Cybercrime tactics and techniques Q1 2019

Provided by

Malwarebytes LABS

Contents

Executive summary

Enterprises, beware. Threat actors are continuing to eye businesses for high returns on investment in Q1 2019, breaching infrastructure, exfiltrating or holding data hostage, and abusing weak credentials for continued, targeted monitoring. From a steadfast increase of pervasive Trojans, such as Emotet, to a resurgence of ransomware lodged against corporate targets, cybercriminals are going after organizations with a vengeance.

Yet every cloud has a silver lining, and for all the additional effort thrown at businesses, consumer threats are now on the decline. Ransomware against consumers has slowed down to a trickle and cryptomining, at a fever pitch against consumers this time last year, has all but died. Interestingly, this has resulted in an overall decline in the volume of malware detections from Q4 2018 to Q1 2019.

While threat actors made themselves busy with challenging new victims, they ensnared targets in the old ways, using tried-and-true malspam and social engineering tactics for distribution, including spear phishing emails and sextortion scams. However, a few noteworthy developments in exploit kits and software vulnerabilities opened the door for interesting experimentation, including a Chrome zero-day that required user action for patching.

Unfortunately, cybercriminals didn't forget about consumers altogether—adware on Macs and mobile devices was rampant this quarter, with supply chain attacks resulting in malicious apps loading pre-installed on mobile phones.

And although businesses are the new black, user data in the form of Personally Identifiable Information (PII) is still the prize, as data leaks via weak third-party security or password hygiene revealed full-fledged breaches were not necessary to bring criminals their pay day. As businesses gather and compile more data about their customers, they become ever-more attractive targets, especially as weak credentials, broad user access, and gaps in infrastructure allow threat actors to practically stroll into many organizations and take with them their customers' database.

To that end, consumers are taking notice, and increasingly growing wary of trusting businesses with their PII. A survey conducted by Malwarebytes this quarter shows that more than 90 percent of nearly 4,000 respondents feel securing their data is of highest importance—yet they trust organizations, especially social media and search engines, about as far as they can throw them. Because of this shift in tactics by criminals and the resulting anxiety it's producing for consumers, we are adding a new section to our report about data privacy, looking at trends in data storage, transfer, exfiltration, and regulation, and exposing pitfalls that may lead to theft of user data.

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 January 1 through March 31, 2019, from our Intelligence, Research, and Data Science teams with telemetry from both our consumer and business products on the PC, Mac, and mobile devices, which are deployed on millions of machines. Here's what we learned about cybercrime in the first quarter of 2019.

Key takeaways

Businesses are still the prime target.
Overall detections of threats to businesses have steadily risen, while consumer threats have dropped off. Business detections increased by about 7 percent from the previous quarter, while consumer detections declined by nearly 40 percent, resulting in an overall dip in malware volume of 35 percent quarter over quarter. Compared to Q1 2018, business detections have skyrocketed 235 percent, with consumer detections dropping 24 percent year over year. This reinforces the observed trend of cybercriminals focusing more on business targets today.

Emotet shows no signs of stopping.
Emotet, the most fearsome and dangerous threat to businesses today, has made a total shift away from consumers, reinforcing the intent of its creators to focus on enterprise targets, except for a few outlier spikes. Detections of Trojans (Emotet's parent category) on business endpoints increased more than 200 percent from the previous quarter, and almost 650 percent from the same time last year.

Ransomware is back to business.
Ransomware has made a tremendous comeback against business targets in Q1 2019, with an increase of 195 percent in detections from Q4 2018 to Q1 2019. In comparison to the same time last year, business detections of ransomware have seen an uptick of over 500 percent, thanks in large part to a massive attack by the Troldesh ransomware against US organizations in early Q1.

Consumer detections of ransomware died down.
Meanwhile, ransomware consumer detections have continued to drop, despite activity by families such as GandCrab, which primarily targeted consumers over the last quarter as it switched to a ransomware-as-a-service and began brute-forcing RDP to infiltrate systems. Consumer detections of ransomware decreased by 10 percent quarter over quarter, and by 33 percent year over year.

Cryptomining against consumers is essentially extinct.
Marked by the popular drive-by mining company CoinHive shutting down operations in early March, consumer cryptomining seems to have gone the way of the dodo. Detections of consumer-focused Bitcoin miners have dropped significantly over the last year and even from last quarter, while business-focused miners have increased from the previous quarter, especially in the APAC region.

Adware in Macs and mobile devices was problematic.
While all Mac malware saw a more than 60 percent increase from Q4 2018 to Q1 2019, adware was particularly pervasive, clocking in at over 200 percent from the previous quarter. Mobile adware detections also trended upward, as supply chain attacks delivered malware pre-installed on mobile devices. However, overall adware detections were fewer in Q1 2019 than they were during the same time period last year.

Exploit authors developed some attention-grabbing techniques.
A new Flash Player zero-day was discovered in Q1 and quickly implemented into popular exploit kits, including Underminer and Fallout EK, as well as a new exploit kit called Spelevor. In addition, a Chrome zero-day required users to take action, fully shutting down and restarting their browser in order to patch the vulnerability. Finally, the popular software WinRAR was being used to deliver payloads to users.

As attacks against businesses ramped up, user trust in businesses to protect their data reached a new low.
In a survey conducted by Malwarebytes in Q1 2019 of nearly 4,000 respondents, users expressed deep concerns about abuse, misuse, and theft of PII, especially from social media and search engine companies. In a new section of our Cybercrime Tactics and Techniques report, we examine how cybercriminals found success by exploiting infrastructure weaknesses, gaps in policy and regulation, and even corporate negligence to not only walk away with valuable data, but establish persistence within the network.

Malware

In the first quarter of 2019, we saw an overall decline in malware detections. This is primarily due to a shift in the focus of cybercriminals to business targets as opposed to consumers. As a result, we observed a decline of 35 percent of total detections this quarter compared to the previous quarter.

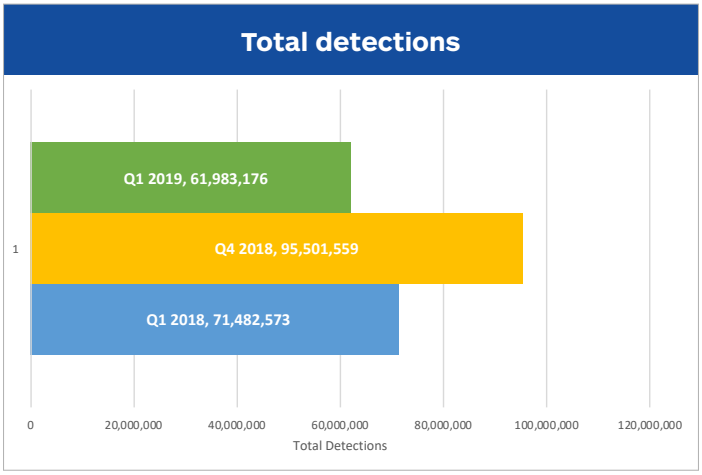

Figure 1. Total malware detections in Q1 2019

Despite a drop in overall detections, businesses have been grappling with a steady increase in malware volume and rate over the last year. While we observed only a seven percent increase in business detections from Q4 2018, detections amped up an astonishing 235 percent year over year. This is likely because some persistent families, such as Emotet, have focused their attacks away from consumers and onto organizations.

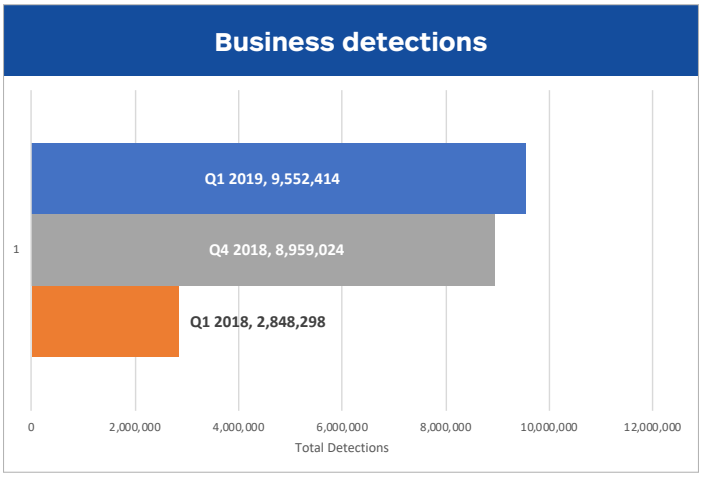

Figure 2. Total malware detections slightly increase for businesses in Q1

Taking a deeper dive into the business malware categories we observed, Trojan malware has increased over 200 percent from the previous quarter and almost 650 percent from the same time last year. Once again, this increase is due to families, such as Emotet, TrickBot, and other information-stealing malware that we classify as Trojans. In addition, we see an uptick in adware and ransomware, but a significant drop in backdoor and hijacker malware from the previous quarter.

Business detections				
Q1 2019	Malware category	Threat count	Q4 2018 %	Q1 2018 %
1	Trojan	4,703,567	222%	649%
2	Generic	1,039,442	-18%	111%
3	Adware	954,674	153%	375%
4	MachineLearning/ Anomalous	895,699	147%	NEW
5	Backdoor	475,314	-80%	485%
6	RiskwareTool	389,357	45%	56%
7	Ransom	336,634	189%	508%
8	Malware	263,035	NEW	NEW
9	Hijacker	91,466	-73%	-69%
10	Exploit	76,784	76%	NEW

Figure 3. Top 10 Malwarebytes detections for businesses

The drop in these categories is likely due to a massive decline in the campaign of Backdoor.Bot in the APAC region between Q4 2018 and Q1 2019. Hijacker detections are usually an indication that other malware is making changes to the system. In this case, we can say that the decline in hijackers is likely due to less backdoor malware.

On the consumer side, we watched as nearly 40 percent of malware detections vanished between quarters. Year over year, the change was a less dramatic but still noticeable 25 percent.

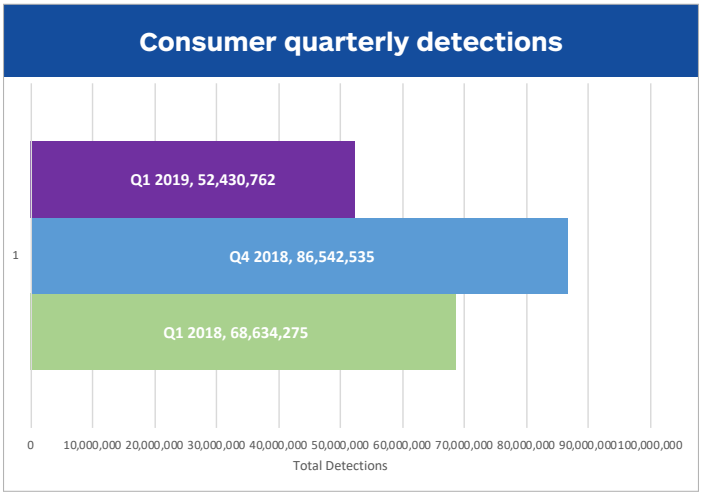

Figure 4. Total malware detections decrease for consumers in Q1

No one specific category of malware is responsible for the drop in consumer detections, as we observed declines in detections of nearly all of our top 10 malware types this quarter. This includes a significant decrease of over 60 percent by Trojan and backdoor categories. As far as miners go, the decline in detections matches with the decline in value of cryptocurrency, as it did back in 2018.

Consumer detections				
Q1 2019	Category	Threat count	Q4 2018 %	Q1 2018 %
1	Adware	15,283,211	-26%	12%
2	Generic	10,269,367	32%	4%
3	Trojan	9,886,157	-61%	-34%
4	RiskwareTool	4,076,250	-32%	-67%
5	Backdoor	2,278,733	-65%	85%
6	MachineLearning/ Anomalous	1,710,503	-21%	221%
7	HackTool	1,543,912	1%	18%
8	MisplacedCertificate	1,214,708	New	New
9	OSX	1,187,836	30%	New
10	Spyware	761,510	-11%	95%

Figure 5. Top 10 Malwarebytes detections for consumers

Overall, the indication that the focus of cybercriminals is shifting to businesses has never been more obvious. This is a good sign for consumers, who are tired of dealing with sophisticated threats like ransomware and worms, however the opposite goes for businesses, who are charged with protecting our data.

The most vulnerable business targets are those of small and medium size (SMBs), whom our study last year on The State of Ransomware Among SMBs demonstrated are battling the same number of threats but with the fraction of the security budget of a large enterprise corporation. Combine lack of resources and increasing threats, and you have the recipe for a ripe season of cybercrime.

Regional breakdown

Stepping back from specific categories of malware, we take a look at threat detections based on region, specifically Asian Pacific (APAC); Europe, the Middle East, and Africa (EMEA); North America (NORAM); and Latin America (LATAM).

APAC

#	Consumer	Business
1	Trojan	Trojan
2	Adware	Backdoor
3	Generic	Adware
4	RiskwareTool	Ransom
5	Backdoor	Malware
6	MachineLearning	Exploit
7	HackTool	Generic
8	Virus	RiskwareTool
9	Worm	Virus
10	Ransom	HackTool

EMEA

#	Consumer	Business
1	Adware	Trojan
2	Generic	Generic
3	Trojan	Adware
4	RiskwareTool	RiskwareTool
5	Backdoor	MachineLearning
6	MachineLearning	Backdoor
7	HackTool	Hijacker
8	MisplacedCertificate	MisplacedCertificate
9	Worm	HackTool
10	Spyware	Worm

NORAM

#	Consumer	Business
1	Adware	Trojan
2	Generic	MachineLearning
3	Trojan	Generic
4	RiskwareTool	Adware
5	OSX	Ransom
6	Ransom	Malware
7	HackTool	RiskwareTool
8	Backdoor	Backdoor
9	Spyware	Spyware
10	Rogue	Hijacker

LATAM

#	Consumer	Business
1	Adware	Trojan
2	Trojan	Generic
3	Generic	Adware
4	RiskwareTool	MachineLearning
5	HackTool	RiskwareTool
6	Backdoor	Backdoor
7	MachineLearning	HackTool
8	Spyware	Ransom
9	MisplacedCertificate	Worm
10	Worm	Spyware

Figure 6. Top 10 Malwarebytes detections for both business and consumer per region

Notable takeaways from this chart include the difference in ransomware rankings between the regions and their business and consumer detections. For example, ransomware is the fourth-most detected threat against businesses in APAC, but is missing from the EMEA rankings. This is due to APAC's continued issues with EternalBlue and its resulting WannaCry infections. In addition, ransomware ranks higher for North American businesses than consumers because of a Troldesh campaign aimed at organizations in the region.

Top countries per region

Each region's various countries battled threats over the last quarter, but some took on higher burdens than others. Not surprisingly, highly populous countries such as the United States and Brazil took top spots for their respective regions. "However, sparsely-populated-but-known-petri-dish-of-malware-development Russia saw the most criminal activity in EMEA. And comparatively-tiny Indonesia swooped up the top spot for APAC.

	APAC	EMEA	NORAM	LATAM
1	Indonesia	Russia	United States	Brazil
2	India	United Kingdom	Canada	Mexico
3	Thailand	France	Puerto Rico	Argentina

Figure 7. Top three countries per region

Breaking down regional barriers, we decided to look at the top 10 countries for global detections. The United States made up nearly half of all Malwarebytes detections, with Indonesia, Brazil, and India taking a distant second, third, and fourth place. The rest of the pie was nearly evenly divided between Russia, the UK, France, the Philippines, and Italy.

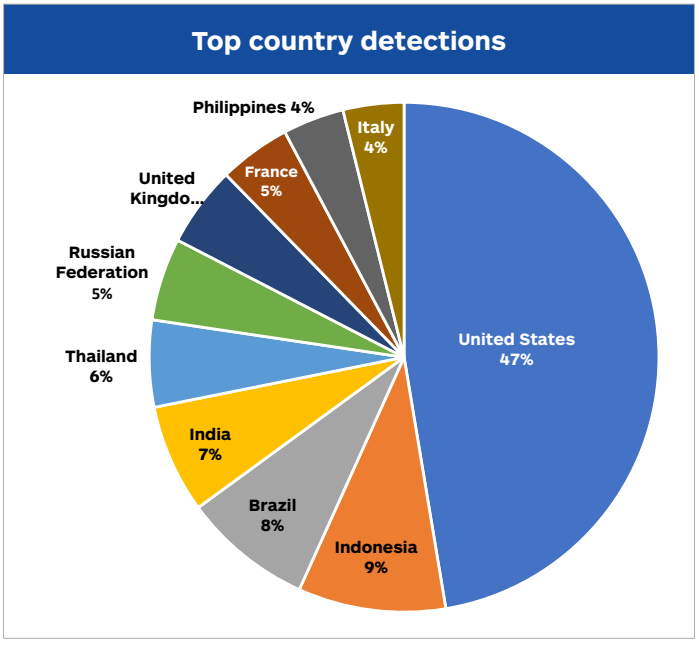

Figure 8. Top 10 detected countries

Trojans

In the world of malware, we can see some favoritism occurring in Q1 2019. While consumers are affected more by adware, Trojans have veered their attention to businesses. In fact, the number of Trojan detections by our products on business endpoints more than tripled, but decreased to less than half on the consumer side.

One of the most prevalent threats detected continues to be Emotet. Not is it only the most common malware, it is also the most invasive and costly to remove. Over the course of the year, its traffic has remained volatile, but looking at longer periods, we can see that the total is still growing. More specifically, we saw a small decrease in Q4 2018 and a big spike in January 2019. Looking at the year-over-year (YOY) statistics, the number of detections grew from 800,000 to 4 million.

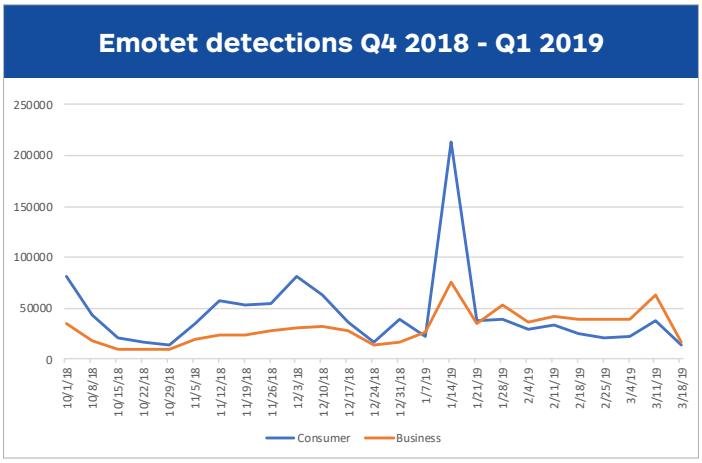

Figure 9. Emotet detections trend line from October 2018 to March 2019

Another persistent Trojan racking up detections in Q1 is TrickBot; its recent revival the result of cooperation with Emotet in multi-pronged attacks.

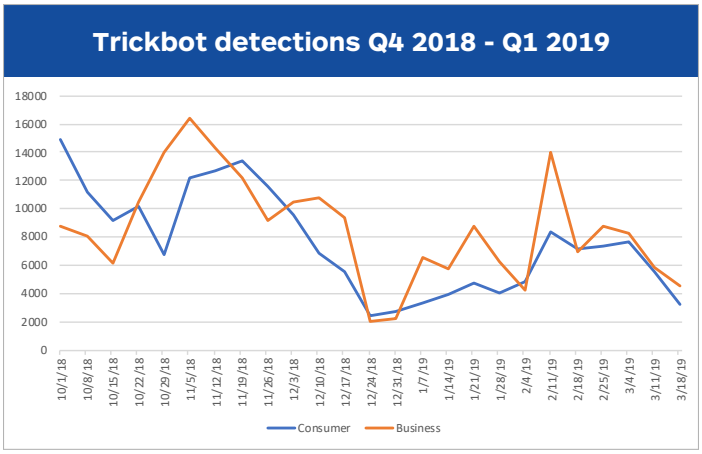

Figure 10. Trickbot detection trend lines from October 2018 to March 2019

As Emotet is designed to be modular, with each component having a designated task—one of which is to be a downloader that retrieves and runs additional malware—other Trojans like TrickBot have tagged along and gotten their money's worth. In fact, the effectiveness and tenacity of Emotet has made it the favorite Trojan downloader for various other malware families, including Ryuk ransomware, an assortment of banking Trojans, and information-stealers alike.

Ransomware

Ransomware authors decided to finally stir up the pot in Q1 2019 after a slow, gradual decline experienced in 2018. Instead of continuing with the same attack pattern, we saw a dramatic rise in the form of a new campaign, even if the ransomware files themselves were less inventive than those in the malware's hey day.

Business and consumer differences

Across the business and consumer sectors, year over year we're down from 12 million detections in Q1 2018 to 4 million in Q1 2019. However, within that dip are some noteworthy changes.

On the consumer side, ransomware was knocked out of the top 10 from its previous steady ranking for several

years running. We also saw a decrease of 10 percent from Q4 2018 to this quarter, and a drop of 33 percent from the previous time last year.

Business ransomware detections, on the other hand, exploded, with nearly 200 percent more ransomware found on endpoints than the previous quarter. In addition, ransomware detections have skyrocketed an incredible 500 percent year over year.

Ransomware	Q1 2019	Q4 2018	% Change	Q1 2018	% Change2
Business	355876	120578	195%	57308	521%
Consumer	482908	538116	-10%	716905	-33%
Total	83874	658694	27%	774213	8%

Figure 11. Ransomware detections for business and consumer Y/Y and Q/Q

Partially responsible for this uptick is a sharp increase in detections for Troldesh, which coincidentally was the top detection for businesses in Q1.

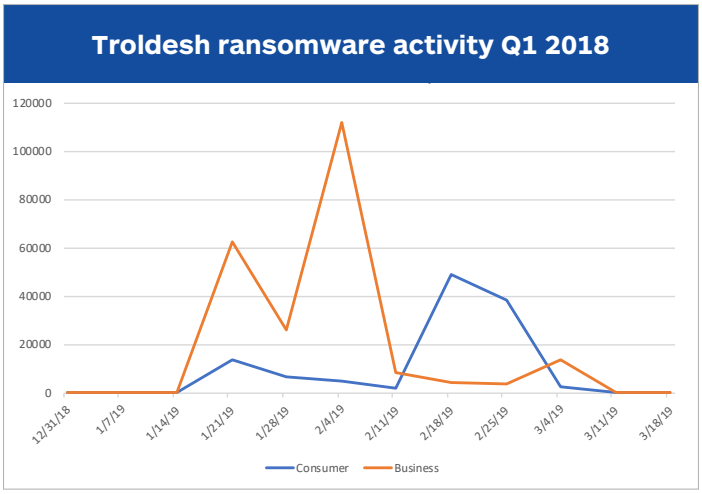

Figure 12. Troldesh trend line from January to March 2019

The significant bump in business ransomware detections can generally be laid directly at Troldesh's door, while most other forms have remained stable, as you can see in the table below.

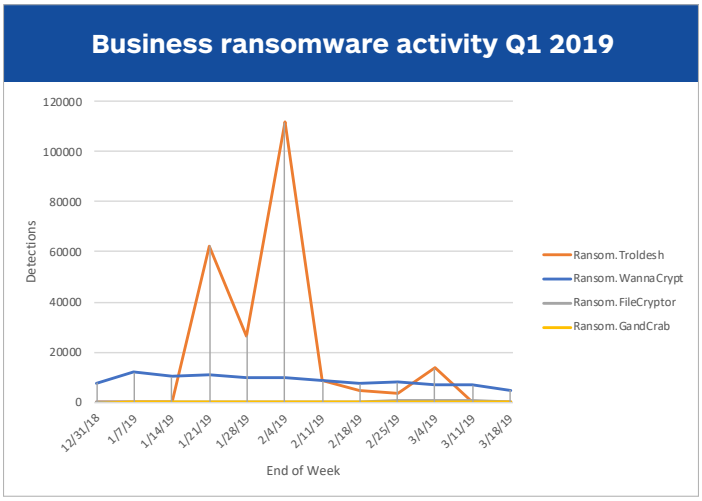

Figure 13. Business ransomware trends from January to March 2019

Troldesh does numbers

In previous reports, we've mentioned how ransomware is no longer the innovative force it once was, instead choosing to rework and update older infections. Troldesh is no exception, having been around since 2014. Despite this, the malware, most likely of Russian origin, still spiked in February 2019 via the crude delivery method of malspam attachment. It also required victims to open the ZIP file and run the JavaScript used to download the malware.

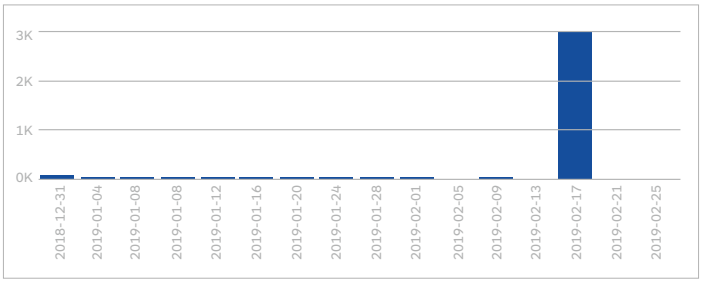

Figure 14. Troldesh spiked in February 2019

Accompanying Troldesh's ransom note were multiple text files to increase the likelihood of victims seeing one. The attack went after many file extensions and drives, whether fixed, remote, or removable.

Figure 15. Troldesh ransomware note written in Russian and English

Top ransomware families

Troldesh didn't quite make the top spot for consumer detections. Instead, it came second to WannaCry, with the ever-present GandCrab lurking in third place.

Meanwhile, targeted attacks from the likes of SamSam haven't gone away. In fact, a degree of innovation is still at the heart of some ransomware attacks in Q1. Case in point, a recent version of Cryptomix Clop made use of digital certificates to distribute rogue files. In much the same way phishers make use of free certificates to make their fake logins look more convincing, these ransomware authors tried a similar tactic. As such, it aided in the appearance of legitimacy, both for end users and (potentially) some security tools.

All in all, ransomware isn't quite firing on all cylinders yet, but this quarter marks a return to form.

Adware (PC only)

Adware detections for businesses are showing a clear upward trend, while consumer detections seem to be holding steady, with an occasional peak. Overall adware detections topped out at over 15 million, which is still a 16 percent decrease from the previous quarter, but a 14 percent increase from the same time period last year.

Q1 2019	Category	#	Q4 2018	Q1 2018
2	Adware	15,639,110	-16%	14%

Malwarenet vendor	Q1 2019	Q4 2018	% Chng	Q1 2018	% Chng2
Adware.Zdengo	1596616	899883	77%	2685	59364%
Adware.Adposhel	468110	311299	50%	124815	275%
Adware.Agent	735959	1061791	-31%	548682	34%
Adware.Csdimonetize	562762	317120	77%	9357	5914%
Adware.Tuto4PC	350137	816141	-57%	295515	18%
Adware.Elex.ShrtCln	673824	918121	-27%	1489929	-55%
Adware.Graftor	1341591	2059291	-35%	602442	123%
Adware.InstallCore	801687	296822	170%	93999	753%
Adware.Yontoo	470365	298320	58%	341602	38%
Adware.DotDo.Generic.TskLnk	481240	703871	-32%	28119	1611%

Figure 16. Top business and consumer adware stats Y/Y and Q/Q

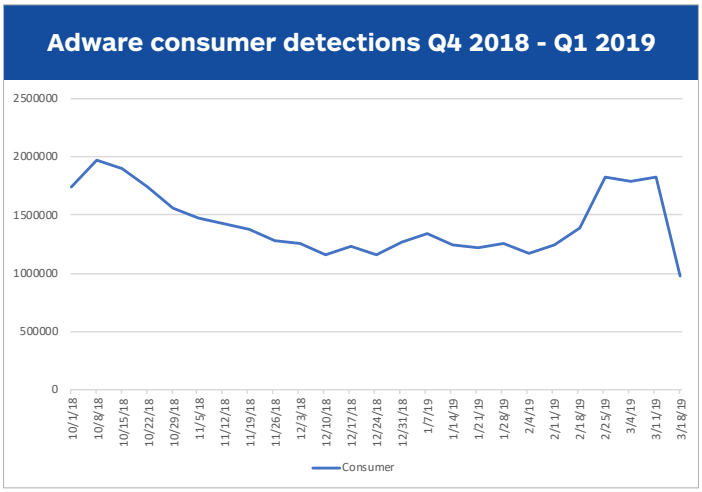

Figure 17. Consumer adware detection trend from October 2018 through March 2019

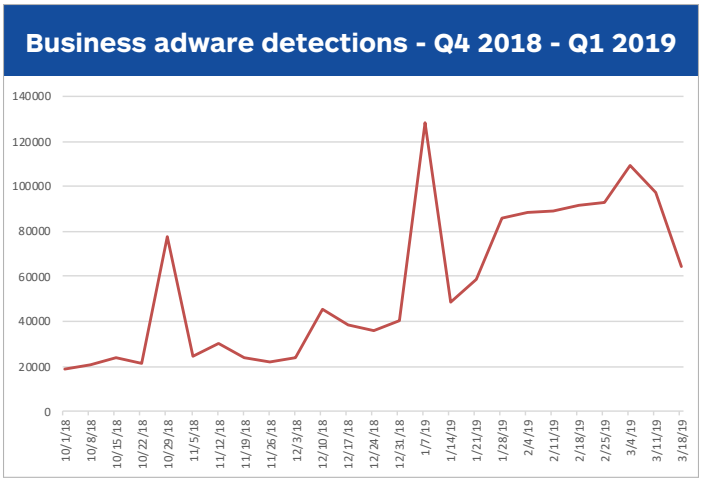

Figure 18. Business adware detection trend from October 2018 through March 2019

The top adware families for Q1 2019 include Zdengo, a large assembly of adware installers and bundlers that saw a 77 percent increase quarter over quarter, and an astonishing 59,000-plus percentage raise year over year. The Zdengo installers promise users a popular functionality and combine the software with one or more Potentially Unwanted Programs (PUPs), as well as an adware component that displays advertisements not originating from the sites they visit.

Graftor, our second-highest adware detection, is another large family that is so aggressive that some of its variants are classified as Trojans. While Graftor detections decreased by 35 percent from last quarter, they've amped up more than 120 percent from the same time last year.

Mac malware and adware

Cybercriminals, not ones to stay content with PC attacks, continued their onslaught against Macs, turning up the heat in Q1 2019 on all threats to the tune of a 62 percent increase quarter over quarter. Adware detections—the vast majority of malware aimed at Macs—increased by 201 percent from Q4 2018 to Q1 2019.

Interestingly, detections of a PUP called PCVARK shot to the top of our Mac malware rankings, while the former top three (MacKeeper, MacBooster, and MPlayerX) have fallen to second, third, and seventh place, respectively. Meanwhile, an adware family detected as NewTab jumped from 60th place to fourth.

Along with a higher volume of Mac attacks, users experienced some devious and novel attack methods in Q1. From open-source code being abused to develop backdoors and cryptomining malware to Windows executables being found on Mac desktops, threat actors put their creativity to good use, taking a bite out of Apple in the process. In fact, while cryptomining continues to decrease across all platforms, Mac users still storing Bitcoin in Electrum wallets might have found themselves fresh out of cryptocash this quarter, as more than US$2.3 million were stolen by cybercriminals that took advantage of a vulnerability in the wallet to serve up Trojanized versions.

Open source

Mac malware and adware is showing an increasing trend toward using open-source Python code. This began back in 2017, with the Bella backdoor being used by a variant of OSX.Dok. It wasn't until late 2018 that this became more widespread, as Mac malware began using a variety of backdoors, such as EvilOSX, EggShell, EmPyre, and a Python reverse shell for Metasploit—all open-source and all written in Python.

Obfuscated Python has become much more common, including those used inside launch agents and daemons:

```
<plist version="1.0">
    <dict>
        <key>Label</key>
        <string>com.xpnsec.escape</string>
        <key>ProgramArguments</key>
        <array>
            <string>python</string>
            <string>-c</string>
            <string>import
sys,base64,warnings;warnings.
filterwarnings('ignore');exec(base64.
b64decode('aWN…pKQ=='));</string>
        </array>
        <key>RunAtLoad</key>
        <true/>
    </dict>
</plist>
```

Figure 19. Code snippet of an obfuscated Python code

On top of these backdoors, several programs—both malware and adware alike—have taken to using an open-source Python program called MITMProxy. This can be used to snoop on all network traffic, including encrypted SSL, with the use of a provided root certificate. Although there are legitimate uses for such tools, when used surreptitiously, it's a man-in-the-middle attack.

How applications like MITMProxy can be used for malicious purposes is obvious. But adware injecting advertisements into web traffic is troubling. Even if the adware itself doesn't abuse these capabilities to steal user data, the installation of such a tool opens the affected computer to abuse by other, more nefarious malware.

Although not built with Python, and recently decreasing in frequency, the open-source XMRig cryptocurrency miner has also been used by Mac cryptomining malware this quarter.

Windows malware on Mac?

We began seeing InstallCapital adware installers in late 2018. They are not particularly remarkable, but they use an interesting new technique that now includes a Windows executable.

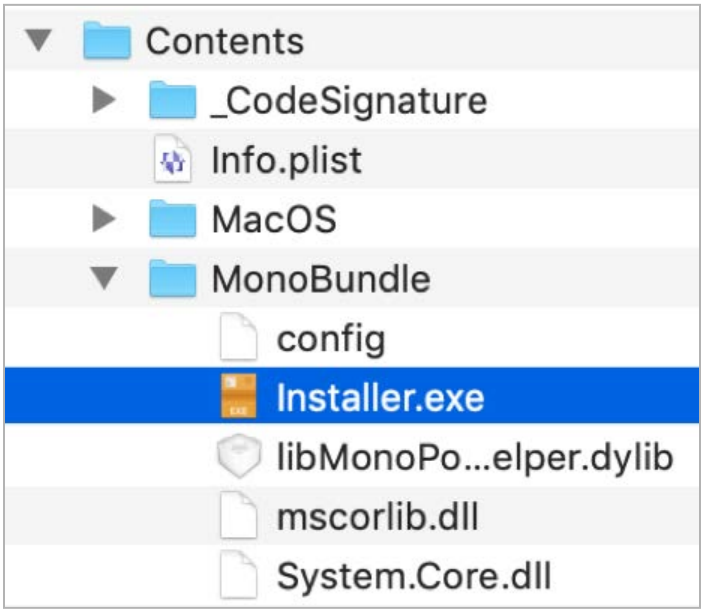

Figure 20. The InstallCapital Mac adware includes…a Windows file?

Normally, Windows executables cannot run directly on the Mac. But thanks to the Mono framework included in the adware installer, Installer.exe can be executed within the installer's context.

There has been much speculation about this being done to bypass Gatekeeper, which is one of the anti-malware features in macOS. However, that is not the case here, as the Mac installer app would already be running—thus, Gatekeeper has already been avoided—long before the executable runs. Also, it would not be related to other anti-malware features in macOS (XProtect and MRT), which do not do generic malware detection. Furthermore, the macOS security features could be updated to detect this adware installer, with or without its Windows executable.

It's likely that the only reason for this Windows executable to be included is simply as an unsophisticated and imperfect approach to avoid having to rewrite the full adware installer code for macOS. It's still worth noting, in case future malware uses Mono for more nefarious purposes.

A Trojanized Bitcoin client

In December 2018, attackers found a vulnerability in the Electrum wallet, a well-known Bitcoin client, that allowed threat actors to inject malicious code in the wallet itself to display arbitrary phishing messages as a pop-up dialog box. This code instructed users to download a security update, which is really a Trojanized copy of Electrum, from several phishing destinations.

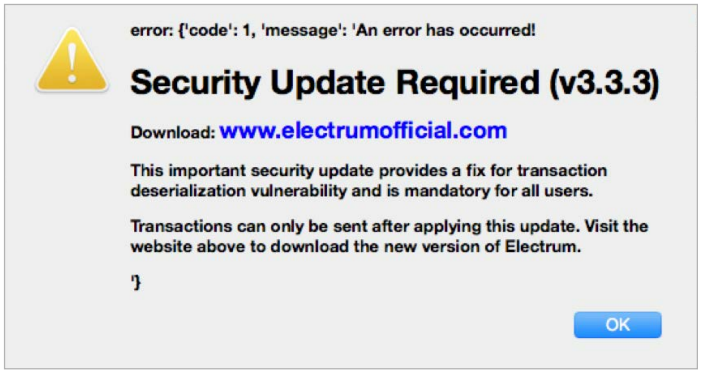

Figure 21. Screenshot of one version of the phishing pop-up message

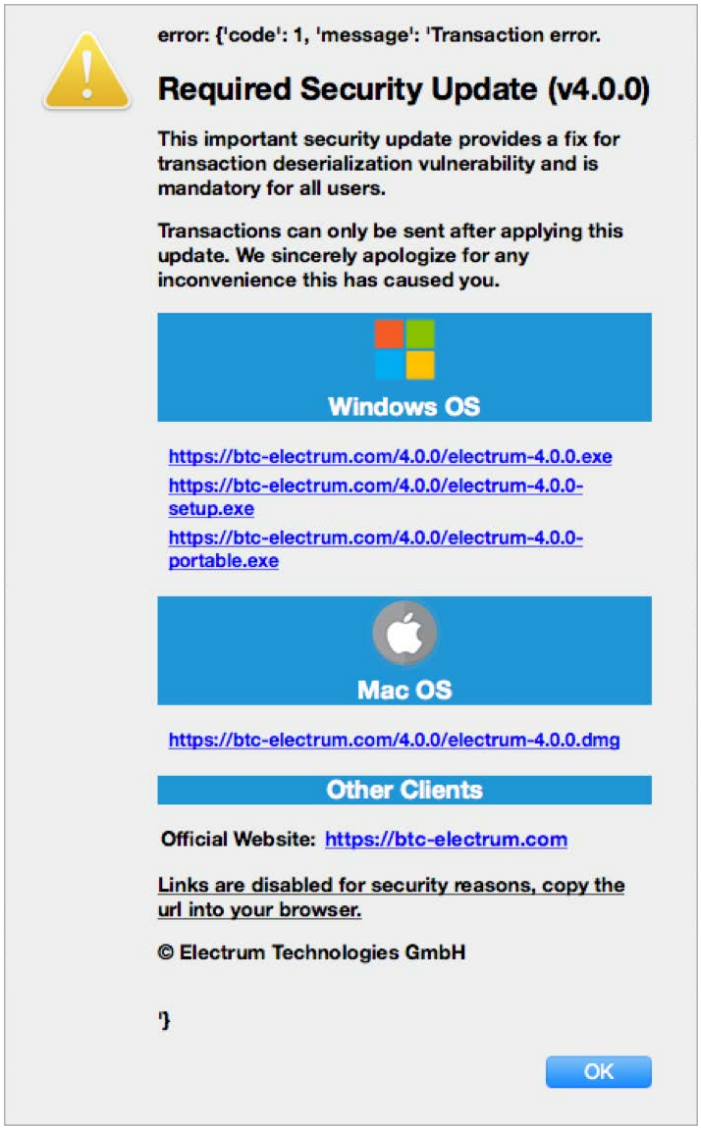

Figure 22. Screenshot of another version of the phishing pop-up message

Once the Trojanized Electrum is installed, it then siphons Bitcoins from owners into a single BTC address. In analyzing the attacker's BTC addresses, we found that they stole a grand total of US$2.3 million in Bitcoins. Mac users were not the only ones affected by this campaign, but also users on the Windows, Android, and Linux platforms.

To solve this problem, Electrum forced its users to

upgrade to versions later than 3.3 to prevent them from getting exposed to the phishing campaign.

Malwarebytes detects the bogus Electrum wallet as OSX.ElectrumStealer.

Mobile malware

This quarter we saw some troubling developments in mobile malware, including an uptick in pre-installed malware on mobile devices, and an adware Software Development Kit (SDK) that briefly went rogue.

Pre-installed mobile malware

Pre-installed mobile malware continues to rise, and it's only become nastier in Q1. As the malware comes loaded with the mobile device, it cannot be removed—only disabled.

A PUP that we detect as Android/PUP.Riskware.Autoins.Fota tops the charts as the most prevalent pre-installed malware on users' devices this quarter. This PUP is a variant of the Adups suite of riskware apps, and it has the potential to auto install other malware apps without user permission or knowledge.

Even worse in Q1, we witnessed pre-installed malware within the code of system apps required for a mobile device to function. This includes discovering a riskware auto installer in the System UI app and Settings app with monitor capacities. System UI contains the functionality for the back/home buttons on Android devices. Removal of these apps leaves the device unusable, and a path to remediation is still unclear.

BatMobi adware

This quarter, an outcry of patrons on the Malwarebytes Forums alerted us of advertising redirects that seemed to come out of nowhere. Patrons verified the ads were popping up whenever an app was updating or installing on Google Play. We tracked the offending websites back to the culprit—BatMobi.

BatMobi is a common ad network SDK used by app developers to gain revenue through ads. Most variants of BatMobi were clean and safe to use—until recently. Furthermore, BatMobi already had a slightly more aggressive version that we detect as Android/Adware.BatMobi.

Sometime in mid-January, BatMobi switched from a safe SDK to adware. The offending components of BatMobi were deeply hidden in apps found on reputable third-party app stores, pre-installed on Mi Mobile Xiaomi Redmi Note 5 devices, and presumably could still be lurking on Google Play. However, the trail went cold and the adware campaign abruptly ended in mid-March.

This leaves us with an uneasy feeling about ad network SDKs as we head into Q2, highlighting their power to swiftly switch from legitimate to malicious overnight.

Exploits

Flash Player zero-day (CVE-2018-15982)

Even though the Flash Player is rapidly losing market share, it continued to be a target in both document and web-based attacks in Q1 2019.

In early December, we reported that a new Flash Player zero-day was used against a Russian facility via an embedded object within a decoy Word document. This Use-After-Free vulnerability in the Flash package, com.com.adobe.tvsdk.mediacore.metadata, was subsequently weaponized in the wild by other threat actors.

We captured an updated Underminer exploit kit only a few days after a Proof of Concept (PoC) for CVE-2018-15982 was made available that was exploiting Flash version 31.0.0.153.

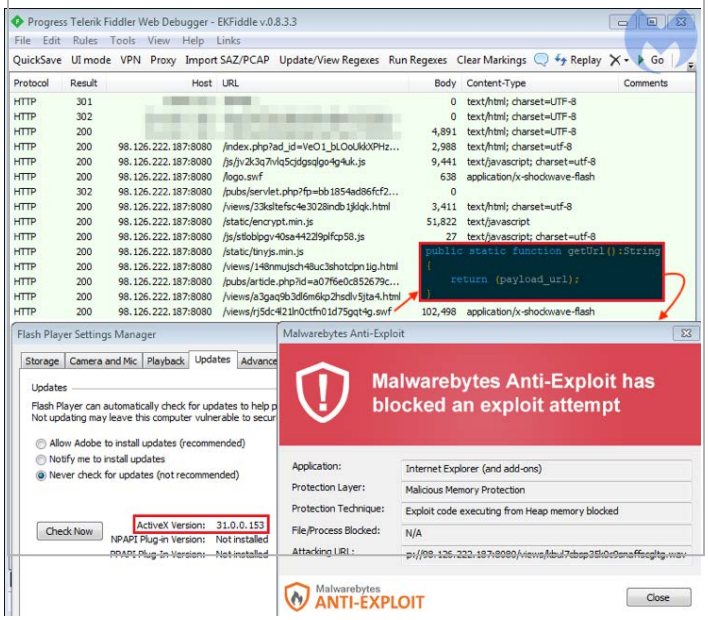

Figure 23. Flash exploit (CVE-2018-15982) blocked by Malwarebytes Anti-Exploit

Within the next few weeks, Fallout EK added the new Flash zero-day and, a few months later, it was spotted in Spelevo, a new exploit kit.

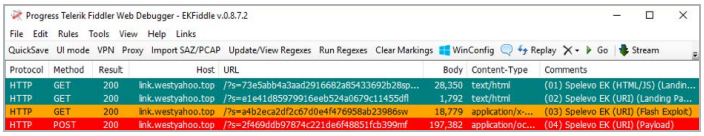

Figure 23. Spelevo EK using CVE-2018-15982

Source: https://pbs.twimg.com/media/D2izMfcUgAAyS6X.png:large

WinRAR exploit

An interesting vulnerability with the popular WinRAR archiver program was found abusing the old ACE archive format in Q1. As a result, this flaw is about just as old as the program itself, affecting WinRAR versions going all the way back 19 years.

While the arbitrary path traversal vulnerability did not lead to remote code execution directly, it achieved the same goal with a little bit of a delay. Indeed, an attacker could embed a malicious file within the archive and have it extracted in a location of their choice.

The Startup folder was a prime candidate, since any program or shortcut files stored there would be executed as part of the OS start-up routine.

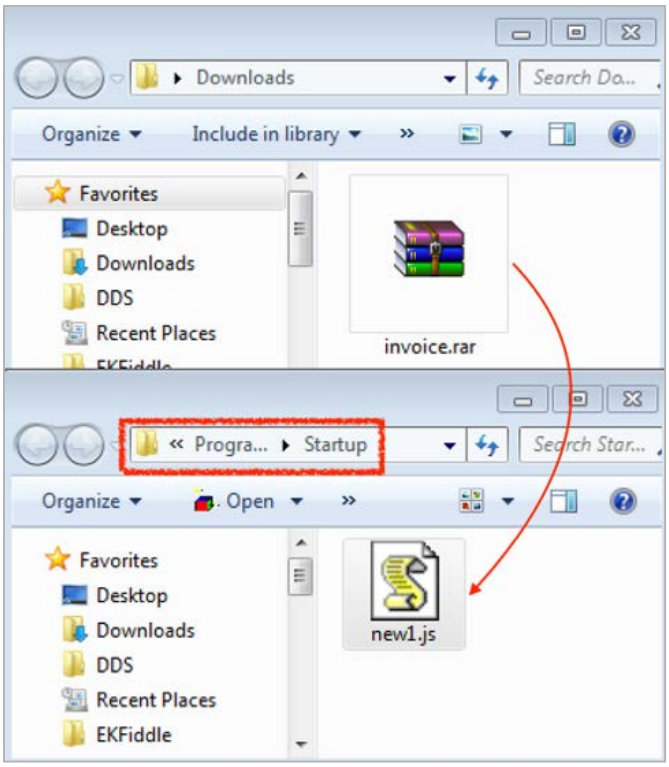

Figure 24. WinRAR archive extracting a malicious script to the Startup folder

Attackers did not pass on this opportunity, and some distribution campaigns incorporated this delivery mechanism this quarter.

Chrome zero-day (CVE-2019-5786)

Over the past few years, we've become used to hearing about exploits affecting Internet Explorer. Meanwhile, Google Chrome has been dominating the browser market share, thanks to its automatic update mechanism.

Indeed, even in the face of exploits affecting third-party plugins (i.e. Flash Player), Chrome still had the ability to update itself in the background with no user interaction. However, Google researchers found a new zero-day in March where this model could no longer apply.

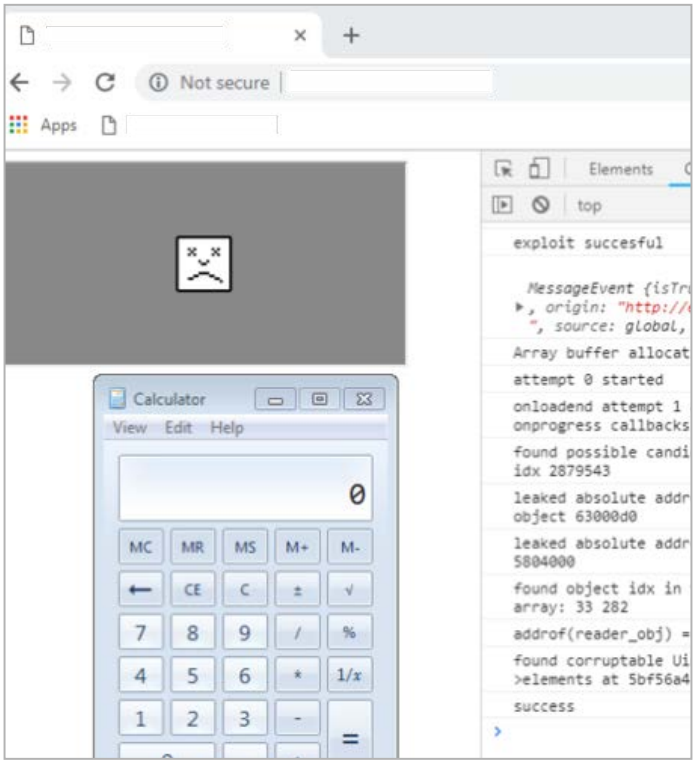

Figure 25. PoC exploit for CVE-2019-5786

The reason for this is that the vulnerability was targeting Google Chrome itself. As a result, for the patch to be installed properly, a full shutdown and restart of the browser was necessary.

Considering how many people keep their computers running and rarely ever close all their browser tabs, this revealed an interesting attack vector with a real window of opportunity. Additionally, since Google had begun to restrict what third-party code could inject into its browser, security products that could have thwarted this zero-day were simply no longer effective.

Privacy

Privacy is a human right. And yet, users' privacy—and trust—have been repeatedly broken in recent years.

In 2013, whistleblower Edward Snowden exposed the US National Security Agency's indiscriminate collection of Americans' phone call records, emails, online chats, and browsing history. According to Snowden, the NSA had "mass access" to user data handled by Google, Apple, Facebook, Microsoft, Yahoo, and YouTube. Immediately following Snowden's disclosures, many of those companies pushed back, publicly denying their active participation in the NSA's warrantless surveillance regime.

Fast-forward to today, the public has a new concern: privacy invasions by companies themselves, no government assistance required.

Data breaches of Yahoo, Uber, Equifax, Marriott, Target, the Sony PlayStation Network, Facebook, Anthem, JPMorgan Chase, and more have put individuals' personal information in the hands of cybercriminals.

Meanwhile, companies have relied on opaque data-sharing agreements to access personal data in ways that users never could have imagined. Last year, published documents revealed that Facebook gave special platform access to Netflix and Airbnb in exchange for favors. Buzzfeed News reported that a DNA-testing company partnered with the FBI to allow the agency to search its database. A menstrual tracking app shared its users' pregnancy decisions and period tracking information with Facebook.

This year, even the potential for surreptitious data collection set off alarm bells when Google failed to tell consumers that its Nest home security product also included a microphone.

Public anger is at its peak, and data privacy has become the key ingredient in today's scandals, including some of the most significant international developments. Questions still remain about data misuse in both the UK's vote to leave the European Union and the US 2016 presidential election.

At Malwarebytes, we wanted to dig deeper. We wanted to know how fallout from data privacy abuse was impacting user behavior, and whether or not businesses were taking the right steps to not only protect themselves from breach, but also their customers' PII. Have world-changing events made users more privacy-proactive? Or has the onslaught of headlines only led them closer to privacy nihilism?

For anyone concerned with privacy, the answers we found were equally encouraging and troubling. While users of every age care about online privacy and take steps to protect their personal information online, many businesses have not kept up their end of the bargain, falling victim to insufficient data protections as a result of lack of resources, budget, lax policies (or lack of policy whatsoever), and in some cases, plain negligence.

Malwarebytes' privacy survey

Between January 14 and February 15, 2019, Malwarebytes surveyed nearly 4,000 individuals across 66 countries—from the UK to the US, from Malaysia to Mexico, from India to Ireland—asking about their online privacy beliefs and cybersecurity practices.

We surveyed individuals from four age groups:

- Under 18 years old (Generation Z/Zed)
- 18-35 years old (Millennials)
- 36-55 years old (Generation X)
- 56 years and older (Baby Boomers)

Here's what we found.

The overwhelming majority of respondents (96 percent) said they care about protecting their personal information online. A similar majority of respondents (97 percent) said they take actual steps in protecting their online data, whether they're using a desktop, laptop, or mobile device.

Relatedly, technology users across the board (95 percent) showed a near-universal distrust of social media companies to protect their online data. A significantly smaller share of respondents (34 percent) held similar distrust towards search engines in protecting their online data.

A full 59 percent of all respondents shied away from sharing any of the types of personal information we asked them about, which included contact information, credit card details, banking details, and health-related information.

That decision to not share information in the first place proved popular with respondents who said they take steps to protect information online. The most utilized practices were:

- Refraining from sharing sensitive personal data on social media (94 percent)
- Using security software (93 percent)
- Running software updates regularly (90 percent)
- Verifying that visited websites are secured before making purchases (86 percent)

On the other side of the cybersecurity equation, though, many respondents admitted to inattentiveness and a lack of understanding about sometimes complex topics. The most common cybersecurity lapses were:

- Skimming through or not reading End User License Agreements (EULA) or other consent forms (66 percent)
- Using the same password across multiple platforms (29 percent)
- Not knowing which permissions users' apps have access to on their mobile device (26 percent)
- Not verifying the security of websites before making purchases, such as, for example, not looking for "https" or the green padlock on sites (10 percent)

Perhaps we can't entirely blame the two-thirds of users who don't read the EULAs, though. After all, the agreements are notoriously long and riddled with legalese. Privacy advocates lobbying for data privacy legislation in the United States have even said that clearer, more transparent terms of service agreements will not empower the public to better protect their own privacy. What the public needs, these advocates argue, is actual respect and better treatment from companies.

Enterprise, privacy, and third-party services

This quarter, we decided to focus on enterprise risks involving privacy and third-party services. Most companies have embraced cloud services as a method of offloading infrastructure maintenance costs and labor, allowing them to devote more resources to core business components. Unfortunately, many of these service providers offer inadequate security defaults for corporate users, or allow use cases that leak data to the public Internet. Why is this a problem for enterprise defenders?

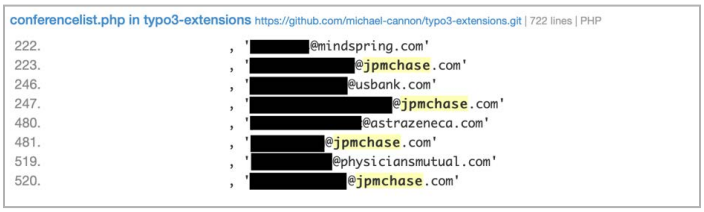

Figure 26. Screenshot sample of leaked email addresses

Leaking otherwise "benign" data to the public is problematic for a variety of reasons—most prominent is that it dramatically cuts reconnaissance time for attackers. Discovering a useful user account in the wild is the difference between a mass phish that gets dropped at the perimeter and a targeted spear phish to an employee's private account that provides a springboard into the organization. Looking at the wild success of Emotet's spear phishing campaigns over the last couple quarters should have organizations reconsidering whether the cost savings of third-party service providers are worth the potential brand and operational damage.

Barring implementation of a password manager, credential reuse is almost impossible to stamp out, exponentially raising the security cost of a single breached account. Employee data leaks can also cost an enterprise competitive intelligence, as well as tie reputationally harming behavior of employees to their company.

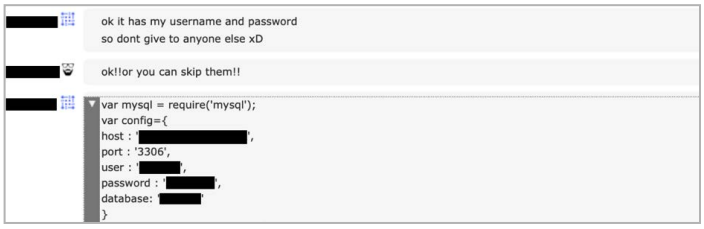

Figure 27. Screenshot sample of employee sharing company credentials to an external party

Web resources for developers, as seen above, can also be a significant source of data loss. Stack Overflow, GitHub, and an assortment of tech stack-specific forums are problematic in this regard, due to an insular community that creates feelings of safeness and privacy amongst its members. While infrastructure-specific vectors like GitHub can be configured appropriately to avoid data loss, employee communications external to the company should have robust policy in place to guard against security issues like those pictured in the above screenshot.

Public data leak damage

In 2015, dating website Ashley Madison suffered a breach of their userbase. In subsequent months, stories of users being blackmailed, harassed, and otherwise manipulated based on their membership emerged.

Somewhat less covered was that a sizeable portion of their clients used corporate email addresses to register for accounts. Any number of those accounts might have reused work passwords, leading to significant risk exposure for the businesses involved. Because of repeated large-scale breaches of this sort, we recommend enterprise defenders devote resources to managing data privacy issues, especially when involving third-party services.

Predictions

As we head into the rest of 2019, there are numerous potential dangers that linger based on what we've already seen this year. These threats span from new vulnerabilities to organizations struggling with the influx of threats to their infrastructure and reputation. We always hope that our predictions don't come true, but just in case we're right (and we have been right before), it's a good idea to keep an eye out for these possible futures.

SMBs will deal with a flood of threats trying to take advantage of still active vulnerabilities and maximize their victim count. If we see more effort to work with managed service/ security providers to boost SMB defenses, a disastrous outcome could be averted.

The APAC region will grapple with a new and dangerous threat based on WannaCry or Backdoor.Vools sometime this year, which may lead to region-specific ransomware or cryptominers. This is a direct result of the ease of infection many families have in this region, where three-year-old vulnerabilities are still being exploited every day.

Ransomware development and resurgence will continue. By the end of the year, we may see an intense campaign against businesses with the intent to ransom as much as possible.

We will see fewer ransomware attacks against consumers, as the technology developed to break through modern defenses will likely be saved for juicier targets. We may also see a decline in malware that is only referred to as "ransomware," as worm, exploit, and information-stealing functionality is being built into emerging ransom families.

Research into vulnerabilities found in the wild, such as what we saw with WinRAR this quarter, is going to be supercharged, as **the cybercrime world looks for a new method of easily infecting targets.** While email infection has been successful for years, being able to attack from an unexpected position is always going to be valuable to criminals and government spies alike.

Conclusion

2019 is off to an action-packed start in cybercrime, and if the last couple quarters are an indication of developments to come, then businesses are going to have their hands full swatting off attacks from a multitude of vectors. From exploits to ransomware to the ever-sinister Trojan downloader Emotet, threat actors have put serious effort into focusing their nefarious activities at more profitable targets than individual consumers.

All but abandoning cryptomining in the face of market downturn, criminals instead looked for higher returns on investments in Q1, breaching organizations to exfiltrate valuable customer data for resale on the black market or to use in still-successful sextortion scams or other phishing campaigns.

In some cases, criminals didn't even have to work too hard at developing sophisticated malware to penetrate enterprise defenses, as data leakage or brute-force password spraying allowed threat actors access to proprietary data or sensitive PII. Unfortunately, that put privacy invasion front-and-center for users in Q1, who expressed concern about protecting their data online and distrust in companies' ability—or even desire—to do so.

As we look ahead to Q2 2019, we hope consumers and businesses alike treat the previous three months as a cautionary tale and better prepare themselves for what's to come. Not ones to abandon successful tactics, cybercriminals will continue to beat the corporate drum until another easier or more profitable technique comes along. In the meantime, businesses need to work on shoring up perimeters, tightening access permissions, and establishing better privacy policies for storing and transmitting data safely for the sake of their customers' well-being—and their own.

Contributors

- Adam Kujawa: Director of Malwarebytes Labs
- Wendy Zamora: Head of Content, Malwarebytes Labs (Editor-in-Chief)
- Jovi Umawing: Senior Content Writer, Malwarebytes Labs (Senior Editor)
- Jérôme Segura: Head of Investigations, Malwarebytes Labs
- William Tsing: Head of Operations, Malwarebytes Labs
- Nathan Collier: Senior Mobile Threat Analyst
- Chris Boyd: Senior Malware Intelligence Analyst
- Pieter Arntz: Malware Intelligence Analyst
- David Ruiz: Content Writer, Malwarebytes Labs