



Cybercrime tactics and techniques

Q1 2017

TABLE OF CONTENTS

- 01 Executive summary
- 02 Windows malware
 - 02 Ransomware trends
 - 04 Cerber, king of ransomware
 - 05 Ransomware as a service
 - 05 New evasion features
 - 06 Where did Locky go?
 - 06 Keep an eye on Spora and Sage
 - 07 Windows malware predictions
- 08 Mac malware
 - 09 Mac predictions
- 09 Android malware
 - 11 Android predictions
- 11 Distribution methods
 - 11 Exploit kits
 - 13 Malicious spam
- 14 Scams
 - 14 Social media scams
 - 14 Social media scams predictions
 - 15 Tech support scams
 - 15 Tech support scam predictions
- 16 Research spotlight: Chris Boyd
- 17 Conclusion
- 18 Contributors

Introduction

The first quarter of 2017 brought with it some significant changes to the threat landscape, and we aren't talking about heavy ransomware distribution either. Threats that were previously believed to be serious contenders this year have nearly vanished entirely, while new threats and infection techniques have forced the security community to reconsider collection and analysis efforts.

In our second Cybercrime Tactics and Techniques report, we are going to take a deep look at which threats got our attention the most during the first three months of the year. In addition to that, we are also going to be providing predictions on what the second quarter of 2017 might look like. We are also going to give you a peek behind the scenes of Malwarebytes Labs, at the analysts who make reports like this possible.

Executive summary

The Cerber ransomware family took the mantle as top ransomware by market share in the first quarter of 2017, leaving all competitors in its dust. In addition to its continued use of the Ransomware as a Service model, new advancements made to the malware's functionality mean that it's unlikely we will see a decrease in the use and spread of Cerber in coming months. At the same time, our prediction that Locky would continue to be a major player in the ransomware market was completely wrong, since by the end of March, it has all but vanished. However, a few new players entering the market appear very promising and might make a bigger splash later in the year.

On the Mac side, a surge of new malware and backdoors plagued the community this quarter, including another Mac-focused ransomware and numerous infiltrations of Potentially Unwanted Programs (PUPs) in the Apple app store. This trend of spreading PUPs through legitimate sources is unlikely to change based on Apple's behavior in the past, which has tended toward avoiding removing PUPs.

Two notable Android threats have been causing a lot of trouble, one of them acting as a ransomware, utilizing Android administrative security features against users, while the other locks the system to ensure continued ad revenue coming from the app. We expect both threats to continue being a problem throughout next quarter.

In malware distribution news, RIG exploit kit continues to reign supreme; however, a lack of new exploits, features, or competition means that it's only a matter of time until RIG is dethroned. Otherwise, distribution continues heavily through malicious spam. An increase in social engineering tactics used by both exploits and malspam to avoid sandbox analysis and add credibility to the attacks means that you can in fact teach an old dog new tricks.

On the scam front, the leak of notable WWE stars' private images has been co-opted by survey scammers to spread fake links through social media. Alternatively, tech support scammers have been observed taking gift cards as payment and using social media to scam... other scammers. They do this by offering out-of-the-box tech scammer packages that fail to live up to their advertisements entirely.

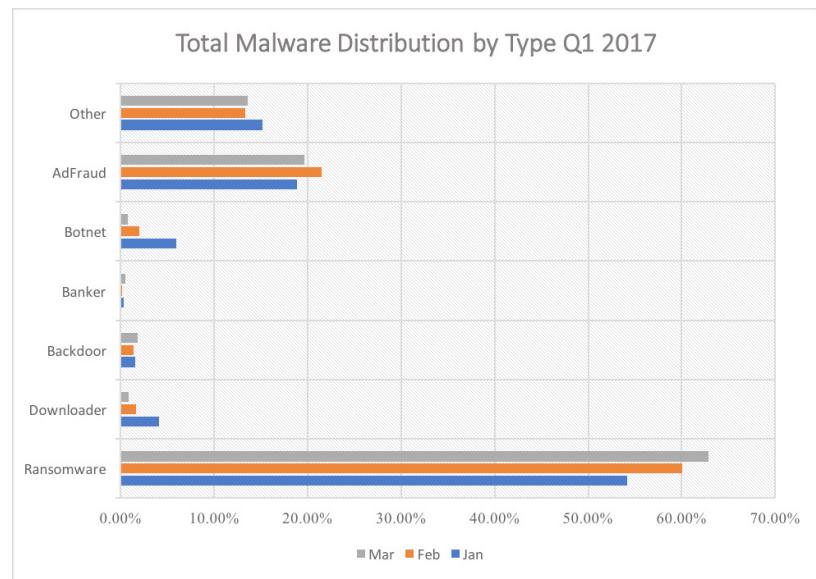
With the chaotic and dynamic nature of the cybercrime world, especially as observed over the last six months, we can expect a very interesting year and predict some serious changes with ransomware distribution and market share by the end of the summer.

Windows malware

The first few months of 2017 revealed much of the same trends we observed moving out of 2016 when it comes to Windows malware—basically, lots of ransomware sprinkled with some ad fraud and just a pinch of everything else. This observation is confirmed by the chart below, which shows malware distribution by malware type for the first three months of 2017.

Figure 1. Malware distribution by type Q1 2017

As you can see, ransomware continues to be the most heavily utilized type of malware by the most popular methods of distribution, both exploit kits and malicious spam (malspam). As such, we are going to delve into this trend even deeper in our first section of this report.

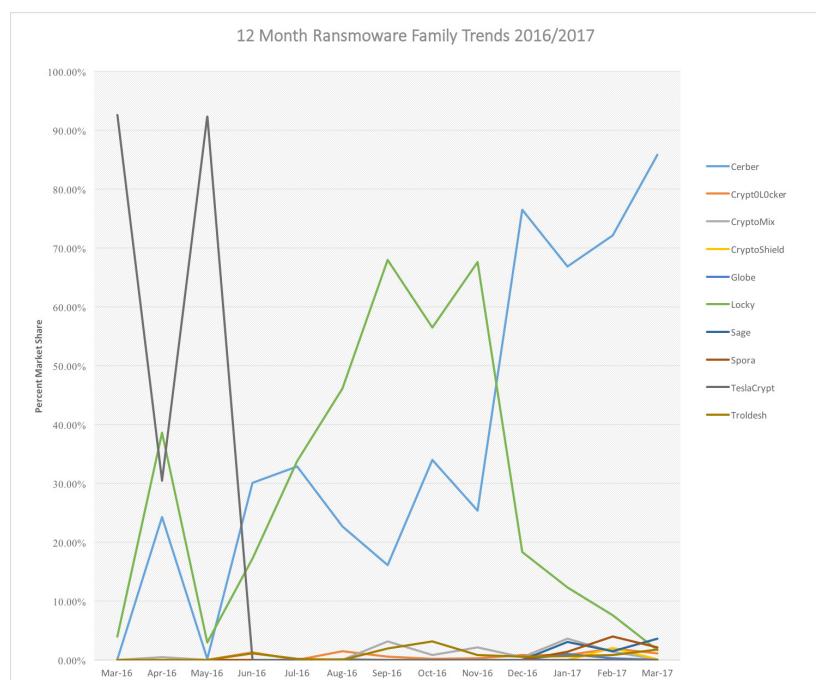


Ransomware trends

If you caught our last Cybercrime Tactics and Techniques report for 2016, we talked about the two contenders for king of ransomware: Locky and Cerber. So far in 2017, we've seen a massive shift in the battle between these two families, with Locky basically dropping out entirely and Cerber expanding its market share by a significant amount.

Figure 2. 12-Month ransomware family trends 2016/2017

The above chart expresses Cerber's complete rise, especially noticeable when compared to other ransomware families over the last 12 months. Not only does it show Cerber reaching market share domination on par with TeslaCrypt during its most popular timeframe (the first half of 2016) but also the quick fall of the very promising Locky family, which we will discuss in more detail later.



Stepping away from analysis of ransomware family statistics obtained from distribution sources (i.e. Malwarebytes controlled honeypots) we look at what our users are dealing with. The below graph charts the top 20 most heavily detected ransomware families of the first quarter of 2017.

Figure 3. Ransomware Top 20 families, Q1 2017

Once again, Cerber not only sticks out as number 1 against all other families, but it completely towers over subsequently ranked ransomware families, such as the quickly vanishing Locky.

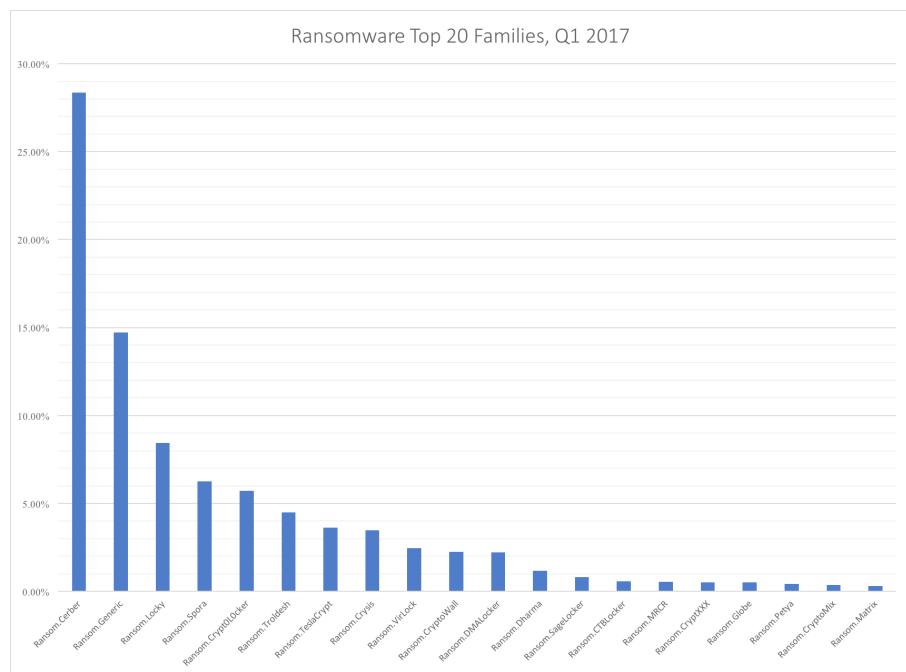
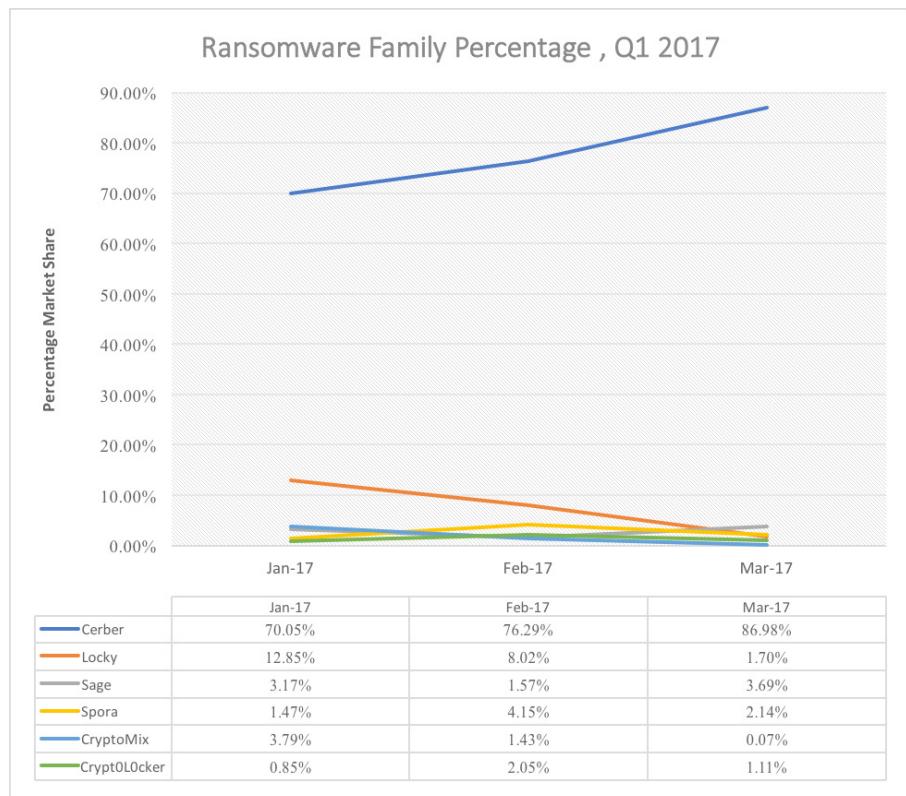


Figure 4. Ransomware family percentage, Q1 2017

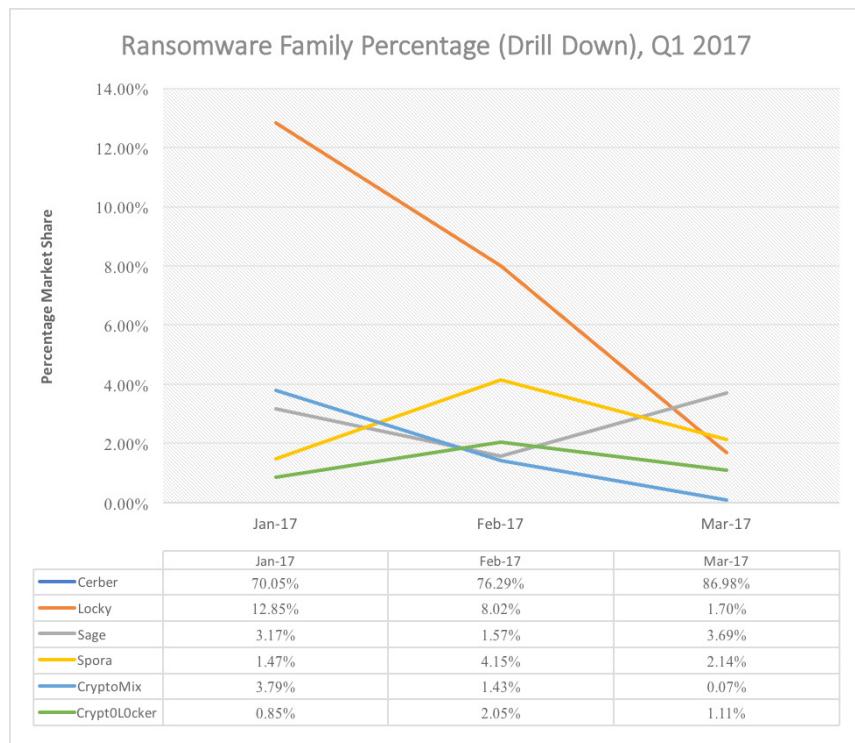
Next, we take a deeper look at just Q1 2017 ransomware family distribution, where Cerber starts off the year with a 70 percent market share and approaches 90 percent toward the end of the quarter.



In order to give some attention to the families that live in Cerber's shadow, we drilled down into the next five top families we observed being dropped. From this view, the fall of Locky is very apparent, with it dropping to under 2 percent market share by the end of March.

Figure 5. Ransomware family percentage (drill down), Q1 2017

This chart does show an interesting new development, with brand-new families like Spora and Sage making a small (but significant) appearance during the first quarter. We might see more from at least one of these families in Q2 2017; however, based on the slight decrease in the distribution of these families during March, it's just as likely they will vanish into obscurity in the next few months.

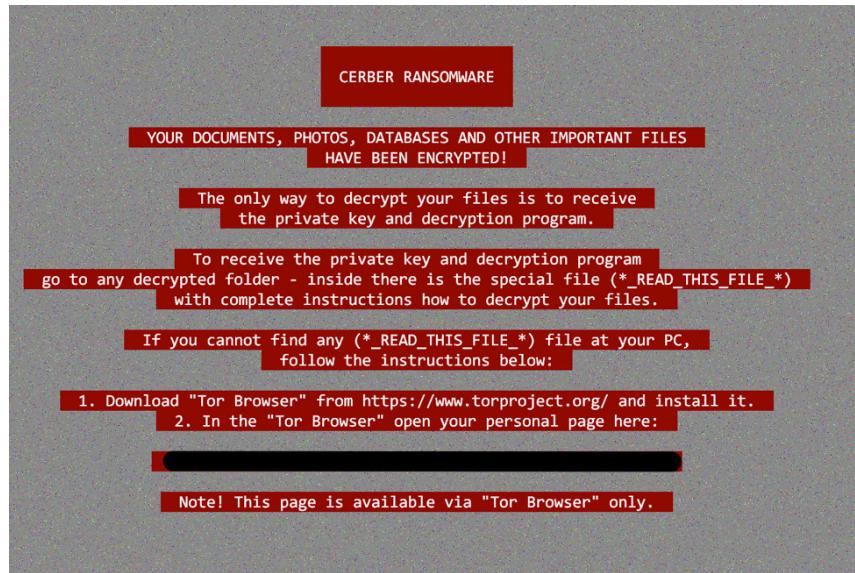


Cerber, king of ransomware

If you read our last report, you know that we considered it a possibility that Locky and Cerber would continue their tug-of-war for distribution market share through Q1 2017. Unfortunately, we were wrong. However, this situation acts as a perfect example of how dynamic and sensitive the cybercrime world is.

Figure 6. Cerber ransomware lock screen

Just like TeslaCrypt, Cerber has risen to the top of the ransomware market, leaving all competitors in its dust. Again, like TeslaCrypt, Cerber can just as easily become yesterday's news. However, there are a few factors at play with Cerber that could make its future different than that of families like TeslaCrypt and Locky.



Ransomware as a Service

Software as a service and security as a service are terms that describe a business/development model that is frequently used in the technology industry. The term refers to software or the deployment of security solutions or even storage “on-demand” or “as a service.”

The “as a service” model is very popular with the larger Internet companies, and you probably interact with it on a regular basis if you use Google Apps (Sheets, Mail, Drive) or the Amazon Web Service (AWS). So it’s no big surprise that the bad guys thought it would be a neat way to do business as well, which brings us to the Ransomware as a Service (RaaS) model.

Cerber is a RaaS, and its spread is largely because the creators have not only developed a superior ransomware with military-grade encryption, offline encrypting, and a slew of new features (which we will discuss later), but by also making it very easy for non-technical criminals to get their hands on a customized version of the ransomware.

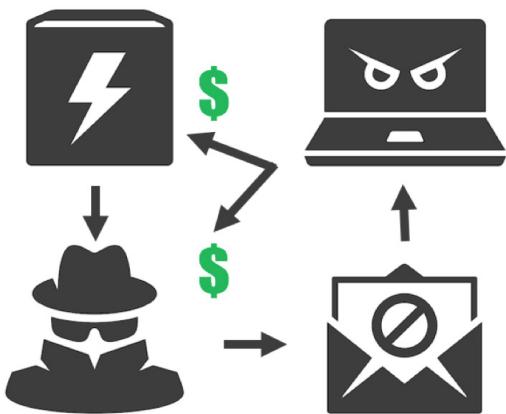


Figure 7. Ransomware as a Service model. Developers sell to affiliates and take a cut of the ransom.

Once the ransomware is purchased, options exist from other parts of the cybercrime marketplace that will distribute the malware through numerous means, ensuring the greatest amount of infection. Once infection and payment occur, the criminals who franchised the ransomware get paid, but the Cerber developers also get a cut of the ransom. You might recognize this process as being akin to an affiliate program used by advertisers.

New evasion features

You can’t expect to stay on top if you aren’t willing to adapt and evolve, which is why Cerber has recently started employing some new tricks, mainly for the sake of avoiding detection by security vendors.

The security vendor Trend Micro recently released its analysis of a new Cerber variant that not only attempts to evade antivirus solutions that employ machine learning, but also detects if the malware is executing within a sandbox or virtual machine.

Basically, this version of Cerber is distributed via phishing emails. These emails include a link to a Dropbox folder to download a self-extracting archive file that has three files inside, each one individually not very dangerous, but designed to work together to execute Cerber functionality. The process works like this:

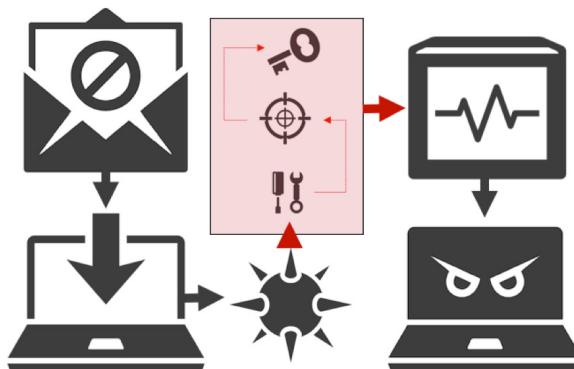


Figure 8. Cerber’s new detection evasion

1. The phishing email includes a link to download a self-extracting executable from Dropbox.
2. The executable extracts and drops three files:
 - a. A Visual Basic Script file
 - b. A library (DLL) file
 - c. A binary
3. The VB script executes RunDLL32.exe and loads the DLL into memory.
4. The DLL reads the binary file and decrypts the malicious code inside.
5. The decrypted code acts as a loader that checks to see if the victim system is a virtual machine and looks for numerous analysis tools and security products (to evade automated analysis).
6. Finally, the loader code injects Cerber code into one of a few possible running processes and starts encrypting user files.

So, what does this mean for stopping Cerber infections in the future? Basically, software that uses machine learning to identify malicious features present in previously unseen (or zero-hour) malware may miss identifying any of the individual parts of this new variant of Cerber. Fortunately, many security companies (including Malwarebytes) don't put all their eggs in one basket and prevent threats at numerous phases of the attack chain. While Cerber may have found a loophole in physical binary detection, memory monitoring, distribution prevention, and behavioral heuristics should still do the trick.

Where did Locky go?

As mentioned previously, the biggest revelation of Q1 2017 as far as malware market share goes is the disappearance of Locky. Over the course of the first three months of 2017, Locky went from nearly a 70 percent market share to 12 percent in January, and by March it had less than 2 percent.

The reason behind why Locky suddenly vanished is anyone's guess—the security industry overall has not discovered a true reason. However, there are a few theories.

Necurs switched to pushing different malware

The Necurs botnet, which is responsible for a lot of the phishing attacks and malicious spam used to distribute malware over the years, seems to no longer be pushing Locky ransomware. Security researchers noticed in June of last year that when Necurs went down temporarily, numbers for Locky also dropped.

Since the beginning of the year, researchers have still observed Necurs spam. However, it seems like they are going in a different direction and have dropped Locky as a primary payload.

No new Locky versions

While not necessarily a different theory from the above, the InfoSec world has noticed a lack of new Locky versions since the beginning of the year, which means either the group behind this heinous ransomware has decided to move on to different business opportunities, or they were caught by law enforcement (or worse).

Either way, we should all be thankful that one of the most dangerous families of ransomware seems to have vanished for the time being. We do still need to worry about an overpowered and heavily distributed Cerber, though, so don't let your guard down just yet. Also, just because Locky seems to be a thing of the past now doesn't ensure that it won't be back in a few months.

Keep an eye on Spora and Sage

The last Windows malware information we want to cover involves two families of ransomware that are beefy in their design but have yet to make a big impact through distribution channels: Spora and Sage.

Figure 9. Spora, Sage, and Cerber comparisons

Sage, Spora, and Cerber all have a lot in common as far as their encryption capabilities and stand-alone encryption models. However, while Sage seems to be your run-of-the-mill ransomware, secure in its encryption but otherwise uninteresting, Spora has decided to set itself apart with superior customer service for its victims.

	SPORA	SAGE	CERBER
ENCRYPTION ALGORITHM	AES	Elliptic Curves / ChaCha20	AES
OFFLINE ENCRYPTING	Yes	Yes	Yes
DECRYPTOR AVAILABLE	No	No	No
TOR PAYMENT SITE	Yes	Yes	Yes

All your work and personal files were encrypted

To restore data, obtaining guarantees and support, follow the instructions in your account.

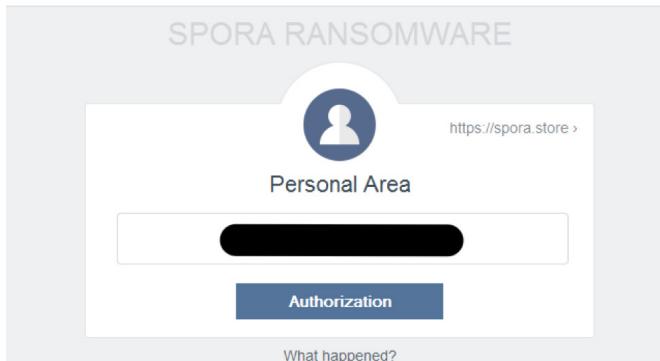


Figure 10. Spora lock screen

The Spora payment site provides a lot of features not frequently seen being used by other ransomware families:

- Immunity from future infections
- Per-file restoration
- Live customer service chat

Sage and Spora had a fair amount of distribution attention in February of 2017, with a slight drop in March, but we will have to wait and see if that trend continues or if we can see one of them going head-to-head with Cerber by the end of Q2.

Windows malware predictions

It has clearly been a very busy quarter for Windows malware, with some families vanishing, others starting to make an impact, and, overall, a complete takeover of Cerber ransomware. So, what are we going to see next quarter?

Cerber is going to continue to be a massive force in the ransomware world. Since the creators of Cerber continue to develop and sell the ransomware to affiliates, it would likely take interaction from law enforcement to halt operations and shut the ransomware down. However, barring a huge mistake from one of the group members that gives some hint as to their identities, it's unlikely this malware will vanish before the end of Q2.

Spora is going to take greater market share. Because of its secure design and professional payment site, Spora could very likely bring in a lot of profit from its operations, which could in turn be invested into greater distribution campaigns. However, catching up with Cerber is no easy feat, so we expect Spora to obtain greater market share over other families but remain far behind Cerber.

Finally, we didn't really mention Windows malware that isn't ransomware in this quarter's report. However, the Kovter Trojan has continued to be the most heavily non-ransomware malware distributed through regular channels. We predict a continuation of its operations through Q2, though we are expecting some changes to either the malware's purpose, function, or distribution very soon. Any modifications made to the Kovter campaign is unlikely going to be beneficial to its victims.

Mac malware

The first quarter of 2017 has seen quite a few new pieces of Mac malware, nearly equaling the number that appeared in all of 2016. Most these threats have been backdoors, varying in capability, delivery method, and sophistication. Even backdoors delivered via Microsoft Office macros have seen a resurgence on the Mac, installing various backdoor components.

Backdoors

These backdoors have varying capabilities, but generally include most or all of “the basics”: the ability to run arbitrary shell commands, download and install files, exfiltrate files from the infected system, stream data from the webcam, and log keystrokes. Some have more specific capabilities, such as capturing password data from the keychain or searching out and exfiltrating backups of iOS devices.

FindZip

Only one threat varied from the backdoor trend, and that was the second-ever ransomware to appear on the Mac (the first one being KeRanger, which appeared in March of 2016). This quarter’s new ransomware, called FindZip, was a rather unsophisticated attempt that didn’t even give the hacker behind it the capability to decrypt files.

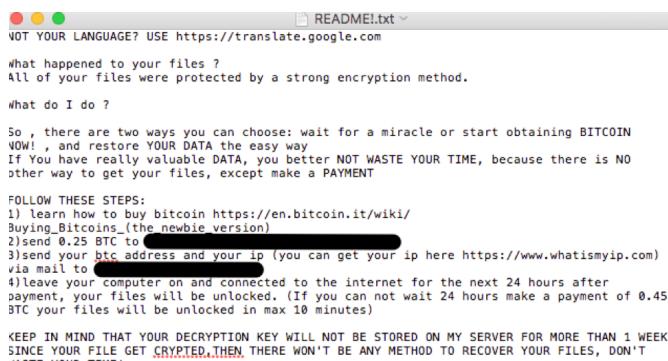


Figure 11. FindZip ransom note

FindZip was found on a piracy site, pretending to be a “crack” for apps like Adobe Premiere Pro or Microsoft Office. To date, the bitcoin wallet meant to collect ransom for this malware has received no payments whatsoever.

Mac PUPs

Potentially Unwanted Programs (PUPs) in the Mac App Store have become a serious problem. As an example, searching for “adware” on the store will result in a list of supposed adware or malware removal apps, and a very large percentage of them are either junk or scams. We have reported many of these to Apple, but most have not been removed.

We recommend taking care about what you download from the Mac App Store, especially when it comes to antivirus or anti-adware software, which is difficult for most people to verify the effectiveness of. (Few people have a ready supply of malware and adware to test with!) Also avoid any kind of system or memory “cleaning” apps.

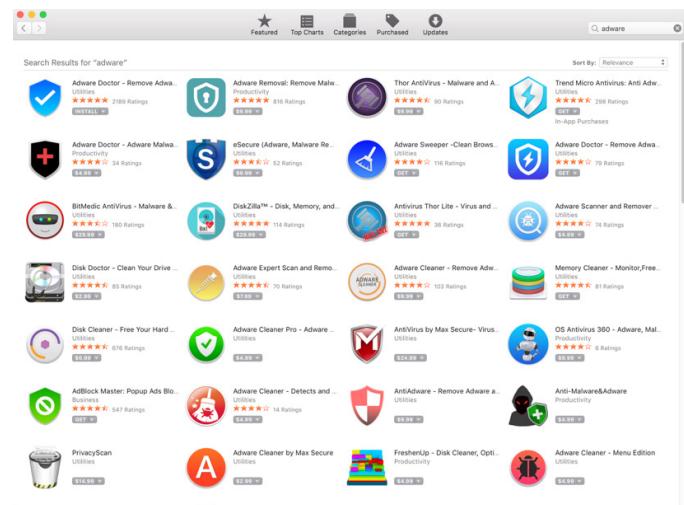


Figure 12. Adware results on the Mac App Store

Phishing has been a problem for iCloud accounts. Common phishing emails have included supposed notices from Apple that an iCloud account has been locked, requests to confirm an iCloud account, or invoices for a purchase from iTunes or the App Store. Such emails contain links that go to look-alike Apple login pages.

Some of these email messages and phishing sites are quite convincing, so it's very important to pay close attention and never click the links in these messages. To manage your Apple ID, go directly to appleid.apple.com, and to view purchases in iTunes or the App Store, use the appropriate features within those apps.

Vault 7

Much ado has been made about WikiLeaks' release about CIA malware for the Mac as part of its Vault 7 leak. None of those tools turned out to be able to infect any modern Macs, as they abused vulnerabilities that had been patched years before, and some only applied to very old hardware. There was nothing particularly surprising or concerning in the leak.

Mac predictions

We anticipate seeing more Mac malware the rest of this year, most likely leading to a spike in malware larger than any year since 2012, the most active year in Mac malware. This year could even surpass 2012 if current trends continue for the rest of the year.

We also predict seeing an increasing problem with PUPs in the Mac App Store, due to Apple's reluctance to act on such apps. PUP developers have been emboldened by this and seem to be swarming to the store in increasing numbers.

Targeted malspam has primarily been a Windows problem to date, but the reemergence of Microsoft Office macro malware capable of affecting Macs may change this. Many of these malicious documents include code that is capable of detecting whether it is running on a Windows or Mac system and taking action appropriate to the system to infect it. This means that malspam will no longer be an issue only of concern to Windows users, and Mac users will need to be increasingly wary of email attachments.

Android malware

If you've read end-of-year summaries from other security vendors in the past, you know that predicting additional Android infections is a common theme. Year after year, however, these predictions generally don't come true. Despite that, we would be remiss if we did not talk about two malware families currently plaguing Android users, especially since they both take advantage of administrative security features.

Trojan.HiddenAds.lck

When it comes to advertising, most Android users are tolerant and will accept some form of advertising, but advertisers and developers can be greedy and will ruin the mobile experience. A few years back, there were a handful of aggressive advertising offenders. Now it's rampant, from full-screen ads to 15-second videos

in between game levels. During the first quarter of 2017, we saw an explosion in a new way of advertising: blocking the removal of an overly advertised app. In comes Trojan.HiddenAds.lck, currently the biggest offender of this behavior. There have been thousands of these samples littered across the Android landscape, even being found in the Google Play Store. Many come bundled with seven or more adware libraries.

Blocking the removal of an app on Android is not a new concept—it was made famous by various ransomware families—but to have this done by seemingly ordinary apps is very interesting. Like most Android malware, the malware author uses Android features against the unsuspecting victim, in this case “Device Administrator.”

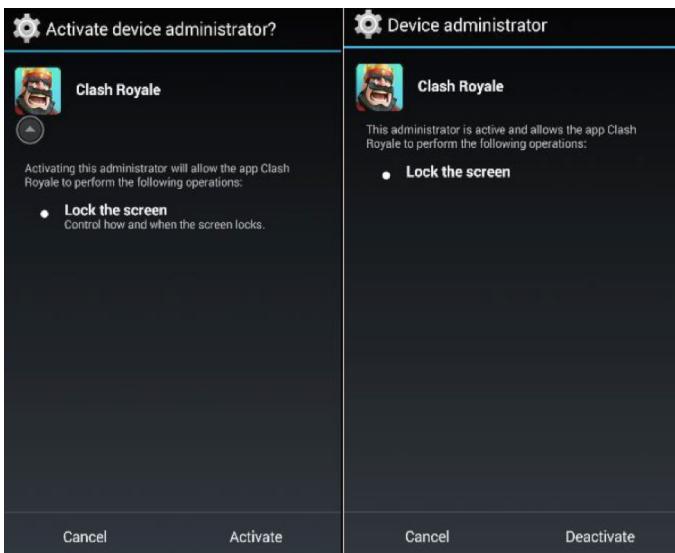


Figure 13. HiddenAds.lck in action

With the rise of the Bring Your Own Device (BYOD) dilemma, Google introduced device administration to give Enterprise app developers added security control. Apps can implement device policies such as password settings, remote wipe, and locking the device. The one big problem with this is that it is available to all Android app developers, and the bad guys have found a way to abuse it. Most Android users are unaware of the power this setting has, so they blindly accept any app request to be added to the list of device administrators.

In HiddenAds.lck's case, it uses the "lock device" policy to prevent itself from being uninstalled. The implantation is rather simple:

- Request Device Administrator privilege
- Add logic to wait for an attempt to deactivate the app from Device Administrator
- Lock device

```
public CharSequence onDisableRequested(Context arg4, Intent arg5) { // Awaiting Device Admin deactivation request
    new Lock(this).execute((String[]) arg5); // Go to 'Lock' class to lock screen on Disable request
    Intent v0 = new Intent("android.settings.SETTINGS");
    v0.setFlags(1073741824);
    v0.setFlags(268435456);
    arg4.startActivity(v0);
    return arg4.getResources().getString(2131034144);
}
```

Figure 14. HiddenAds.lck lock access code

This creates a cycle of events where the victim cannot uninstall the offending app, which equals continued ad revenue.

```
public class socabafuc extends DeviceAdminReceiver {
    class Lock extends AsyncTask {
        // 'Lock' class which invokes screen locking
        Lock(socabafuc arg1) {
            socabafuc.this = arg1;
            super();
        }

        protected Object doInBackground(Object[] arg2) {
            return this.doInBackground((String[])arg2);
        }

        protected String doInBackground(String[] arg5) {
            int v0;
            for(v0 = 0; v0 <= 1000; ++v0) {
                try {
                    socabafuc.this.Manager.lockNow(); // Lockscreen
                    TimeUnit.MILLISECONDS.sleep(5);
                } catch(Exception v1) {
                }
            }
            return null;
        }
    }
}
```

Figure 15. HiddenAds.lck lock screen code

Often the victim can remove HiddenAds.lck and similarly behaving apps by restarting the device in Safe Mode and removing the app from device administration access. Other times, there are more advanced steps needed. Not many Android users even realize there is a Safe Mode on Android, but it is there and can help save the day. Check with your device manufacturer on the button sequence to restart into Safe Mode.

Ransom.Jisut

Jisut is an Android ransomware that has continued to outpace other ransomware with new sample output. The previous quarter saw a huge increase in Jisut samples, and the first quarter of 2017 did not disappoint, with tens of thousands of new samples being introduced into the wild.

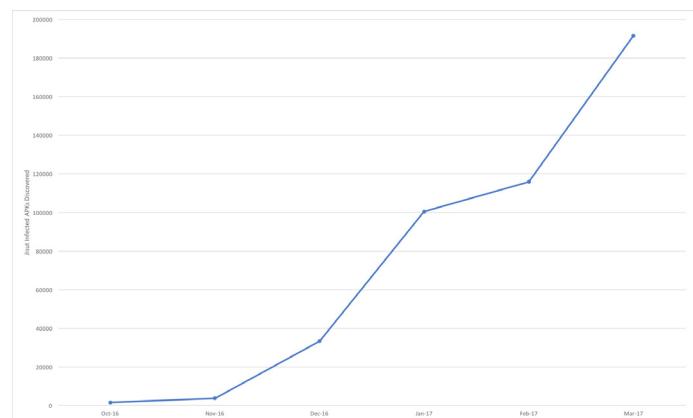


Figure 16. Jisut-infected APKs discovered October 2016–March 2017

The Jisut ransomware can act as a stand-alone app or just infect a legitimate app with the Jisut payload or the ransom logic embedded. Like HiddenAds.lck, Jisut also uses device administration against the user. The tactic of this threat is to reset the password or PIN code for the lock screen. If changing these access codes is successful, the malware can threaten the victim with the encryption of files, demanding a ransom for access.

As you can see with these two examples, there is a fine line between what the developers of grayware and those of ransomware do: they prevent users from removing malicious apps and use the device as a revenue maker.

Distribution methods

The first part of 2017 brought much of the same trends as far as malware distribution mechanisms go, with exploit kits taking a back seat to malicious spam. However, the quarter did bring a few new developments in the form of greater social engineering tactics added to previously effective methods of infection.

Exploit kits

In Q1 2017, exploit kit activity remained low, with even fewer antagonists than in the past quarter. In particular, RIG EK has continued to serve the Cerber ransomware via compromised websites and malvertising campaigns.

The lack of new exploits has led to an increase in social engineering to infect users, especially if they are running a different browser than Internet Explorer. Traffic distributors will triage potential victims upstream and choose to redirect them to an exploit kit (if they are potentially vulnerable) or to a fake page with the same goal of delivering malware.

For instance, the “ElTest” campaign targets Chrome users by tricking them into installing a fake font (“[HoeflerText](#)”), which turns out to be the Spora ransomware.

Android predictions

For this next quarter, we don’t expect to see any new and innovative malware on Android, but we do expect to see a lot of the same. Jisut will continue to churn out new samples, the distribution model appears to be working, and they are able to get new infected apps out quickly.

There will likely be another infestation of HiddenAds introduced into the Google Play Store, disguising in-app advertising as the way to go when trying to evade the notice of Google as well as Android security companies.

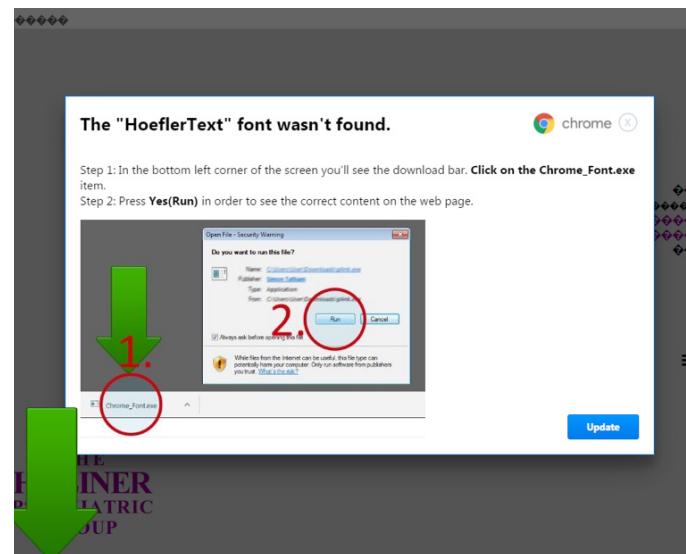


Figure 17. HoeflerText font scam, spreading Spora

It's interesting to note that stale exploits are becoming less effective to the point that threat actors are opting for social engineering instead.

In-the-wild exploits

There haven't been many changes with the type of exploits being used, despite notable security fixes from both Microsoft and Adobe. In [mid-March](#), Microsoft patched an XML Core Service Information Disclosure Vulnerability (CVE-2017-0022), which had been used to profile users and evade unintended targets in several large malvertising campaigns.

These types of exploits have been greatly abused in the past and will most likely continue to be abused for some time. These vulnerabilities are not rated as severe and tend to get patched on longer cycles. Attackers are also keen on finding bypasses to retain their ability to [fingerprint users](#).

Top vulnerabilities exploited

INTERNET EXPLORER	INFO DISCLOSURE VULNERABILITIES	FLASH	SILVERLIGHT
CVE-2016-0189	CVE-2016-3351	CVE-2016-4117	CVE-2016-0034
CVE-2015-2419	CVE-2016-3298	CVE-2016-1019	
CVE-2014-6332	CVE-2016-0162	CVE-2015-8651	
CVE-2013-2551	CVE-2017-0022		

Figure 18. Q1 2017 targeted vulnerabilities

Active exploit kit families

RIG EK is still the most active exploit kit used in various malware campaigns. Its landing page structure both in URL and body patterns remains very much the same. Some RIG EK campaigns use a pre-filtering gate, a mechanism to weed out bots and other non-valuable targets. We have seen such gates with other EKs (for example, Neutrino).

Figure 19. RIG EK traffic

Protocol	Method	Host	URL	Body	Comments
HTTP	POST	best.neighborhoodreunion.com	/ct=Vivaldi&q=z37QMvXcjwDQDoTAMvE8LlEMU_OFUK...	5,234	RIG_EK_URL (Landing Page)
HTTP	POST	best.neighborhoodreunion.com	/ct=Amaya&q=qWRxfAuf7fQawLhjeAKQZomYcOVFIX9...	31,249	RIG_EK_URL (Landing Page)
HTTP	GET	best.neighborhoodreunion.com	/?oq=u7tQawXhjEyAKQFomYcOVFOX9_qr20jdnRac0ZLQ...	15,787	RIG_EK_URL (Flash Exploit)
HTTP	GET	best.neighborhoodreunion.com	/?biw=Amaya.126kj112.406i3y5k1&br_fl=1407&tui=4...	224,768	RIG_EK_URL (Malware Payload)

Sundown EK took a step back and even disappeared briefly while [copycats emerged](#). (Ironically, Sundown stole code from other EKs, so it has really gone full circle now.) It's hard to know for sure what is next for Sundown other than the fact that it has lost its contender position in Q1 2017.

Figure 20. Sundown EK traffic

Protocol	Method	Host	URL	Body	Comments
HTTP	GET	in.2tc4.xyz	/index.php?6CvtOlaMs8t5fW-f1dwM=uXvuZG3w1...	52,715	Sundown_EK_URL (Landing Page)
HTTP	GET	in.2tc4.xyz	/0E2/7947545190441	29,450	Sundown_EK_URL (Flash Exploit)
HTTP	GET	mfs.rqrqbq.com	/d.php	769,504	Sundown_EK_URL (Malware Payload)
HTTP	GET	mfs.rqrqbq.com	/e.php	769,504	Sundown_EK_URL (Malware Payload)

Figure 21. Magnitude EK traffic

Protocol	Method	Host	URL	Body	Comments
HTTP	GET	701434b724q.betbusy.site	/	...	600 Magnitude_Redirect_Campaign
HTTP	GET	bd4wdq2512b3m4bdam.tindead.bid	/		31,024 Magnitude_EK_Code (Landing Page)
HTTP	GET	bd4wdq2512b3m4bdam.tindead.bid	/291nc0xe39128		32,299 Magnitude_EK_URL (Landing Page)
HTTP	GET	bd4wdq2512b3m4bdam.tindead.bid	/e32ha39104c181m		10,083 Magnitude_EK_URL (Flash Exploit)
HTTP	HEAD	bd4wdq2512b3m4bdam.tindead.bid	/e32ha39104c181m		0 Magnitude_EK_URL
HTTP	GET	bd4wdq2512b3m4bdam.tindead.bid	/bd4wdq2512b3m4bdam.tindead.bid/e32ha39104c181m		847 Magnitude_EK_URL
HTTP	GET	bd4wdq2512b3m4bdam.tindead.bid	/win%2017_0,0,134		10,083 Magnitude_EK_URL (Flash Exploit)
HTTP	GET	164.132.140.81	/faaf059813e68041f00b721875fe5183		65,088 Magnitude_EK_URL
HTTP	GET	164.132.140.81	/db0a7848565cc4d3738fb06a9897facc		279,013 Magnitude_EK_URL (Malware Payload)

Neutrino EK (a private exploit kit) is a rare occurrence these days—or at least finding it requires more work. It still makes use of fingerprinting, not in the Flash exploit like it used to in the past, but rather in several checks up-front (i.e., gate).

Figure 22. Neutrino EK traffic

Protocol	Method	Host	URL	Body	Comments
HTTP	GET	cndnsilo.space	/impotences/mateys/phalluses/oudly/longshot/...	189,300	Neutrino_Redirect_Campaign
HTTP	POST	cndnsilo.space	/sooth/mousses/arrogate/pavement/awardee/den...	2,580	Neutrino_Redirect_Campaign
HTTP	POST	cndnsilo.space	/cobalt/conjugators/frenchman/vailed/pensioner...	0	Neutrino_Redirect_Campaign
HTTP	GET	cndnsilo.space	/recuperated/allegories/mincer/blithely/numerolo...	172	Neutrino_Redirect_Campaign
HTTP	GET	pweki.uquahcrai.space	/1981/03/12/bitter/snort/criminal/fearful-wick-lar...	3,592	Neutrino_EK_Code (Landing Page)
HTTP	GET	pweki.uquahcrai.space	/1996/10/23/auant/they/hiss/uneasy-stre-bank-bu...	49,954	Neutrino_EK_URL (Flash Exploit)
HTTP	GET	pweki.uquahcrai.space	/ladder/bloom-10765976	0	Neutrino_EK_URL
HTTP	GET	pweki.uquahcrai.space	/trial/1331460/fellow-twinkle-week-term	274,432	Neutrino_EK_URL (Malware Payload)

We should also mention the very stealthy Astrum EK, which is very hard to identify but actually strikes on very big targets. We saw traces of it in our telemetry in March via attacks on several major UK outlets.

Exploit kit predictions

At the moment, we are in a strange situation of RIG EK monopoly by default. Contrary to its predecessors, RIG EK is not chosen for its advanced exploits and delivery mechanisms, but rather because it is not really facing any direct competition.

There is room for a new contender to bring in some fresh exploits, but so far, we have seen more efforts to leverage social engineering than to innovate. Where this is going next is anyone's guess, but even if exploit kits lose importance, the distribution campaigns will continue to redirect users to scams or trick them into installing malware.

Malicious spam

Spam continues to be a major infection vector for malware delivery. After a long year-end holiday for spammers, we started to see an uptick in campaigns in February. Campaigns by the notorious Necurs botnet, which had primarily been delivering Locky, suddenly stopped operations, coming back shortly after, and has since been observed delivering “pump and dump” stock campaigns, refraining from malware campaigns for the time being.

While Locky may be in decline, other malware families such as Cerber are quick to take over. Malware downloaders of all types have been seen installing various ransomware families, Banking Trojans such as Dridex, password-stealing Trojans such as Pony, and the Kovter malware family, which uses “fileless” techniques to help remain undetected for the purposes of click-fraud. Kovter manages this fileless technique by utilizing Powershell scripts to execute various commands and eventually JavaScript to deploy objects via the registry.

Social engineering

Social engineering is still the preferred mechanism for spam delivery. Campaigns surrounding shipping notifications and purchase notifications have been seen from many major companies. Also, the use of fax notifications, scanned images, resumes, and traffic tickets continues to be a primary tactic being used.

Spam campaigns are routinely being detected using password-protected documents to thwart automated analysis. The password necessary to unlock the macro file is provided within the body of the email and typically is a seemingly random string of alphanumeric characters. Cerber is routinely seen being delivered with password-protected macro files.

Spammers attempt to deliver malspam using any file type or compression method available, and dozens of types of files have been detected. The primary file types:

.zip	.docx	.lnk
.rar	.jar	.svg
.doc	.js	.7zip
	.gz	

Figure 23. Commonly observed malspam attachment types

Most modern archive managers are capable of opening archives of various formats, so the user may notice little difference between a .zip and .gz. The use of these other file types are merely attempts to thwart spam filters and anti-malware engines.

Scams

Social media scams

March saw the arrival of a new, so-called “Fappening/Celebgate” scandal, where leaked images and videos of naked celebrities found their way onto the web. This content was prime real estate for scammers, who started peddling numerous links across sites such as Reddit, and social networks such as Twitter.

Over a 24-hour period, hundreds of compromised accounts (possibly more) began tweeting links to supposed images of WWE wrestler Paige with the following titles:

- VIDEO: WWE Superstar Paige Leaked Nude Pics and Videos
- Incredible!!! Leaked Nude Pics and Videos of WWE Superstar Paige!!!!: [url] (Accept the App First)

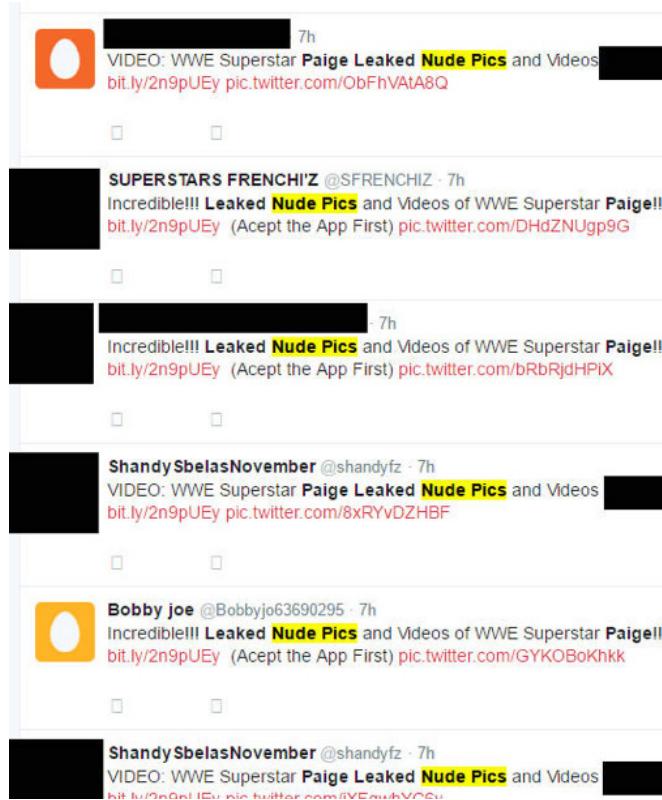


Figure 24. WWE scammer links via Twitter

The links, via Bit.ly redirects, took clickers to a Twitter app install that (once tied to an account) would post

more messages similar to the above, designed to keep clicks rolling in. Photo hunters would then be led through a daisy chain of successive websites, arriving at last at an Amazon gift card survey page.

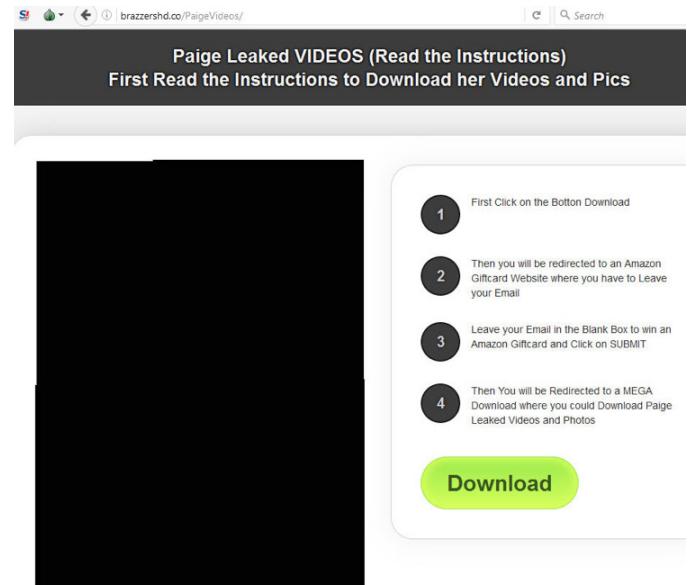


Figure 25. WWE scammer page leading to gift card survey scam

As with most scams of this type, the idea is to fill in the survey and hand over personally identifiable information (PII) to a third-party marketer to obtain the “reward.” In reality, there are few (if any) survey setups such as this where the person in front of the keyboard actually receives anything.

Social media scams predictions

We expect to see scammers continuing to make creative use of social networks and social systems on gaming platforms in order to drive potential victims to phishing sites. Breaking news will provide a hook for easy clicks, and the current unstable political climate globally may well see a rise in so-called “fake news” bots driving traffic to pages with malware and/or rogue adverts.

The rising popularity of “alternative” forms of social media services such as Mastodon may well mean bad actors poking around in these different systems to see what makes them tick.

Tech support scams

As referenced in the previous quarterly report, the lowest sophistication actors in tech support scams are either exiting the market, transitioning into a PUP-driven threat model, or augmenting income with harvesting PII for resale, or even direct phishing. In February, [Fortune reported](#) a tech support variant where a cold caller would claim that the user had been hacked, and require the user's information to investigate.

These trends have been influenced by increased consumer awareness, difficulties with finding North American payment processors to exfiltrate funds, and increased scrutiny on the part of search engines. Bing, which banned third-party tech support ads entirely last year, [released a report](#) stating they blocked 17 million of these ads in 2016.

Payment processors have followed along with heightened vetting of tech support companies, levying additional restrictions on their advertising or, in many cases, not working with the companies to begin with. As a result, alternative payment methods have seen an upswing, including Apple or Amazon gift cards, bitcoin, ACH, or physically mailing payment via courier service. We suspect the common thread connecting these new payment methods is their limited fraud protection and difficulty in analyzing fraud after the fact.

Intramarket fraud

With increased limitations on successfully executing a straightforward scam, some threat actors have moved to marketing sales and services to fraudulent scammers. As covered in the previous quarterly report, Malwarebytes has identified several entities providing a Scam as a Service (SCaaS), or a fully packaged suite of services allowing a call center to start up a criminal operation quickly.

Monitoring these SCaaS companies over time has revealed that a significant portion will simply take a center's money and provide skeleton services or nothing at all. Call centers have taken to [compiling lists of service providers](#) who simply fail to pay, in an effort to self-police.

The exit scam

An exit scam is when the owner of a (typically illegal) online business stops fulfilling orders, takes the customer's assets, and disappears. This type of scam is common to marketplaces on the dark web, where finding owners can be difficult. But in late 2016, a prominent tech support scam company seems to have executed an exit scam as well.

Employees of iyogi.com have complained publicly about months of non-payment for roughly 2,000 employees after the original company owners shut down the consumer-facing division and rebranded as itech.club. Given the significant assets of iyogi's owner, it's probable that his employees were exit scammed.

Tech support scam predictions

In the next quarter, we predict an uptick in exit scams and service provider non-payment, because the market incentivizes this type of behavior. As enforcement efforts ratchet up, stealing from other criminals affords a much safer and immediate opportunity to make money. Threat actors at the bottom tier of sophistication are predicted to continue a transition to traditional phishing, both for direct theft as well as for resale of PII.

Across all segments, traditional static browser lockers will lose market share to Windows lockers, and PUP-driven tech support scams. Lastly, call centers will seek to further monetize their sales channels by collecting victim PII alongside the traditional scam for a blended attack.

Researcher spotlight



CHRIS BOYD

Lead Malware
Intelligence Analyst

To give you a better look at the folks behind Malwarebytes Labs, we decided to start including a Q&A section for a researcher spotlight. Every quarter, we will bring you some questions and answers from one of the many Malwarebytes Labs team members. This quarter, we are talking to Chris Boyd.

Chris is a seven-time Microsoft MVP in consumer security and former director of research for FaceTime Security Labs. He's presented at RSA, InfoSec Europe, and SecTor, and has been thanked by Google for his contributions to responsible disclosure in its hall of fame. He's been credited with finding the first rootkit in an Instant Messaging hijack, the first example of a rogue browser installing without permission, and the first DIY botnet creation kit for Twitter. He currently acts as a lead malware intelligence analyst for Malwarebytes Labs.

Q. How long have you worked in InfoSec, and how did you get into it?

CB: Roughly 12 years, but I started in my spare time while doing other jobs. I got into it because something bad happened to a friend who had been hacked, and at the time, nobody could figure out what happened. I slowly pieced it together, and started to teach myself about security.

At night, I'd help people on grassroots security forums and learn how to remove infections manually. I set up a blog and started writing about the scams and infections going around. I kept finding things that ended up in the press, and from there, I was hired by FaceTime Security Labs and moved to Sunbelt Software and (eventually) Malwarebytes.

Q. Tell us three things about yourself.

CB: I love Dreamcast consoles, and have quite a few of them (some modded, some vanilla) along with a lot of other older consoles that I've collected for some time now. I've conducted on stage in a philharmonic hall, after going into schools and training kids to play classical instruments and

getting them up in front of an audience. I remove the cucumber and lettuce from ploughman's sandwiches, leaving me with bread and cheese. I guess I should just buy cheese sandwiches.

Q. What do you like to work on?

CB: I've always been interested in video game hacks/modding (console and PC), and was talking about this subject at security conferences back in 2009. I used to get asked, "Why/how is this relevant? You should talk about something else; I don't get it," but now it's a common subject. Never think something you're interested in is some fringe thing that won't ever be important or relevant, because you just can't tell.

Q. What cool/interesting things have you written about/researched/discovered?

CB: I'm credited with what is likely the first IM (Instant Messaging) rootkit, and have also had issues fixed across various sites such as ImageShack and Myspace, and killed off a worm on Google's Orkut, which got me on its hall of fame page (or what counted as its hall of fame page before it became "official." Yes, this is quite a long time ago now).

Q. What's the biggest security failure you've seen/experienced?

CB: A relative, despite me telling them as much as I could about security and scams, phoned me up one day to tell me they'd had a "security alert" on their desktop and they'd paid someone to fix their computer via a telephone call. On the bright side, I could use their "customer support" login to access the scammer's fake support portal and got a blog out of it. Probably not such a good thing for the relative, but at least they got their money back.

Q. Advice for newcomers to the field?

CB: Your background doesn't have to be awash with security certs or even a computing degree. My degree is fine art. Many of the tools you use now were made by non-STEM people. You're as likely to run into musicians, filmmakers, and mountain hikers as you are "pure" computer programmers.

Conclusion

This wraps up our review of Q1 2017, the most prominent threats and our predictions of what we might see next quarter. To review, here is a list of the key takeaways from this report that you can share with friends and family over the coming weeks:

- Cerber ransomware took over as the top dog as far as distribution and market share.
- Locky ransomware has dropped off the map, likely due to a desired change by the controllers of the Necurs spam botnet. However, with a lack of new Locky versions being developed since before the beginning of the year, the fate of its creators are unknown.
- The Mac threat landscape saw a surge of new malware and backdoors in Q1 2017, including a new Mac ransomware (FindZip).
- On the Android side, two notable malware families have been causing a lot of trouble. HiddenAds.lck, which locks the device from being able to remove the app, therefore allowing for more advertisement revenue for the creators, and Jisut, a mobile ransomware family that has been spreading like wildfire.
- In the exploit kit world, RIG EK continues to have the greatest market share of the few exploit kits that are still active, and we expect this to continue. RIG's exploit kit remains on top mainly due to its lack of competition rather than its technical sophistication.
- Malicious spam campaigns have also started using password-protected zipped files and protected Microsoft Office documents to evade auto-analysis sandboxes used by security researchers.
- In social media scams, users were bombarded with links to WWE nude photo dumps that led to gift card survey scams.
- Tech support scammers, finding difficulty working with North American payment processors, have begun accepting alternate forms of payment, such as Apple gift cards and bitcoin.

Looking ahead to Q2 2017

- We expect to see continued heavy distribution of Cerber through Q2 2017 due to new developments made to the malware design and its continued use of the Ransomware as a Service (RaaS) model.
- As far as Cerber losing its crown, it is unlikely within the next quarter that any competitor will rise in market share enough to dethrone Cerber, barring something happening to the developers of Cerber and their ability to develop and distribute the ransomware.
- The continued heavy development of Mac malware throughout Q2 is highly likely.
- The Android ransomware Jisut is expected to continue its trend of high distribution and spread; we predict the same for HiddenAds.lck.
- Distribution mechanisms are likely going to develop new features and functionality, be it through social engineering tactics employed by exploit kits and malicious spam or from the discovery of new exploits, potentially revitalizing the exploit kit market.
- Finally, in the world of scams, we expect to see an uptick of exit scams and tech support scammers using social media advertising to scam each other. At the same time, we predict the increase collaboration of PUPs and TSS through the spread of tech support scammer advertisements being pushed alongside Potentially Unwanted Programs.

It has been a fascinating quarter, and if this year sticks with the same trends seen in previous years, we can expect very interesting spring and summer months. Thanks for reading; catch you next time.

Contributors

Pedro Bustamante – Editor-in-chief
Adam Kujawa – Editor/Windows malware
Thomas Reed – Mac malware
Armando Orozco – Android malware
Nathan Collier – Android malware
Jerome Segura – Exploits
Adam McNeil – Malicious spam
William Tsing – Tech support scams
Christopher Boyd – Social media scams

ABOUT MALWAREBYTES

Malwarebytes is the next-gen cybersecurity company that millions worldwide trust. Malwarebytes proactively protects people and businesses against dangerous threats such as malware, ransomware, and exploits that escape detection by traditional antivirus solutions. The company's flagship product combines advanced heuristic threat detection with signature-less technologies to detect and stop a cyberattack before damage occurs. More than 10,000 businesses worldwide use, trust, and recommend Malwarebytes. Founded in 2008, the company is headquartered in California, with offices in Europe and Asia, and a global team of threat researchers and security experts.

 Santa Clara, CA

 malwarebytes.com

 corporate-sales@malwarebytes.com

 1.800.520.2796