# TABLE OF CONTENTS

| 01 | Introduction |
| 02 | Executive summary |
| 03 | Windows malware |
| 03 | GlobeImposter |
| 05 | Locky |
| 06 | Trickbot |
| 08 | Emotet |
| 09 | Mac malware |
| 10 | Android malware |
| 11 | Malicious spam |
| 13 | Exploit kits |
| 14 | Astrum via AdGholas |
| 15 | New exploit kits |
| 16 | Experiments with current EKs |
| 17 | EKs and ransomware |
| 18 | Potentially unwanted programs |
| 18 | SmartScreen |
| 20 | Adware.Elex update |
| 21 | Tech support scams |
| 22 | FTC pays back victims |
| 23 | Breaches |
| 24 | Equifax |
| 25 | Personally identifiable information |
| 26 | Data breaches |
| 27 | Arrests and convictions |
| 27 | MalwareTech |
| 27 | Game of Thrones leakers |
| 27 | OPM breach |
| 28 | Crackas with Attitude |
| 28 | Fireball malware |
| 29 | Researcher profile |
| 29 | Mieke Verburgh |
| 31 | Key takeaways |
| 32 | Key predictions |
| 33 | Conclusion |
| 33 | Contributors |
Introduction

As summer comes to an end and the leaves begin to change, it’s time again for the Malwarebytes Cybercrime Tactics and Techniques report.

The third quarter of 2017 brought with it a number of events that left us in awe and disbelief. From the embarrassing leak of over 143 million confidential records from one of the world’s largest security and fraud mitigation specialists, to the arrest of the famed security researcher dubbed “hero” after helping to stop the most widespread ransomware attack of all time—this quarter has seen it all.

In this edition of the Cybercrime tactics and techniques report, we’ll cover the latest in malware and other threats, including one of the most sophisticated malvertising operations we’ve ever seen, and discuss how spam is a driving factor in the spread of dangerous ransomware families such as Locky and GlobeImposter. We’ll also highlight a number of insights for Mac users and detail information surrounding a new Trojan targeting Android phones. Finally, we’ll profile long-time research employee Mieke Verbugh.

So hold on to your hats and let’s dive into this report as you would a freshly raked pile of leaves on a cool fall day!
Executive summary

Ransomware is once again showing no signs of stopping this quarter. The Cerber ransomware family continues to dominate the ransomware scene, but the reemergence of Locky will challenge its dominance in quarters to come. The continued use of spam as a driving force behind the distribution of new samples remains constant between both malware families.

While spam may be the catalyst to deliver new malware samples to unsuspecting email recipients, attackers continue the use of exploit kits to install various ransomware strains to vulnerable machines.

In the second half of the quarter, popular exploit kit Rig started serving up the PrincessLocker and GlobeImposter ransomware families. To provide some competition in an otherwise slow market, the Disdain exploit kit appeared on the scene in early August.

Thankfully, our predictions of future NSA-style exploits have insofar failed to materialize. Thus, exploit kits must rely on outdated vulnerabilities and poorly maintained computers for successful exploitation to occur. Luckily for the attackers, there are still plenty of these machines available.

In breach news, the Equifax breach affecting an estimated 143 million confidential records has dominated the news cycle. From botched responses to fake websites, the handling of this incident by one of the world’s leading fraud mitigation and security specialists leaves a lot to be desired. Although attacks against retail institutions have been on a decline, the number of compromised records remains on par with quarters past. Breaches of proprietary systems remain high, but law-enforcement continues to make strides in their efforts to combat such attacks.

This quarter also marked arrests relating to several high-profile incidents, including those responsible for the attack on the Office of Personnel and Management, HBO, CIA Director John Brennen, as well as the alleged operators of the Fireball and Kronos malware families. Additionally, the FTC announced a $10 million dollar fund that will be used to assist the recovery efforts of victims from one of the most successful tech support scams ever, Advanced Tech Support.

The evolutions in the tactics and techniques of cybercriminals never ceases to amaze, and this quarter proves yet again that determined attackers will stop at nothing to compromise valuable information. The increasing attacks on corporate infrastructure are terrifying when taking into account the sheer volume of data companies possess on their clients. Companies and individuals must remain diligent in the efforts to combat unauthorized access, and we all must be proactive in the fight by applying timely updates to crucial systems and ensuring full compliance of standard security practices.
Windows malware

The last quarter really shook up the Windows malware scene. Ransomware flooded the marketplace, unobfuscated for the most part. However this quarter, the main channels of distribution for malware (exploit kits and malicious spam) started pushing out more obfuscated malware in an attempt to hide from security solutions.

That being said, we are still observing an immense amount of ransomware hiding in plain sight, as well as cryptocurrency miners and spyware.

This time, we are going to look at a few malware families that are up-and-coming, and provide updates on families that just wont quit.

**GlobeImposter**

**GlobeImposter** derives its name from a previous ransomware known as **Globe Ransomware**, mimicking the same language and format of the Globe family.

GlobeImposter has undergone a number of changes in the past few months and is mostly distributed via spam. In a campaign called **Blank Slate**, emails arrive with no subject or text, but instead a malicious attachment.

Victims who open the specially-crafted Office documents or Microsoft script files will get infected with the ransomware binary. This binary will be retrieved by the decoy attachment from a remote server.

![GlobeImposter encryption screen](Image)
In a recent spam campaign, we witnessed emails containing both an attachment and a malicious URL that resulted in different variants of GlobeImposter:

![Spam email example](image)

Figure 2. GlobeImposter malSpam attack email

You may notice the typo ‘TOP’ instead of Tor, which should be all lowercase.

Finally, it’s worth noting that some spam campaigns have spread Locky instead of GlobeImposter, with a very similar modus operandi.

![Decryption page example](image)

Figure 3. GlobeImposter decryption page
Locky

If you’ve been keeping up with Malwarebytes Labs blog and our Cybercrime tactics and techniques reports, then you’re probably getting tired of hearing about Locky. Trust us, we are too!

As a refresher, this ransomware is known for its huge campaigns with daily payloads. Locky is not the work of newcomers—lots of time and money was invested in the spam botnet consisting of compromised web servers used to host malicious Locky payloads.

In May of this year, Locky was nowhere to be found. Instead, the ransomware Jaff was being spread by the Necurs botnet, which is currently the largest malicious spam spreading botnet. Jaff was being distributed through email with a zipped attachment which, when opened, would execute a script that downloaded and executed the ransomware.

In June, Locky came back after a free decryptor for the Jaff ransomware was released. Locky was using the extension .loptr and was being distributed the same way as Jaff. By August, Locky changed extensions again. This time .diablo6 was being used as the extension and the attack email included a zipped .vbs file attached to it. Shortly after, Locky used another new extension: .lukitus.

Finally, in September, new variants of Locky were observed using the latest extension, .ykcol. Locky developers must be running out of creative ideas for extensions, since .ykcol is just Locky spelled backwards.

Locky has proven to be a resilient ransomware strain with a history of long periods of inactivity. Instead of trying to make predictions on how this family may perform in Q4, we would instead like to remind readers to be careful when opening attachments, and to always keep security solutions updated and ready to mitigate these types of attacks.
Last year, a credential stealing malware called TrickBot was first observed in the wild. Based on analysis performed by the Malwarebytes Labs team, as well as other notable security researchers, it was determined that TrickBot was the next project of the team behind Dyreza, another popular information-stealing malware. Although not as technically sophisticated as other families, researchers observed the potential this malware had to do some serious damage in the future.

Fast forward to July of this year. A new version of TrickBot started showing up via drive-by exploits and malicious spam. On the drive-by front, we observed RIG exploit kit pushing this malware. On the malspam side, it's your run-of-the-mill bank fraud phish, where a user is expected to open a link or attachment based on the assumption that the email has come from a legitimate banking organization.

More data theft

One feature that is included in the newest version of TrickBot is the ability to steal data, including saved credentials from Microsoft Outlook. It also grabs browser cookies and history, likely to steal as many valid credentials as possible.

An interesting and somewhat rare characteristic we observed while analyzing this sample was the immense amount of debug strings for every action being taken by the malware. This points toward two possibilities. First, it's possible this code could have been stolen from a legitimate software source and incorporated into the malware. Second, this version was not meant to be released in the wild, as it's still in development.

```c
Fetch_outlook_data( 
    (Int)L"Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook", &v1);
Fetch_outlook_data((Int)L"Software\Microsoft\Office\15.0\Outlook\Profiles\Outlook", &v1);
  v3 = &v1;
Fetch_outlook_data((Int)L"Software\mchar t[56]\t\Office\16.0\Outlook\Profiles\Outlook", &v1);
  System::linkproc__DynArraySetLength(v6);
  *(V[1] + unk_487670 + v6 - 1) = v10[v6 - 1];
  ++v6;
  --v5;
}while ( v5 );
)
  v7 = dword_487670;
  v8 = unknown lname 63(unk_487670);
  unknown_487670(dword_487670, "getdata", "test", unk_487670, v8, "test", v7, v10, v11, v12, v13, v14, v15, v16);
  writefsword(0, v17);
  v19 = (char -)gloc_4DA4D8;
```

Figure 5. TrickBot data theft functionality
**New infection feature**

TrickBot also adds the functionality to enumerate the victim network, scan for vulnerable Server Message Block (SMB) ports, steal login credentials, and propagate through a network, all while installing itself on connected systems using a PowerShell script.

So as it turns out, TrickBot turns into TrickWorm! This functionality was originally discovered by [FlashPoint](https://www.flashpoint.com/) and [Deloitte](https://www2.deloitte.com/).

The good news is, based on analysis, this functionality isn’t operational in the versions we have observed in the wild. However, since the code to utilize worm functionality is included in the binary, it’s likely only a matter of time before the actors behind TrickBot start using it.

**Why is it important?**

What’s the relevance of TrickBot using worm functionality in this way? Utilizing SMB exploits, credential stealing, and lateral movement is not unlike the functionality of the WannaCry and NotPetya ransomware families observed earlier this year.

This does not imply attribution, but rather something we see all the time in the InfoSec community: bad guys copying bad guys. When one attack method is observed as being successful, criminals often flock to that method and either directly copy or adapt their attacks to match. We’ve seen it before with exploit kits and ransomware, and will likely see it again.
Emotet

In recent months, Malwarebytes Labs has observed several active spam campaigns delivering the Emotet malware through malicious .doc files containing obfuscated macros.

Emotet is a banking Trojan first detected by Trend Micro in 2014. The malware is used to steal bank account details by intercepting network traffic, and is still actively being developed with different function modules.

In order to be infected, four user interactions are required:

- Malicious email is received.
- Attached Word document is opened.
- Enabling the macro allows malicious activity spawned through PowerShell.
- Emotet Trojan is installed to victim machine.

Once a foothold is established, the Emotet malware turns each infected machine into a bot that is then used to target and infect new victims.

Since its first version, Emotet has continued to evolve into a modular Trojan horse to take advantage of several evasions, persistence, and spreading techniques. It also downloads additional malware such as Dridex or TrickBot to harvest banking and other credentials.

This method of social engineering via malicious spam has become the norm this year, with a major increase in malicious spam malware distribution and a drop in exploit kit infections. You can expect that as we move into Q4, we will see continued use of this distribution method and its associated tricks from multiple malware families.

The Word document uses a well-known social engineering trick to entice users to install the malware. The document claims it has been “protected” and requests that the user activate macros in order to see its contents.
Mac malware

Mac malware has seen a significant rise this year. There has been more than a 240 percent increase in malware over the last year—and we still have one more quarter to go. And while Mac malware proliferation slowed slightly in Q3, PUPs were Mac users biggest problem this quarter.

PUP vendors are becoming bolder on the Mac, even invading the Mac App Store. PUPs are likely to continue to increase in prevalence on the Mac since they are not blocked by the Mac’s built-in anti-malware protections and are not well detected by most security vendors.

Among malware threats on the Mac, an interesting new trend has emerged. Until recently, most Mac malware would be detected by Apple and blocked at the system level, thus shutting down the ability for the malware to run forever. In rare cases, malware would continue to mutate for a short while, but would eventually disappear after adequate detections were released. The perfect example of this is the now defunct MacDefender, which was involved in an escalating war where the malware would re-appear with a new name as soon as Apple blocked the old one. However, this only lasted for a few weeks, and then the threat of MacDefender ended forever.

Recently, however, this has changed. In June, a new variant of OceanLotus, first seen in 2015, was discovered. In July, a variant of the Fruitfly (aka Quimitchin) malware, originally discovered by Malwarebytes in January, was found infecting victims in different circumstances than the original. Later that same month, a new variant of Leverage, last seen in 2013, was found circulating the web.

This shows that Macs are beginning to attract more persistent adversaries who are starting to see the value in infecting Mac users. Macs still have a minority market share, but they have become increasingly popular, and their mythical immunity to malware has been revealed to be just that: a myth.
Android malware

Over the last couple of quarters we've seen a steady rise in clickers targeting Android users. Clicker Trojans attempt to generate revenue by continually making website connections behind the scenes, without the victim's knowledge. A new family we're seeing is Android/Trojan.Clicker.hyj. This Trojan is capable of click fraud, as well as spamming a victim's contact list as a means to infect additional users.

These apps have interesting package names like com.java.mail and org.mac.word that are likely used to throw off victims and researchers by making them appear legitimate and trustworthy.

Android/Trojan.Clicker.hyj is a heavily obfuscated app that is capable of a variety of actions due to an included set of functions packaged within the app. Stored within that package are multiple JavaScript files used to carry out actions when a URL is encountered, such as finding the buttons to click on a website, and then actually clicking the button to facilitate an action.

As with most malware, the end goal for Android/Trojan.Clicker.hyj is to make money. It has two methods of generating revenue—fake site visits and paid subscription services. It also helps that the authors have a high number of apps being distributed, which lines their pockets with a steady income stream.

This threat can be found in alternative markets and not in Google Play. We suggest sticking to trusted sources for your favorite and new apps.

Along with click fraud, this threat is also capable of accessing the victim's contact list and spamming those entries with messages to sign up for a paid video library subscription.
Malicious spam

As we have seen throughout this report, spam continues to be a catalyst to aid malicious actors in the collection of information, infiltration of networks, and the delivery of malware to vulnerable systems. Some of the most widely-distributed malware families use spam as a driving force for the proliferation of new samples. Why? Because spam is a simple, reliable, and time-tested mechanism to distribute malware and phishing campaigns.

Threat attackers have a number of tools at their disposal to facilitate the spread of malicious spam. Mass mailing botnets, such as the well-established Necurs botnet, are capable of disseminating millions of emails on a daily basis. These emails may contain anything from pump-and-dump schemes to the latest samples of Locky or Trickbot. This barrage of mail floods inboxes around the globe in the hopes of enticing even just a fraction of the recipients into clicking the attached file or link.

Spammers are aware that users of popular email programs rarely see these types of emails due to strict filtering. To attempt to bypass these constantly evolving protections, they utilize automated technologies to aid in the generation of content and the randomization of payloads. Thus, it’s not uncommon to see hundreds of thousands of variations in a single campaign.

For those without access or resources to acquire potentially costly botnet services, there are more economical means to distribute emails to the masses.

Bulk emailing programs allow anyone with the technical ability to cut and paste to send emails to unsuspecting victims, all while working to hide the perpetrators’ identity and origin. These programs are capable of using email addresses and passwords of previous and unrelated data breaches to send emails to potential victims. They can also use previously compromised login credentials to send mail on behalf of established users, thus helping to bypass spam filters. If you’ve ever received a fake email from a friend that distributes a phishing or malware campaign—this infection vector is the likely culprit.
While large campaigns such as Locky or Cerber receive lots of publicity due to their size, a myriad of unreported campaigns distribute email on a smaller scale. These smaller campaigns, often using bulk emailing programs and craftily worded emails, are directed toward well-researched targets and distributed with custom malware to help improve the success of infection rates.

It's common for the malicious traits of these smaller campaigns to be grouped within broadly-defined signatures due to the relatively small sample set. These signatures, often referred to as generic signatures, encompass a vast array of malware characteristics and behaviors.

The following chart highlights the top 20 malware variants we have seen with the Malwarebytes Email Telemetry system over the last quarter. The chart helps visualize the percentage that these generic signatures make up of the overall collection of received samples compared to that of more established campaigns.

The vast majority of sent emails are never seen by human eyes. While millions of emails may be sent in a particular campaign, only a small subset will ever be read, and even fewer will click on the embedded attachment or link. It's for this reason that success of these campaigns is measured in the hundredths of a percent compared to the number of messages sent. As the saying goes: Spam filters and signatures have to be successful 100 percent of the time; attackers need to be successful only once.

For this reason, we will continue to see spam as a dominant force in the spread of malicious campaigns.
Exploit kits

In this quarter we have noticed some interesting developments in the exploit kit landscape, with various experiments taking place. For instance, the use of SSL by a smaller player shows us defenders what we might be dealing with soon, and a new exploit kit appeared on the scene targeting Internet Explorer. Will this new EK become a threat to existing players? Additionally, the decrease in ransomware distribution is an unexpected but pleasant change.

Compromised sites leading to exploit kits?
Compromised sites continue for the most part to redirect to social engineering schemes such as tech support scams (via EITest, which seems to be one of the few long-standing campaigns still active) or the HoeflerText trick. But there are some exceptions every now and again when a personal website is used to redirect to an exploit kit.

There’s no question that the quality of exploitation tools has a direct impact on the drive-by distribution landscape. It’s not because Content Management Systems all of a sudden became more secure (they haven’t) but rather it’s the ever-important ROI that dictates online criminals’ actions.
Astrum via AdGholas

In late June and early July, we spotted a few waves of one of the most sophisticated malvertising operations to date. This provided us with a glimpse of some campaigns that are going on but are hard to identify.

AdGholas is the name given to a group of malvertisers that have mastered the skills to fly under the radar. By creating fake identities and triaging web traffic with great granularity, they are able to avoid getting caught.

Another interesting aspect is their use of SSL to mask traffic between client and server. This is combined with an exploit kit that also uses encryption (on top of other tricks such as steganography) to silently infect victims.

Figure 13. AdGholas malvertising example

In addition to using an information disclosure bug (CVE-2017-002), Astrum uses several vulnerabilities for Flash Player (CVE-201508651, CVE-2016-1019, CVE-2016-4117).

Figure 14. SSL used in exploit kit communication
New exploit kits

Disdain EK is the name given to a new exploit kit that appeared in early August via malvertising. It resembles Terror EK since both have similar URI patterns. Although both share this semblance, the code comprising the two families is quite different.

Disdain is primarily exploiting Internet Explorer vulnerabilities. Despite several campaigns witnessed distributing different payloads, we saw a reduced number of infections toward the end of this quarter.

We have also seen variations of existing or defunct exploit kits in the past few months. At the moment, it appears more work is being put into distribution campaigns (i.e. malvertising) than the toolkits necessary to infect victims.

![Disdain exploit kit traffic distributing different payloads](Figure 15. Disdain exploit kit traffic distributing different payloads)
Experiments with current EKs

Despite a slow-down in development and new features within common exploit kits, we spotted an interesting—and worrying—trend. It's one thing for top exploit kits to try evasion techniques and make detection via Intrusion Detection Systems (IDS) more difficult, but it's another when the less sophisticated ones start testing these things out.

This was the case with Terror EK, itself largely inspired by other exploit kits such as Sundown EK.

The challenge for defenders is in the lack of visibility when network traffic becomes encrypted. The types of tools or techniques necessary for deobfuscation (i.e. man-in-the-middle) may not always be successful, and often aren’t accepted in enterprise environments.

We expect to see more and more malicious traffic (including exploit kits) moving towards HTTPS since its overall adoption is progressing at a fast pace—and rightfully so.

Figure 16. Terror EK experimenting to avoid IDS detection
EKs and ransomware

Malicious spam is the main source of ransomware infections. For this reason, it is a little bit unusual to catch exploit kits distributing such payloads.

In late August and September, we witnessed the RIG EK serving up the PrincessLocker and GlobeImposter ransomware families. These were not the most popular distribution campaigns (Seamless and Fobos are by far the most common ones), which made us wonder if this was some kind of experiment by a new affiliate.

PrincessLocker was already around last year and its developer made some changes to render decryption without the key impossible.

While GlobeImposter is a popular ransomware, it is still surprising to see it in an exploit kit delivery flow. This was not a widespread campaign like the others, and could indicate someone testing various delivery mechanisms and payloads.

These days, there is no excuse for getting infected with a drive-by download attack. Indeed, the vulnerabilities used by exploit kits have been patched (years ago in some cases). But we need to remain vigilant, as there is some renewed activity with actors trying to compete with interesting new features to rival the dominant, but technically weak, RIG EK.
Potentially unwanted programs

When we started detecting Potentially Unwanted Programs (PUPs), the majority were toolbars and fake scanners. We still see many of the same type of PUPs today. The biggest differences are the efforts undertaken by PUP developers to spread their wares and ensure they can’t be removed. This quarter, we’ve seen this goal realized in the SmartScreen program.

In addition, we learned more about a PUP case that reached a bit too far into a user’s system and what the fallout was when law enforcement got involved.

**SmartScreen**

The adware industry is starting to use more aggressive methods to get their advertisements to potential viewers. In the past, a lot of programs that displayed advertisements could be classified as PUPs. That’s because they gave the user something in return that could be conceived as useful or beneficial. Nowadays, most programs whose main purpose is to advertise are classified as malware, because they offer nothing in return besides false promises. On top of this, the programs are getting more and more intrusive.

SmartScreen is an outstanding example of this behavior. It’s one of the more nasty examples of an adware trend we’ve witnessed. This software is bundled with adware and PUPs to act as protection against their removal. It uses two methods to achieve this goal.

Figure 20. SmartScreen software termination functionality
SmartScreen hooks into the Windows `CreateProcess` function so it can inspect new processes before they are allowed to run. In order to prevent the adware from being removed from the affected system, it blocks security software from running or even being installed. It does this based on the security certificate and the process name. The user will get an error message stating, “The requested resource is in use.”

The program also protects certain processes from being terminated and stops the user from removing critical files and registry keys. The user will get an error message that says “Unable to delete” when attempting to perform this action.

The suspected business model is not hard to ascertain since SmartScreen includes an adfraud component capable of earning money for threat creators. The bundlers are also happy to include the package, as it prevents victims from being able to remove the unwanted software. So it’s a win/win for the bad guys.

Being able to remove this infection is an ongoing battle, as the threat actors actively monitor what the research community is doing and develop countermeasures as soon as new defenses are published.
**Adware.Elex update**

Last quarter we wrote about a pretty ominous threat in the form of an adware family called Fireball. This family was of Chinese origin and included a backdoor that allowed full remote command execution on the victim machine.

The adware came in a bundler with other potentially unwanted software, and at one point was reported to have spread to 250 million systems worldwide. The potential threat could have resulted in the victim systems being:

- infected with spyware or ransomware
- used in a botnet to DDoS web servers
- used as a farm for Bitcoin miners
- used to spread malicious spam to other users

The good news is that in June of this year, arrests of 11 Rafotech employees (the company behind Fireball) were made in Beijing. Apparently, the employees arrested were aware of the adware’s capabilities and still allowed it to infect users.

The targets of this malware were specifically non-Chinese users as the adware avoided infecting Chinese systems so as not to break domestic laws.

This is not entirely uncommon to see in countries that spend more time chasing after foreign attackers than internal ones. We’ve seen this kind of behavior especially in eastern Europe and Russia where attacking Western users instead of anyone in their country of origin is a better way to do business and keep the officials off your tail.

With the Fireball creators in police custody, this means that we won’t be seeing any more infections, right? Not exactly. Looking at our stats from this quarter, you can see a significant decrease in the amount of infected systems where we detected Fireball, however it is not gone entirely. As a refresher, our detection name for this threat is Adware.Elex.

This continued infection stream is likely related to users who had a pre-existing infection that finally got around to using Malwarebytes to clean their system. It is also possible that versions of Fireball are still being distributed through third-party bundlers. Either way, we hope this threat goes away soon and that all developers understand the importance of securing their code so it can’t be used by unintended attackers to cause havoc.
Tech support scams

It is no surprise that most tech support scams are aimed at English speakers. In fact, you can often see fraudulent sites showing the flags of the US, Canada, the UK, and Australia as countries for which they offer support. When taking into account that many boiler rooms are located in India (where English is an official language), this makes sense.

However, tech support scammers have been diversifying into other languages for some time. The modus operandi remains the same, the only difference is where the operators are located.

We have noticed an increase in tech support scams targeting Francophones and have launched some investigations to identify sources. Victims are typically lured via malvertising and custom landing pages that use scare tactics.

We tracked two different operations: one located in Quebec and the other out of Mauritius. The technicians had a slight accent, but their French was otherwise impeccable.

Needless to say, the courtesy stopped there. Scammers are scammers, no matter what language they speak.

Some payment summaries are provide below, including the dreaded notepad invoice.

The fake Microsoft calls are well known in the US, but not as much in other countries, although this change is on the horizon. One of the best ways to avoid getting scammed is to be aware of the tactics and techniques they use.
FTC pays back victims

On August 28, the FTC announced a 10 million dollar fund directed towards victims of one of the most successful tech support scams ever, Advanced Tech Support. ATS is a rare example of a win against scammers. Starting with an initial injunction on December 22 of last year, Florida law enforcement and the FTC conducted a successful shutdown of operations, and recovered a significant amount of funds for restitution. They were able to do this largely because ATS kept significant infrastructure, assets, and personnel in the United States. In addition, ATS had numerous employees leaking incriminating details of the company via social media and website comments. This allowed law enforcement to build a clear, compelling case proving malfeasance.

Unfortunately, $10 million is only a small fraction of the damage done to end users during ATS’ time of operation. Most tech support scams structure their finances in such a way that a small circle of founders get an overwhelming majority of the proceeds. Anecdotally, these founders tend to spend on ostentatious displays of wealth and gifts, making recovery of funds difficult. In the specific case of ATS, the company had financial ties to an external payment processor in Canada allowing them to move funds overseas before coming to the attention of law enforcement. Although mixed outcomes like the above are frustrating, obtaining a clear legal success against a tech support scammer is a rare occurrence, and likely to serve as a mild deterrent against future scams in the US. In the past quarter, Malwarebytes has seen a sharp decline in victim reporting from US-based tech support scammers, and an increase in Canadian-based scams.
Companies face a barrage of attacks from dedicated intruders who will stop at nothing to achieve successful exploitation of confidential systems. From malware and vulnerabilities to phishing attacks and ransomware demands, companies must mitigate a wide range of attack vectors to maintain the integrity and security of their systems. The failure to apply timely updates or to provide the proper training has devastating effects for companies both large and small, and often leads to costly litigation and severe damage to the credibility of the organization.

While there was an overall decrease in the number of high-profile financial attacks against major retailers, the third quarter of 2017 still proved just as dangerous for individual security, as we saw the credentials and personal information of hundreds of millions of people compromised.

Companies ranging from credit bureau Equifax to content provider HBO and even the social media platform Instagram fell victim to cyberattacks and were forced to sit helpless from the sidelines as their proprietary customer information and company data was leaked in a destructive and embarrassingly public fashion.

This section will showcase the largest and most damaging breaches of the past quarter. As always, this report will exclude the various database vulnerabilities reported by security researchers encompassing potentially hundreds of millions of personal records, yet have not been proven to have been compromised by malicious actors.
Equifax

By far the giant elephant in the room is the unfortunate breach of the Equifax database, which compromised the valuable personal information of a whopping 143 million Americans. This means there is a good chance that nearly every US citizen reading this report has been affected. Names, social security numbers, birth dates, addresses, and even in some cases driver’s license IDs and credit card numbers are now at the disposal of the perpetrators responsible for the attack.

To make matters worse, the manner in which Equifax handled the disclosure of this breach could go down in history as a text-book example of how not to handle a public relations disaster.

From the delayed disclosure of information and the early sales of roughly $2 million in shares on behalf of company executives, to the litigation waivers tucked within the flawed verification and fake websites, the response to this breach was bungled from start to finish. What was made clear was how shockingly ill-prepared Equifax was for potential cyberattack. The discovery of company databases secured with the shockingly simple credentials of “admin/admin,” not to mention the disclosure that the Security Chief is a music major whose login credentials were found for sale on the dark web, would make this entire fiasco seem downright comical if not for the severe destruction the release of the information would cause the general public.

Simply put: The operational security (OPSEC) on display by one of the worlds’ largest holders of personal information and self-regarded fraud mitigation and security specialists is shocking and grossly appalling.

The crisis has spawned discussions with security professionals and legislators alike regarding the need to overhaul the mechanisms of how a seemingly simple 9-digit number can be used to uncover all of our most personal information.

If there is any silver lining to this story, it’s that as of this writing the information obtained within this breach has not been made available through any discovered channels. The implications of this are unknown as the attackers may be using the information for their own purposes, or as a means to potentially extract a ransom in exchange for return of the information.

Provided the information stays out of the public domain, damage from the breach will likely remain low. If, however, the information is distributed to the Internet for anyone to download, there could be devastating consequences for decades to come.

For more information on the breach and what to do in the aftermath, read our article: Equifax aftermath: How to protect against identity theft.
Personal identifiable information

In the largest domestic medical breaches of the quarter, Womens Health Group of PA reported a potential compromise of their database affecting 300,000 patients. The Notice of Security Breach incident dated July 18 indicates that patient names, addresses, social security numbers, and medical records could have been affected.

A breach of the Kansas Department of Commerce exposed the records of more than 5 million people located across 10 states to attackers. The information was uncovered through an Open Records request rather than any public disclosure. According to the July 20 report by the Kansas News Service, roughly 5.5 million user accounts and social security numbers were compromised.

On July 21, The New York Times released an article detailing the loss of 1.4 GB of data of an estimated 50,000 Wells Fargo clients. While this number pales in comparison to the Equifax breach, the total sum of funds in the possession of this small group of customers is in excess of tens of billions of dollars. Those who might have such healthy bank accounts with Wells Fargo should monitor their financials closely.

On August 10, reports surfaced of an anonymous attacker who claimed to have stolen the NHS medical records of 1.2 million UK residents. NHS has disputed the claim, although it acknowledges that a breach of the system occurred. Personal details such as names, dates of birth, phone numbers, and email addresses have reportedly been compromised.

The UK-based second-hand electronics dealer CEX announced on August 29 a breach of their system that affects 2 million customers. The company advised attackers may have compromised personal information including names, addresses, and phone numbers.

On August 30, Troy Hunt reported on a massive spambot that had released the credentials of 711 million email users. These email addresses can be used to facilitate the delivery of additional spam messages, or the email credentials can be used by spammers to deliver email from compromised accounts.

On September 1, reports began to surface of a potential attack against Instagram. The company later confirmed that the account credentials of 6 million users may have been compromised. Shortly thereafter, attackers began selling the information of celebrities to willing purchasers on the dark web.

On September 4, the breach notification service LeakBase informed industry members of a database containing over 28 million accounts that included the usernames, email addresses and MD5 hashed passwords for users of Taringa, Latin America's largest social network. Unfortunately for members, MD5 hashing of the passwords won't protect their information.

On September 26, notable security blog KrebsOnSecurity reported a potential breach of Sonic restaurants. The drive-in chain, which has nearly 3,600 locations across the US, was notified about suspicious transactions on some Sonic customers' cards. According to the KrebsOnSecurity post, this breach could affect an estimated 5 million cards—thus making this one of the largest attacks of the quarter.

To round out the quarter, Whole Foods reported on September 28 that customers who made purchases at its in-store restaurants or bars have had their credit card information exposed to hackers. Whole Foods elaborated that those venues used a different point-of-sale system than the primary store checkout systems. Amazon Inc, which recently purchased the national grocer chain, announced that no other Amazon service has been affected.
Data breaches

HBO was the subject of a number of attacks and an apparent massive breach after criminals reportedly obtained everything from full episodes of unreleased shows to sensitive internal documents. The company even saw a number of episodes of fan favorite “Game of Thrones” leaked to the web prior to their official air date.

In September, the popular malware cleaning tool CCleaner, operated by Avast, had its development server compromised. This unfortunate incident allowed an attacker to deploy malware within the legitimate CCleaner application, which was then distributed to users downloading the software. As it turns out, reports at the time of this writing indicate that at least 20 different high-profile technology companies were being targeting with mysterious payloads.

Popular video sharing website Vevo suffered a breach and the subsequent disclosure of 3.12TB of company data. Fortunately for the company, the release of information appears to have been extremely limited. The attackers even removed the information at the request of Vevo admins.

In late September, the Security Exchange Commission (SEC) revealed that hackers may have utilized a vulnerability in 2016 to compromise its database of corporate announcements. This database, known as EDGAR, houses all filings and notices that companies are required to disclose. The SEC regulates the information as a means to keep investors on a level playing field. While the breach of the SEC database does not seem to pose a threat to consumers, it may have allowed hackers to trade on the stock market using the unfair advantage of unpublished information.

On September 25, global accountancy firm Deloitte announced that attackers had compromised confidential emails and the plans of several blue-chip clients. As of this writing, Deloitte says only six companies and some governmental agencies have been affected, but so far these organizations have not been identified.
Looking at the number of breaches and notable attacks, as well as the sheer number of users impacted this quarter, can leave you feeling a bit uneasy, if not downright exposed. That’s why we wanted to offer a brief glimpse into some of the industry and law enforcement successes. Q3 2017 marked the apprehension of several high-profile targets suspected of criminal activity online.

**MalwareTech**

By far one of the most surprising arrests this quarter was of Marcus Hutchins, aka MalwareTech. Just a few months ago, we all praised Hutchins for his assistance in the demise of the infamous WannaCry ransomworm infection. But at the close of this year’s DEF CON convention, FBI agents arrested Hutchins for his reported association with the Kronos malware. (We covered the Kronos malware in two different blog entries on Malwarebytes Labs [here](#) and [here](#).)

Due to a lack of publically available information, we have refrained from offering much perspective on the Marcus Hutchins case. While there are plausible scenarios where a researcher could be affiliated with unsavory individuals in order to extract valuable information that could be used to safeguard the public, we also don’t have enough information to discount the FBI’s claims of his alleged involvement in criminal activity. While the proceedings are on-going, we’ll continue to follow any developments in the case.

**OPM breach**

On August 24, CNN reported that the FBI had arrested a Chinese national for allegedly developing the malware used in the 2015 data theft from computer systems at the Office of Personnel Management (OPM). That particular breach exposed the records of a reported 21.5 million government employees, including those with security clearance applications. The attack was one of the largest breaches of the year.

It’s unclear what role the man had in installing the malware or harvesting the information. Currently, the FBI is only accusing the man of creating the Sakura malware which was used in the attack. As this is an ongoing case, we will continue to follow any developments.

**Game of Thrones leakers**

On August 15, [CNN reported that four men](#) had been arrested in Mumbai, India, in association with the leak of an episode of “Game of Thrones” before its scheduled release date. The individuals in question reportedly worked for Star India, an Indian broadcaster with rights to air the series. A Star India spokeswoman told CNNMoney that the Indian leak is not connected to the larger HBO hack.
Crackas with Attitude

You may recall in late 2015 the shenanigans of the hacking group Crackas with Attitude, who notoriously hacked various US government officials and then leaked the contents of former CIA Director John Brennan’s email account. The group was able to compromise the security of top government officials by simply breaching Brennan’s AOL account. These emails were subsequently leaked to Wikileaks for publication.

On September 8, a federal judge handed down a five-year prison sentence to 23-year-old Justin Liverman for his role in the attacks. While Liverman is not known as the group’s mastermind, he is linked to a number of attacks on behalf of the group.

Fireball malware

Law enforcement authorities in China have arrested 11 individuals suspected of developing the Fireball malware. The malware reportedly infected an estimated 250 million computers across the globe and earned an estimated 80 million yuan ($11.84 million) for the creators. You can read more about the arrests here.
Tell us about how you got started in malware research.

In 2002, I bought my first computer and I still remember that day. I had to call my brother to find out how to shut this thing off. I really didn’t know anything about computers, but that changed very soon.

I love to learn, so that’s why I started to learn basics about Windows. Then I wanted to learn more about websites and web design, so I made some websites and learned how to use Flash. After a while, I got bored with this, and I wanted to learn something new. And that’s how it all started—what I’m doing now.

At the time, when I was still into web design, I registered on some forums to ask for help. I noticed that there were a lot of subforums related to Windows security, and every day a lot of new posts were added. I wondered why these subforums were so popular, so I started to read the posts. It came to my attention that most of the Windows-related issues were a result of malware.

I decided that I wanted to learn all about this because it was a real pest then (and still is a real pest now). I started to follow these posts, reading the instructions and solutions, and asking questions. After a while, when I saw a similar issue posted somewhere else, I realized I could help these people. But I always wanted to learn more and more and more, so I registered at several other security-related forums to gain as much info as I could.

I started to help people in other forums and even started to teach people who wanted to become “malware fighters.”

On one of these forums, I met Marcin (our CEO). His parent’s computer was infected, and I helped him to get rid of the infection. That’s how Marcin also started to become a volunteer in these forums, helping other people.

Marcin then started developing small removal tools and that’s how Malwarebytes came to be. In 2009, I joined the Malwarebytes team.
What do you like to work on?

I like challenges—solving puzzles. If something doesn’t work the way it should, I want to understand why, instead of just being satisfied with the solution. This has helped me a lot with computer and security issues, as every day there’s something new to learn. So this is really general. I like working on anything that I can learn from.

What is the coolest, most interesting, nastiest, or most clever infection you’ve seen?

It was a search engine hijacker that had a very unusual loading point, under the HKLM\software\microsoft\windows nt\currentversion\drivers32 key with value and valuedata:

“aux”=“sysaudio.sys” or “aux2”=“sysaudio.sys”

This was quite a clever approach, as it was hiding in plain sight, especially with the unusual loading point. This was then known as Trojan.Danaol. We saw variants of this afterwards (Gumblar), which were even more advanced.

I’m not a writer at all, but wanted to make people aware of this one, so I blogged about it here, where it has helped many users. I even received a response from the malware authors. They used my nickname “miekemoes” in the version info of their files and blocked every site where it had my name in the url or contents.

Anyway, that was an interesting period.

What’s the biggest security failure you’ve seen or experienced?

I don’t have typical examples of security failures, but the most important thing is that security awareness is still lacking for a lot of people. They aren’t securing their company’s data enough, they’re using weak passwords, or they’re click-happy and will click on any link or attachment they receive in their email.

Basically, human error is a big factor in breaches. I believe everyone should be trained and made aware of the dangers of the Internet before even using it.

Advice for newcomers to the field?

Passion and interest for the work is the most important thing here. If there’s passion and a little bit of patience and persistance, then you can learn almost everything.

Who are some of your heroes in the industry?

My boss, Marcin. He’s an example of being passionate, persistant, and willing to learn. Starting from a 14-year-old kid developing his own removal tools and volunteering to help other people to what he is now: CEO of Malwarebytes.

What do you like to work on?

I like challenges—solving puzzles. If something doesn’t work the way it should, I want to understand why, instead of just being satisfied with the solution. This has helped me a lot with computer and security issues, as every day there’s something new to learn. So this is really general. I like working on anything that I can learn from.
Key takeaways

• Equifax breach compromised the names, social security numbers, addresses, driver’s license IDs, and credit card numbers of an estimated 143 million individuals.

• Cerber remained the dominant ransomware for the fourth quarter in a row, but Locky is closing in on that lead.

• Spam continues to be a dominant force in the spread of malware. Dominant malware families such as Locky, Trickbot, GlobeImposter, PrincessLocker, and Emotet all use spam as a distribution mechanism for new samples.

• Activity from exploit kits is on the decline, although RIG, Disdain, and Terror continue to spread various ransomware campaigns.

• Astrum via AdGholas is one of the most sophisticated malvertising operations we’ve seen to date due to the use of SSL and additional exploits to evade detection.

• Mac users have seen a 240 percent increase in the number of malware variants over the last year.

• Android users are being targeted by a new clicker Trojan named Android/Android/Trojan.Android/Trojan. Clicker.hyj that can spread itself through a victim’s contact list.

• Tech support scammers continue their barrage of attacks against English-speaking consumers and are also now targeting Francophones.

• Police across the globe have made arrests in connection with various cybercrimes, including attacks against HBO, the Office of Personnel Management, and CIA Director John Brennen.
Key predictions

Every quarter, we provide you with not only what has happened in the world of cybersecurity, but also what we think might happen in the next quarter. Sometimes we are right, sometimes we are wrong.

The biggest prediction we made was that there was going to be another attack like WannaCry or NotPetya. Fortunately for the people of Earth, this hasn’t happened yet.

We see plenty of cryptocurrency miners being deployed on unpatched systems that could have fallen victim to the WannaCry attack, and we even describe malware that is developing functionality to take advantage of this loophole. However, there has not been a massive, worldwide attack using the Shadowbrokers’ leaked exploit against SMB ports.

We were also wrong about Jaff ransomware. We thought, because of the massive malspam distribution campaign during the WannaCry attack, it would be a big contender for top ransomware this quarter. Once again, fortunately, Jaff seems to be dead. Now you can never expect good malware to stay dead for very long, as we’ve seen time and again with Locky. So, it’s not impossible for Jaff to be back, with better functionality and more capable than before.

The lesson to learn here is to always predict and prepare for the worst and be pleasantly surprised when the world doesn’t actually end.

Key predictions for Q4 2017

- Spam will continue to be a driving force in the delivery of new malware variants.

- Multi-language tech support scams will be on the rise globally, driven by geo-targeted malvertising campaigns.

- We predict a seasonal shift of Indiabased scammers to focus on IRS scams through the next quarter, taking advantage of the upcoming tax season.

- North American tech support scams will most likely shift the majority of their lead generation to a blend of malvertising and license PUP deals.

- We may see a return of fake virus scanners used by system optimizer PUPs to push their products. This is similar to the landscape a few years ago, where you could find a “cleaner” around every corner, and nearly all of them lied to you.

- Exploit kits using SSL in their infection chain will become more common and create new challenges.

- Variants of existing exploit kits or newcomers are likely to show up as there is still room and market share to take away from RIG EK.

- The increase in malware for Android devices is expected to continue into the last quarter.

- The latest clicker malware for mobile devices will morph with new code and more obfuscation to avoid detection by security vendors and to bypass Google Play Protect.

- Emotet has demonstrated the ability to evolve as a highly modular banking Trojan. With the continuing development of this malware family, we will surely see new features soon.
Conclusion

What a quarter it turned out to be! While many of our key predictions from last quarter have yet to materialize, we saw our share of fireworks with the vast number of attacks against critical networks and the prevalence of malware campaigns targeting multiple systems and devices. Attackers never fail to disappoint in their ability to conduct operations that garner the attention of security professionals and the public alike.

As we wrap up the third edition of the Malwarebytes Cybercrime tactics and techniques quarterly report, we would like to remind readers that attacks are indiscriminate, and no system is immune. Remember to conduct regular backups of sensitive information and to always perform due diligence when handing out your confidential information to others. And as always, use a combination of security solutions and best security practices to help mitigate attacks against computer networks.

So as you prepare for Halloween festivities, you may find yourself frightened at all the goblins and monsters that appear on your doorstep demanding your candy. But beware: the truly terrifying monster could be the undiscovered data breach lurking in the darkness waiting to steal your livelihood.

Trick or Treat!

Contributors

Adam Kujawa
Windows malware, Editor-in-Chief

Adam McNeil
Malicious spam, breaches, arrests, Editor-in-Chief

Wendy Zamora
Editor

Jerome Segura
Exploits, Windows malware, Editor

Marcelo Rivero
Windows malware

Siri
Windows malware

Thomas Reed
Mac malware

Armando Orozco
Android malware

William Tsing
Tech support scams

Pieter Arntz
Potentially unwanted programs

Mieke Verburgh
Researcher profile
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.

Copyright © 2017, Malwarebytes. All rights reserved. Malwarebytes and the Malwarebytes logo are trademarks of Malwarebytes. Other marks and brands may be claimed as the property of others. All descriptions and specifications herein are subject to change without notice and are provided without warranty of any kind.