resulting in a lower number of reporting victims over the past quarter.

Another response to increased enforcement activity has been a gradual shift away from blind cold calls to voice messages requesting a call back. Callbacks are a well-tested means to get in touch with only the most vulnerable victim populations, excluding people inclined to ask probing questions on an initial call.

A look ahead

Moving forward, we expect PII-enabled social engineering attacks similar to the sextortion email wave to gain popularity. Given the escalating tempo of large-scale breaches, combined with widespread credential reuse across platforms, leveraging leaked PII to increase social engineering efficacy offers a threat actor a force multiplier with limited downside or expense. Best of all for the attacker—as demonstrated with the sextortion campaign—PII used in a social engineering pitch doesn't even have to be accurate or up to date to be effective. As a result, more campaigns of this tenor are expected in the future.

2019 predictions

As we look forward to the new year, we're often asked to predict which trends will die down and which new ones will appear. While we can use our intel to make educated guesses about the ebbs and flows of cybercrime, no amount of experience can prepare us for disruptive innovations the likes of which we experienced with the cryptomining craze. When it comes to cybercrime, we still don't know what we don't know.

But that doesn't mean we shouldn't take some time to think about the future and prepare ourselves for potential dangers around the corner. Here's what we think could take place in 2019. Hold onto your butts.

New, high-profile breaches will push the security industry to finally solve the username/password problem.

The ineffective username/password conundrum has plagued consumers and businesses for years. There are many solutions out there—asymmetric cryptography, biometrics, blockchain, hardware solutions, etc.—but so far, the cybersecurity industry has not been able to settle on a standard to fix the problem. In 2019, we will see a more concerted effort to replace passwords altogether.

IoT botnets will come to a device near you.

In the second half of 2018, we saw several thousand MikroTik routers hacked to serve up coin miners. This is only the beginning of what we will likely see in the new year, with more and more hardware devices being compromised to serve up everything from cryptominers to Trojans. Large scale compromises of routers and IoT devices are going to take place, and they are a lot harder to patch than computers. Even just patching does not fix the problem if the device is infected.

Digital skimming will increase in frequency and sophistication.

Cybercriminals are going after websites that process payments and compromising the checkout page directly. Whether you are purchasing roller skates or concert tickets, when you enter your information on the checkout page, if the shopping cart software is faulty, information is sent in clear text, allowing attackers to intercept in real time. Security companies saw evidence of this with the British Airways and Ticketmaster hacks.

EternalBlue or a copycat will become the de facto method for spreading malware in 2019.

Because it can self-propagate, EtnernalBlue and others in the SMB vulnerability, including EternalRomance and EternalChampion, present a particular challenge for organizations, and cybercriminals will exploit this to distribute new malware.

Cryptomining on desktops, at least on the consumer side, will just about die.

Again, as we saw in October (2018) with MikroTik routers being hacked to serve up miners, cybercriminals just aren't getting value out of targeting individual consumers with cryptominers. Instead, attacks distributing cryptominers will focus on platforms that can generate more revenue (servers, IoT) and will fade from other platforms (browser-based mining).

Attacks designed to avoid detection, like soundloggers, will slip into the wild.

Keyloggers that record sounds are sometimes called soundloggers, and they are able to listen to the cadence and volume of tapping to determine which keys are struck on a keyboard. Already in existence, this type of attack was developed by nation-state actors to target adversaries. Attacks using this and other new attack methodologies designed to avoid detection are likely to slip out into the wild against businesses and the general public.

Artificial Intelligence will be used in the creation of malicious executables.

While the idea of having malicious AI running on a victim's system is pure science fiction at least for the next 10 years, malware that is modified by, created by, and communicating with an AI is a dangerous reality. An AI that communicates with compromised computers and monitors which and how certain malware is detected can quickly deploy countermeasures. AI controllers will enable malware built to modify its own code to avoid being detected on the system, regardless of the security tool deployed. Imagine a malware infection that acts almost like "The Borg" from Star Trek, adjusting and acclimating its attack and defense methods on the fly based on what it is up against.

Bring your own security grows as trust declines.

More and more consumers are bringing their own security to the workplace as a first or second layer of defense to protect their personal information. As industries become more aware of the dangers associated with BYOS, they are taking proactive measures to protect their company from the breach of sensitive data. In fact, Malwarebytes recently conducted global research and found that nearly 200,000 companies had a consumer version of Malwarebytes installed.

Education was the industry most prone to adopting BYOS, followed by software/technology, and business services.

Conclusion

2018 was yet another banner year for malware. From frenzied, fresh cryptomining attacks that seemed to happen daily to cool, calculated ransomware campaigns, the pendulum shifted multiple times to follow market trends, adjust to fallout from new regulations, and keep businesses, consumers, and, yes, us security researchers on our toes.

As we look ahead to 2019, we anticipate the game of cat and mouse to continue on and on, with old tricks applied to new threats and new tactics used for old favorites. As always, our advice remains to stay informed, stay vigilant, and never take the security of your data or devices for granted.

As awareness increases, threat actors will adapt. But if we make their targets that much harder to reach, we can keep ourselves, our organizations, and our online communities that much safer in 2019.

Contributors

Adam Kujawa: Director of Malwarebytes Labs

Wendy Zamora: Head of Content, editor-in-chief

Jovi Umawing: Senior Content Writer, editor

Jerome Segura: Head of Threat Intelligence

William Tsing: Head of Threat Operations

Pieter Arntz: Senior Malware Analyst

Chris Boyd: Senior Malware Analyst