Security Report

2018 GLOBAL SECURITY REPORT

appriver

EXECUTIVE SUMMARY

The AppRiver Global Security Report for 2018 highlights the threats and trends AppRiver Security analysts saw throughout the year.

In 2018, analysts saw banking Trojans gain in popularity, while ransomware usage dipped and became more of a secondary tactic. AppRiver analysts also noted that attackers sent less malware through attachments in favor of sending malicious payloads via infected URLS. Spearphishing attacks remained popular – leveraging lots of new twists on recent attack vectors.

In this report, we will take a deep dive into many of the threats and trends we saw in email security as well as discuss examples of prevalent attacks and explore potential impacts.

TABLE OF CONTENTS

INTRODUCTION

In 2018, threat actors' tactics, traits and techniques continued to morph while security solutions proved they had to be agile enough to evolve and respond just as quickly.

WHILE 2017 WAS DEFINED BY RANSOMWARE RUNNING RAMPANT AND LARGE DATA BREACHES, **APPRIVER SAW A SHIFT TO NEW, YET FAMILIAR TACTICS,** BEING EMBRACED BY THE ADVERSARY ON A WIDE SCALE.

While 2017 was defined by ransomware running rampant and large data breaches, we saw a shift to new, yet familiar tactics, being embraced by the adversary on a wide scale.

In 2018 banking trojans (info stealers) were being distributed at a fever pitch, superseding ransomware. And while malware delivered as an email attachment saw a slight decline, the means of distributing malicious payloads via infected URLs more than made up for the attachment decrease.

Spearphishing attacks such as Business Email Compromises (BECs) continued to turn up the heat in 2018 as they leveraged lots of new twists on recent attack vectors as well as launching attacks from further embedded positions.

Large data breaches continued to dominate 2018 headlines on a nearly daily basis. By the end of the year, most everyone that wasn't already suffering from a serious case of breach-fatigue was by the time January 2019 rolled around.

In this report, we will take a deep dive into many of these and other trends in email security. We will also discuss examples of prevalent attacks and explore potential impacts.

BANKING/INFO-STEALER TROJANS ON THE RISE, CONTINUALLY EVOLVING

Banking trojans have seen somewhat of a renaissance in 2018. Over the course of the year, banking trojans became the most commonly distributed threat type. Though some new ransomware threats such as GandCrab emerged in 2018, the banking malware families dominated the email-threat landscape.

While the ransomware technique has proven to be a very viable cyberattack technique, the attack pendulum has swung from the in-your-face attacks that force victims to pay a ransom to siphoning funds completely under the radar. Many of these malware types are threats that have been around before 2018 but as their use has continued to grow so has their functionality and capabilities.

Unlike ransomware, this family of threats goes to great lengths to keep their infection invisible to the end user and the security measures. They operate stealthily, live off the land by taking advantage of native process, inject code directly into memory to avoid detection and transfer away funds without setting off alarms. Unlike with a Ransomware attack, the victim may not realize they are a victim until funds have been whisked away to some offshore account, most often never to return.

EMAIL-BASED THREATS

Email is by far the most frequent source of advanced attacks. Studying attackers' tools, techniques and procedures, such as Trickbot Trojan, helps us spot emerging threats and protect against them.

The majority of these banking trojans rely heavily on email as a crucial part of their infection chain.

TRICKBOT TROJAN

Trickbot is one of the more recent banking Trojans (2016). Besides targeting a wide array of international banks via its webinjects, Trickbot can also steal from Bitcoin wallets.

The Trickbot Trojan has been consistently attempting to find its way into users' inboxes throughout the year. Trickbot relies heavily on spoofed emails that are carefully crafted to look like legitimate email notifications from reputable financial institutions. The messages AppRiver filters captured were crafted to appear as legitimate "secure" emails from Lloyds Bank. The email requested the recipient to review attached documents, sign and fax back.

This approach is one we have seen before as the purveyors of Trickbot have often used Lloyds, HSBC, Barclays and NatWest themes in their malicious email campaigns. Trickbot distributors usually deliver their malware payload within a macro-enabled word or excel attachment.

Trickbot has received consistent upgrades over its lifecycle. It was seen leveraging the Eternal Blue exploit with MS17-010, thus giving it worm capabilities, not long after WannaCry had such success spreading via its use.

However, its primary functionality is to commit financial theft. Late last year, Trickbot was updated with modules to target cryptocurrency wallets such as Coinbase. It contains routines to disable Windows Defender and other AV, evade sandboxing, code-injection, key-logging, contact scraping and startup persistence. This evolution shows an effort on the part of the distributors to vary their business model to what works best to maximize their return per infection.

EMOTET

EMOTET

Emotet is a banking Trojan that peaked in distribution in Q1 2018 with modules for direct theft from victim bank accounts, information theft, DDoS, and more.

Another and even more prominent threat that we are seeing at an alarming rate is the Emotet banking Trojan. Emotet is another custom Banking Trojan that relies on heavy obfuscation and evasion techniques to go undetected while committing financial theft. Similar to Trickbot, Emotet spreads itself throughout the network by making use of its spreader module which uses brute force attacks within the network as well as leveraging the SMB worm vulnerability EternalBlue. US Cert has said that "Emotet infections have cost SLTT governments up to $1 million per incident to remediate."

Emotet is a very fluid and evasive polymorphic Trojan loader. It was first spotted in the wild in 2014. Since then it has been continuously refined by the authors and has escalated to one of the largest players in the email-spread Malware threat landscape. It began as a Trojan loader for the group's own nefarious purposes.

To avoid detection, indicators of compromise (IoCs) may change as quickly as every 10 minutes with payloads (file hashes) changing every couple of hours or in some cases, quicker. Emotet has morphed into a modular loader where different payload components may easily be utilized by the malicious actors. Some modules or dll's currently or previously used include:

- Enumerator and Worm Spreading Capability – enumerates other resources in the environment, attempts to brute-force admin and user account passwords, and spread laterally throughout the network via the SMB protocol.
- NetPass.exe – a legitimate utility for administrators created by Nirsoft to recover network passwords stored on the system or external drives, mail passwords on Exchange, browser stored passwords (IE7.x & IE8.x), and Messenger passwords.
- WebBrowserPassView – Nirsoft utility designed for recovery of passwords stored

by the most common web browsers.

- MailPassView – Nirsoft utility for the recovery of email passwords. This includes Outlook, Thunderbird, Windows Mail, Gmail, Hotmail and Yahoo Mail accounts.
- Outlook scraping – harvests contacts from Outlook to use for attacks against address book contacts. Exploits the trust between sender and recipient for spreading further.

REMOTE ACCESS TROJANS

Remote Access Trojans, or RATs, provide attackers with complete administrative control of the victim's system. RATs are used for reconnaissance, espionage, financial gain, credential theft, loading additional malware, and more.

In addition to the modules listed above, Emotet also has been observed dropping the following secondary payloads post-infection:

- Banking Trojans: IcedID, Trickbot, Qakbot, Gootkit, Zeus Panda and Dridex
- Remote Access Trojans (RATs): Azorult
- Ransomware: Bitpaymer, Ryuk and Umbrecrypt have been documented from the secondary payload infections, especially after Trickbot.

RANSOMWARE

This type of malware locks away victims' data by encrypting it, then demands a "ransom" to unlock it with a decryption key.

In addition to the modules, some of the latest updates to Emotet include the ability to extract up to 180 days of emails and history from an infected system. The infrastructure also has been upgraded to include dual independent server clusters. This allows for redundancy if one goes down.

From an incident response standpoint, Emotet's aggressive spreading and persistence abilities make it an extremely difficult piece of malware to remove. There are reports, such as the city of Allentown, PA's remediation, where the cost has exceeded a million dollars. In addition, secondary payloads such as Trickbot contain their own unique removal challenges. Remnants of some infections may remain in memory even if the malicious items on disk are removed.

Messages come in a variety of methods, some appear to be typical phishing message with a link to download a malicious Word document. Alternatively, we capture messages with directly attached malicious Word and PDF documents. Quite often these different attack methods run simultaneously. Emotet has been one of the most prolific pieces of malware that our email filters have caught this year with well over 20 million examples caught this year.

MESSAGES COME IN A VARIETY OF METHODS, SOME APPREAR TO BE A **TYPICAL PHISHING MESSAGE** WITH A LINK TO DOWNLOAD A MALICIOUS WORD DOCUMENT.

However, as the coding and sophistication became increasingly refined over time, so did the business model. As such, it has evolved to a distribution model for other threat actors to utilize while the Emotet authors take a cut of the profits. Historically speaking, it does appear there is little variance between follow-up (secondary) malware payloads. This could be interpreted as Emotet authors being very selective in who or what groups they allow to use their loader. The afore mentioned Trickbot happens to be one that we have observed using the Emotet downloader.

GOZI and the CHA

Another malware family that falls squarely into the "Banking Trojan" category is Gozi. We have seen this payload being distributed heavily throughout 2018.

GOZI BANKING TROJAN

Gozi Ursnif virus is one of the most active and widespread bank Trojans in the world. This malicious software was discovered in 2007 and can be installed on your PC without your knowledge, spy and monitor all your activities and behaviors on the Internet.

The Gozi/Ursnif Trojan, whose source code has leaked several times over the years, has a rootkit component, it captures browser and email application passwords, logs keystrokes and captures screenshots. While this malware poses a great threat to the individuals being targeted, an even greater risk is for the business or organization whose network would be exposed if the attack is successful.

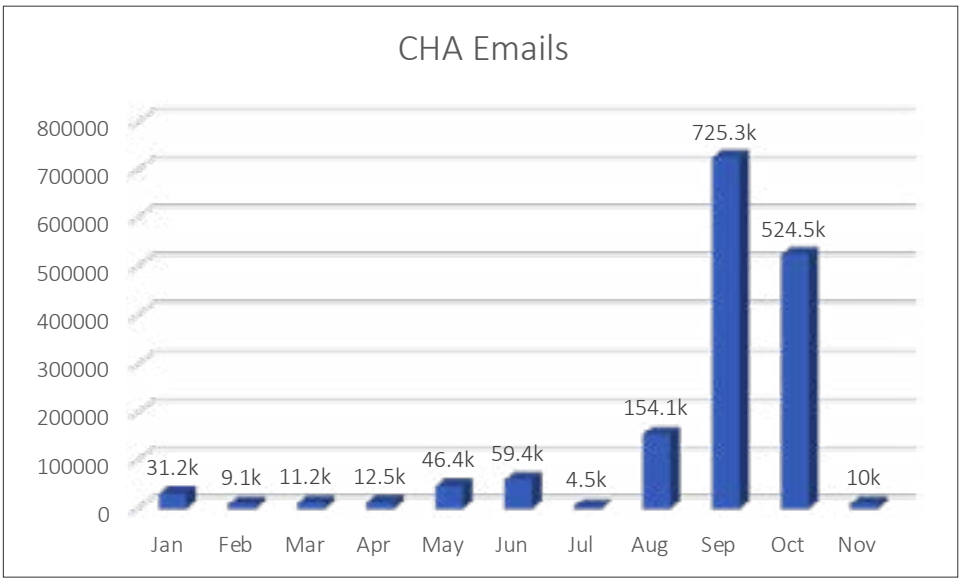
The primary vector of distribution for this attack has been in the form of **Conversation Hijacking Attacks (CHAs)**. We have reported extensively on these attacks over the past several years. They are particularly concerning in that they are a highly effective means of social engineering and the accounts/machines being used to launch these attackers already are compromised.

CONVERSATION HIJACKING ATTACKS

This type of phishing campaign is designed to acquire email credentials with the ultimate goal of spreading banking Trojans A recipient is more likely to open this attachment because they assume it's from someone they know and trust.

A product of account takeovers, CHAs have been capitalizing on the trust established by two individuals that have had a prior conversation (You can read more here for a detailed look at how these attacks work.).

These attacks reached a fever pitch in late summer, peaking in September.



Better protection against banking Trojans

Although the aforementioned malware strains could easily be referred to as Spyware, however, the main focus of their activities is to commit financial theft against businesses and individuals' bank accounts. A robust defense-in-depth approach is necessary to harden your business against these and the vast number of other malware threats that are constantly competing to finding their way onto your network.

DSD ARE PEAKING IN ACTIVITY

Distributed Spam Distraction attacks have been increasing over the past several years. This attack utilizes what is sometimes referred to an **"email bomb"** on the Dark Web, where it is available as a service to anyone willing to spend a few bucks to make an individual's email inbox unusable at the drop of a hat.

DISTRIBUTED SPAM DISTRACTION

The distributing of spam messages specifically by flooding inboxes with a plethora of messages. By flooding the recipient's inbox with emails, attackers can hid fraudulent purchase transaction emails.

DSD attacks are initiated by a web crawler that scours the web for legitimate but unsecured web forms and signs up a user for newsletters and free memberships in-masse. The target then receives a flood of "welcome" emails that make the inbox unusable for a period. This could be used with several different motivations in mind.

What differentiates the **"DSD"** from an **"email bomb"** is the motivation behind flooding the inbox. In a DSD attack the email flood is being leveraged is so that the attacker can hide a fraudulent purchase transaction email in the veritable haystack of noise created by this flood of "welcome" emails, essentially aiming to blindfold the victim to the theft being committed. Often these are purchases from an online retailer that are being shipped to what are very likely an unwitting participant's address.

Unfortunately, there are no preventative measures that can be taken to prevent this attack. Aside from protecting your online accounts and passwords as you normally would. Another annoyance of the attack is that once launched, your email address is destined for a life of bulkmail servitude. Making sure that your email security provider provides a means to direct bulkmail to a dedicated folder is essential once this attack has been launched against you. If you think an attack like this is being levied against you, take immediate action to root out any fraudulent purchase activity and stop the transactions while there is still time.

BECs

BUSINESS EMAIL COMPROMISE

Email impersonation attacks have tricked individuals into sending wire transfers and sensitive customer and employee information to attackers who are impersonating their CEO, boss, or trusted colleague.

While the high-tech Banking Trojans have become more advanced so have social engineering attacks. These attacks put the human employee directly in the crosshairs. Many of these which can be classified as **Business Email Compromise (BECs)** generally take a very low-tech approach but dial up the social engineering to dupe unsuspecting employees into financial loss. These attacks are being committed by an increasingly wide spectrum of attackers and vary in level of complexity. When these phishing attacks are successful it ends with the employee making a major blunder and willingly giving over company money to the bad guys. Don't be that person!

Let's get into the nuts and bolts of some of these type of attacks so you know how to identify them should you ever are hit with one.

HOW BECs WORK

Most of these attacks rely of deception as it relates to the identity of the sender. Most often they are spoofing the "display name" of the CEO and making financial requests. However, we also have seen many other variations where attackers are spoofing the identity of vendors or lower tier employees. Keep in mind that the "From" field in an email can say ANYTHING the sender wants it to.

EXAMINING THE ATTACKS

One example we saw had the attacker posing as the CEO. The message, which is requesting gift cards, is addressed to an employee in the Finance department.

This type of attack is very common, and the litany of reasons the gift cards are needed is endless. If the attacker can sink the hook with this one, they will in turn ask for images of these gift cards with PIN number exposed to be emailed to them which they can then use to make online purchases.

In another variant, the attacker spoofed the name of a lower-level employee in a message to the company Human Resources director. In this attack they are posing as the employee and asking that their payroll information be changed to a new account number.
Of course, they plan on making away with the deposit amount once payday has arrived.

Another type of this attack had the attacker posing as the CEO or another high-ranking executive and requesting a wire transfer. These type of attacks are often the most damaging, with the average cost of this type of attack being $130,000.

Of course, there are all sorts of variations of this third version. Some are so involved that the attacker has breached the inbox of the target to conduct reconnaissance in advance. They study business dealings in depth and learn about relationships with vendors, who's paying who and for what, which enables them to craft a spoofed message for a phony invoice that comes across so naturally that it far more likely to be treated as legitimate and paid. It is not unusual to hear of organizations that have suffered seven figure losses in these elaborate phishing attacks.

It is evident that the rise of professional networking sites such as LinkedIn have helped to fuel this trend by providing the attackers with a never-ending list of names and job titles to appropriately contextualize these phishing attacks. In fact, in virtually every deep dive we do with one of these attacks we find the message recipient is active on LinkedIn, except for a few cases where they were likely gathered from company press releases or websites. We have also observed a recent twist to the BEC. In some instances where the attacker is attempting to channel hop by sending a very vague email to the target with the request to **"text them back"** at a phone number provided. Since this immediately takes the email security out of the equation (by switching to SMS) this could be embraced more going forward.

AN ATTACKER'S INFRASTRUCTURE

Behind the Curtain of Business Email Compromise Wire Transfer Attacks

It's a cautionary tale yet one we see happen over and over - and one that could have cost a company more than $250,000.

Earlier this year, AppRiver's Advanced Email Filtering service successfully blocked an attempted Business Email Compromise attack in which the malicious actor was seeking a wire transfer totaling more than $250,000.

Here is how it happened.

The attacker was able to compromise the email account of Company A. Once inside the email account, he was able to gather information to initiate an attack.

Once the attacker had what he needed, he went to work crafting a simple invoice email from a vendor Company A had previous and multiple dealings with. To add an air of legitimacy, the attacker went so far as to create a false history of previous responses and dates on the email chain – giving it the appearance of a typical invoice payment request. Taking it one step farther, the cybercriminal registered a domain just one letter different from the vendor's legitimate domain.

Similar to most higher-end BEC attacks, this one simple invoice led to banking information changes combined with the wire transfer request.

Thankfully, AppRiver's Advanced Email Filtering service was able to stop the transaction from happening.

How Deep Does This Rabbit Hole Go?

This specific actor/group responsible for the attack had sent two of these wire transfer attacks that same day using the exact same techniques, tactics and procedures. Since their emails were so easily attributable, our curiosity was sparked, we wanted to see how much more could be exposed. We began to perform DNS who is queries and ended up with some common patterns.

The actors had used the same nonexistent street address with minor, but easily recognizable, variations when registering their fictitious domains. That pattern alone made it much easier to find additional information on their attacks. For the domains still active, they use the same hosting provider who specializes in payment via Bitcoins for domain registration and hosting.

During our research, we found other internet posts related to this actor or group on ripoffreport and reddit. These detailed similar scams or fraudulent purchases this same actor/group had used in the past.

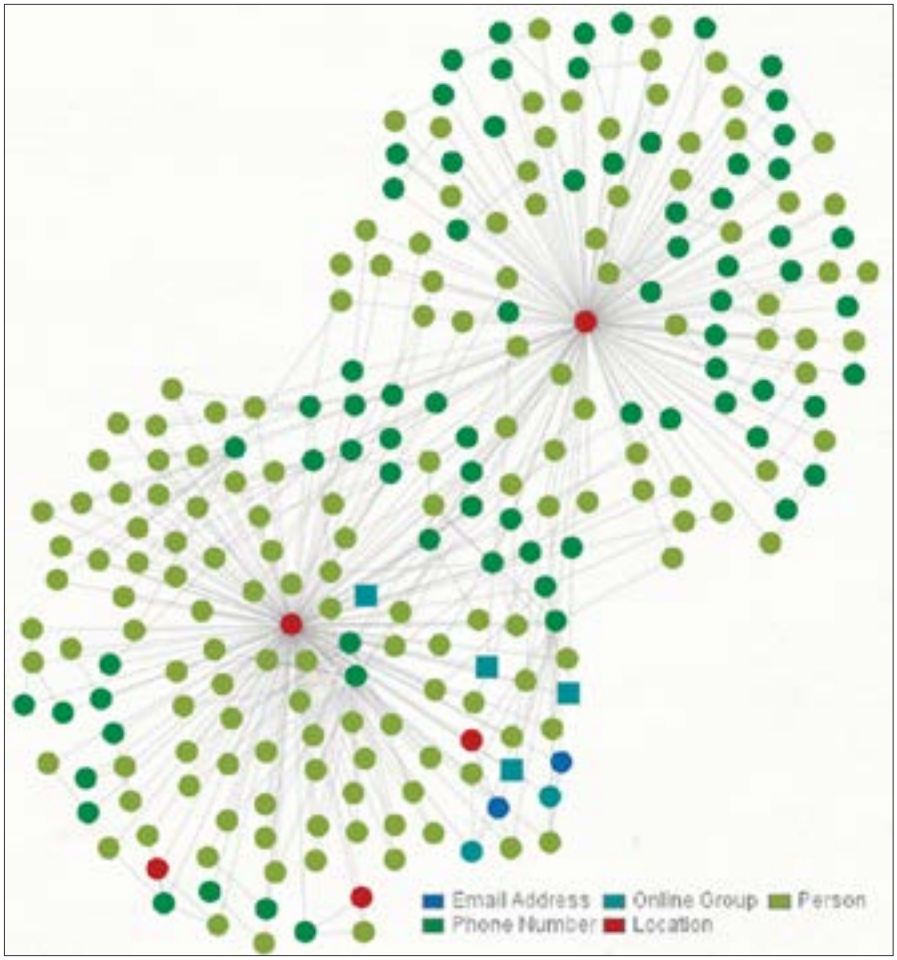
After the dust settled, we had uncovered the below:

- 1,103 fraudulent dspoofing legitimate companies going back to June 2015 - present
- 293 fictitious personal names used to register the domains (including one Biggy Smallz)
- 77 unique phone numbers for the registrations

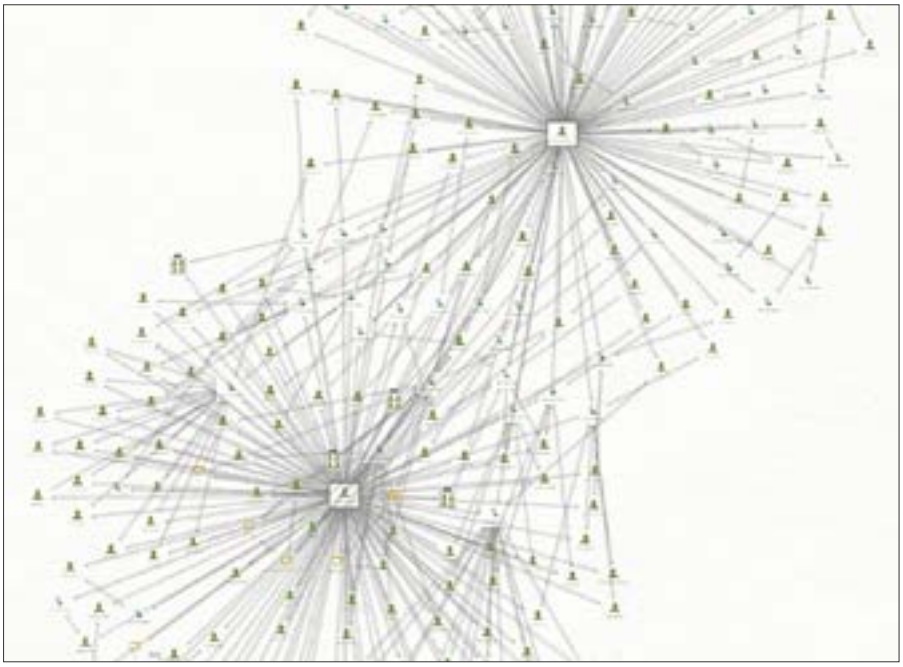
Visualizing the Infrastructure Connections

Pardon the vagueness in defining what every detail means below. However, we wanted to provide a quick visualization of the DNS-related connections they used - without giving away the attacker's techniques. This way AppRver can continue monitoring them and using intelligence gathered for the benefit of all 60,000+ AppRiver customers.

This first map is a zoomed-out overview of common DNS-related connections utilized by the attackers.



This second visualization, zoomed in a bit more, shows the level of detail and relationships between the fraudulent identities and DNS information connecting them.



RANSOMWARE

For the majority of businesses, Ransomware is the largest security concern due to the potential of bringing operations to an immediate halt.

Analysts saw a decline in attachments being used as a primary infection but saw an increase of banking stealers, cryptominers and Remote Access Trojans (RATs). Most of the ransomware attacks seen this year were the result of previous infections.

RANSOMWARE IS THE LARGEST SECURITY CONCERN FOR THE MAJORITY OF BUSINESSES BECAUSE IT HAS THE ABILITY TO **BRING OPERATIONS TO AN IMMEDIATE HALT.**

For example, the ransomware payload would be downloaded after the Trickbot Banking Trojan or Azorult stealer was loaded onto the infected machine. This allowed malicious actors to launch multiple styles of attacks against the target to maximize profit.

The Necurs Botnet was AppRiver's highest volume sender of ransomware. It began 2018 with an enormous GlobeImposter ransomware campaign sending via 7zip attachments with malicious scripts inside that pulled in the GlobeImposter payload. Between Jan. 11 and 12, AppRiver filters captured 56.7 million of these messages that were destined to customers. Other notable ransomware families our filters captured in 2018 include Gandcrab, Scarab, Sigma, and Hermes.

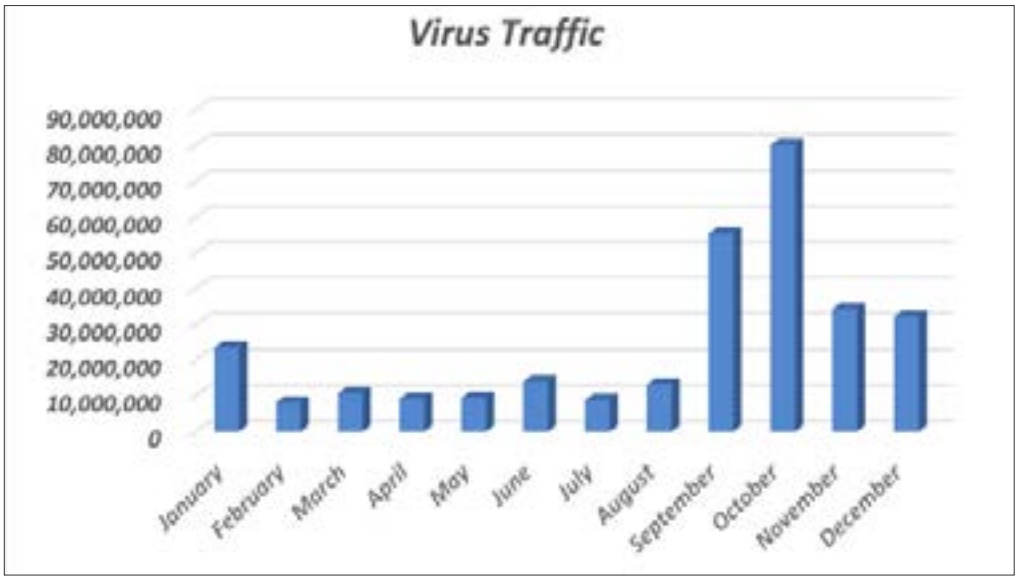
Of special interest this year was the rise of Remote Desktop Protocol- (RDP) based ransomware attacks. These types of attacks have become such a problem that the FBI issued a public service announcement.

Attackers would scan for open RDP machines, outdated RDP versions, or even brute-force into systems by exploiting weak and commonly used passwords. This was made even easier for attackers for user accounts without proper invalid password lockout policies. Notable ransomware families found after RDP infiltration include CrySiS/Dharma, SamSam, Matrix, and CryptON.

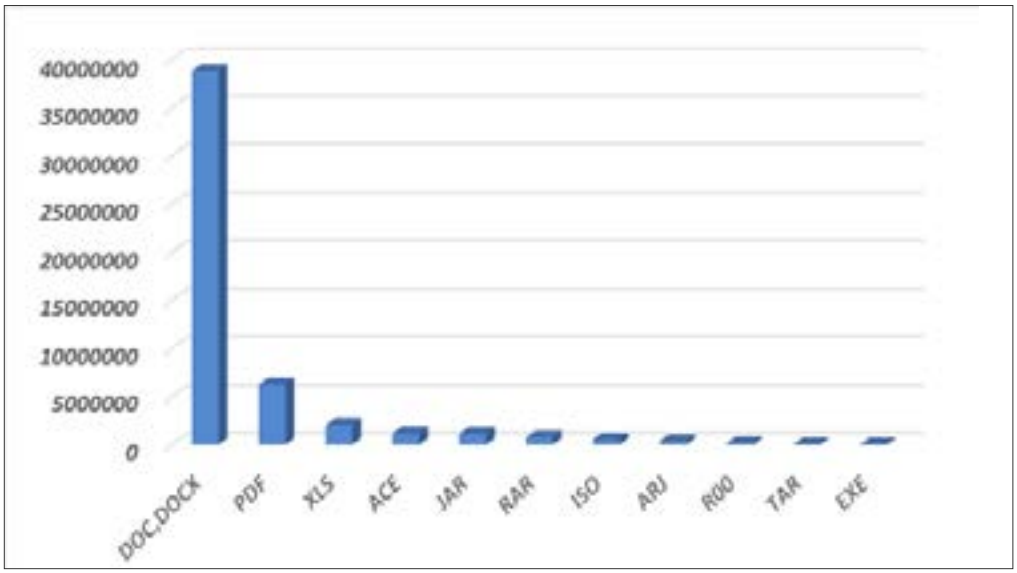
METRICS

Malware Traffic

In 2018, our SecureTide email security quarantined about 300 million emails containing malware in a message attachment. Malware activity was again most active in the latter part of the year as traffic ramped up significantly in September.

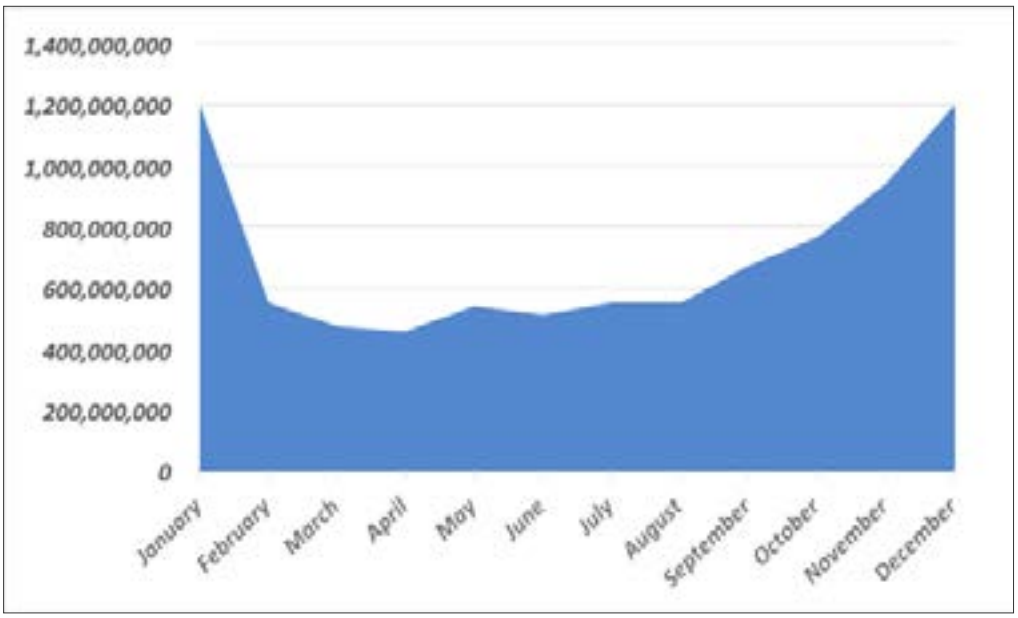


This year's malicious traffic was similar in that malicious Word files with embedded macro's were the most prevalent attack vector. Word Documents were flowed closely by PDFs and Excel spreadsheets(XLSX).



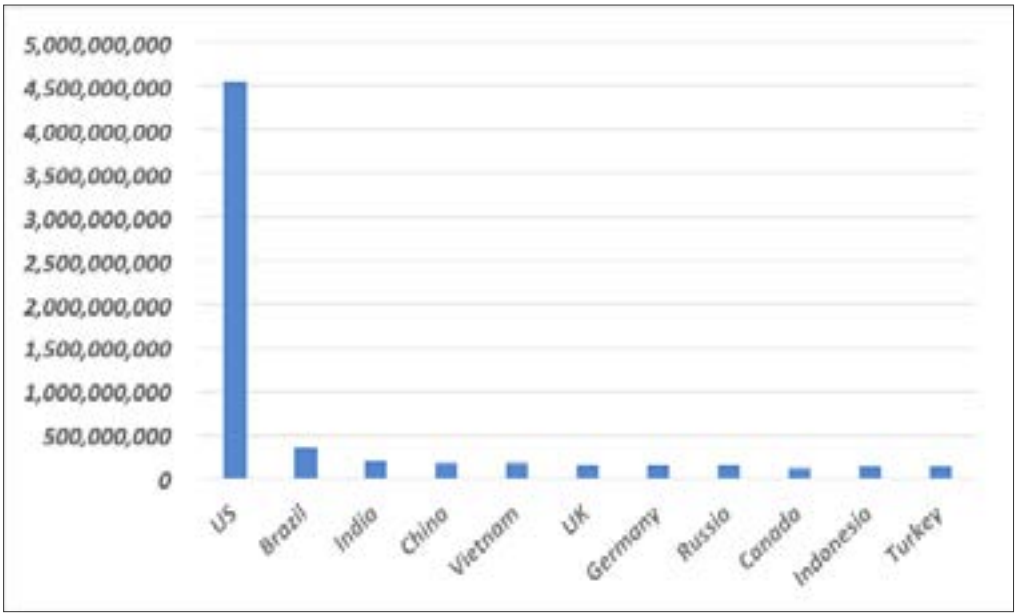
URL- and text-based attack traffic

The following chart depicts all other quarantined email traffic. The majority of which contains URL based malware and phishing attacks as well as text-based attacks, which rely on social engineering tactics. In all we quarantined 8.3 billion of these message in 2018.



Top Ten

Of the billions of bad email messages quarantined in 2018, the majority originated in one of these 10 countries. As the chart below depicts, the most common origination points for email-based attacks was the United States.



BREACHES

At this point it's safe to assume that most everyone is suffering from Breach Fatigue. It doesn't seem like a day in 2018 went by without news of some big data breach that exposed large swaths of sensitive personally identifiable information and associated data. And though you may be numb to it, we all need to take each and every breach seriously. 2018 was no exception to the ongoing trend of large data breaches happening across the globe.

IN THE WAKE OF SO MUCH BREACH NEWS, SOME INDUSTRY EXPERTS FEAR THAT CONSUMERS AND EMPLOYEES ALIKE WILL START EXHIBITING SIGNS OF **"BREACH FATIGUE"** AND TREAT SUCH INCIDENTS APATHETICALLY - ESPECIALLY IF THEY BELIEVE THERE'S NOTHING THEY CAN DO TO PREVENT FUTURE BREACHES.

—BANKINFO SECURITY

In April, it was disclosed that Hudson's Bay Co. had fallen victim to a security breach which compromised payment card data for purchasers at Saks and Lord & Taylor. One firm estimated that millions of payment card numbers were taken in the breach, making it one of the largest of this sort in 2018. The attack was later attributed to JokerStash, an underground criminal group, after they were seen selling the stolen card data on the Dark Web in multiple batches.

Among the more noteworthy of breaches this year was Under Armour, more specifically users of their MyFitnessPal app. In late March, the company disclosed that they believed they were a victim of a breach that allowed unauthorized access to an estimate 150 million usernames, email addresses and hashed passwords. The news of the breach had an immediate impact on their stock price.

The very same month, it was reported that India's national ID database (Aadhaar) which has been plagued with past security problems, was once again found to have a major flaw. It was subsequently reported that a New Delhi-based security researcher (Karin Saini) had discovered a vulnerability that allowed a malicious actor to gain a lion's share of sensitive data on anyone with an "identity number." This reportedly included names, ID numbers as well as other data about connected services, which could include bank details and other personal information.

Another breach garnering a lot of headlines in 2018 was that of social media giant Facebook. In a year in which Facebook already had found itself under a microscope for the ways it protects user data, it was discovered that hackers had made off with the data of some 29 million users in late September. Attackers reportedly used several vulnerabilities to gain access to multiple Facebook accounts, some of which allegedly included top executives. Of the 29 million effected, 14 million users suffered the greatest loss with the attackers having taken details such as date of birth, employer, Education, device data, pages they follow, religious preference, search history and some location data. This breach serves as a prime example that even a company that claim data collection and storage as a primary objective will still suffer security failures resulting in losses.

Other data breach victims this year included:

- **Panera Bread** (April) which leaked names, emails, physical addresses, dates of birth and the last four credit card digits of millions of users.

- **TicketFly** (June) also found itself on the 2018 victims list after a breach leaked PII for about 27 million user accounts. In addition to the leaked data, the hackers also took over the TicketFly website, at one point replacing the homepage with an image of the "V for Vendetta" character donning the Guy Fawkes mask. This of course had a cascading effect which disrupted many businesses which rely on TicketFly to service their events ticketing needs.

- **Target** (November) reported that its official Twitter account was taken over and used to perpetuate cryptocurrency scam. Although the retailer was able to regain control after a short period of time, many people were expected to have fallen victim to a scam requiring them to pay the scammers small sums of cryptocurrency with the promise of receiving more in return—along with other special offers. A similar attack was committed when attackers created an account impersonating Elon Musk and used it to perpetuate a nearly identical scam.

- **Quora** (December) the Q&A site reported it had lost an estimated 100 million user records in a breach that reportedly included names, email addresses, passwords and content posted to the site.

- **Marriott/Starwood** (December) found themselves embroiled in the biggest breach of the year when it was disclosed that a breach compromised the personal data of 500 million Marriott/Starwood hotel guests. Unfortunately, this breach not only exposed the names, phone numbers and email addresses of millions of previous guests but also—passport numbers, dates of birth, credit card numbers and expiration dates. This information can and will be used to create fraudulent purchases and possibly commit identity theft.

WHAT TO DO IF YOUR DATA IS BREACHED

With the stunning volume of breaches happening, it can be overwhelming at times to know what to do if you find your data was involved.

It is important to remember the basics to avoid as much fallout as possible:

- Use strong and unique passwords for each site, even if doing so means you need to employ a password manager to help you keep them organized.
- Enable Multifactor Authentication (MFA) whenever possible.
- Monitor accounts closely by opting in for notifications such as credit card charge alerts.
- Always keep your credit report locked by all three credit agencies.

A PERSONALIZED ATTACK THAT GAINED POPULARITY IN THE LATTER PART OF 2018 CAME IN THE FORM OF AN EMAIL ATTEMPTING TO **BLACKMAIL THE TARGET INTO PAYING A RANSOME** TO KEEP **"EMBARRASSING IMAGES"** TIED TO THE TARGET A SECRET.

Data breaches spawn personalized blackmail attacks

One of the numerous outcomes (all bad, by the way) of the continuous onslaught of breaches, is that the attackers are armed with data that can be used to commit additional personalized attacks.

One of the personalized attacks that gained popularity in the latter part of 2018 came in the form of an email attempting to blackmail the target into paying a ransom to keep "embarrassing images" tied to the target a secret.

In this attack, the unsuspecting victim would receive an email stating that an attack had infected one of their devices with malware and had gathered all of their contacts, taken screenshots of the precarious websites they were visiting, as well as taking photos of the target with the target's webcam. The attackers threaten to email these images to their contacts unless they paid the ransom.

How does this relate to a data breach? Within this personalized attack, the malicious actors have included within the message an actual password the target had used at some point. These passwords were almost certainly leveraged from a past data breach and found their way to forums and chat rooms on the Dark Web. By including these real passwords, it gives the attackers email an air of legitimacy. And serves as a prime example of how data breaches lead to many different secondary attacks and compromises.

Given that these types of attacks increased over the latter months of 2018, it appears attackers are netting a pretty good profit. By the end of 2018, these types of personalized attacks started being produced on a large scale and were being pumped out in massive botnet-driven email blasts.

PREDICTIONS

1. "Living off the land" - internal ecosystem attacks will increase. For example, a malicious actor will send a Microsoft phishing email from Microsoft servers (typically compromised accounts) and use Microsoft Azure storage/custom DNS to host the phishing site. Everything appears legit but uses built-in functionalities of the service itself to further establish credibility and appearance.

2. More bleeding-edge attack methods will reach mainstream malware distributors. With the success that malware authors/distributors had leveraging the Eternal Blue exploit to spread malware across an organization via worm capabilities. We expect to see more advanced attack techniques trickle down from the Nation State attack level and being used in for-profit attacks against the public.

3. More shock and awe. Attackers will become more emboldened to use scare tactics to extort victims. This year's sextortion, multiple bomb hoax campaigns and acid attack threats were examples of an increasing intent to scare victims into hurriedly paying a ransom.

4. Ransomware will continue to proliferate, but in a different way. It may become more common as the end-stage payload vs the first. For example, this year we saw Emotet infections lead to Trickbot infections which then led to Ransomware being dropped on the system after attackers had time to steal banking information. Attackers will continue to maximize profits by chaining successful attacks.

5. Cryptocurrency miners will continue to increase in popularity as attackers begin to leverage other platforms such as Internet of Things to increase computing power and in turn profits. The stealth factor associated with these programs allows attackers to persist on a machine or device much longer and use other's computing power to generate profits.

6. IoT devices will rapidly grow through the foreseeable future. It's scary to think how many of these devices already are in use while market penetration has yet to peak. Couple that with very little security features being built into many of these devices and the door for attacks is wide open. Exploits, malware and botnets associated will ride the IoT wave into the future.

7. The Artificial Intelligence field will continue to mature and evolve, however, not at the rate the marketing hype has led most businesses to believe. Attackers and defenders are utilizing the technology increasingly for the never-ending cat and mouse scenario.

8. 5G will enter the scene and roll out. Any vulnerabilities or risks associated with it also will be exposed. Because more devices will become wireless, this will expose additional attacks on endpoints that were traditionally hard-wired.

9. Nation state actors will continue to decreasingly honor cyber rules of engagement. Indictments and accusations levied at China by the US and UK in late December underscore the scope of activity happening on this front across the world. As a result, things may get worse before they get better. From a global perspective, political policies and trade agreements could potentially escalate cyberwarfare as a whole. False-flag operations will increase in scope and attribution will become more difficult. We also expect to see more disruptive cyberattack events committed by Nation States that masquerade as financially motivated attacks.

For the latest threat research and guidance about
today's advanced threats and digital risks,
visit **appriver.com**

ABOUT APPRIVER

AppRiver is a channel-first provider of cloud-enabled security and productivity services, with a 4,500-strong reseller community that protects 60,000 companies worldwide against a growing list of dangerous online threats. Among the world's top Office 365 and Secure Hosted Exchange providers, the company's brand is built on highly effective security services backed by 24/7 white-glove Phenomenal Care® customer service. AppRiver is headquartered in Gulf Breeze, Florida and maintains offices in Georgia, Texas, New York, Canada, Switzerland, United Kingdom and Spain. For more information, please visit www.appriver.com.