Cybercrime tactics and techniques: Q3 2018

Provided by

Malwarebytes LABS

Contents

Executive summary

After a sleepy first two quarters, cybercriminals shook out the cobwebs and revved up their engines in Q3 2018. With cryptominers and exploit kits maturing, ransomware ramping up with steady experimentation and more sophisticated attacks, and banking Trojans experiencing a renaissance, we're having one heck of a season. Attack vectors were at their most creative—and most difficult to remediate—especially for businesses.

In fact, businesses saw far more action this quarter than consumers—their total detections trended upwards by 55 percent, while consumer detections increased only by 4 percent quarter over quarter. It looks like threat actors are searching for more bang for their buck, and business targets are returning more value for their efforts. Banking Trojans and ransomware, traditionally aimed at both businesses and consumers, leaned much harder into their business targets this quarter. Even malware that's generally favored consumers, such as cryptominers and adware, seems to have graduated to a more professional prey.

Consumers saw a whole lot of scam action this quarter, especially using the ever-classic sexploitation technique, but this time it came with a twist—scammers used stale personally identifiable information (PII) likely pulled from breaches of old to scare users into action. And although scammers were up to no good in Q3, we at Malwarebytes had a field day taking a bunch of bad guys down.

So how did we draw our conclusions for this report? As we've done for the last several quarterly reports, we combined intel and statistics gathered from July through September 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 third quarter of 2018.

QUICK FACTS

- Banking Trojans were the number one detection for both businesses and consumers in Q3.
- Malicious cryptomining **decreased by 26 percent** for businesses from Q2 2018.
- Ransomware business detections **increased 88 percent** while consumer detections decreased in Q3.
- Adware **decreased 19 percent** for consumers but **increased 15 percent** for businesses in Q3.

Key takeaways

Several new banking Trojans came on the scene in Q3. Coupled with smart evolutions to older strains, these developments brought this traditional malware back into favor. In fact, banking Trojans were the number one detection for both business and consumer Malwarebytes customers this quarter, thanks in part to an active and widespread Emotet campaign.

Cryptomining has matured in the face of market downturn, continuing to diversify its offerings and attack methods. While it's not going away anytime soon, malicious cryptomining has experienced a gradual decline over the year since Bitcoin value spiked. Interestingly, the opposite has happened to business users. Over the last year, malicious cryptomining has increased—although a sharp dive at the end of this quarter has resulted in a 26 percent decrease from Q2 2018.

Ransomware made some noise in Q3 with new developments to GandCrab making it even more dangerous, including new fast and robust encryption features and the ability to reach and encrypt network shares. In addition, Magniber ransomware expanded to other regions, and 40 new ransomware variants were developed, although they were not all released into the wild. Ransomware turned on its heel rather quickly, pivoting toward businesses to the tune of a 88 percent increase in detections from last quarter. Consumer detections, however, decreased in Q3.

Remote Access Trojans (RATs) ramped up the action this quarter, and were distributed primarily via malspam, though exploit kits also played their part. The KaiXin exploit kit was caught distributing a version of the Gh0st RAT this summer. Meanwhile, the njRat Trojan and FlawedAmmyy RAT have also been trending upwards in Q3, delivered through malspam and social engineering tactics.

Adware hid in plain sight in Q3, using browser extensions and rogue apps to serve up its payloads, and hitting users with promises to protect privacy while doing just the opposite. While adware dipped by 19 percent quarter over quarter for consumers, it increased by 15 percent on the business side, marking another business-focused trend for malware this quarter.

Exploit kits (EK) saw their busiest quarter in well over a year, with targeted action continuing in Asia and expanding from South Korea into Japan. Two new exploits, Underminer and Fallout, breathed life into an otherwise struggling space, fueling continued EK activity for quarters to come. However, instead of being used as the sole weapon, EKs are now being adopted as an additional component of web-based attacks, with social engineering used in tandem.

An interesting development for scammers this quarter included the use of stale PII in phishing attacks, most notably tied to a large sexploitation campaign that made the rounds via email. As data breaches become more and more common, we expect to see more campaigns using the tossed-out remains of old breaches for classic social engineering-based fear mongering.

And in closing, we whooped a lot of scammer butt this quarter, taking down many foes posing as Malwarebytes tech support, unauthorized resellers, fake Twitter accounts, and more.

Malware

Remember last quarter when we said everything was going to change in Q3? Looks like we nailed that prediction, as the third quarter of 2018 is shaping the rest of the year into something nobody expected. The big push this quarter seems to be from information-stealing malware—like Emotet and LokiBot—especially on the business side. Interestingly, we have observed a drop in some of the most common categories for consumer detections.

Those that have been following our reports for a while know that, while this might seem backwards, a lull in volume typically signals that criminals are busy working on new attack vectors or new forms of malware.

For now, they're saving the good stuff for businesses and stealing all their data. But in another quarter or two, expect to once more see something entirely new for consumers.

In Q3, banking Trojans nudged out all other malware categories for the top business threat, rising 84 percent from last quarter's output. Trojans also took the top spot for consumer detections, rising by 27 percent from last quarter. RiskwareTool, a detection name for cryptomining malware, fell from its first-place ranking for businesses last quarter all the way down to fourth, with a decrease of 26 percent. In fact, cryptominers fell on the consumer side as well, slipping down to fourth place behind Trojans, adware, and backdoors.

Top 10 Detections By Category

Rank	Business	Q/Q	Rank	Consumer	Q/Q
1	Trojan	84%	1	Trojan	27%
2	Hijacker	57%	2	Adware	-19%
3	Adware	15%	3	Backdoor	-21%
4	RiskwareTool	-26%	4	RiskwareTool	-32%
5	Backdoor	-33%	5	HackTool	21%
6	Ransom	88%	6	Worm	-8%
7	Spyware	-41%	7	Spyware	39%
8	Worm	91%	8	OSX	18%
9	HackTool	23%	9	Ransom	-24%
10	Exploit	-41%	10	Hijacker	-41%

Total Detection Count Change

Q2	Q3	Q/Q	Q2	Q3	Q/Q
3.1 Million	4.8 Million	54.8%	77.3 Million	80.3 Million	3.9%

Figure 1. Top 10 Malwarebytes detections

Total detection changes

In new data we added to this quarter's report, we wanted to show how much malware we actually detect during these report periods, specifically the overall trend changes for all malware. As has already been mentioned, we are seeing a shift, albeit a slow one, in more sophisticated and dangerous malware being aimed at businesses. This is further backed up by an increase of 5 percent, or 1.7 million more detections in Q3 than in Q2.

On the flip side, as we've observed throughout the year, consumers just aren't the juicy target they used to be for novel malware. The last quarter brought with it only a 4 percent increase in detections, which can also be seen by the drop in popular consumer malware categories of the past, such as adware, backdoors, miners, and ransomware. A 39 percent increase in spyware detections, however, shows a return to stealing and selling data, a common trend in the late 2000's and early 2010's before the flood of ransomware happened.

Banking Trojans

Banking Trojans are a favorite malware payload for attackers due to the direct financial reward the malware can produce. 2018 has seen a continual uptick in banking Trojan activity, with several new variants coming onto tvhe scene in Q3, as well as various evolutions to other well-known strains.

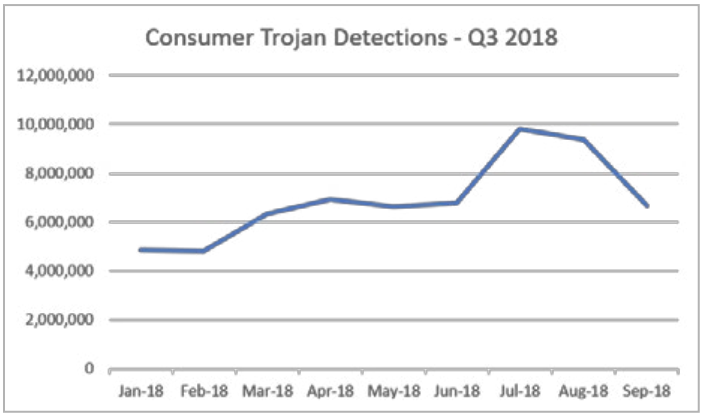


Figure 2. Consumer banking Trojans trend upward in Q3 2018.

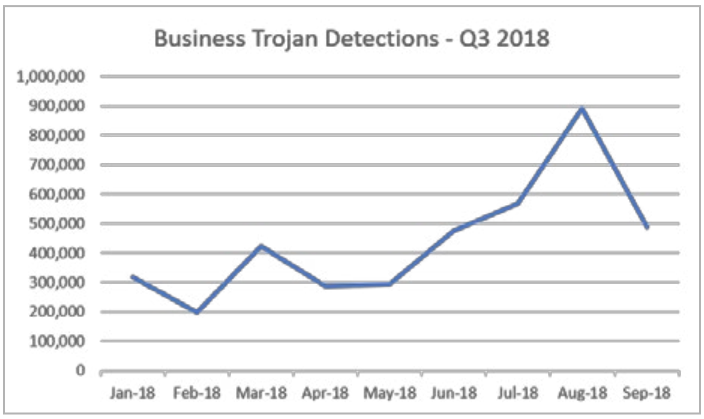


Figure 3. Business banking Trojans spike in August 2018.

So why did Trojans take the lead for both business and consumer detections this quarter? This is primarily due to an active Emotet campaign that started in August 2018 and, as of this writing, shows no signs of stopping. In addition, a slew of other generic detections (Trojan.FakeMS for example) kicked the Trojan category into high gear. However, it's Emotet that is leading the charge in a resurgence of malware designed to steal financial information.

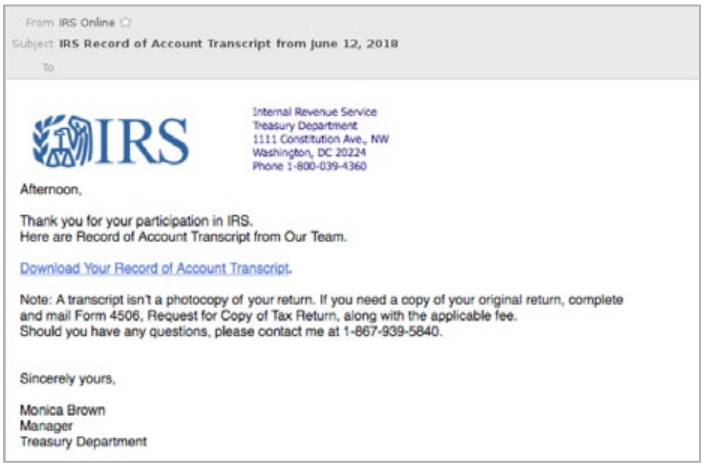
Emotet

The Emotet Trojan originally appeared in 2014 as an information-stealer targeting primarily European banking customers. It is the most prevalent banking Trojan for enterprise users and poses a challenge to IT administrators with its ability to self-propagation, allowing infections across a network without any user action required. We've seen such spreading capabilities with recent campaigns, such as WannaCry and the NotPetya attacks, which crippled businesses across the globe from Maersk to FedEx. Q3 has seen a significant increase in Emotet detections, and the malware ranks in the top six for enterprises.

Emotet contains a spam module for the mass-mailing of malicious payload to recipient email addresses found on targeted systems. This allows the malware infection to continue spreading without assistance from the operator. Because of this capability, malspam continues to be the primary infection vector for the attackers.

Though the spoofed subject lines and sender details can change, recent Emotet spam emails apply various tactics to try and convince users to open the email and included attachments. This spoofed information come in the form of tax information from the Internal Revenue Service (IRS), payroll information, or even greeting cards. Examples of subject lines may include:

- IRS Tax Account Transcript
- IRS Verification of Non-Filing
- IRS Wage and Income Transcript
- Pay Invoice
- Payment
- Payroll Tax Payment
- Tax Account


From IRS Online
Subject IRS Record of Account Transcript from June 12, 2018
To

IRS

Internal Revenue Service
Treasury Department
1111 Constitution Ave., NW
Washington, DC 20224
Phone 1-800-039-4360

Afternoon,

Thank you for your participation in IRS.
Here are Record of Account Transcript from Our Team.

Download Your Record of Account Transcript.

Note: A transcript isn't a photocopy of your return. If you need a copy of your original return, complete and mail Form 4506, Request for Copy of Tax Return, along with the applicable fee.
Should you have any questions, please contact me at 1-867-939-5840.

Sincerely yours,

Monica Brown
Manager
Treasury Department

Figure 4. Example of Emotet malspam

The malware payload is spread through malicious macro-enabled Microsoft Word files that are included with the original email. Though macros are disabled on most systems by default, users who choose to ignore the warnings unwittingly install the malware within their environment.

Another way that malware authors can increase the value of their software is to bundle additional malware payloads. And this past quarter, Emotet has evolved in this particular arena.

We've seen a number of malicious packages installed alongside Emotet. These may include other banking Trojans or infostealers, such as Trickbot or Dridex. Such partnerships allow the compromise of information from multiple malicious operators, and the collected information can be shared with attackers to help better construct cash-out procedures and maximize the profit ratio on a per-infection basis.

Other payloads we have seen being distributed by Emotet include Qakbot. Qakbot is another self-spreading Trojan that attempts to brute-force password authentication using the Mimikatz open-sourced password stealing tool. Mimikatz is a hacking tool that is capable of moving laterally through networks and can be made active on compromised machines.

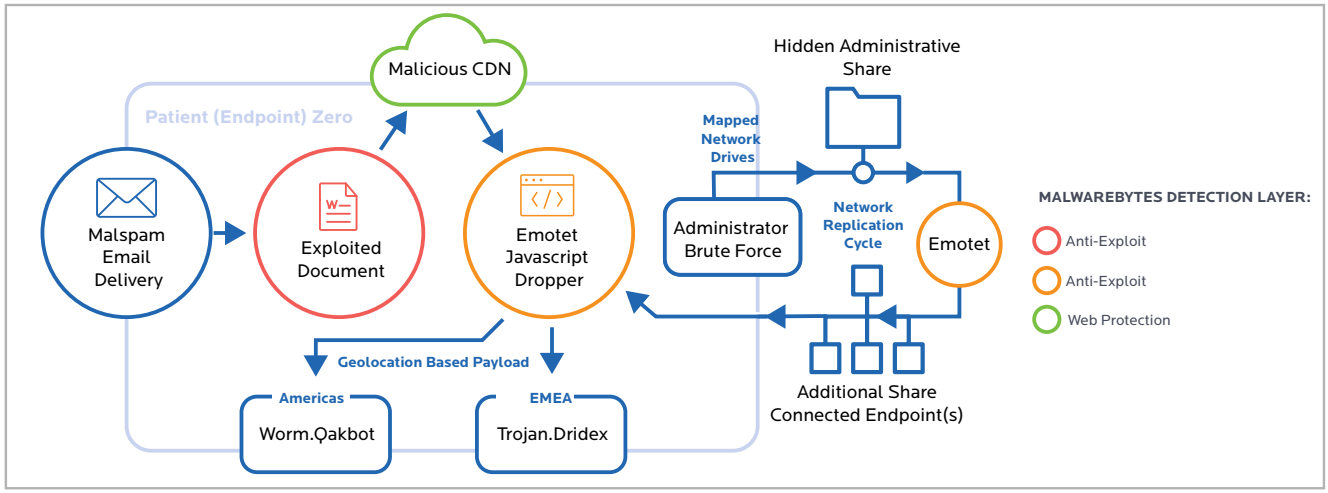


Figure 5. Emotet infection vector

Osiris

But Emotet isn't the only banking Trojan to make waves this quarter. A new evolution of the Kronos malware has also been detected in recent weeks. The malware, dubbed Osiris, uses a new technique to evade detection and prevent antivirus products from scanning the malicious files.

The technique, known as Process Doppelgänging, is used to impersonate legitimate system processes, but it's rarely used in the wild. This technique was first uncovered at the 2017 BlackHat conference as a mechanism that keep processes from being visible. Soon after, it was used in a SynAck ransomware campaign.

The Osiris dropper has significantly improved its infection tactic by using a hybrid of the best elements of Process Hollowing and Process Doppelgänging, making the act of introducing Osiris to target systems stealthier than ever.

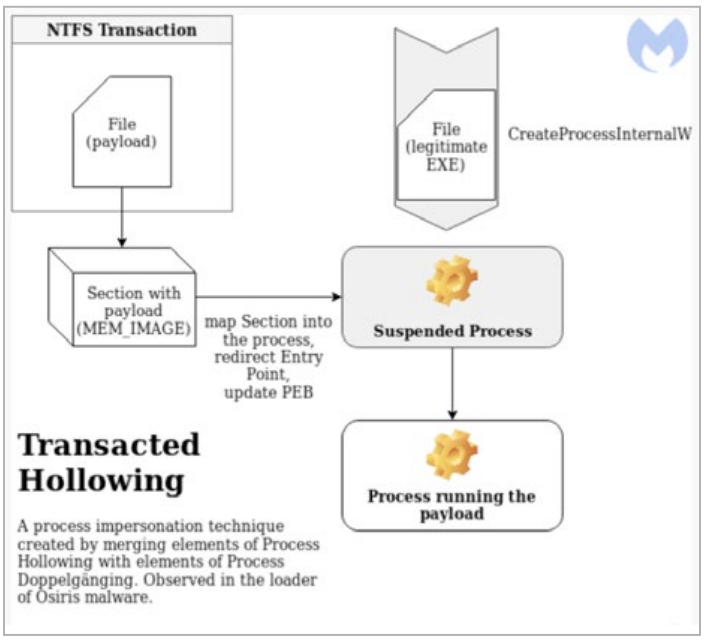


Figure 6. Transacted Hollowing combines elements of both Process Hollowing and Process Doppelgänging.

After successfully compromising the system, Osiris can then perform a number of reconnaissance and collection activities, web injections, and man-in-the-middle/man-in-the-browser attacks, as well as a number of other techniques. As an additional feature, all communication from Osiris funnel through the TOR network to thwart the possibility of researchers or law enforcement dismantling of the attacker's infrastructure.

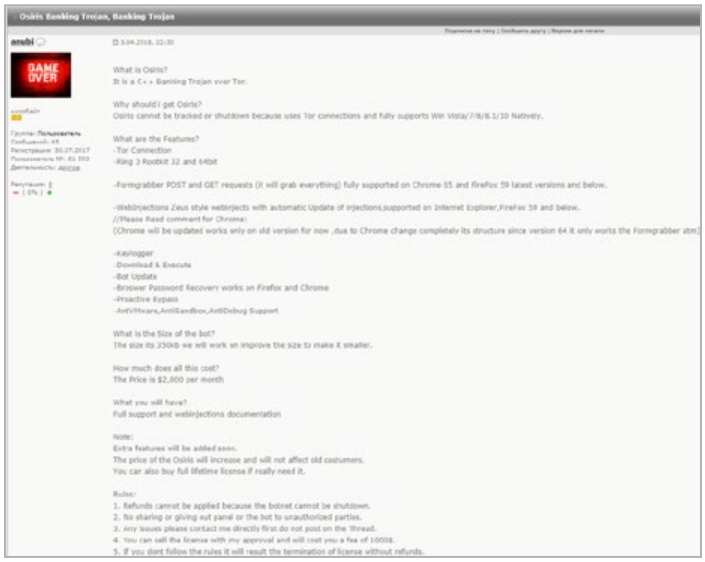


Figure 7. Sales post for the Osiris malware

Looking ahead

The wide-scale distribution of Emotet has proven successful for the malware author, and its continued development and refinement demonstrate the commitment of those responsible for its creation. The addition of new banking Trojan families to the scene also demonstrates the continued success of these malware and the attackers' desire to design more efficient systems. This is why we expect to see more banking Trojans and with more robust functionality in quarters to come.

Cryptomining

Cryptomining is still a problem for both businesses and consumers, with the lowest detection count in a year being nearly 2 million, at least on the consumer side. Our stats, however, show that miners are no longer the most prevalent threat. We can see a gradual decline in miners being encountered by our customers in the wild. This could be due to the minimal difference between the price of Bitcoin and the cost to mine it, even though cybercriminals have no intention to use their own resources for the mining process.

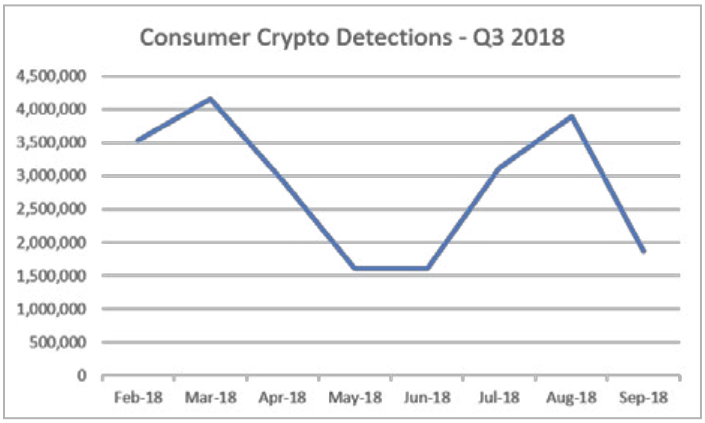


Figure 8. Consumer cryptomining trend line from February – September 2018

Taking a look at the consumer and business cryptomining charts, their trend lines nearly match, although businesses have seen 4 million fewer detections on the whole. There was a slight spike in July and August for both consumers and businesses, but this pales in comparison to the massive surge in consumer detections we witnessed in October 2017, which coincided with the spike in value of Bitcoin and other cryptocurrencies. From there, cryptomining detections have gradually slid downward over the year, and they are just about back to where they started before October 2017.

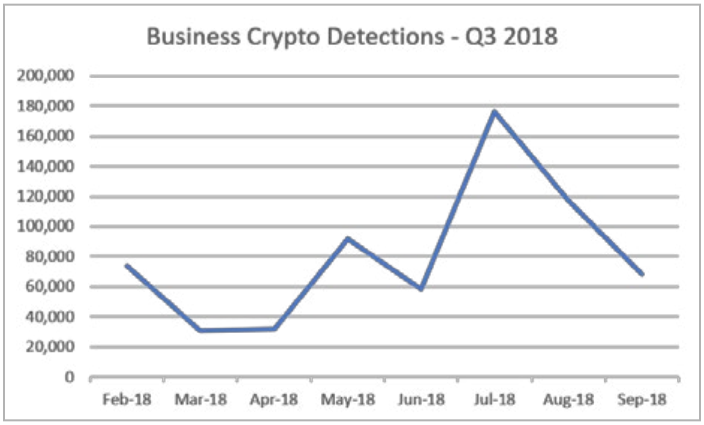


Figure 9. Business cryptomining trend line from February – September 2018

The business side, however, seems not to have been bothered by the new value of cryptocurrency. We didn't observe any serious miner infections until July 2018, long after the value had dropped. Does this upward climb mean that businesses are now a greater target for miner pushers? Considering we've seen such a big jump between June and July, we may be witnessing a single month campaign push. Once we take a look at the first few weeks of Q4, we'll have a better idea if this is an ongoing trend.

New methods

Even though malicious cryptomining was still a large participant in the threat landscape, there was a noticeable shift to different methods. Threat actors seemed to have learned that using compromised websites pays off a relatively low return on the effort involved in finding and using vulnerable sites for their purposes. This was especially true if the compromised website was not highly trafficked. As cybercriminals tend to go for the jackpot, they looked for ways to take down popular websites, which are usually better maintained and secured, or switched to using IoT and server vulnerabilities to make headway.

Some examples:

- A massive cryptomining infection targeted MikroTik routers in Brazil.
- A new Apache strut vulnerability was actively exploited to deploy cryptominers.
- Malicious cryptominers masqueraded as a game on the Steam gaming platform.
- Threat actors abused vulnerabilities in Content Management Systems to mine for cryptocurrency.

So, even though the volume of cryptomining malware seems to be declining, cybercriminals are continuing to use new methods and other resources to mine their cryptocurrencies. In fact, some have stepped away from cryptominers altogether to use social engineering techniques like ICO scams to simply steal cryptocoin from others.

Staying safe from miners has never been easier. As a result of a year-long onslaught of cryptomining, many vendors now specifically target mining software as potentially malicious. Consumers should be less worried about getting infected with miners and more concerned with banking Trojans and spyware. However, if the trend continues, businesses might want to keep an eye out for any resource-hogging applications on endpoints. For companies, it's never the miners themselves that are dangerous—it's how they got on the machine or network and what else they might bring.

While the technology behind miners had increased dramatically (without the promise of riches), it's still a watch and wait game to see how many more criminals will keep pushing miners and how many will pivot back to familiar territory, such as ransomware.

Ransomware

In what we consider a continuing trend of switching targets from consumers to businesses, we have observed an 88 percent increase of ransomware aimed at our business customers, the majority of which have been served GandCrab. Flipped from early last year, consumer-facing ransomware attacks have continued to decline as it becomes more and more apparent to cybercriminals that attacking businesses is more profitable than attacking grandmothers.

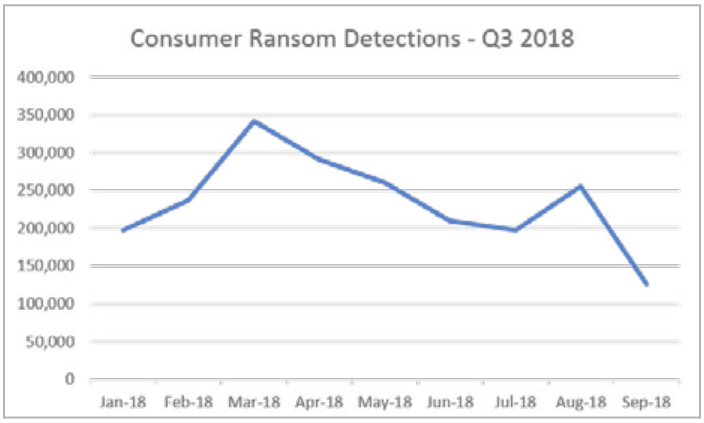


Figure 10. Consumer ransomware detections January – September 2018

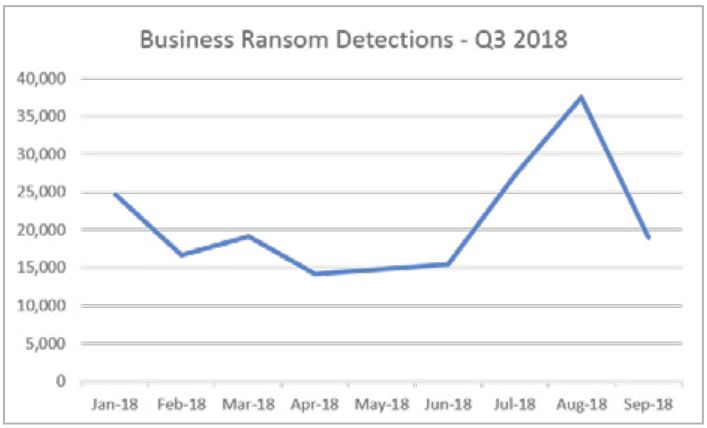


Figure 11. Business ransomware detections January – September 2018

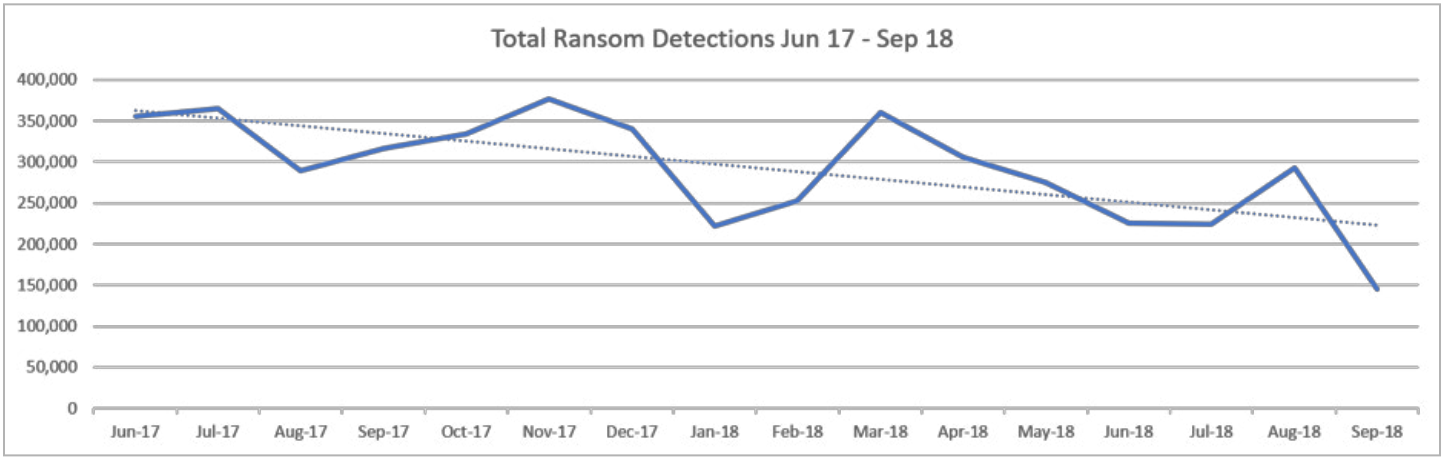


Figure 12. Overall ransomware detections from June 2017 to September 2018

Q3 has largely been without much ransomware activity, at least compared to what we had seen in quarters prior. In fact, by looking at the detection trends for ransomware over the last year and a half, the downward slope of the dwindling ransomware market is evident.

Despite this, security researchers around the world have discovered new families of ransomware—almost 40 of them. In addition to that, some families have made immense updates this year, leading to the release of more dangerous and powerful variants. The interest of criminals in ransomware isn't dead; we are seeing just as much innovation in the technology as we did when Cerber was number one. However, the distribution, despite being chaotic at times, has remained relatively small. Will this change next quarter or next year? Time will tell.

GandCrab

For those unfamiliar with this malware family, GandCrab was first discovered on January 26, 2018, and has been an ongoing threat ever since. GandCrab v4 was first seen in the beginning of July, and there have been multiple updates to the malware since then, including the release of GandCrab v5 shortly before we published this report.

GandCrab originally set itself apart from other popular ransomware families by accepting the cryptocurrency DASH instead of Bitcoin. Since then, the ransomware creators have opened the door to Bitcoin as well. The ransom requested by attackers ranges from $800 to over $1,000, and the ransom doubles after a set amount of days have passed without payment.

Version 4 of GandCrab switched from using an RSA-2048 encryption algorithm for encrypting files to Salsa20, the same encryption algorithm used with the Petya ransomware. This method of encryption is more robust than RSA-2048, meaning files can be encrypted faster. Petya's use of Salsa20, however, was flawed in its implementation, which led to the creation of Petya decryptor tools. Unfortunately, it doesn't seem that the authors of GandCrab made the same mistake.

Another new feature of GandCrab is the ability to encrypt network shares if they are remembered by the victim system. GandCrab can now encrypt files without an Internet connection, as the previous versions' requirement to communication with the command and control server is no longer necessary to begin the attack.

Finally, GandCrab, like other ransomware families we've seen in the past, avoids infecting the systems of Russian speakers. GandCrab has used this method of checking keyboard language layouts to identify potential Russians, but it now also checks the language used for the user interface.

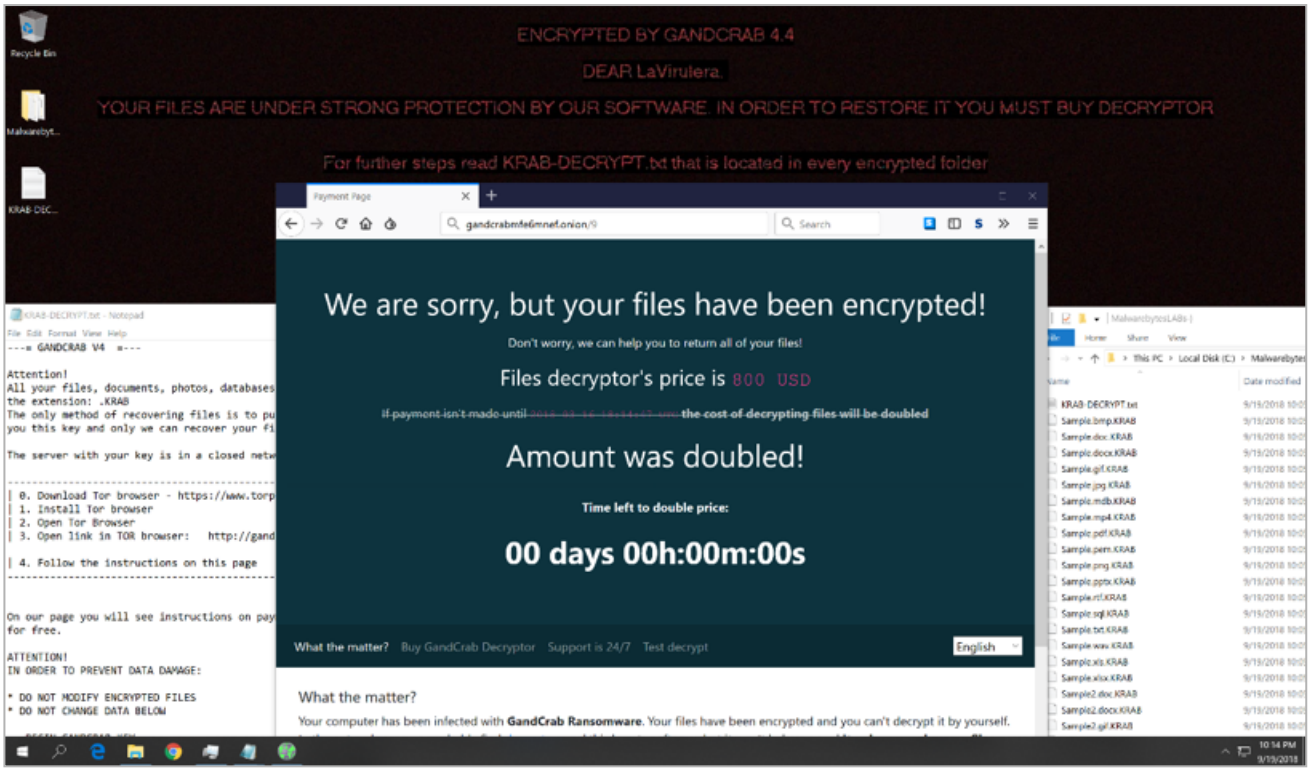


Figure 13. This is your PC on GandCrab.

Figure 14. GandCrab author saying hello to one of our researchers, Marcelo Rivero

Was GandCrab created by a Russian or someone who just doesn't want to upset the Russians? Either way, the people or person behind GandCrab enjoys the back and forth with the security community and frequently leaves little "shout-outs" to security researchers.

However, when AhnLab created and released a tool to prevent GandCrab infections, the ransomware author(s) became far less friendly. They were so upset that they called out AhnLab in their code after releasing what they considered to be a zero-day exploit for AhnLab's products. This so-called exploit turned out to be only a bug that caused the application (and sometimes the system) to crash.

GandCrab trends

Despite numerous platforms being used by the creators of GandCrab to distribute to as many people as possible, we have not observed a constant stream of infection against our customers.

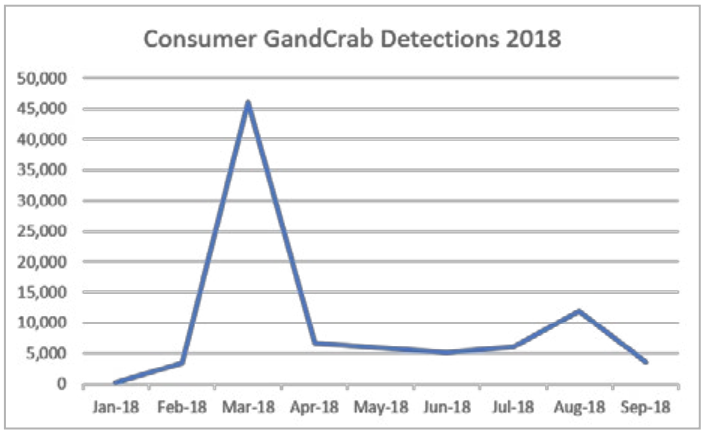


Figure 15. GandCrab consumer detections January – September 2018

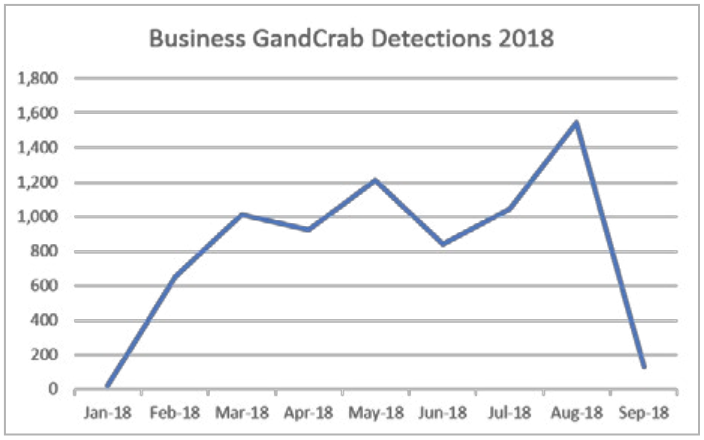


Figure 16. GandGrab business detections January – September 2018

Figure 16 shows the spike in business detections of GandCrab this quarter, with the biggest push starting in July and coming full force in August. September, however, has slowed down to basically the same level we saw at the beginning of the quarter. Despite this dip, with the amount of activity, investment, and press this ransomware has experienced, there is little doubt that we will see a bigger campaign push in October or November.

Distribution methods

As mentioned before, GandCrab has gone around the block when it comes to distribution mechanisms. We saw it pushed by the RIG exploit kit for a short while, by malicious spam distributed through the Necurs botnet, by the EITest campaign that had victims download a missing "font," by the Fallout EK (in action now), and finally, by posing as cracked versions of software.

There doesn't seem to be a primary target for this ransomware. We have observed high detection counts for both businesses and consumers over the year, and the spread of different infection methods makes it seem like the creator(s) are casting a wide net, making this ransomware our biggest concern out of all the others currently in the wild.

Magniber

The second ransomware family we wanted to feature in this report is Magniber, a ransomware family that has historically targeted South Korea.

Magniber ransomware came into existence after the operators of the Magnitude exploit kit either anticipated the end of Cerber or decided they wanted to make their own ransomware. The name Magniber is probably a mashup of Magnitude and Cerber, although we aren't sure who decided it was better than "Cerbitude."

The latest versions of Magniber ask for around $2,000 in Bitcoin as ransom and can begin the encryption process without communicating with the command and control (C&C) server. It also includes the same "pay now or pay double" model that GandCrab uses. Previous versions of Magniber had the ability to identify keyboard language layouts, focusing only on South Korea. However, now it also checks for a number of other languages native to Asian countries, such as Hong Kong, Singapore, and Malay.

Our initial analysis of Magniber last year showed a relatively unimpressive ransomware. However, with the commitment its creators have made, as well as the upgrades to its code, we can safely say that Magniber has taken off its training wheels and is ready to ride.

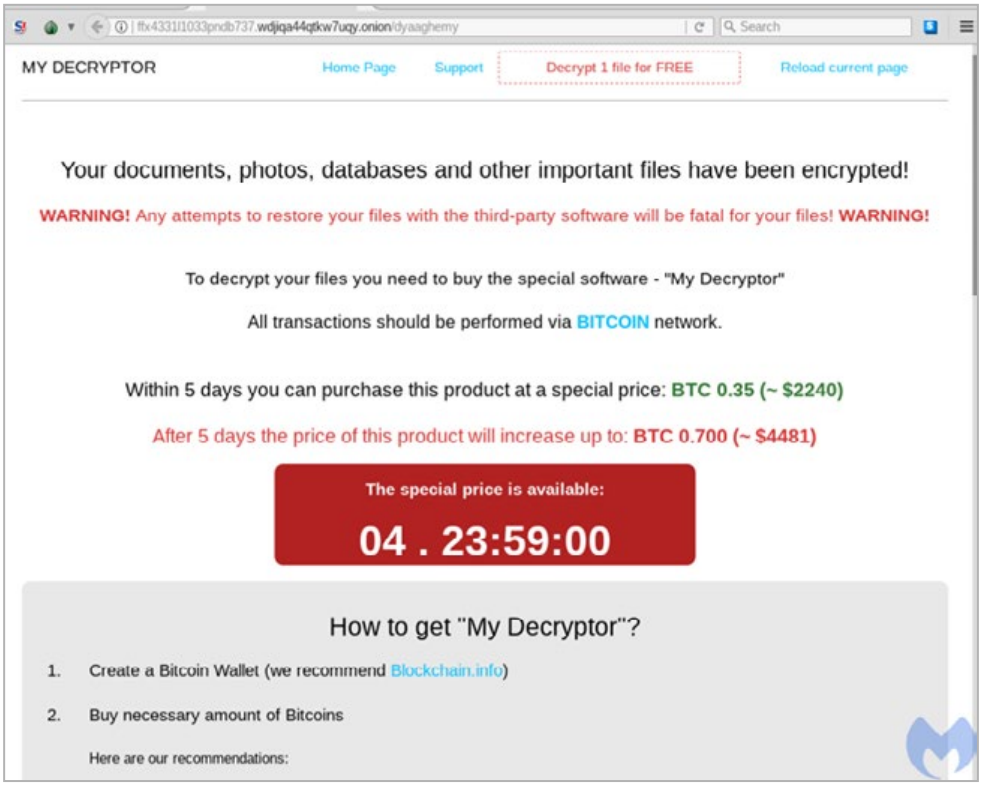


Figure 17. Magniber ransom screen

We believe that because of the quick evolution this ransomware has made, as well as the associated upgrades to the Magnitude exploit kit (making it better at spreading Magniber), Magniber is a ransomware family to look out for, especially if you live in Asia. We aren't sure of the motivations behind the creation and distribution of this ransomware to the countries it has targeted, but one day you infect China, the next—the whole world.

New ransomware families/variants this quarter

If there is anyone out there that misses the constant flood of ransomware attacks we experienced in past years, rest assured that while the market is nowhere near where it was (and let's hope it never is), there are still numerous potential cybercriminals who are creating or updating their own ransomware, even if they never make the news.

Here is a listing of 39 ransomware families that were either created or came out with new variants in Q3 of 2018:

KingOuroboros	Meduza	Armage
Whoopsie	Shrug	Dharma
Nozelesn	Rakhni	Yyto
RaRansomware	Everbe	Like
Scarab	24H	Cryptes
Gollum	Xorist	DDE
Boris	LanRan	CoinVault
The Brotherhood	Fantomas	Xiaoba
Jigsaw	Unlock92	MVP
NotAHero/ KyMERA	Desu	Matrix
Kraken Cryptor	SAVEfiles	Rektware
WannaCash	Animus Aurora	Locky (imposter)
Ann	Paradise	WannaCryV2

Figure 18. New and updated ransom families in Q3. Special thanks to Lawrence Abrams for writing over 100 "This Week in Ransomware" articles and all the security researchers that help bring awareness to new and lesser-known ransomware.

This has not been the strongest year for ransomware, as most detections have revolved around Bitcoin miners, adware, and banking Trojans. Regardless, ransoming is an effective method of "fundraising" for cybercriminals, and the bad guys know they can leech more from businesses, who have the funds and possess more critical files than consumers.

Attackers who manually break into a network to launch malware like SamSam and other rare but powerful families of ransomware are the ones who are making the most cash right now. This is absolutely going to result in copycats, and therefore it is incredibly important to utilize technology that targets ransomware.

Remote Access Trojans (RATs)

The third quarter of 2018 has seen a slight uptick in RAT activity delivered from both spam and exploit kits, and from players old and new. However, malspam continues to be the primary mechanism for attackers to deliver RATs, and the Malwarebytes Email Telemetry System saw no shortage of them in Q3.

RATs are often called the Swiss-Army knife of malware, as they can carry out a variety of attacks with relative ease. Their software allows for the collection of credentials, and many RATs contain self-spreading modules to help infect other machines. Though RATs don't often garner the media attention of a high-profile breach or a far-reaching ransomware campaign, they are still a major component of the threat landscape.

As we reported in the Malwarebytes exploit kits: summer 2018 review, the KaiXin exploit kit has been recently caught distributing a version of the Gh0st Rat Remote Access Trojan.

Gh0st RAT is a well-known RAT that has been making waves since at least 2008 and has been linked to the Gh0stNet Advanced Persistent Threat (APT). Researchers noted that Gh0stNet appeared to be controlled by computers using IPs based in China and had infected machines in more than 103 countries.

Like many other Remote Access Trojans, Gh0st RAT has a number of capabilities that allow attackers to steal data from affected computers. This includes the ability to capture keystrokes and contents of the screen, to record audio and video from connected cameras and microphones, and to covertly browse, copy, and move files from the infected computer using a remote shell. This capability also extends the other way to allow attackers to install additional malware or other harvesting tools to infected machines.

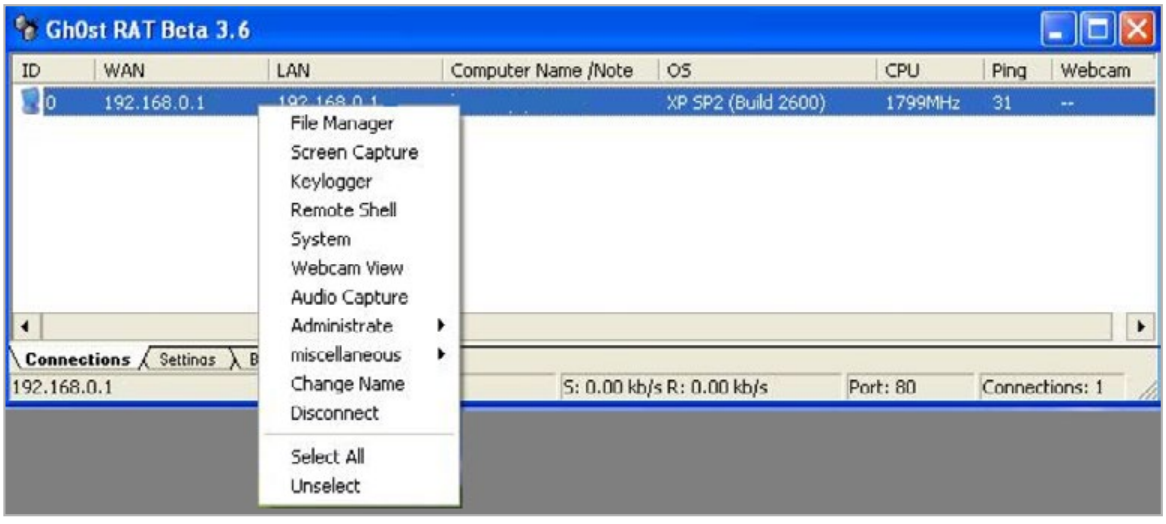


Figure 19. Gh0st RAT user interface

The njRat Trojan has also been trending upwards in the last few months. This can be traced back to various malspam campaigns using macro-based attacks to facilitate installation of the malicious payloads. njRat is a Remote Access Trojan that dates back to late 2012. This malware has been linked to a number of attacks targeting Discord software, VMware, and even the Islamic State.

Like other RATs, njRat has the ability to log keystrokes and screen captures, monitor webcam and microphone activity, launch applications, and more depending on the version being used.

Q3 also saw the continued use of the FlawedAmmyy RAT, first discovered earlier this year, which is based off the leaked source code of the AmmyyAdmin client. The attackers use malspam as a catalyst to drive delivery of the malicious payload and use various social engineering tactics to convince users to click on the included attachment or link.

Once users have been tricked into installing the payload, the attackers will have full control of affected computers to unleash any number of attacks, including installing additional malware, monitoring keystrokes and Internet activity, and spying on webcams and microphones.

RATs have been around since the dawn of the Internet, and they aren't going away any time soon. We expect to see old RATs continue to be repurposed for many years, as well as the continual development of new RATs and tools to fit the ever-changing needs of malicious attackers.

Figure 20. njRat user interface

Adware

The last quarter has seen a number of interesting adware techniques deployed, and a return to prominence for rogue files masquerading as legitimate applications. A lot of these recent issues have revolved around browser extensions as opposed regular executables—a timely reminder that not every bad file comes from a random website, but rather trusted sources such as the Google Chrome Web Store.

Where Malwarebytes adware statistics are concerned, we continue to see the same trend repeated across the entire threat landscape—a slight drop for consumer detections, and a slight increase for businesses.

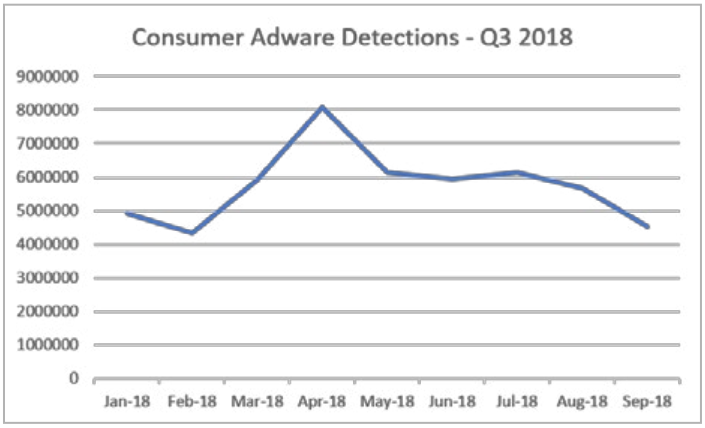


Figure 21. Adware detections decrease slightly for consumers in Q3.

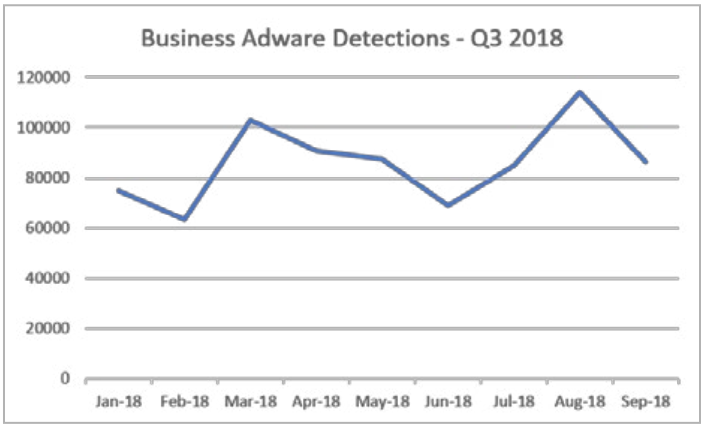


Figure 22. Adware detections increase for businesses in Q3.

As for mobile and Android adware detections, they continue on a slight downward trend after rising to a peak in May. It appears hackers are training their eyes on business entities as the main go-to source for data theft, blackmail, extortion, and other valuable pieces of data that convert to profit in a way that consumers currently can't match.

Adware-laden "ad blockers"

As many as 20 million devices were potentially compromised by rogue apps posing as genuine ad blocker extensions this quarter. While fake ad blockers and tools that claim to bypass website ad block detection are common, a tally of fake ad blockers on this scale is almost unheard of.

Using names such as uBlock Plus, Adblock Pro, HD for YouTube, and Webutation (some of which are based on legitimate program names), the fake extensions dropped users into a botnet. From there, they sent back information on browsing habits to a server, received instructions from the command and control center, and finally performed whatever task inside the browser that the adware author desired—generally that meant serving ads and tracking analytics.

Although official app stores are policed by Google, Firefox, Apple, and other tech giants, the fact that so many rogue apps can gain immense popularity gaining as many as 10 million users by stuffing their listings with a few basic keywords is cause for concern. In many cases, the reviews for said apps are often positive (and also often stuffed with praise from bots), so it can be difficult to use those as a gauge for whether or not the app in question is trustworthy.

Privacy searches stuffed with adware

Over the last quarter, we analyzed 25 extensions (primarily for Chrome, and a handful for Firefox) that claim to offer safe, secure searching.

Only a few of these search extensions actually use HTTPs, meaning searches are less secure by design and are potentially more susceptible to eavesdropping. The code we analyzed gave no evidence of developers paying attention to the privacy of both searches and results.

One of the largest families we looked at redirected all searches through to Yahoo! Search, whereas the rest made use of their own branded portals alongside additional advertisements placed on the results page.

The domains playing host to the extensions only promoted more general offerings, and not the privacy-enhancing files. The irony in all of this is by downloading an extension offering private, non-tracking searches, users instead opened up their PC and personal browsing habits to exactly that, with the addition of even more targeted advertising that provides these extension developers with a revenue stream. Claiming to give the end-user some form of privacy while bombarding them with ad is a traditional, old-school adware technique that's been around for at least a decade.

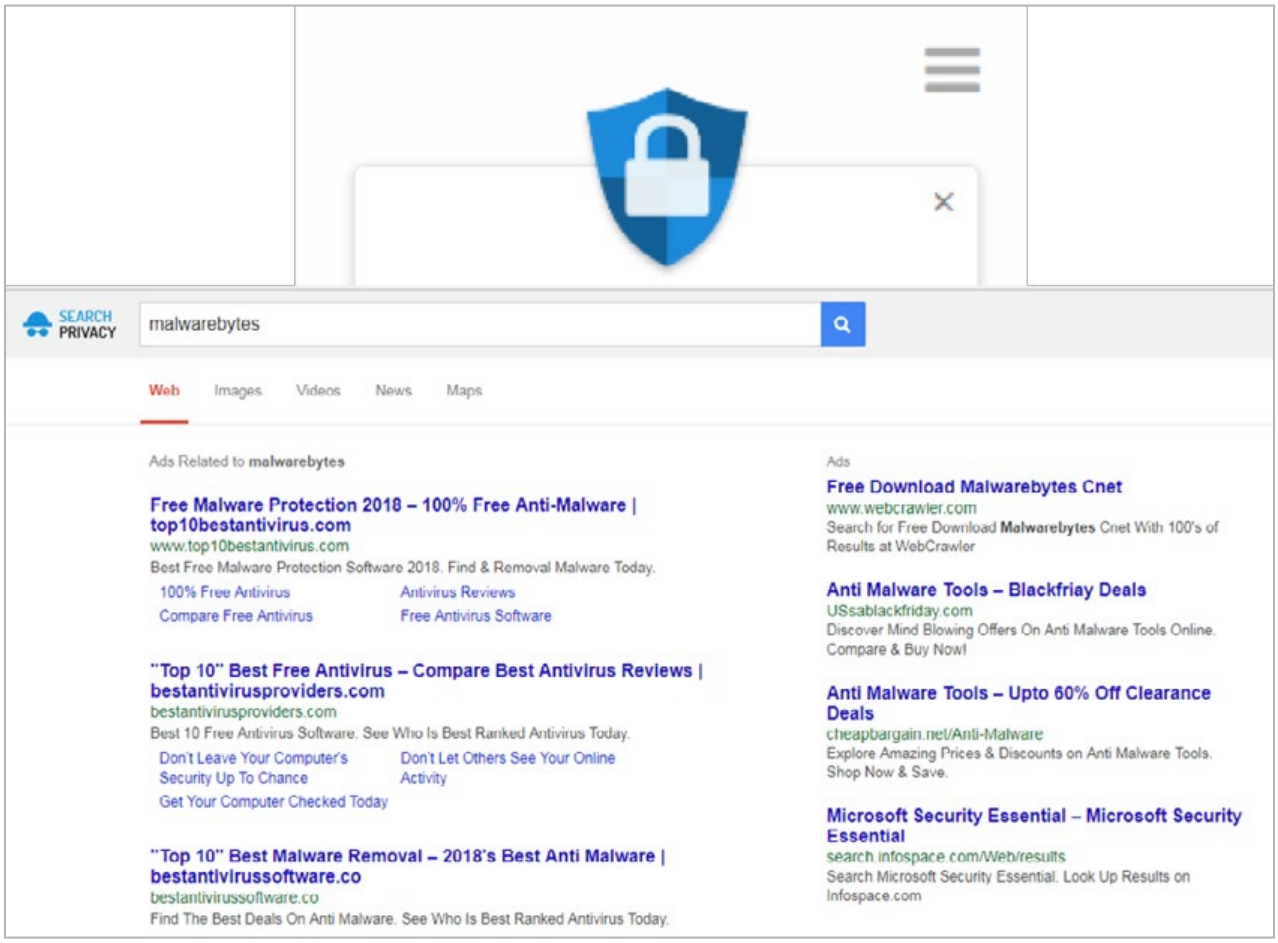


Figure 23. Rogue search extension claims to protect privacy but instead serves up adware.

MobiDash, a stealthy Android malware

MobiDash is a form of adware that displays ads after a typical wait period of three days when installed on an Android alongside an app. This quarter, MobiDash returned with some new stealth features to make removal more difficult than a typical adware install.

On mobile, the device owner must give permission for the app to obtain device administrator rights upon install. This often happens alongside a list of permissions requested, and many people will simply click "Allow" without reading and realizing what each individual permission means.

Figure 24. Once users realize this is adware, they can't easily uninstall it.

Once the permission is granted, it cannot be removed without first removing it from the device administrator list. This sounds simple enough, except the entry for the program is essentially blank and would again be missed by many users.

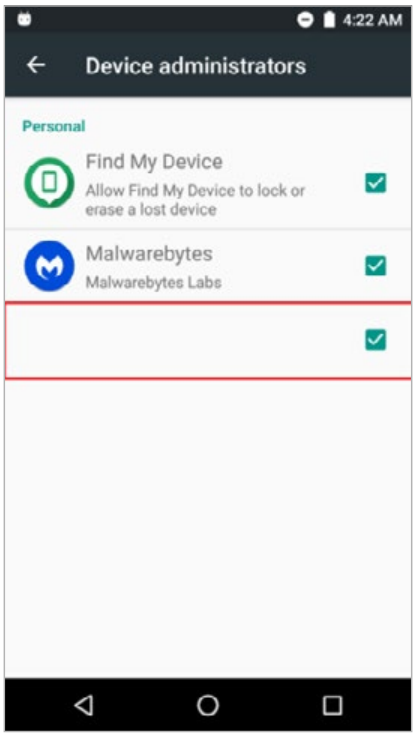


Figure 25. The adware has obfuscated its own entry in the device administrators list.

This is an incredibly deceptive technique and it ensures device owners would be plagued by impossible-to-remove advertisements. Even an attempt at manual removal would be hindered by the shortcut icon being disguised as a Settings option.

When high-level permissions such as device administrator are granted by the device owner, it's almost impossible to remove even with the assistance of dedicated removal tools. This marks another shift toward making adware as difficult as possible to extract from a device, in the same way adware programs used to operate back in the "bad old days" when desktop adware vendors did everything they could to remain on a system.

In summary, this quarter has been a mixture of tricky tactics to confound device owners, offering "increased privacy" as ironic bait for those on the lookout for secure searches and fake ad blockers that do little to bar serving ads. The reliance on using the illusion of security and blocking to fool people into installing adware is a worrying trend that we hope will quickly pass.

Exploit kits

Much has been said about the decline of exploit kits during the past couple of years, and indeed they are no longer the threat that they used to be. However, as we hinted in our Q2 report, one of this year's zero days in Internet Explorer (CVE-2018-8174) has given threat actors enough fuel to keep exploit kits relevant.

In the last few months we witnessed vintage exploit kits that are still in use, containing a mix of old and new vulnerabilities. Another sign that there is interest in drive-by infections is the discovery of new exploit kits, breathing new life into an otherwise struggling space.

Tighter geographic focus

Drive-by download activity has been observed for the most part in the Asia Pacific region, with South Korea and Taiwan being the most affected countries, according to our telemetry. Other researchers have also noted attacks on Japanese users, distributing malware to steal banking credentials.

The browser market share for many of these countries shows that Internet Explorer usage is still much higher than at the worldwide level.

This is a big reason why exploit kits have been relegated as a less potent infection vector in otherwise sought-after geolocations, such as North America. The domination of Google Chrome and user migration toward Windows 10 have changed the playing field when it comes to web-based attacks.

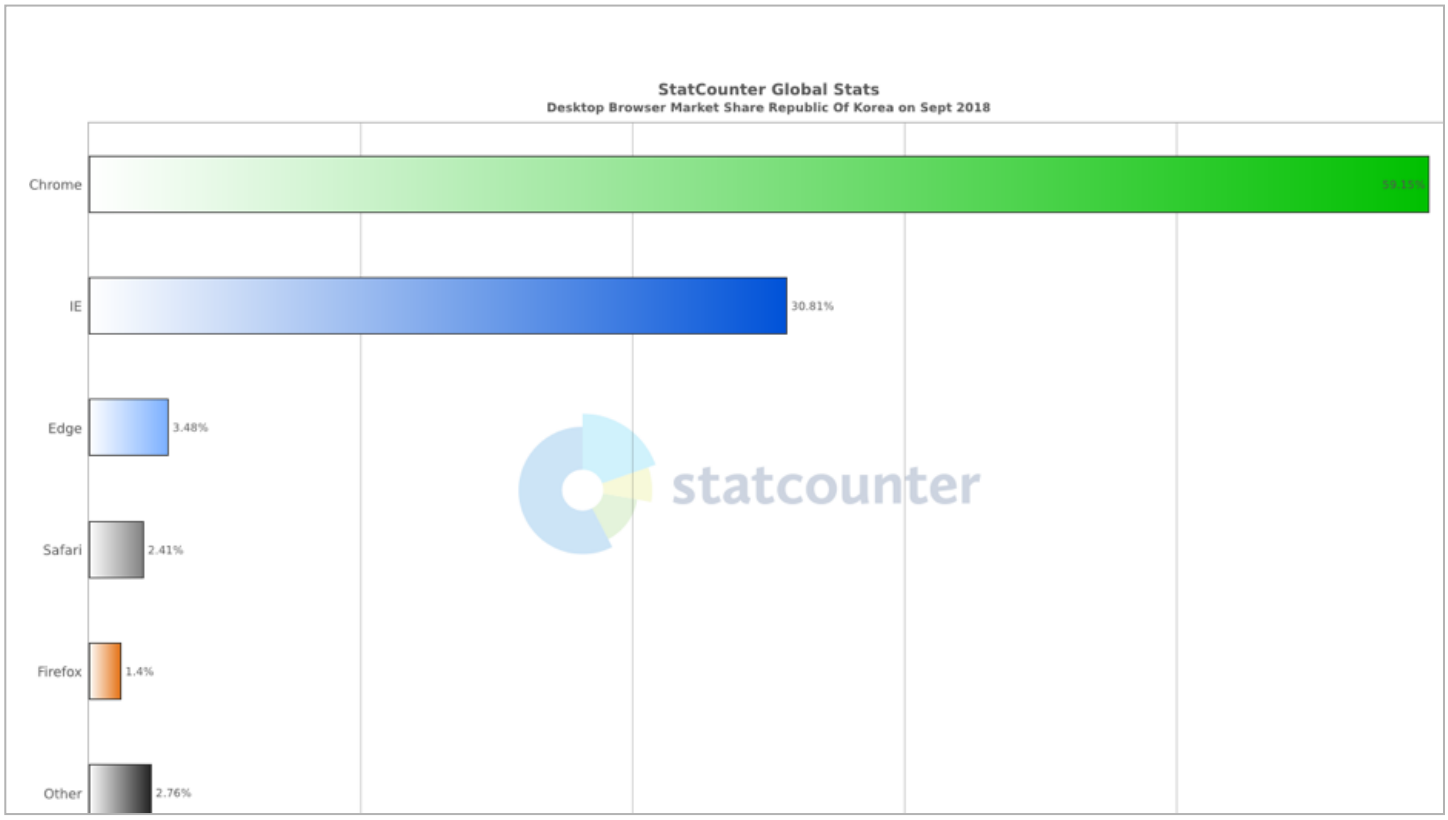


Figure 26. Browser market share in South Korea (courtesy of StatsCounter)

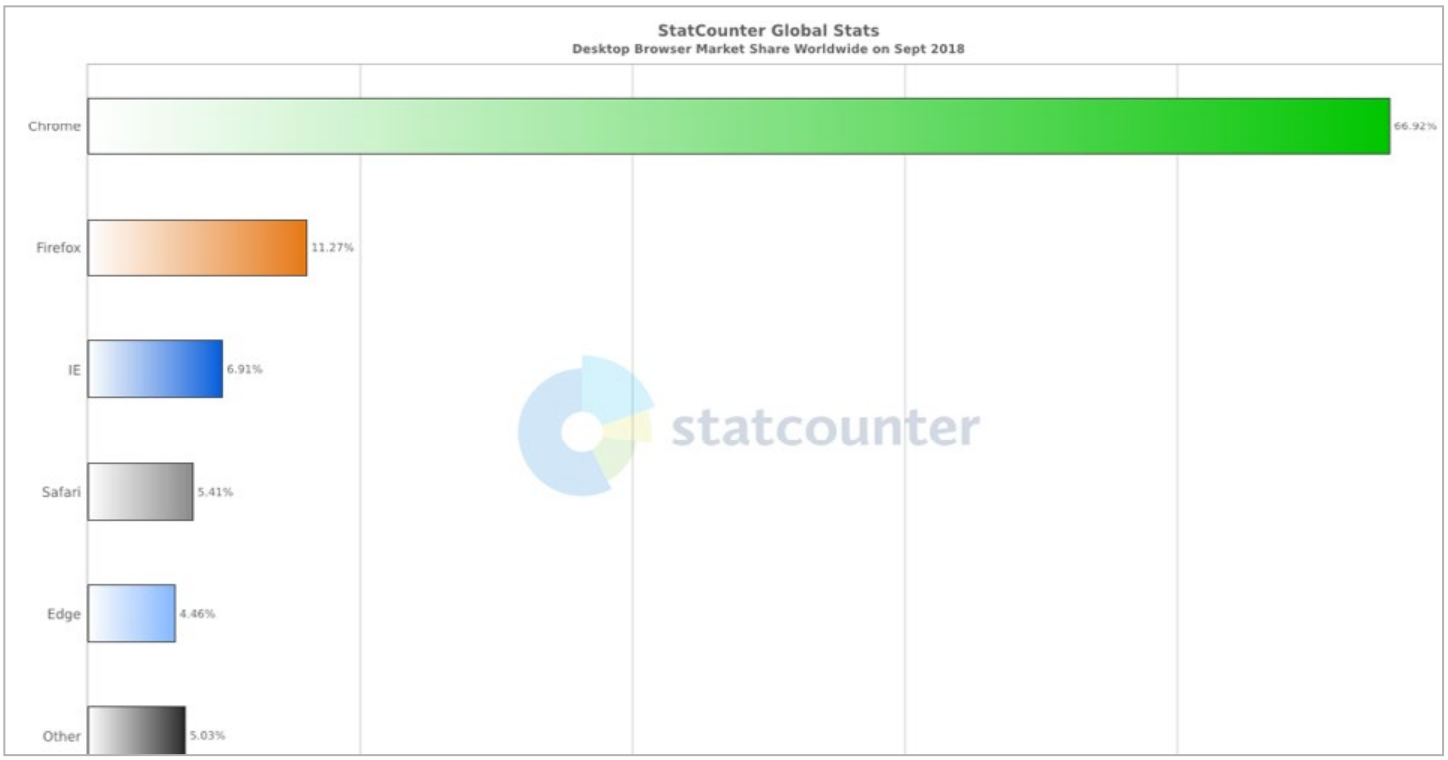


Figure 27. Global browser market share

Vulnerabilities

Identical to the previous quarter, the main vulnerabilities present in exploit kits have been focused on Internet Explorer—particularly the VBScript engine—and Adobe Flash Player.

CVE-2018-8174 and CVE-2018-4878 are the most popular due to their ease of implementation (proof of concepts are available), as well as having a surprisingly long shelf life.

It's interesting to note that another VBScript Engine zero-day was found in August (CVE-2018-8373), but has yet to be targeted by exploit kits.

Exploit kits and CVEs (September 2018)			RIG EK	GrandSoft EK	Magnitude EK	GF Sundown EK	KaiXin EK	Underminer EK	Fallout EK
Internet Explorer	CVE-2016-0189	9 to 11		x			x		
	CVE-2018-8174	VBScript engine	x		x		x	x	x
Edge	CVE-2016-7200	Chakra JS engine					x		
Flash Player	CVE-2015-3105	up to 18.0.0.160					?		
	CVE-2015-5119	up to 18.0.0.194							
	CVE-2018-4878	up to 28.0.0.137	x			x		x	x
Java	CVE-2011-3544	JRE 7 and 6 Update 27					x		
	CVE-2012-4681	SE 7 Update 6					x		
	CVE-2013-0422	7 Update 10					x		

Figure 28. Table showing vulnerabilities by CVEs used by exploit kits in September 2018

New exploit kits

We observed a new threat in July that was using a drive-by framework to deliver a cryptocurrency miner in a rather novel way. This was later named the Underminer exploit kit, and its origins and activity could be traced back to fall 2017, with a special focus on Chinese users.

In contrast to many other exploit kits, this one made clever use of encryption and communication with the backend server to deliver the exploit only once and prevent attack replays from saved packet captures. This reminded us of the powerful exploit kits of the past such as Angler, Nuclear, and Astrum, which abused the Diffie-Hellman key exchange protocol in similar ways.

A truly new exploit kit named Fallout came out at the end of August. Discovered by Team nao_sec, Fallout tries to draw some attention by registering domain names mocking security researchers. Apart from that, Fallout EK has implemented the most recent exploits available on the market to offer yet another malware infection vector to its potential buyers.

While initially detected via Japanese-bound traffic, we have been recording other geolocations similar to what we see with the RIG EK, suggesting that there are already different operators of this exploit kit. While it might still be too early to say, Fallout EK is looking to take the top spot from its rivals.

Although the golden era appears to be over, the presence of several active exploit kits indicates that there is still a demand for such automated infection toolkits. However, instead of being used as the sole weapon, exploit kits are now an additional component of web-based attacks in tandem with social engineering tactics.

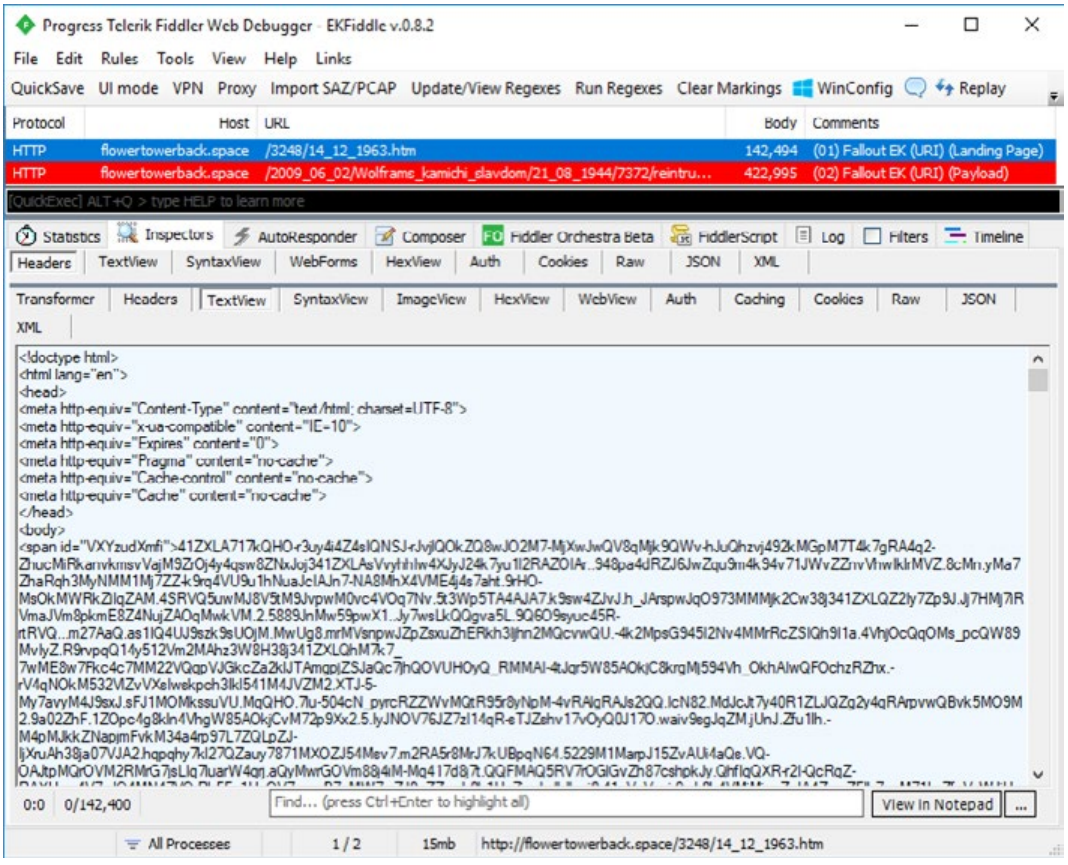


Figure 29. Fallout EK

Scams

For the last few CTNT reports, we've traditionally discussed new attack methods, campaigns, or noticeable trends in fraudulent activity. However, this quarter we wanted to try something new. We wanted to share how the Intel Operations team's efforts in snuffing out scams translates to cold, hard action—whether that's taking down a website (or 10) or serving up a few cease and desists. In addition, we'll cover a large sextortion campaign with a twist: resurrected passwords from ancient breaches.

What has Malwarebytes done for you lately?

Figure 30. Twitter bot spreading fake Malwarebytes technical support numbers

Over the past quarter, Malwarebytes has made efforts in expanding our enforcement actions against tech support scammers. In Q3, we successfully executed the following:

- 10 takedowns of websites impersonating Malwarebytes, or selling fake keys
- 41 takedowns of YouTube videos promoting tech support scams or keygens
- 4 cease and desists to unauthorized resellers
- 4 takedowns of Twitter accounts impersonating Malwarebytes
- 3 PUPs blacklisted based on fraudulent tactics of their support staff
- 105 sting calls to various tech support scammers, predominantly those impersonating Malwarebytes support

While takedowns are an ongoing process, we expect to continue to press hard against scammers in Q4, making sure customers get the real thing when they look for Malwarebytes support.

Sextortion

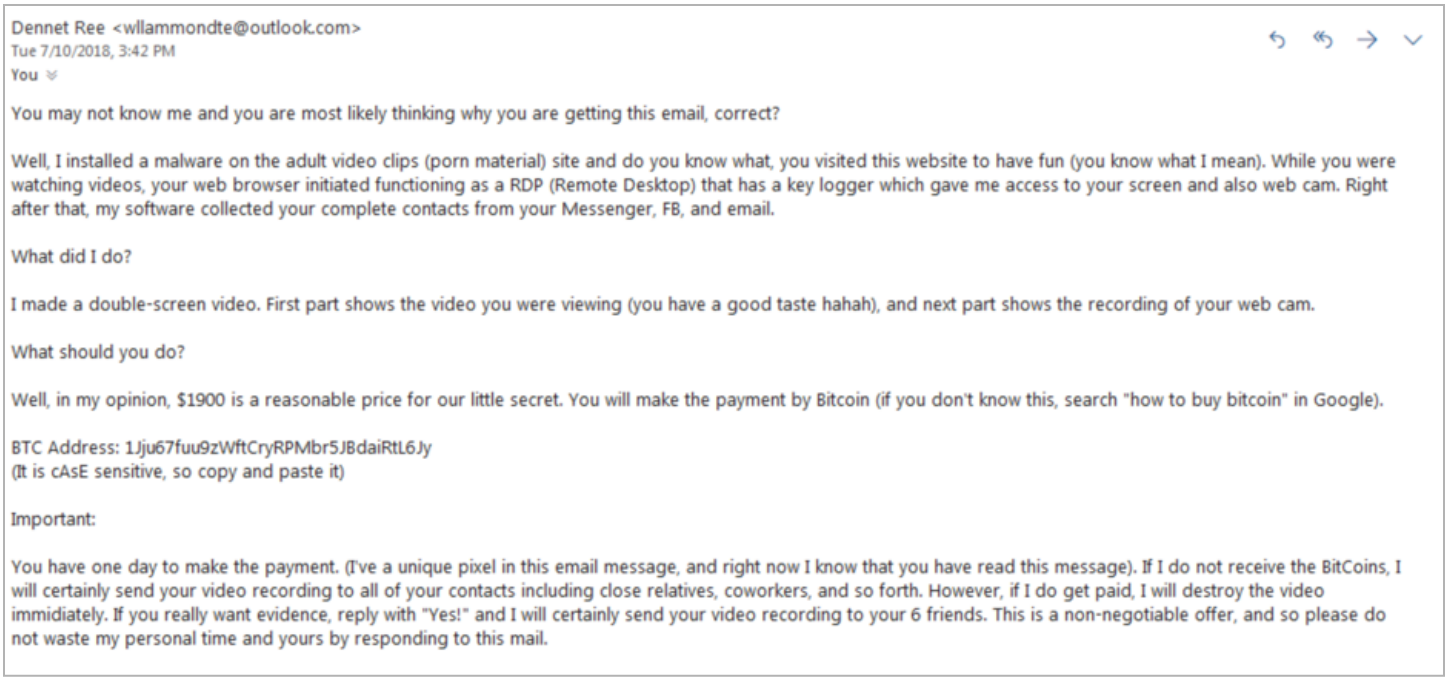
In early July, an extortion scam campaign attracted our notice due to its large scale and unique twist. Unlike traditional sex-based extortion scams, this email campaign came with a user's password as a sign that the sender had "hacked" the victim. These credentials came from a variety of past high-profile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


Список файлов в базе:

```
2017-08-07:
cadd71d0757703a6d8ec4186a59aec2342206fbd115ed3b30
e79cd64b7b385ee ./inputbreach/100.txt 113M
2017-08-07:
927d5a5c539542e63afa2d4069c3be0adfca815bc1fb54bef
01e8586143f33e9 ./inputbreach/101.txt 305M
2017-08-07:
df7aab5b9c1db76ca4ed101170dc4a98bf9dc5dec7ca080ff
a4a8f7f14758980 ./inputbreach/102.txt 96M
2017-08-07:
0b11afcbaacf190f42a43d3fcaa081d3de2f893a4fe8a30da
6908b639d2e01cd ./inputbreach/103.txt 101M
2017-08-07:
a65465ec2021f6c2bcb64e6db62dedb352c855931d24ed26f
a2464aa3cf62a27 ./inputbreach/104.txt 135M
2017-08-07:
b3d47b685e949ec1eb384d49d05c811520da000b9bab6723e
100ce360c21fb9e ./inputbreach/105.txt 183M
2017-08-07:
4a329979b0bf0cd460eb4d9fab892e17a4e54c26cd90a2c7c
f3cf8e0cf43cce2 ./inputbreach/106.txt 317M
```

Figure 31. Cybercriminals advertise torrented dumps of stolen personal information.


Dennet Ree <wllammondte@outlook.com>
Tue 7/10/2018, 3:42 PM
You

You may not know me and you are most likely thinking why you are getting this email, correct?

Well, I installed a malware on the adult video clips (porn material) site and do you know what, you visited this website to have fun (you know what I mean). While you were watching videos, your web browser initiated functioning as a RDP (Remote Desktop) that has a key logger which gave me access to your screen and also web cam. Right after that, my software collected your complete contacts from your Messenger, FB, and email.

What did I do?

I made a double-screen video. First part shows the video you were viewing (you have a good taste hahah), and next part shows the recording of your web cam.

What should you do?

Well, in my opinion, $1900 is a reasonable price for our little secret. You will make the payment by Bitcoin (if you don't know this, search "how to buy bitcoin" in Google).

BTC Address: 1Jju67fuu9zWftCryRPMbr5JBdaiRtL6Jy
(It is cAsE sensitive, so copy and paste it)

Important:

You have one day to make the payment. (I've a unique pixel in this email message, and right now I know that you have read this message). If I do not receive the BitCoins, I will certainly send your video recording to all of your contacts including close relatives, coworkers, and so forth. However, if I do get paid, I will destroy the video immidiately. If you really want evidence, reply with "Yes!" and I will certainly send your video recording to your 6 friends. This is a non-negotiable offer, and so please do not waste my personal time and yours by responding to this mail.

Figure 32. Example of sextortion email phish

Predictions

We predicted last quarter that the threat landscape would be different this time around, and we weren't off base on that prediction. Now that we have seen the beginning of the next wave of threats, we can expect a doubling down of these same efforts by cybercriminals through the rest of the year. Here's where we think trends are leading in Q4:

GandCrab is going to make waves and bring other ransomware families with it to the limelight.

This quarter saw a lot of evolution for the GandCrab ransomware. That kind of activity doesn't go unnoticed, and we believe there will be a greater call for more ransomware families available to greedy criminals. This could signal the return of ransomware—or at least the beginning of the return.

Exploit Kit activity will be rekindled.

With a new VBScript vulnerability in the wild, criminals may pick it up and start running. We could see more activity in Q4 2018 than we've seen in over a year! Ransomware may become one of the major malware types distributed by this new generation of exploit kits. However, it's fileless malware that will take center stage as the primary threat delivered by EKs, as they are difficult to detect and remediate.

Cybercrime is going to spike through October and November, but plateau or slightly drop near the end of the year.

As summer comes to a close, historically we have seen greater activity from cybercriminals during October and November. Taking it easy during the holidays seems to be universal. Cybercriminals are people, too.

Heavy distribution of information-stealing malware will continue.

Distributing info-stealers, such as Emotet and Trickbot is a proven method of attack and doesn't require user interaction to get paid. Policies like GDPR protect user data more than ever before, making it more difficult to obtain by criminals. Therefore, it may be a better investment to steal data and sell it to other criminals (like the old days) than trying to extort users for ransomware payments.

Process Dopplegänging and EternalBlue exploits are going to become commonplace for delivering tomorrow's malware families.

The trends in malware development are clear: Malware families of the future will do whatever they can to both spread quickly and be difficult to detect and remove. May 2017 saw WannaCry, the first instance of malware using leaked NSA exploits. Shortly after, we started seeing the same exploits show up in other families of malware. Now, many of the top malware families currently in the wild are putting these exploits to use in an attempt to spread to more victims.

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

However, we're curious to see what happens with miners on business networks, where you can obtain numerous nodes for your miners from one infection. A focus on business victims for miners is a double-edged sword. On the one hand, you've got a group of systems waiting to be used as miners. On the other hand, there are more eyes and usually more security tools keeping an eye on those systems, so an infection hanging around for a long enough time to be profitable seems less likely.

We will see a decline in adware being installed on Windows desktops and a rise in adware detections on mobile and through malicious browser extensions.

We've been fighting the same kinds of adware on desktops for years. Now the bad guys have thrown down the gauntlet and are moving on to different platforms, with the hope that security vendors won't be as quick to follow. (In our case, they hoped wrong.)

Attackers are going to come up with some creative methods of using stolen personal information from breaches for social engineering campaigns.

All the personal information we freaked out about losing with Equifax and Facebook and Spotify and basically every year since 2013 may now be used to trick the same victims into clicking, downloading, or paying for something. As with the sexploitation malicious emails in this quarter, we can promise that similar data will be used with the same intent in the near future.

In our opinion, there are a lot of security concerns to look out for in Q4, but as long as you've got a comprehensive security solution, use basic security best practices, and remember to update software you will be prepared.

Conclusion

Q3 2018 proved that more and more cybercriminals are willing to put on their big boy pants and put their software to the test in a much larger arena—whether that's going toe to toe with businesses who have more robust security practices (but much juicer, profitable targets) or spreading out into new geolocations. The big story here is how many different malware authors (and thus different families and categories of threats) turned their attention at once to organizations, leaving their experimentation to the consumer side.

However, consumers shouldn't be lulled into a false sense of confidence. Continued evolution for ransomware variants, social engineering scams, and rogue browser extensions spells trouble ahead. All this to say: strap into your seatbelts, kids. It's going to be a bumpy Q4.

Contributors

Adam Kujawa: Director of Malwarebytes Labs

Wendy Zamora: Head of Content, Malwarebytes Labs (editor-in-chief)

Jovi Umawing: Senior Content Writer (editor)

Jerome Segura: Head of Investigations, Malwarebytes Labs

William Tsing: Head of Operations, Malwarebytes Labs

Adam McNeil: Senior Malware Analyst

Pieter Arntz: Malware Analyst

Chris Boyd: Malware Analyst