PHISHLABS

2018 PHISHING TRENDS & INTELLIGENCE REPORT

Hacking the Human

www.phishlabs.com

CONTENTS

HOW?

WHO?

WHEN?

WHERE?

INTRODUCTION

Welcome to the 2018 Phishing Trends and Intelligence (PTI) Report. The purpose of this report is to provide insight on significant industry trends, tools, and techniques being used by threat actors to carry out phishing attacks. It also sheds light on why shifts are occurring and what to expect in the coming year.

The most significant trend observed in 2017 was the shift from targeting individual consumers to enterprise-focused phish. Threat actors are targeting enterprises by impersonating services that enterprises rely on such as email service providers and Software as a Service (SaaS) platforms. This shift to enterprise targeting is alarming and indicates a change in threat actor motivations. Threat actors can use stolen credentials to pursue many different aims and all of which pose significant risk to victim companies. They can be used to steal data, access corporate systems, or they can be packaged up and sold to the highest bidder.

Another key trend observed in 2017 is a case study on unintended consequences. Last year there was a surge in phishing sites using HTTPS. Over the years, the general population has been taught (erroneously) that sites using HTTPS can be trusted. Threat actors are taking advantage of free SSL certificates to exploit this misplaced trust.

Overall, the changes observed in the phishing threat landscape continue to demonstrate that users are the most prominent and exploitable vulnerability.

This report provides a first-hand, in-depth review of cyber-attacks that are designed to exploit the human vulnerability. The intelligence shared in this report comes directly from the continuous work PhishLabs does to fight back against phishing attacks and the threat actors behind them. The trends highlighted in this report will help organizations better assess the risk of modern phishing attacks, which the detailed findings can then be used to mitigate these risks.

PhishLabs R.A.I.D. (Research, Analysis, and Intelligence Division), which is comprised of some of the world's most respected threat researchers, created this report. The information and analysis contained in this report is sourced from PhishLabs' operations and technology systems used to fight back against phishing, malware, ransomware, and mobile attacks. To provide context for our intelligence holdings, consider:

- We analyzed more than 1.3 million confirmed malicious phishing sites in 2017 that resided on nearly 300,000 unique domains.
- We investigated and mitigated more than 12,000 phishing attacks every month, identifying the underlying infrastructure used in these attacks and shutting them down.
- Leading financial institutions, social media sites, healthcare companies, retailers, insurance companies, and technology companies use our services to fight back against phishing threats.

> Social engineering continues to be at the forefront of all attacks that target people. Because of the push for more widespread adoption of HTTPS for encrypted communication, there is a surge of HTTPS phishing sites. Phishers are preying on the common misconception that HTTPS means a site is legitimate or trustworthy.

EXECUTIVE SUMMARY

Phishing continues to be the top threat vector for cyberattacks. Exploiting human vulnerabilities continues to be the most successful path for threat actors targeting the assets of organizations and individuals. As the adoption of technology gains momentum, we see threat actors progressively shifting methods and leveraging social engineering through email, social media, and mobile attacks to trick users.

The 2018 PTI Report provides analysis of trends in phishing attacks and insight into the techniques being used in those attacks. It provides clarity on who is being targeted and gives perspective into how and why victims are being targeted. Those who read this report will have a better understanding of phishing threats and be better equipped to protect against them.

Key findings in the 2018 PTI Report include:

- Industry shift shows signs of threat actors switching from primarily targeting individuals to targeting organizations.
- Email and online services (26% of all attacks) overtook financial institutions (21%) as the top phishing target.
- Nearly one-third of all phishing sites observed by the end of 2017 were located on HTTPS domains, up from only five percent at the end of 2016.
- Attacks targeting SaaS exploded with more than 237% growth.
- Attacks targeting social media platforms have nearly tripled since last year due to the inherent trust between users and the platform or brand.
- The ransomware landscape is maturing and is no longer experiencing exponential growth of new threat families.
- Mobile malware continues to rise, and new techniques take advantage of the increased use and security shortcomings of mobile devices.
- The share of attacks against targets in the United States continues to grow, now accounting for more than 86% (up from 81% last year) of all phishing attacks.
- Some countries that saw significant increases in phishing activity in 2016, such as Canada, France, and Italy, experienced substantial decreases in phishing volume in 2017.

WHO IS BEING TARGETED?

[TL;DR — In 2017, email/online services overtook financial institutions as the top phishing target. This monumental diversion from historical trends indicates an increased focus on the use of phishing to steal enterprise user credentials. While profit from enterprise-focused phishing is less direct than compromising consumer financial accounts, the payout is often much higher.]

In 2017, we identified 1,165 different brands from 754 parent institutions (private companies, government agencies, schools, etc.) that were targeted by phishing attacks. More than 84 percent of all phishing attacks in 2017 targeted five industries: email/online services, financial institutions, payment services, cloud storage/file hosting services, and e-commerce companies.

Although the total number of phishing attacks grew two percent in 2017, the financial industry's share of phishing attack targets has decreased substantially in recent years when compared to the growth in SaaS. In 2013, attacks targeting financial institutions accounted for more than one-third of all phishing attacks. This has steadily decreased over the past four years, and now comprises only a fifth of the global phishing volume.

FIGURE 1: Industries Targeted by Phishing (2017)

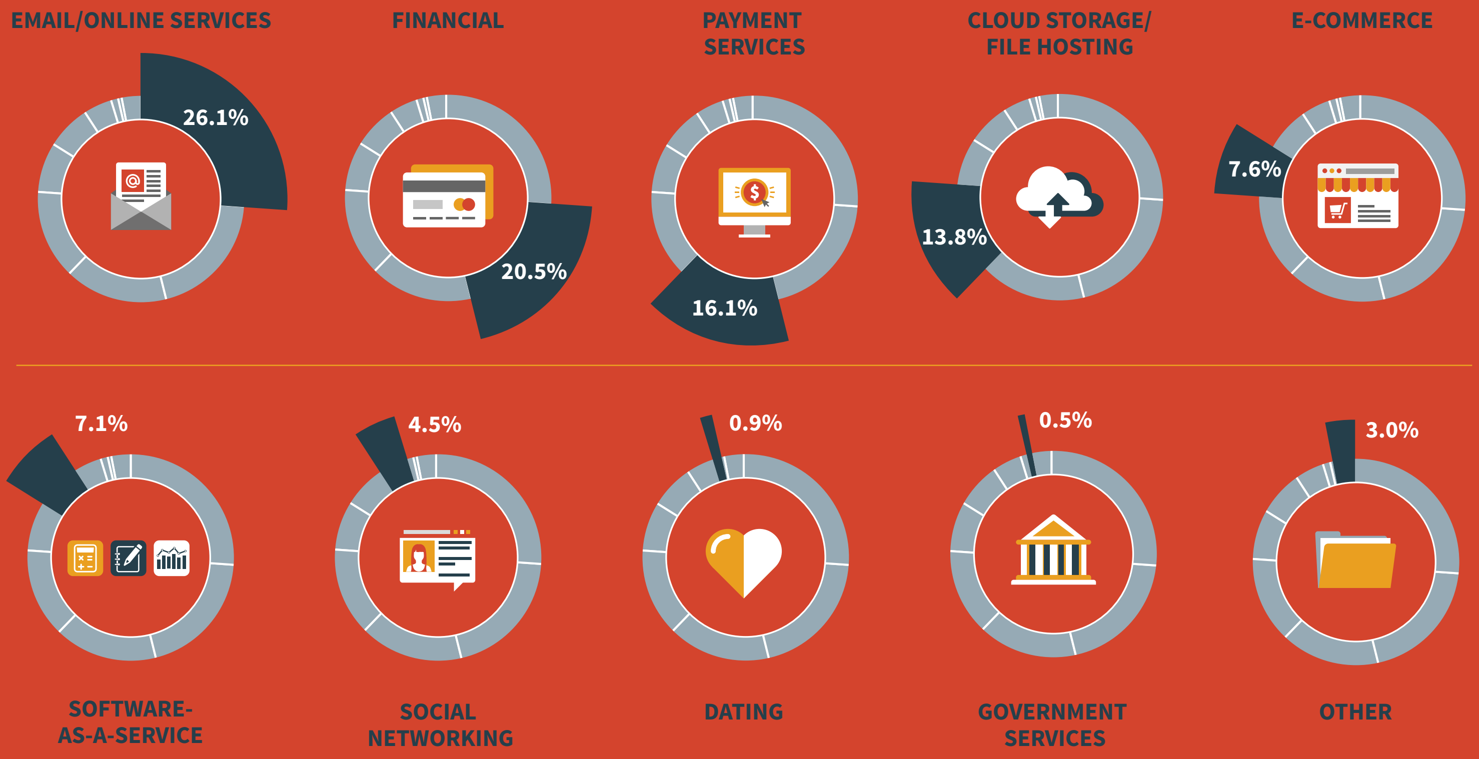


FIGURE 2: Industries With Declining Shares of Phishing Attacks (2013–2017)

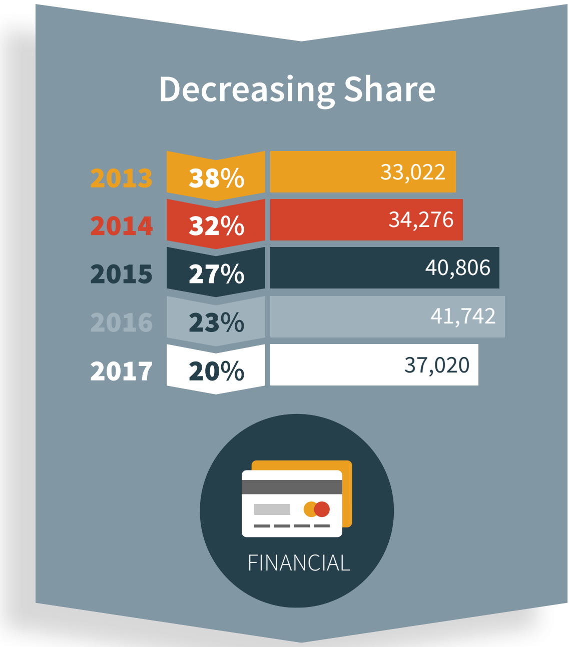
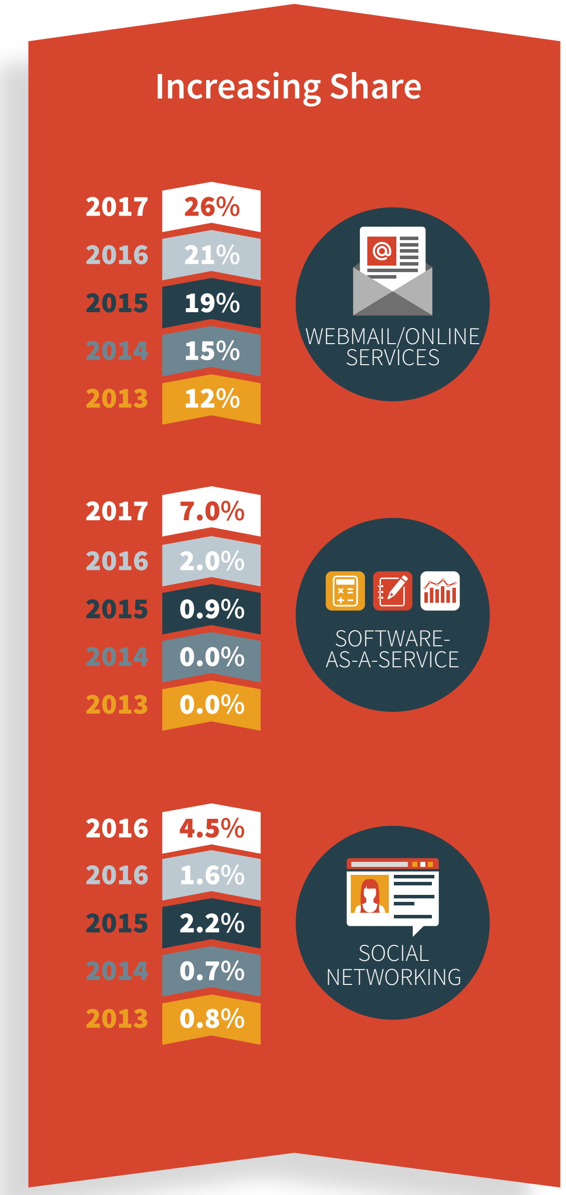


FIGURE 3: Industries With Increasing Shares of Phishing Attacks (2013–2017)



As the share of attacks targeting financial institutions has declined, other industries have seen shares increase substantially. In 2013, just 12 percent of phishing attacks targeted email/online services. However, in 2017 the industry's share has grown to more than a quarter of the year's total volume. The widening gap between email/online services and all other industries became very pronounced during the second half of 2017 when the industry's share accounted for a third of all phish. Specifically, the increase in email/online service phishing attacks in 2017 was driven almost exclusively by a concentrated rise in attacks impersonating Microsoft Office365 login pages.

Another industry that has seen exceptional growth in the number of phishing attacks targeting consumers is software-as-a-service (SaaS). Prior to 2015, phishing attacks targeting these companies were nearly non-existent. After breaking out in 2015, the number of attacks targeting SaaS companies has more than doubled two years in a row. The primary focus? It's not about stealing credentials to the SaaS offering, but more so lures and phishing sites that use the brand's trust to social engineer a victim into giving up information, which in most cases are their email credentials.

In 2017, SaaS-based phish made up seven percent of all phishing attacks, which makes it the sixth most targeted industry. It's also important to note that phishing attacks impacting SaaS almost exclusively target only three companies: Adobe (Adobe ID) and DocuSign. Like email/online service phish, SaaS phish often target companies frequently used by enterprises.

media volume increased by nearly 200 percent. It now comprises nearly five percent of all phish and is the seventh most targeted industry. Like compromised email/online services accounts, stolen social media accounts can be used to facilitate additional cybercrime.

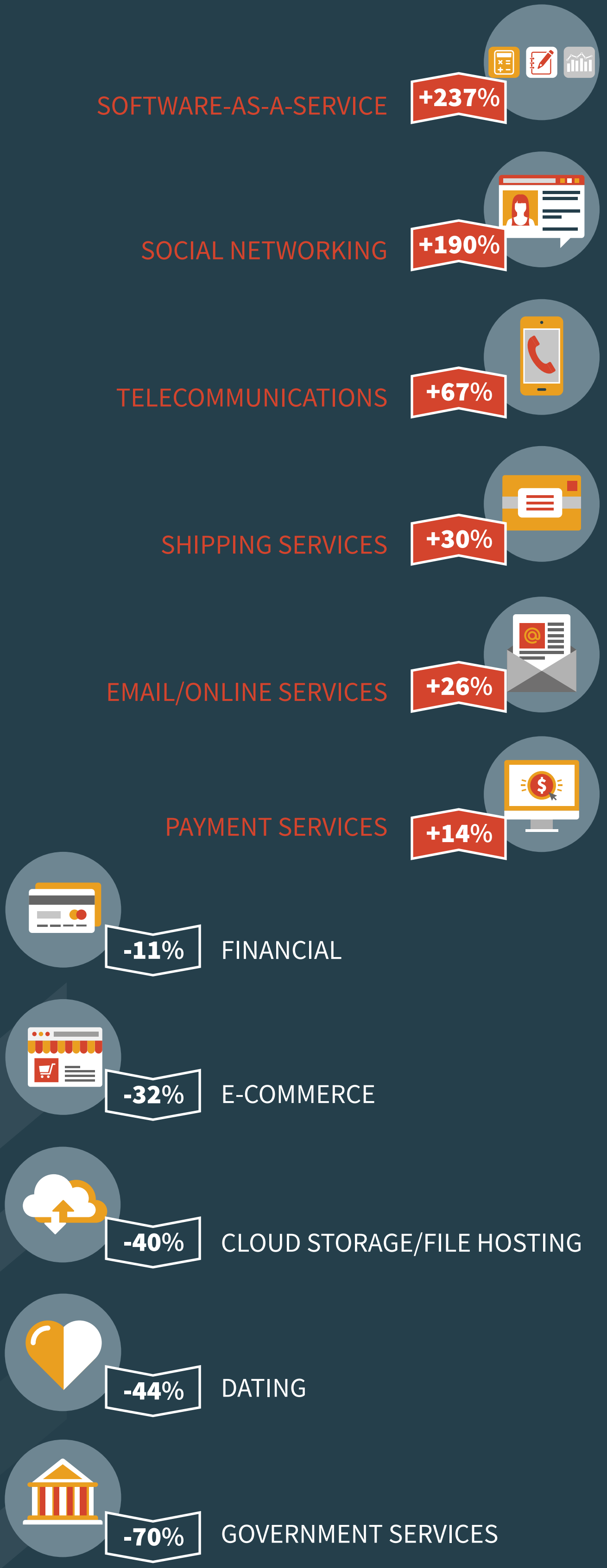
After seeing decreases in attack volume in both 2014 and 2015, the share of attacks targeting the payment services industry has been on the rebound. However, payment service companies also saw significant increases in 2016 and 2017. In 2015, the number of attacks targeting payment service companies fell by more than 28 percent and was the only industry to see a decrease in total phishing volume. Over the past two years, phishing attacks against payment service companies have more than doubled, now accounting for 16 percent of the total phishing activity.

In addition to financial institutions, two further top-five targeted industries saw decreases in the number of phishing attacks last year. After seeing volume increases for the past three years and almost becoming the most phished industry in 2016, cloud storage sites saw a drastic decrease of nearly 40 percent in 2017. Ecommerce companies also saw a significant decrease, with volume cut by more than a third.

So, why are we seeing these changes?

In 2016, we saw a shift in **how** phishers targeted

FIGURE 4: Changes in Phishing Volume (2017)



their victims. Noting the tendency of most people to use the same login credentials for everything, phishers began spoofing a small number of high-value targets such as the Google Docs login page. Mass harvested credentials from these attacks could then be used to facilitate secondary password reuse attacks. In essence, phishers evolved to make credential collection more efficient and ultimately more effective.

In 2017, we saw an evolution in **who** phishers targeted. The significant increase in attacks against specific email/online services and SaaS companies indicates phishers have started shifting their focus from individual victims to enterprise targets. While the same tactics we observed in 2016 continued, most of the targets that saw the largest increase in phishing attacks were services that are primarily used for business purposes.

This change in targeting shouldn't come as a complete surprise. In 2016, PhishLabs observed a similar evolution in the targets of ransomware campaigns. At the beginning of 2016, when ransomware became the most pervasive threat in the malware threat landscape, most campaigns were distributed in broadcast attacks, generally targeting individual consumers. As the year progressed, however, these shotgun-style attacks evolved into targeted spear phishing campaigns, focused on small businesses, schools, government agencies, critical infrastructure facilities, and medical facilities. This shift occurred because cybercriminals saw attacks targeting these enterprise entities as being more effective and profitable.

The same line of thinking is likely the driving force behind the shift in credential phishing attacks. Compromised business accounts can be leveraged in several different ways, all of which can be very lucrative. An increasingly common way for attackers to use compromised enterprise accounts is to send additional spear phishing emails to other employees in the company.

WHO?

MAY AUGUST DECEMBER

WHEN ARE ATTACKS HAPPENING?

[TL;DR — In 2017, phishing volume increased steadily throughout the year until leveling out in the fourth quarter which is consistent with previous years. Attacks targeting email/online services and SaaS companies increased steadily throughout 2017 while attacks targeting cloud storage services, payment services, and e-commerce companies decreased as the year progressed.]

After 2016, which saw a substantial mid-year spike in phishing volume due to global events and a large number of attacks hosted on compromised web servers, the spread of attacks in 2017 returned to historical norms. Prior to 2016 phishing attacks followed a predictable pattern, increasing throughout the year and ending with a surge in the fourth quarter during the holiday season. In line with this trend, volume steadily increased throughout 2017, leveling out in the last quarter of the year.

It is interesting to note that three months in 2017 had notable spikes in volume: May, August, and December. The spike in volume seen in May is associated with a rise in phishing attacks targeting social networking sites. Social media phishing attacks more than doubled (+111%) compared to April's volume. An analysis of these attacks showed that nearly two-thirds of the social networking phishing attacks observed in May were linked to a single, massive campaign that utilized dynamic DNS, specifically ddns.net, to generate a large volume of phishing sites. DynDNS is a service offered by companies, such as Dyn, that allows rapid updating of name servers and IP addresses. Phishers can use these services to quickly create many domains and subdomains that all resolve to the same IP address.

The phishing attack increase observed in August 2017 can be attributed to a large increase in email/online services phish, which increased by 34 percent. It should be noted that while email/online services overtook all other industries as the primary target of phishing attacks in 2017, it wasn't until August when attacks against these targets really started to dominate. In December, attacks rose against a number of different industries, which is likely the result of phishers taking advantage of the holiday season when potential victims are expecting more emails from companies in certain industries. This is supported by the surge of payment services phishing attacks we observed at the end of the year (+38%) after attacks against these targets decreased substantially throughout the second half of the year.

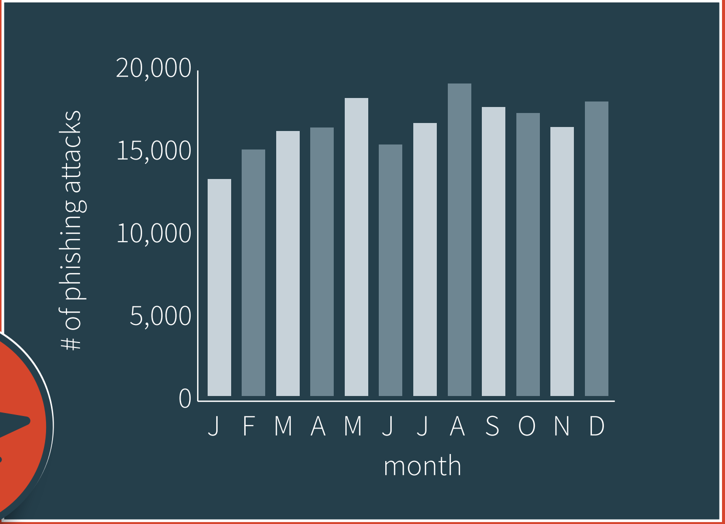


FIGURE 5: Phishing Attacks by Month (2017)

Unlike previous years, the monthly phishing volume for financial institutions stayed relatively consistent in 2017. Email/online services and SaaS companies both saw an increase in phishing activity as the year progressed. Conversely, attacks targeting cloud storage services, payment services, and ecommerce companies decreased throughout the year. While the overall yearly volume of phishing attacks targeting payment services was much higher than in 2016, nearly a third of that volume occurred during a short, three-month timespan at the beginning of the year. Attacks against ecommerce companies gradually decreased throughout the year with an exception of a one-month spike in April, when volume increased by 22 percent. The timing of this spike corresponds with the end of tax return season, so it's possible that phishers were targeting the ecommerce industry when people often have more money to spend.

FIGURE 6: Industries With Increasing Phishing Volume Throughout Year (2017)

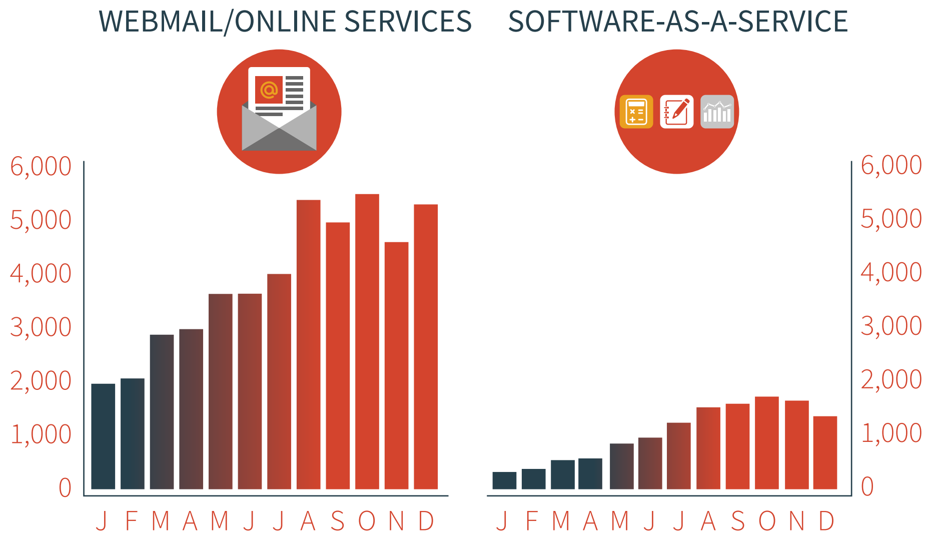
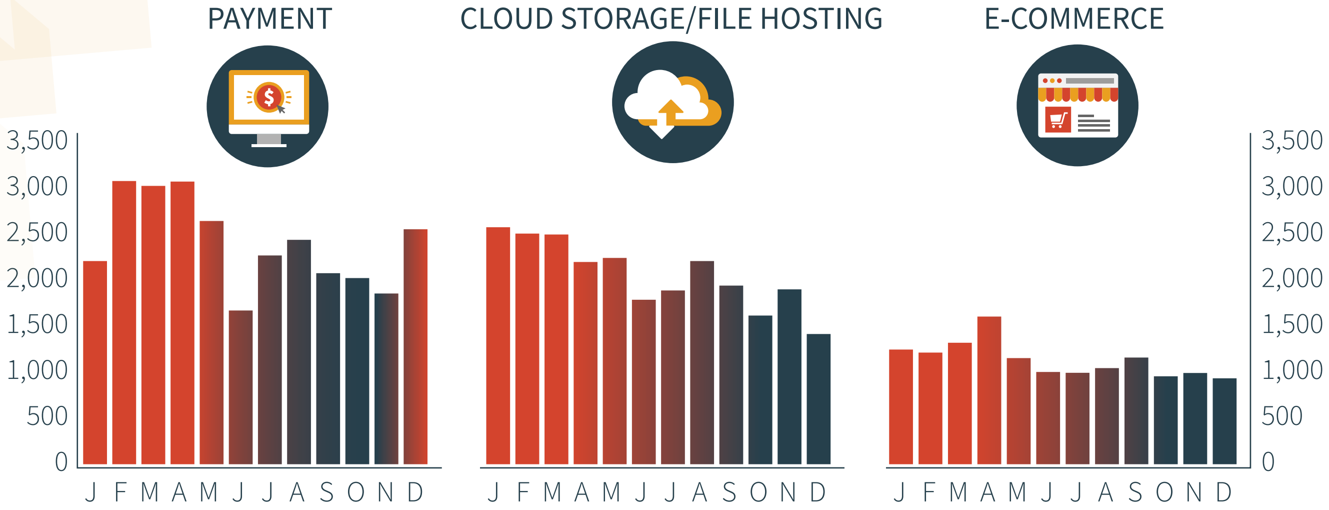


FIGURE 7: Industries With Decreasing Phishing Volume Throughout Year (2017)



WHERE ARE ATTACKS HAPPENING?

[TL;DR — The share of phishing attacks against US-based targets continues to grow and now account for 86 percent of global phishing volume. Some countries that saw significant increases in phishing activity in 2016, such as Canada, France, and Italy, experienced substantial decreases in phishing volume in 2017. The number of phishing attacks targeting British organizations fell for the fourth straight year, now comprising less than two percent of global phishing volume. Countries that had the largest increases in phishing activity included India, Colombia, and the United Arab Emirates.]

As expected, institutions in the United States remained the most targeted in 2017, comprising 86 percent of global phishing volume. Compared to other countries, the share of phishing attacks targeting U.S. organizations continue to grow each year, indicating US-based companies have become the primary focus of phishing threat actors. In 2014, 71 percent of all phishing attacks targeted entities in the United States, and in 2016 this figure has grown to 81 percent. Since 2014, the total number of annual phishing attacks against U.S. targets has more than doubled.

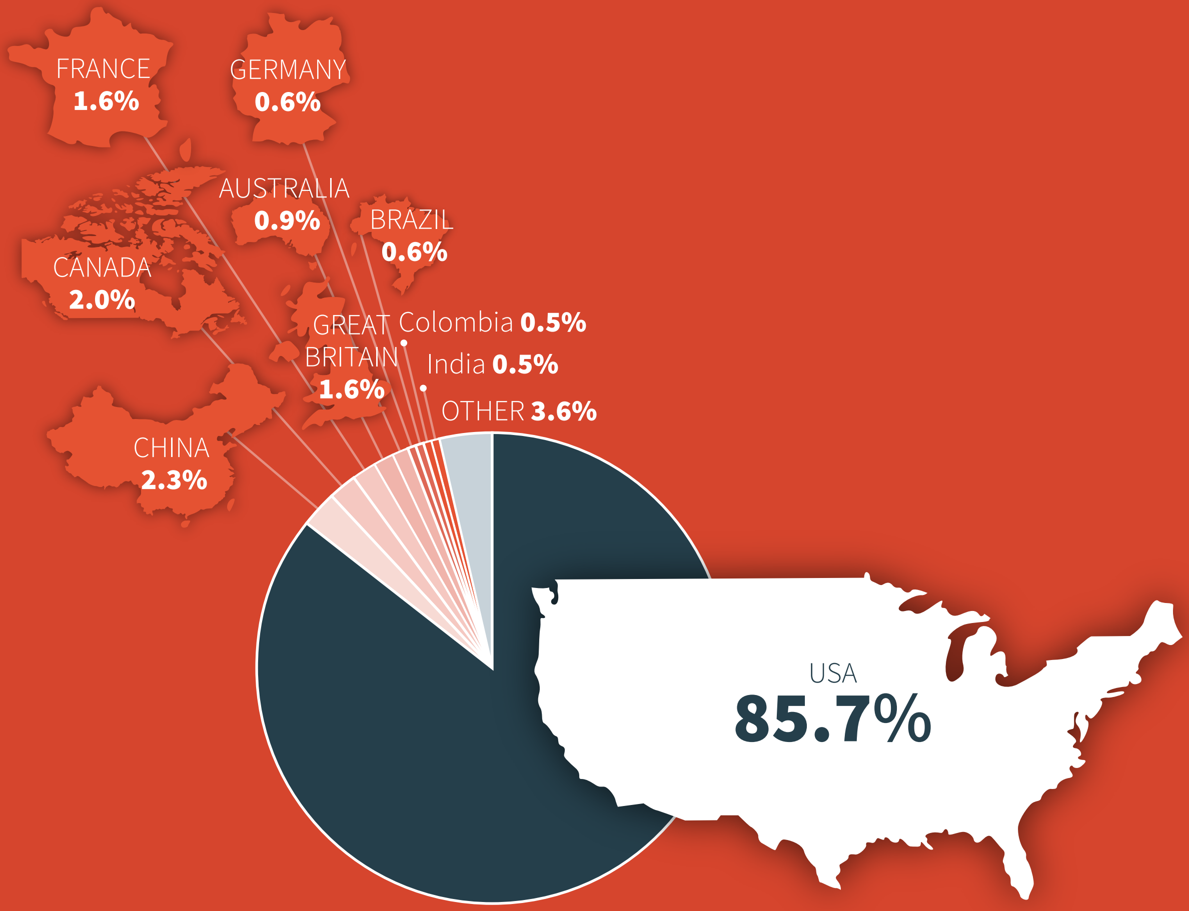
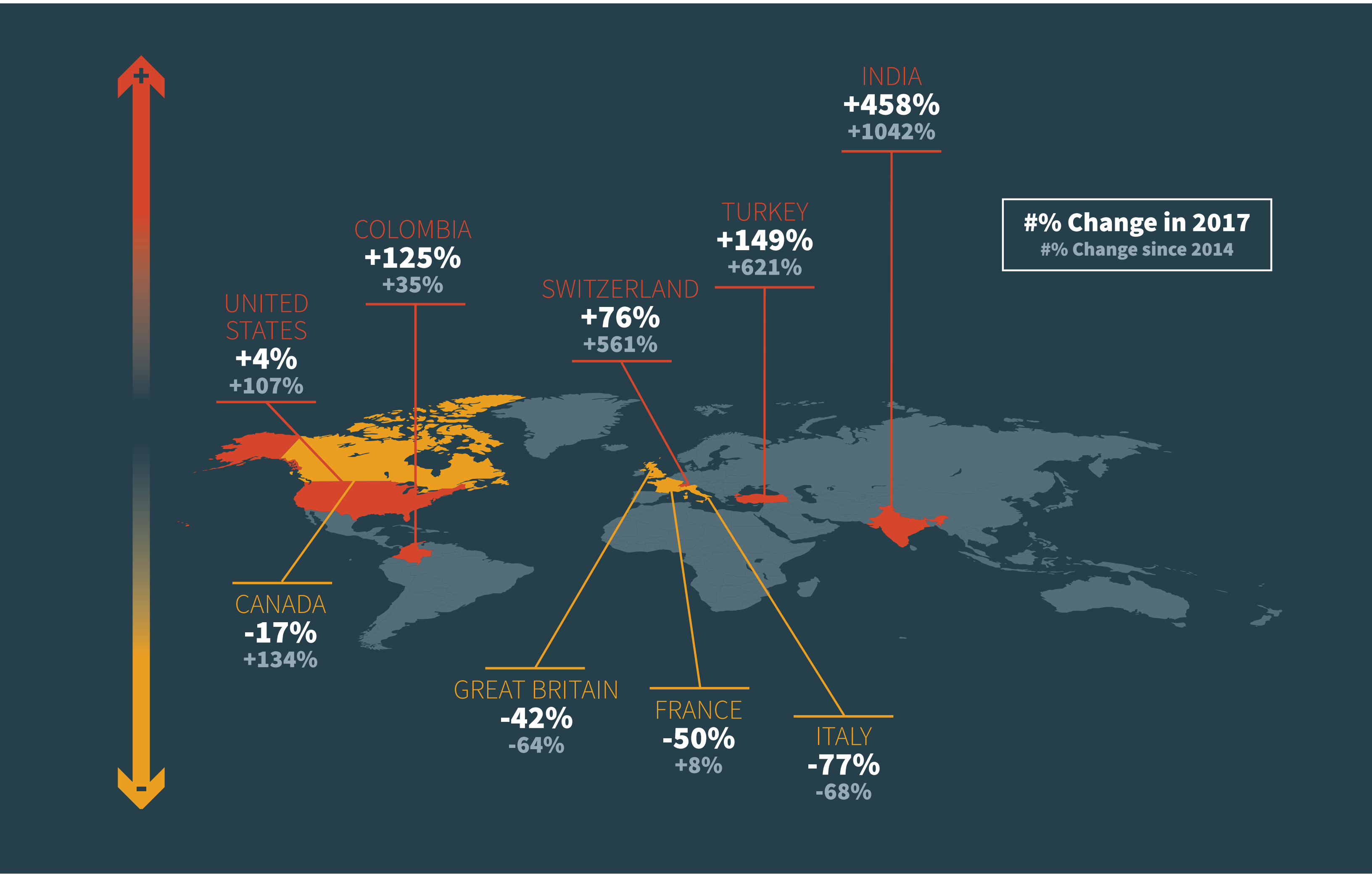


FIGURE 8: Phishing Targets by Country (2017)

Interestingly, some countries that saw significant increases in phishing volume in 2016 experienced decreases in 2017. Phishing attacks targeting Canadian institutions for example, which grew more than 237 percent in 2016, saw a 17 percent decrease in attacks in 2017. Targets in Italy and France experienced similar decreases. After increasing 31 percent in 2016, the volume of phishing attacks against Italian companies declined more than 75 percent in 2017. Driven by a decreasing number of attacks against government and financial institutions, phishing attacks against French targets fell more than 50 percent in 2017, after increasing 39 percent in 2016.

Another interesting change was a significant decline in phishing attacks targeting British organizations. In each year following 2014, the number of attacks against British institutions has fallen substantially. In 2014, British institutions were the second-most popular target of phishers, comprising eight percent of all phishing attacks globally. Over the past four years, the number of attacks against British targets has fallen nearly 80 percent and are now only the fifth-most common target of phishing attacks.

FIGURE 9: Notable Country-Specific Trends in Phishing Volume



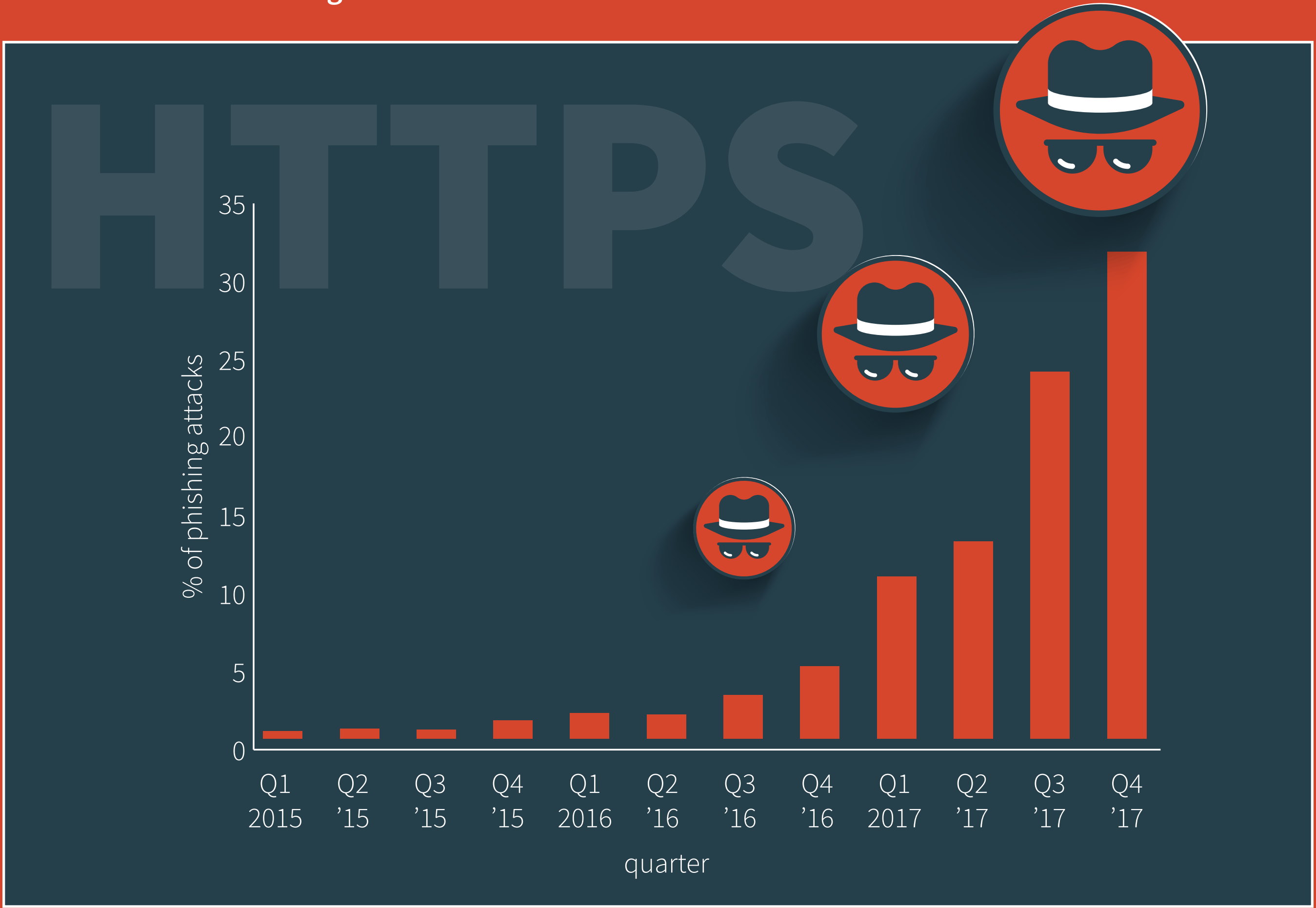
HOW ARE PHISHING ATTACKS BEING CARRIED OUT?

HTTPS Phishing Sites

[TL;DR — By the end of 2017, nearly one-third of all phishing sites were hosted on HTTPS infrastructure, compared to just five percent at the end of 2016. This evolution in tactics is fueled by the increased adoption of HTTPS by the general Internet population, as well as phishers taking advantage of unclear security messaging.]

One of the most dramatic changes in the phishing landscape in 2017 was the rapidly increasing number of phishing sites hosted on HTTPS domains. At the end of 2016 less than five percent of phishing sites were found on HTTPS infrastructure, but that figure had risen to almost 33 percent by the fourth quarter of 2017. Overall, nearly 20 percent of all phishing sites observed in 2017 were found on HTTPS domains.

FIGURE 10: Trend of Phishing Sites Hosted on HTTPS Domains



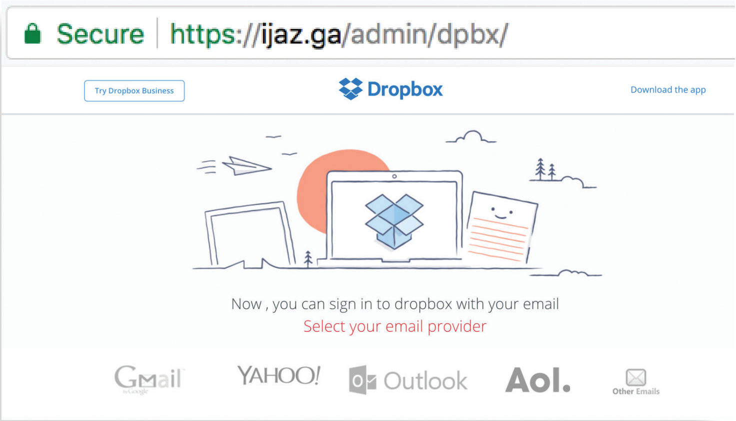
The increase in HTTPS uptake is significant for two primary reasons:

1) More HTTPS websites = more HTTPS phishing sites

According to Let's Encrypt, two-thirds of websites loaded by Firefox at the end of 2017 used HTTPS, compared to just 45 percent at the end of 2016. An HTTPS domain is displayed by any website with an SSL certificate, and indicates simply that communications between that site and a web browser are encrypted during transit.

Despite what many people believe, HTTPS domains do NOT mean a website has been secured, or that any vulnerabilities on the site have been patched. Consequently, attackers can exploit vulnerabilities in HTTPS websites just as easily as they can compromise standard HTTP websites.

As more websites obtain SSL certificates, then, the number of HTTPS websites available for compromise also increases. And since HTTPS websites are no less vulnerable than non-HTTPS sites, when attackers scan for domains to compromise and host malicious content they will naturally identify more HTTPS sites to target as SSL certificate adoption rises.



Secure https://ijaz.ga/admin/dpbx/

Try Dropbox Business

Dropbox

Download the app

Now , you can sign in to dropbox with your email

Select your email provider

FIGURE 11: Example of a Dropbox HTTPS Phishing Site Labeled as Secure in Chrome

2) Phishers are taking advantage of unclear security messaging

While the presence of phishing content on HTTPS websites is partly based on a natural shift in SSL adoption, a significant number of phishing sites are hosted on HTTPS domains registered by the phishers themselves.

An analysis of phishing attacks against two of the most phished brands in the world found that nearly three-quarters of HTTPS phishing sites employed were hosted on maliciously registered domains rather than compromised websites.

The use of infrastructure registered by threat actors for the explicit purpose of hosting phishing content is important because it's a conscious choice made by an attacker. Why should they take the additional step of obtaining an SSL certificate? After all, without an SSL certificate the phishing page would still function as intended.

The answer is simple: Phishers believe that an HTTPS domain makes a phishing site seem more legitimate to potential victims, increasing the chances of a successful outcome. And, unfortunately, they're right.

In November 2017, we conducted a poll to see how many people knew the real meaning of the green padlock associated with HTTPS websites. More than 80 percent of respondents believed the padlock meant a website was either legitimate and/or safe… neither of which are true.

Adding to the confusion, browsers like Google Chrome label websites with SSL certificates as "Secure" in the URL bar, which only reinforces the idea that HTTPS = safe.

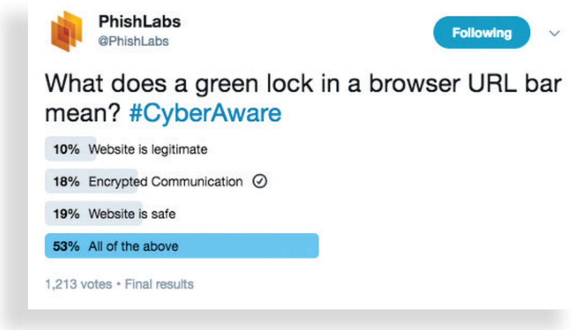
Phishers have been quick to capitalize on this misconception by obtaining SSL certificates for their maliciously registered domains (often for free through services like Let's Encrypt or Comodo) and we can expect to see this trend continue throughout 2018.

In November 2017, we conducted an informal poll to see how many people actually knew the meaning of the green padlock that is associated with HTTPS websites. More than 80 percent of the respondents believed the green lock indicated that a website was either legitimate and/or safe, neither of which is true.

Adding to the confusion, browsers like Company Chrome label websites with SSL certificates as "Secure" in the URL bar. Another word for secure: safe.

Due to the accelerated adoption of HTTPS among website owners globally, we can expect to see the number of HTTPS phishing sites continue to grow rapidly.

FIGURE 12: Results of an Informal Poll About the Meaning of the Green Lock in a Browser URL Bar



PhishLabs
@PhishLabs

What does a green lock in a browser URL bar mean? #CyberAware

10% Website is legitimate
18% Encrypted Communication ✓
19% Website is safe
53% All of the above

1,213 votes • Final results

Free Hosting Providers

[TL;DR — The number of phishing sites using a free hosting provider more than doubled in 2017. The use of free hosting providers has been on the rise in recent years. Nearly eight percent of all phishing sites are hosted on a free provider. This trend will likely continue due to free hosts being an economical and simple option to host phishing sites.]

Since 2016, the use of free hosting providers to host phishing sites has been rising. In both 2016 and 2017, the use of free hosts doubled, and they are now associated with eight percent of all phishing sites. This is not a total surprise since phishers are always looking for ways to make their jobs easier. Free providers offer phishers the ability to create phishing sites without having to either compromise a website or purchase their own site. In addition to being cheap and easy, many free hosts offer subdomain customization of the free site. This allows phishers to easily create legitimate looking URLs that increase the chances of tricking potential victims.

The most popular free hosting provider in 2017 was 000Webhost. This particular provider is home to 32 percent of all freely hosted phish, which is 50 times more than in 2016. The popularity of 000webhostapp.com started to grow in December 2016 and continued to increase throughout 2017. In December 2017, the use of 000Webhost was at an all-time high, when one out of every two freely hosted phish used the provider. Another popular option was 5GBFree, which was used by five percent of all freely hosted phish in 2017. This provider also saw a huge growth with over 17 times more phish using the provider in 2017 than in 2016.

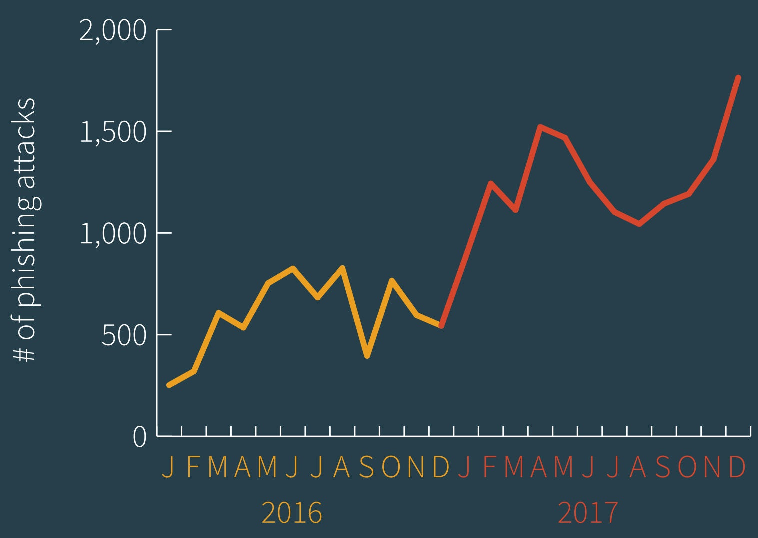
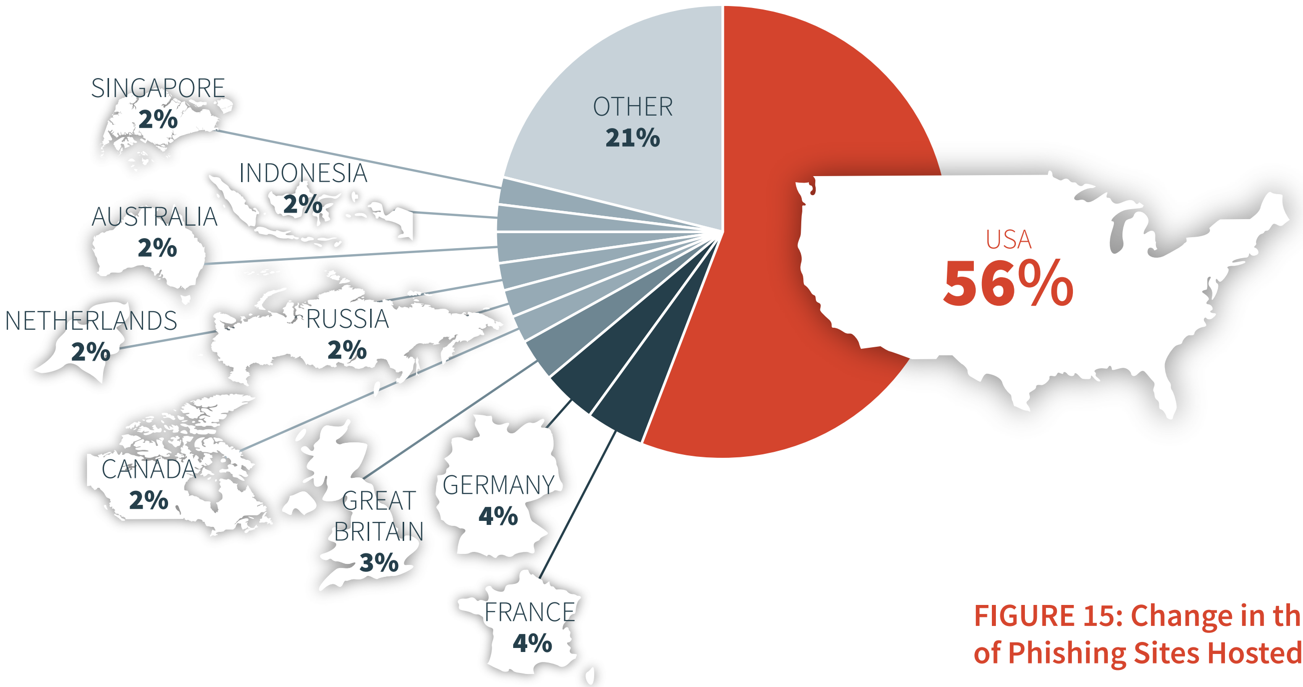


FIGURE 13: Phishing attacks hosted on free hosting providers (2016–2017)

FIGURE 14: Phishing Site Hosting Locations (2017)



Hosting Locations

[TL;DR — In 2017, 56 percent of phishing sites were hosted in the United States. Many countries in South and Southeast Asia saw a sharp increase in phishing sites hosted on their infrastructure in 2017]

Most phishing sites are located on compromised web hosting networks, which are exploited by phishers using a variety of different tools and techniques. Similar to 2016, about 80 percent of all phishing sites were hosted in only 10 countries. The United States continues to be the most popular choice for phishers and hosts 56 percent of all phishing sites. After the United States, the next most common countries hosting phishing infrastructure were France (4%), Germany (4%), Great Britain (3%), and Canada (3%).

Countries in South and Southeast Asia saw tremendous growth in the number of phishing sites hosted on their infrastructure in 2017. Many of the countries in these regions saw a significant uptick in phish hosting, including Bangladesh (+321%), India (+121%), Singapore (+88%), Indonesia (+40%), and Malaysia (+39%). Other countries also saw significant increases, such as Japan (+168%), South Africa (+110%), France (+82%), and Ukraine (+70%).

While a few East Asian countries saw increases in volume, Hong Kong (-28%) and China (-40%) saw decreases. After seeing a drastic increase of 123 percent in 2016, Poland saw a drop of 51 percent in 2017. Great Britain is another country that had a sizable increase in 2016, but it decreased by 28 percent in 2017.

FIGURE 15: Change in the Number of Phishing Sites Hosted (2017)

+121%	INDIA
+110%	SOUTH AFRICA
+88%	SINGAPORE
+82%	FRANCE
+70%	UKRAINE
+40%	INDONESIA
+39%	MALAYSIA
+34%	CANADA
+32%	ROMANIA
+26%	TURKEY
-9%	UNITED STATES
-13%	RUSSIA
-16%	ITALY
-21%	NETHERLANDS
-28%	GREAT BRITAIN
-29%	HONG KONG
-51%	POLAND

TOP-LEVEL DOMAINS

Top-Level Domains (TLDs)

[TL;DR — The use of generic top-level domains (gTLDs) in phishing attacks continue to grow quickly, doubling in 2017 to comprise nearly four percent of all phishing domains. This suggests new gTLDs are continuing to become a more popular option for phishers, likely due to the cheap cost of some new gTLDs and the ability to create phishing sites that appear more legitimate.]

Unsurprisingly, the most commonly used TLD remained unchanged. Slightly more than 49 percent of all phishing sites were hosted on domains registered with the .COM TLD in 2017, which is nearly identical to the amount seen in 2015 and 2016. After .COM domains, the most common TLDs found in phishing sites were .NET, .ORG, .BR, .INFO, .RU, .IN, .AU, .TK, and .CF. These top ten TLDs were associated with 70 percent of all phishing sites.

Because the vast majority of phishing sites are located on domains that have been compromised by phishers rather than maliciously-registered, we would expect the share of TLDs associated with phishing sites to closely resemble the distribution of TLDs among the general websites population. When we see a TLD that is significantly over-represented among phishing sites compared to the general population, it may be an indication that it is more apt to being used by phishers to maliciously register domains for the purposes of hosting phishing content. Some TLDs were seen more than ten times as frequently in phishing site than in the general population as shown in the table below.

FIGURE 16: Top TLDs Hosting Phishing Sites in 2017

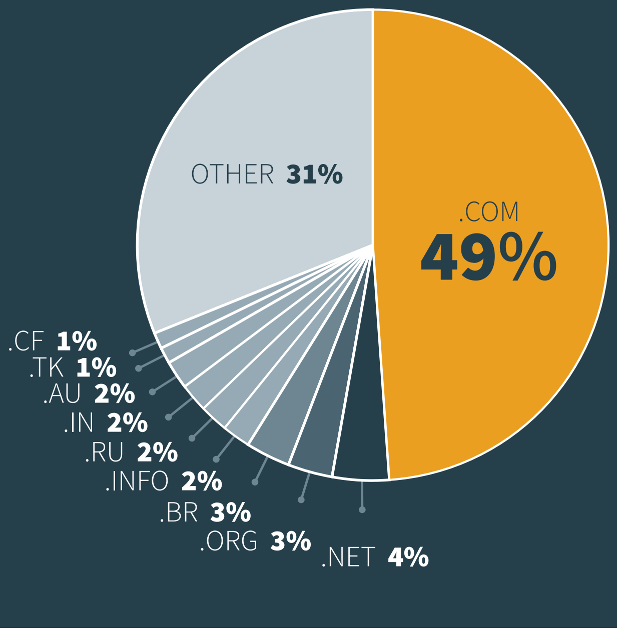
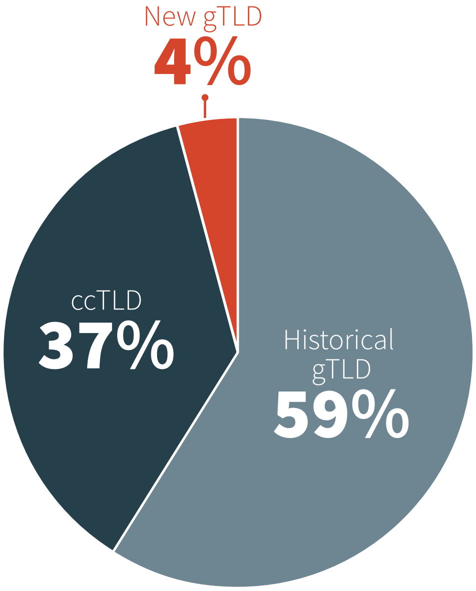


FIGURE 17: TLDs Over-Represented in Phishing Sites

TLD	Phishing Sites	General Population
.TK	1.5%	0.1%
.CF	1.5%	<0.1%
.GA	1.5%	<0.1%
.ML	1.4%	<0.1%
.CC	1.1%	0.1%
.GQ	1.0%	<0.1%

FIGURE 18: Type of TLD Associated with Phishing Sites (2017)



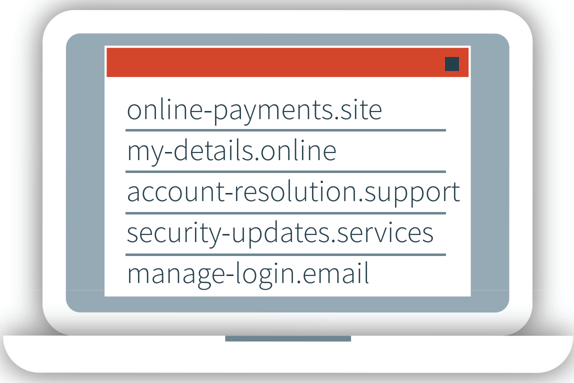
In 2017 we identified phishing sites hosted on 485 different TLDs, a nine percent rise from 2016. This increase is primarily due to increased uptake of generic TLDs (gTLDs) which were approved during ICANN's 2011 expansion program.

After increasing by over 1,000 percent in 2016, the number of gTLDs used for phishing attacks rose yet again. 258 new gTLDs were observed to host phishing content in 2017, an 18 percent increase over the previous year, and gTLDs now comprise nearly four percent of all phishing domains, up from two percent in 2016.

The gTLDs most commonly used to host phishing content during 2017 were: .TECH, .XYZ, .TOP, .ONLINE, . CLUB, .SITE, .WEBSITE, .BID, .CENTER, and .GDN.

After increasing by over 1,000 percent in 2016, the volume of newly-available gTLDs used for phishing attacks increased yet again. Generic TLDs now comprise nearly four percent of all phishing domains, doubling the two percent seen in 2016. This suggests new gTLDs are continuing to slowly become a more popular option for phishers when building their phishing sites.

gTLDs are gaining traction in the phishing ecosystem for a number of reasons. For one, some gTLDs are incredibly cheap to register, making them a compelling alternative for phishers wanting more control over their infrastructure than they would have if they chose to compromise an existing website. At the same time, certain gTLDs can be used to create phishing sites with legitimate-seeming URLs. As an example, the following gTLD domains were observed hosting phishing content in 2017:



online-payments.site
my-details.online
account-resolution.support
security-updates.services
manage-login.email

At a glance, each of these domains looks as though it could contain legitimate, helpful content to an unsuspecting victim. In the past, when phishers registered domains, they would commonly include branding associated with the target in the domain name, which adds an aura of legitimacy to the site. Now, using gTLDs, phishers have yet another tool to trick their victims.

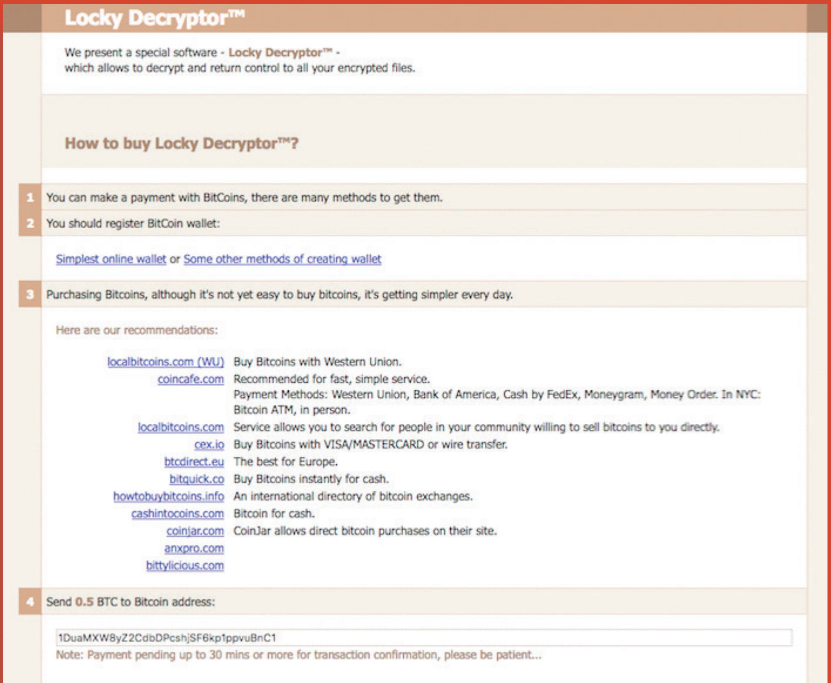
THE EVOLUTION OF RANSOMWARE IN 2017

[TL;DR — Last year ransomware reached a level of maturity and has begun to stabilize with only a few new families emerging. While familiar names like Locky and Cerber were still present, new families, often appearing during lulls in Locky distribution, presented significant threats. While the number of new families is estimated to have grown slightly, the increase is nowhere near the exponential rise we saw in 2016.

While these attacks were consistent throughout the year, the headlines were taken by the large-scale exploit-leveraging attacks that quickly crippled businesses across the world. While the exact motivation of the threat actors responsible is unclear, they represent an important evolution in cyberattacks and raise critical questions about vulnerability disclosure, patching best practices, and how to deal with the overlap of digital and physical security.

Ransomware Maturity

Ransomware remained a potent threat throughout 2017 as it continued to lock down hospitals, local governments, and end-users. We believe the increase in demand for security awareness training offset the successfulness of these attacks, which in turn make them less profitable for threat actors.



Locky Decryptor™

We present a special software - Locky Decryptor™ -
which allows to decrypt and return control to all your encrypted files.

How to buy Locky Decryptor™?

1 You can make a payment with BitCoins, there are many methods to get them.

2 You should register BitCoin wallet:

Simplest online wallet or Some other methods of creating wallet

3 Purchasing Bitcoins, although it's not yet easy to buy bitcoins, it's getting simpler every day.

Here are our recommendations:

localbitcoins.com (WU)	Buy Bitcoins with Western Union.
coincafe.com	Recommended for fast, simple service. Payment Methods: Western Union, Bank of America, Cash by FedEx, Moneygram, Money Order. In NYC: Bitcoin ATM, in person.
localbitcoins.com	Service allows you to search for people in your community willing to sell bitcoins to you directly.
cex.io	Buy Bitcoins with VISA/MASTERCARD or wire transfer.
btcdirect.eu	The best for Europe.
bitquick.co	Buy Bitcoins instantly for cash.
howtobuybitcoins.info	An international directory of bitcoin exchanges.
cashintocoins.com	Bitcoin for cash.
coinjar.com	CoinJar allows direct bitcoin purchases on their site.
anxpro.com	
bittylicious.com	

4 Send 0.5 BTC to Bitcoin address:

1DuaMXW8yZ2CdbDPcshjSF6kp1ppvuBnC1

Note: Payment pending up to 30 mins or more for transaction confirmation, please be patient...

FIGURE 19: Locky Decryptor Demanding Ransom (August 2017)

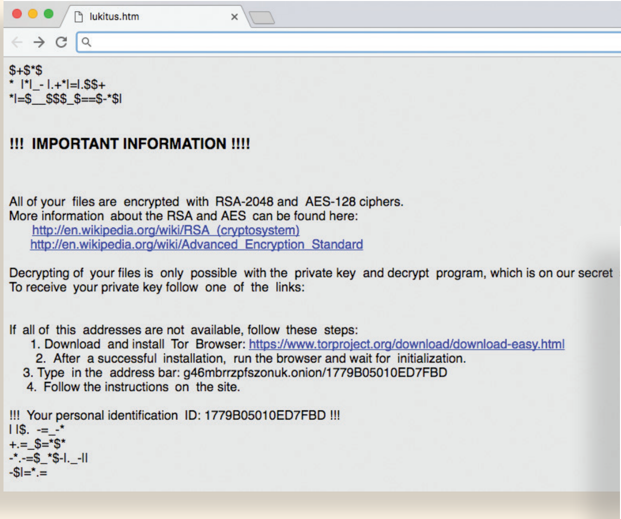
Due to the volatility in cryptocurrency prices, ransomware demands can range from a few hundred to thousands of dollars. Samples analyzed by PhishLabs in 2017 routinely showed a demand for ransoms in the thousands of dollars, which indicates the threat actors are more interested in less frequent, larger ransoms compared to previous years. In contrast, in 2016 the most prevalent ransomware families generally offered decryption in the hundreds of dollars, not thousands. The slow decline in low dollar demands shows that ransomware operators, like their banking trojan associates, are reliant on one infection out of a thousand to provide profit.

Largest Ransomware Threats of 2017

Locky

Locky remained a significant, though inconsistent, threat throughout 2017. After flooding inboxes in 2016, it disappeared for months at a time in 2017 only to come roaring back after most thought it was defeated. Delivered through phishing emails, Locky used a variety of techniques to deliver the program needed to encrypt a victim's files, with the primary attack consisting of a compressed script and macro-laden Microsoft Office document.

The code underlying Locky underwent only a few revisions in 2017, however, the threat actors behind it frequently changed other tactics, techniques and procedures associated with this ransomware. These changes included varying delivery mechanism, updating lure emails, and frequent modification of the extension that Locky appends to encrypted files. At the end of 2016 and into 2017, Locky samples were encrypting using files and appending the names of mythological deities such as Osiris, Thor, and Odin. The threat actors then moved on to Norse and Egyptian gods, before shifting to less thematic extensions such as lukitus, diablo, and ykcol.



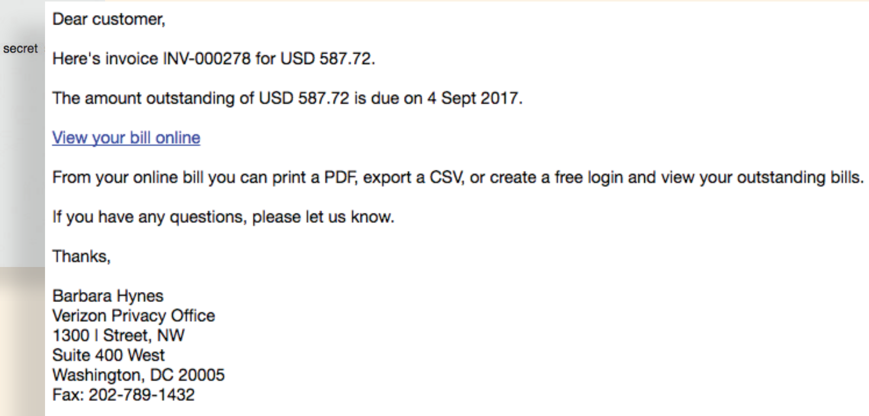
```
$+$*$
*  I*I_- I.+*I=I.$$+
*I=$__$$$_$==$-*$I

!!!  IMPORTANT INFORMATION !!!!

All of your  files are  encrypted  with  RSA-2048 and  AES-128 ciphers.
More information  about the RSA and AES  can be found here:
      http://en.wikipedia.org/wiki/RSA_(cryptosystem)
     http://en.wikipedia.org/wiki/Advanced_Encryption_Standard

Decrypting of  your files is  only  possible  with the  private key  and decrypt  program, which is on our secret
To receive  your private key follow  one  of  the  links:

If  all of  this  addresses are not  available, follow  these  steps:
     1. Download  and install  Tor  Browser: https://www.torproject.org/download/download-easy.html
      2.  After  a successful  installation,  run the browser and wait for  initialization.
   3. Type  in the  address bar: g46mbrrzpfszonuk.onion/1779B05010ED7FBD
    4.  Follow the instructions  on  the site.

!!!  Your personal identification  ID: 1779B05010ED7FBD !!!
I I$.  -=_-*
+.=_$=*$*
-*.-=$_*$-I._-II
-$I=*.=
```

FIGURE 20: Ransom Note From Lukitus Locky Variant

Globeimposter

Globeimposter first appeared in the second half of 2017, and it continues to launch several campaigns a month with some delivered en masse by the notorious Necurs botnet. Like most malicious software delivered by email, Globeimposter has repeatedly used lures warning victims of overdue invoices that require their immediate attention. The attacks are continuing in 2018, which makes it one of the more resilient ransomware threats. We have observed campaigns designed to convince victims to open an attached JavaScript file. Once the file is launched, it immediately attempts to communicate with its command and control (C2) server through one of several hardcoded URLs.

When a successful C2 connection is made, the real payload is downloaded and dropped onto the victim's machine. Again, the precise download locations appear to change with each script and have been observed using hosting services in Taiwan (203.74.203.14) and Turkey (37.230.110.87). The payload download URLs are hosted on compromised websites, so the hosting location is likely opportunistic rather than planned. As with most ransomware scams, victims are instructed to visit a TOR-hosted onion site to make their ransom payment, after which they are provided with a decryption key/software.



Dear customer,

Here's invoice INV-000278 for USD 587.72.

The amount outstanding of USD 587.72 is due on 4 Sept 2017.

View your bill online

From your online bill you can print a PDF, export a CSV, or create a free login and view your outstanding bills.

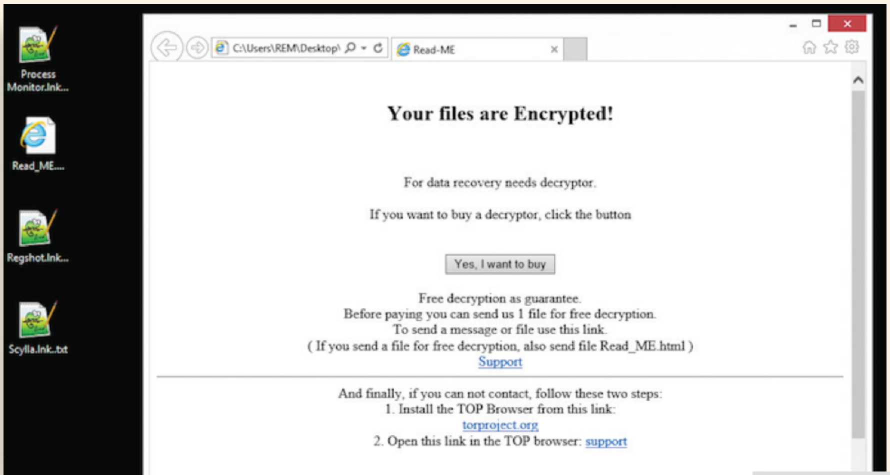
If you have any questions, please let us know.

Thanks,

Barbara Hynes
Verizon Privacy Office
1300 I Street, NW
Suite 400 West
Washington, DC 20005
Fax: 202-789-1432

FIGURE 21: Globeimposter Lure Email

FIGURE 22: GlobeImposter Ransom Note



Your files are Encrypted!

For data recovery needs decryptor.

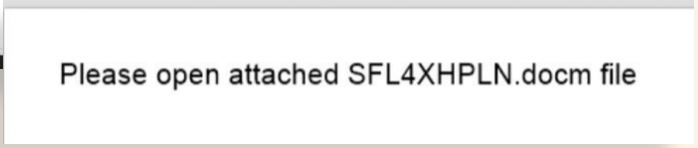
If you want to buy a decryptor, click the button

Yes, I want to buy

Free decryption as guarantee.
Before paying you can send us 1 file for free decryption.
To send a message or file use this link.
(If you send a file for free decryption, also send file Read_ME.html)
Support

And finally, if you can not contact, follow these two steps:
1. Install the TOP Browser from this link:
torproject.org
2. Open this link in the TOP browser: support

FIGURE 23: Cerber Ransomware's Logo



Please open attached SFL4XHPLN.docm file

FIGURE 24: A typical Jaff Dropping Attachment

Jaff

The substitution of Jaff for Locky in May and June 2017, was likely just that: A planned short-term substitution through which Locky's operators were able to test a variant with more substantial changes than previously attempted.

Jaff first appeared a day before the May 2017 WannaCry attack, delivered by the massive Necurs botnet via a malicious PDF hidden inside a Word document. Named after its encrypted file name, Jaff underwent some minor updates during its two months of activity. Originally hailed as a replacement for the seemingly absent Locky, distribution ended abruptly in late June.

Analysis of Jaff's code revealed enough similarities to Locky to indicate a shared threat actor, with some researchers going as far as to classify it as a variant, rather than a family in its own right.

Cerber

Cerber is one of the most advanced ransomware families, and has undergone constant updates to evade detection and maximize profit for its operators. Delivered via email and an exploit kit, Cerber's evolution has ensured a constant stream of infections and reliable profits without relying on well-known botnets.

While the other ransomware families hammer inboxes for months and subsequently disappear, Cerber has maintained a persistent low-level presence, and is likely to remain a threat in 2018.

Wannacry Trojan

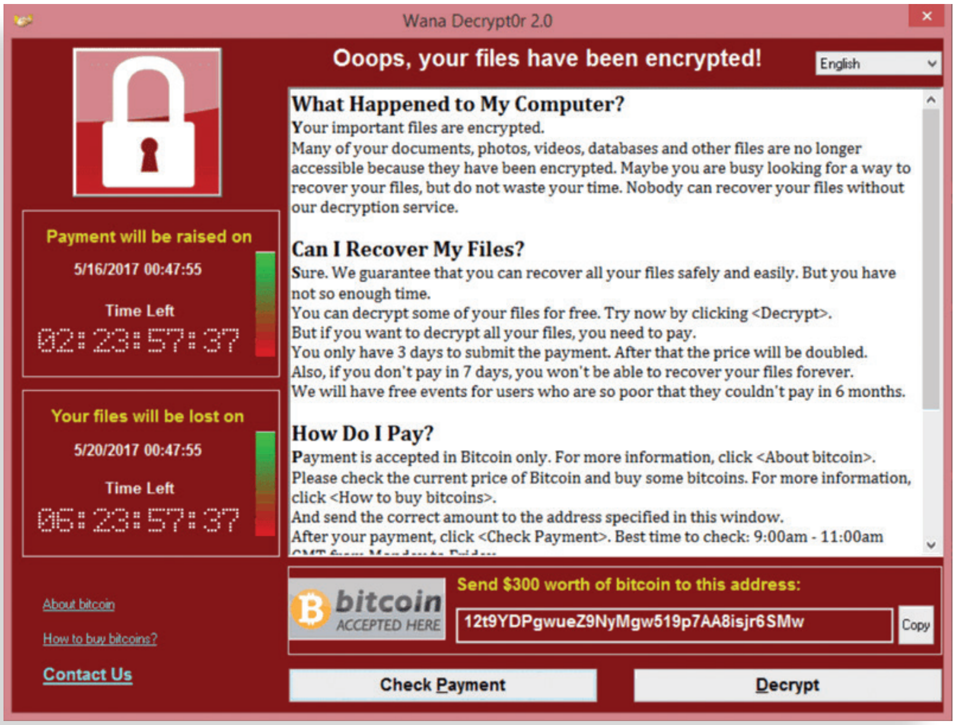
In the early hours of May 12, 2017 users around the world fell victim to a new ransomware threat, which, unlike most ransomware, did not rely on email for distribution. Instead, WannaCry gained an initial foothold via Internet exposed SMB ports, and subsequently scanned for connected machines over TCP port 445.

When a target is identified, the WannaCry Trojan searches to see whether the DoublePulsar backdoor already exists on that machine. If it doesn't, the EternalBlue exploit will be used to initiate a new infection. Either way, both DoublePulsar and WannaCry will quickly be installed on every unpatched machine within a target network. While attribution is always difficult the overwhelming consensus suggests North Korea was responsible for the attack, but may have been unaware of how quickly it would spread worldwide.

Petya/NotPetya

On June 28, 2017, NotPetya, which also leverages the exploits leaked by The Shadow Brokers, quickly locked down computers and crippled networks across the world. Similar to WannaCry, NotPetya's original infection vector is not email, but an infected mandatory update to a popular Ukrainian tax software, MeDoc. However, when infected by WannaCry, the user had the option of paying the ransom and possibly receiving a decryption key, but there was no such option with NotPetya. The virus will encrypt the victim's files, destroy the key necessary to decrypt, and then overwrite the data needed to boot the machine. Multinational corporations, who would likely have gladly paid the ransom to restore their machines and resume operations had to wipe and rebuild each infected device. The total cost is likely measured in the hundreds of millions.

FIGURE 25: The Ransom Note that Appeared on Screens Worldwide



Wana Decrypt0r 2.0

Ooops, your files have been encrypted!

Payment will be raised on
5/16/2017 00:47:55
Time Left
02:23:57:37

Your files will be lost on
5/20/2017 00:47:55
Time Left
06:23:57:37

What Happened to My Computer?
Your important files are encrypted.
Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.

Can I Recover My Files?
Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time.
You can decrypt some of your files for free. Try now by clicking <Decrypt>.
But if you want to decrypt all your files, you need to pay.
You only have 3 days to submit the payment. After that the price will be doubled.
Also, if you don't pay in 7 days, you won't be able to recover your files forever.
We will have free events for users who are so poor that they couldn't pay in 6 months.

How Do I Pay?
Payment is accepted in Bitcoin only. For more information, click <About bitcoin>.
Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>.
And send the correct amount to the address specified in this window.
After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am GMT from Monday to Friday.

Send $300 worth of bitcoin to this address:
12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw

LOOKING FORWARD

Ransomware will undoubtedly remain a threat throughout 2018. However, the rise of cryptocurrency, which allowed ransomware to flourish through anonymous payments, has also precipitated a rise in cryptojacking and cryptomining malware.

Cryptocurrencies even more focused on anonymity, like Monero, have become both valuable and mineable by distributed infections. These cryptojacking attacks are likely to dethrone ransomware as the tool of choice in the pursuit of quick and low overhead profit. Cryptomining attacks have the potential to be much more profitable than ransomware. Instead of blackmailing a victim out of a few hundred dollars of bitcoin, a threat actor can now infect that victim's machine and hijack their CPU and bandwidth to constantly create cryptocurrency.

Unlike the growth in cryptocurrency related ransomware , nation-state sponsored wormable ransomware is unlikely to make as significant an impact in 2018. Whether or not the governments responsible for WannaCry and NotPetya considered them successful, the public release of exploits that allow attacks of that size is what made them possible.

Exploits that allow remote code execution like EternalBlue and DoublePulsar are incredibly rare, incredibly valuable, and coveted by intelligence agencies. Their public release meant they could no longer be used for information gathering and infiltration by NSA as the vulnerability was quickly patched by the intelligence agencies they targeted. Knowing the window of opportunity was quickly closing, North Korea deployed WannaCry to make money, and Russia likely deployed NotPetya to both damage Ukraine and test the destructive capabilities of workable disk wiping.

Attack Vectors

For decades, email-based phishing has been and continues to be the primary mode of attack in phishing campaigns. As more companies adopt security awareness training and technical defenses improve, threat actors have started exploring other phishing attack methods. Among the areas being experimented with, SMS or mobile messaging and social media have experienced significant growth as an attack vector.

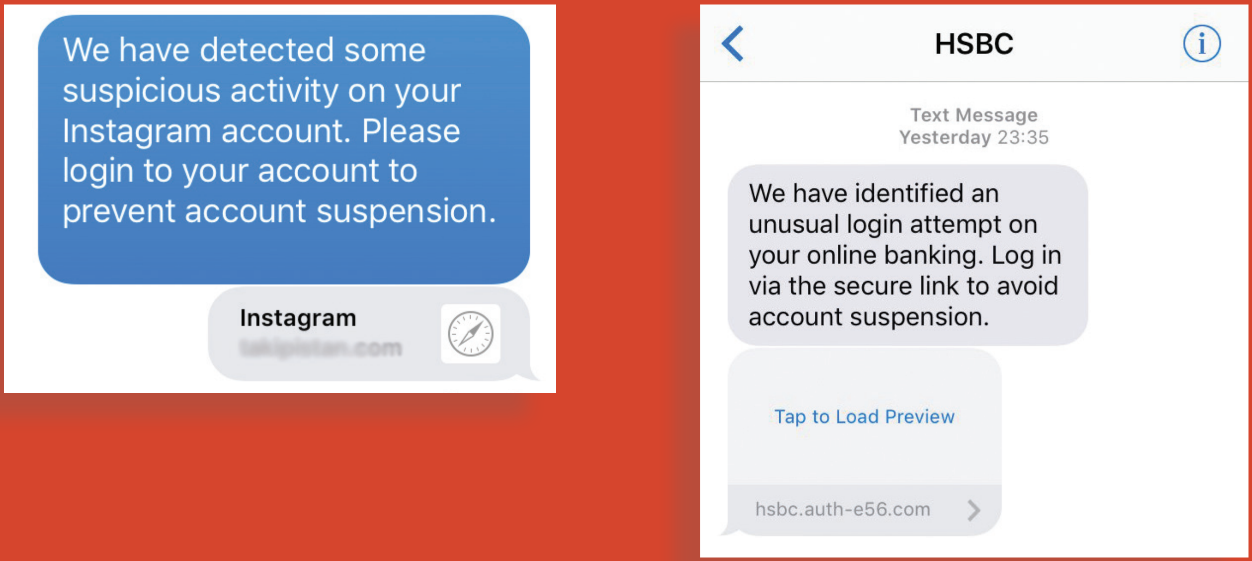
This section will dive into the two mediums that are being used to launch phishing attacks. It will also provide a better understanding of how and why cyber threat actors are using these particular attack vectors.

SMS/Mobile Messages

Until recent years, phishing was commonly thought of as an entirely desktop attack vector. Since the overwhelming majority of internet access in the U.S. has historically occurred using a desktop or laptop computer, little attention was paid to the rapid rise of mobile devices. However, that changed at the end of 2016 when Android devices overtook Windows desktops as the most commonly used devices for accessing the internet. As with most technology, innovation tends to outpace security aspects critical for a stabilized user-base, which makes mobile a viable medium for phishing attacks.

Mobile attacks have become increasingly popular as mobile devices are typically much less secure and offer more variables for the attacker to manipulate. While the hardware is becoming more secure with encrypted fingerprint sensors and even facial recognition, the user is the primary weak point. People are not yet conditioned or vigilant when it comes to mobile attack campaigns, especially when they come through text messages, social messaging,

FIGURE 26: Examples of SMS Phishing Lures



We have detected some suspicious activity on your Instagram account. Please login to your account to prevent account suspension.

Instagram
[redacted]

HSBC

Text Message
Yesterday 23:35

We have identified an unusual login attempt on your online banking. Log in via the secure link to avoid account suspension.

Tap to Load Preview

hsbc.auth-e56.com

or other chat messaging services. In many cases users simply don't review the contents of a mobile message when it appears to come from a trusted source, even though the same telltale signs of a phishing attack are typically present.

Mobile messaging attacks are also convenient for attackers because of the rise in two-factor authentication. If a threat actor gains access to (or can port) a mobile number, they can intercept the keys necessary to access everything from financial sites to social media accounts.

URL Padding

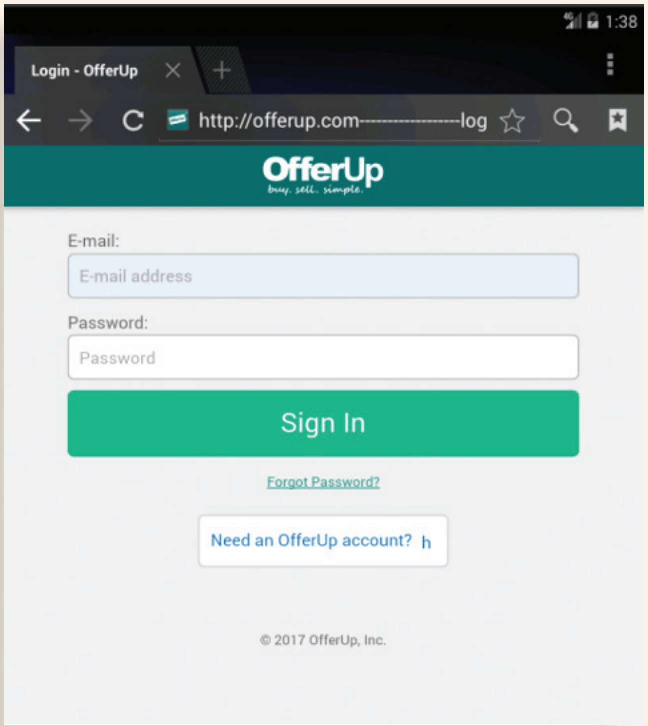
In January 2017, PhishLabs observed a new tactic used by phishers that creates a more realistic-looking URL. We call it ***URL padding***, and it takes advantage of the limited screen size of mobile devices. Unlike desktop screens where a user can typically observe a full URL with ease, mobile screens are quite small. and in some cases, it's impossible to see any of the URL text.

Now, instead of using gTLDs to simulate authenticity, threat actors have identified a new way to create believable URLs. Instead of trying to create legitimate-looking URLs, threat actors have started including real, legitimate domains within a larger URL, and padding it with hyphens to obscure the real destination. (See Fig. 27)

While there appears to be something fishy in the URL, it can be easily overlooked. In fact, with the phishing site setup as an almost perfect replica of specific social media genuine mobile login pages, and the addition of the favicon in the address bar, the site looks remarkably genuine. In each case, the tactic of padding the URL with hyphens makes it possible to obscure the real domain, and makes it appear that the victim has been directed to a legitimate website. To take things a stage further, in most cases another legitimate-seeming word (e.g., login, secure, account) has been inserted immediately following the string of hyphens, further adding to the illusion of authenticity.

To date, attacks that employ URL padding have targeted well-known financial or retail industry sites in addition to social media brands. Typically, threat actors will go after companies that have a user base that is comfortable accessing accounts on mobile devices.

FIGURE 27: URL Padding Example



The Rise of Mobile Trojans

While mobile banking trojans were a persistent threat throughout 2016, in 2017 the number of active families and their targeting scope exploded. Marcher and BankBot, the most prevalent mobile trojans in 2016, were joined by variants like BankBot Budda, MarcherOBF, and newcomers such as Catelites, RedAlert2, and LokiBot. As the consumer market continues its shift towards mobile, specifically AndroidOS, so do cybercriminals. In the past, the vast majority of people (over 80 percent) accessed the Internet using Windows desktop and laptop machines, with similar OSX devices taking a distant second spot. By the end of 2016, Android mobile devices overtook Windows desktops as the most common means of accessing the Internet. Naturally, this trend hasn't gone unnoticed, and threat actors leverage every vector possible to gain access to devices, and ultimately, credentials.

Mobile Trojan Infection Vectors

Unsurprisingly, with so many threat actors operating in the mobile banking trojan space, quite a range of delivery methods have been observed. The three dominant infection vectors observed are similar to the methods employed by their desktop brethren, with the exception of mobile use of app stores as a distribution method.

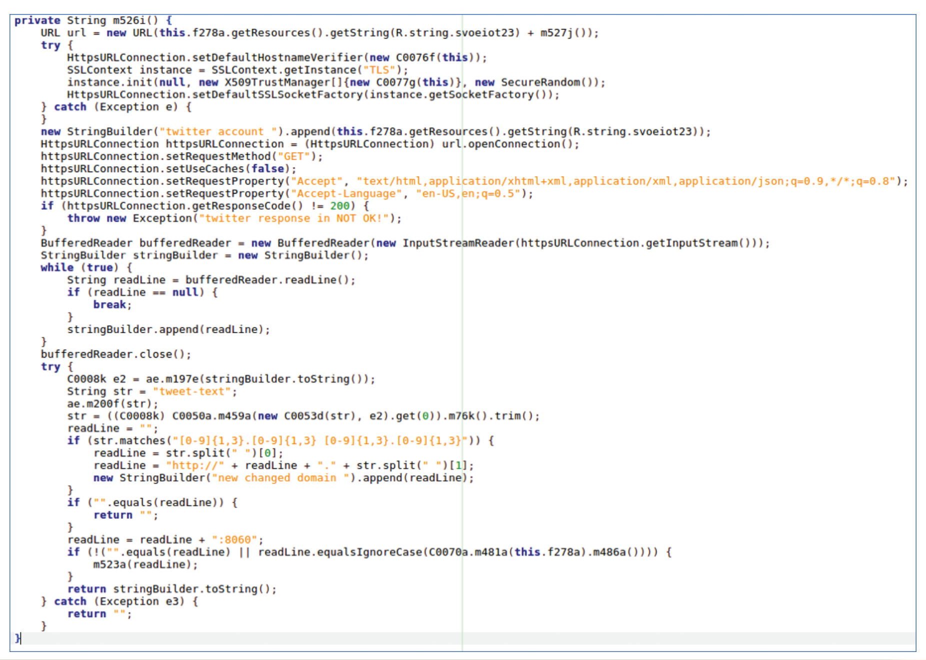
Email

To mobile threat actors, email is less attractive than SMS, because there is no guarantee of an email lure being opened on a mobile device and exploits are device specific. As a result, these attacks often incorporate additional social engineering techniques designed to convince victims to open them via their mobile device.

App Stores

Distributing trojans via app stores is less common than one would think primarily due to the difficult nature of getting apps approved on official app stores. Naturally, it's much easier to get apps approved for third-party app stores, but far fewer users visit these stores. In order to download content from a third party store, device settings must be changed to allow applications from unknown sources.

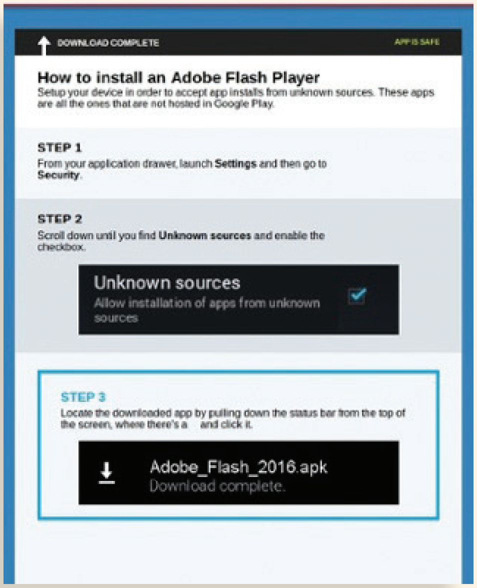
FIGURE 28: Twitter Command and Control Server Update Code



```
private String m526i() {
    URL url = new URL(this.f278a.getResources().getString(R.string.svoeiot23) + m527j());
    try {
        HttpsURLConnection.setDefaultHostnameVerifier(new C0076f(this));
        SSLContext instance = SSLContext.getInstance("TLS");
        instance.init(null, new X509TrustManager[]{new C0077g(this)}, new SecureRandom());
        HttpsURLConnection.setDefaultSSLSocketFactory(instance.getSocketFactory());
    } catch (Exception e) {
    }
    new StringBuilder("twitter account ").append(this.f278a.getResources().getString(R.string.svoeiot23));
    HttpsURLConnection httpsURLConnection = (HttpsURLConnection) url.openConnection();
    httpsURLConnection.setRequestMethod("GET");
    httpsURLConnection.setUseCaches(false);
    httpsURLConnection.setRequestProperty("Accept", "text/html,application/xhtml+xml,application/xml,application/json;q=0.9,*/*;q=0.8");
    httpsURLConnection.setRequestProperty("Accept-Language", "en-US,en;q=0.5");
    if (httpsURLConnection.getResponseCode() != 200) {
        throw new Exception("twitter response in NOT OK!");
    }
    BufferedReader bufferedReader = new BufferedReader(new InputStreamReader(httpsURLConnection.getInputStream()));
    StringBuilder stringBuilder = new StringBuilder();
    while (true) {
        String readLine = bufferedReader.readLine();
        if (readLine == null) {
            break;
        }
        stringBuilder.append(readLine);
    }
    bufferedReader.close();
    try {
        C0008k e2 = ae.m197e(stringBuilder.toString());
        String str = "tweet-text";
        ae.m200f(str);
        str = ((C0008k) C0050a.m459a(new C0053d(str), e2).get(0)).m76k().trim();
        readLine = "";
        if (str.matches("[0-9]{1,3}.[0-9]{1,3} [0-9]{1,3}.[0-9]{1,3}")) {
            readLine = str.split(" ")[0];
            readLine = "http://" + readLine + "." + str.split(" ")[1];
            new StringBuilder("new changed domain ").append(readLine);
        }
        if ("".equals(readLine)) {
            return "";
        }
        readLine = readLine + ":8060";
        if (!("".equals(readLine) || readLine.equalsIgnoreCase(C0070a.m481a(this.f278a).m486a()))) {
            m523a(readLine);
        }
        return stringBuilder.toString();
    } catch (Exception e3) {
        return "";
    }
}
```

Threat actors choosing to distribute their wares via app stores also need to decide how their store URL will be shared. Once again, phishing campaigns seem like the obvious choice, but taking this route often results in speedy detection and mitigation. Instead, many threat actors now choose to allow users to come across their apps purely through searching the relevant app store, which results in substantially better longevity, but an even narrower opportunity for distribution.

FIGURE 29: Marcher Download Disguised as Adobe Flash



DOWNLOAD COMPLETE

APP IS SAFE

How to install an Adobe Flash Player

Setup your device in order to accept app installs from unknown sources. These apps are all the ones that are not hosted in Google Play.

STEP 1

From your application drawer, launch **Settings** and then go to **Security**.

STEP 2

Scroll down until you find **Unknown sources** and enable the checkbox.

Unknown sources ☑
Allow installation of apps from unknown sources

STEP 3

Locate the downloaded app by pulling down the status bar from the top of the screen, where there's a and click it.

Adobe_Flash_2016.apk
Download complete.

Increasing Sophistication

In 2017, mobile trojans greatly increased their level of sophistication. Previously, these trojans relied on hardcoded overlays and command and control (C2) servers that were easily detected and mitigated by security researchers. Over time, they have evolved to incorporate techniques previously observed only in desktop trojans. Mobile trojans analyzed by PhishLabs were found to be utilizing social media accounts as their C2 infrastructure, as well as server-side injects and non-hardcoded configuration files. These techniques make analysis much more difficult, and reflect a dynamic threat landscape that will only increase in sophistication and severity throughout 2018.

TWO-FACTOR AUTHENTICATION BYPASS

In response to increased attacks targeting users, many companies now offer SMS-based two-factor authentication (2FA) to limit or prevent fraudulent access. As a result of these defensive measures, attackers have created SMS interceptors that are used in some threat campaigns. Using these tools, attackers can obtain a user's credentials via a phishing campaign and then intercept the user's 2FA mobile message. As a result, the attacker would then have all the necessary information needed to pass authentication tests and gain access to a user's account.

The use of 2FA bypass has also become an increasingly common feature in mobile malware, especially mobile banking trojans. Often used for credential and SMS theft, mobile banking trojans possess the ability to intercept or steal SMS messages, system information, contacts, call history, and other user data. Some of the most prolific mobile banking trojans in 2017 included BankBot, Marcher, RedAlert2, Mazar, and LokiBot.

Social Media

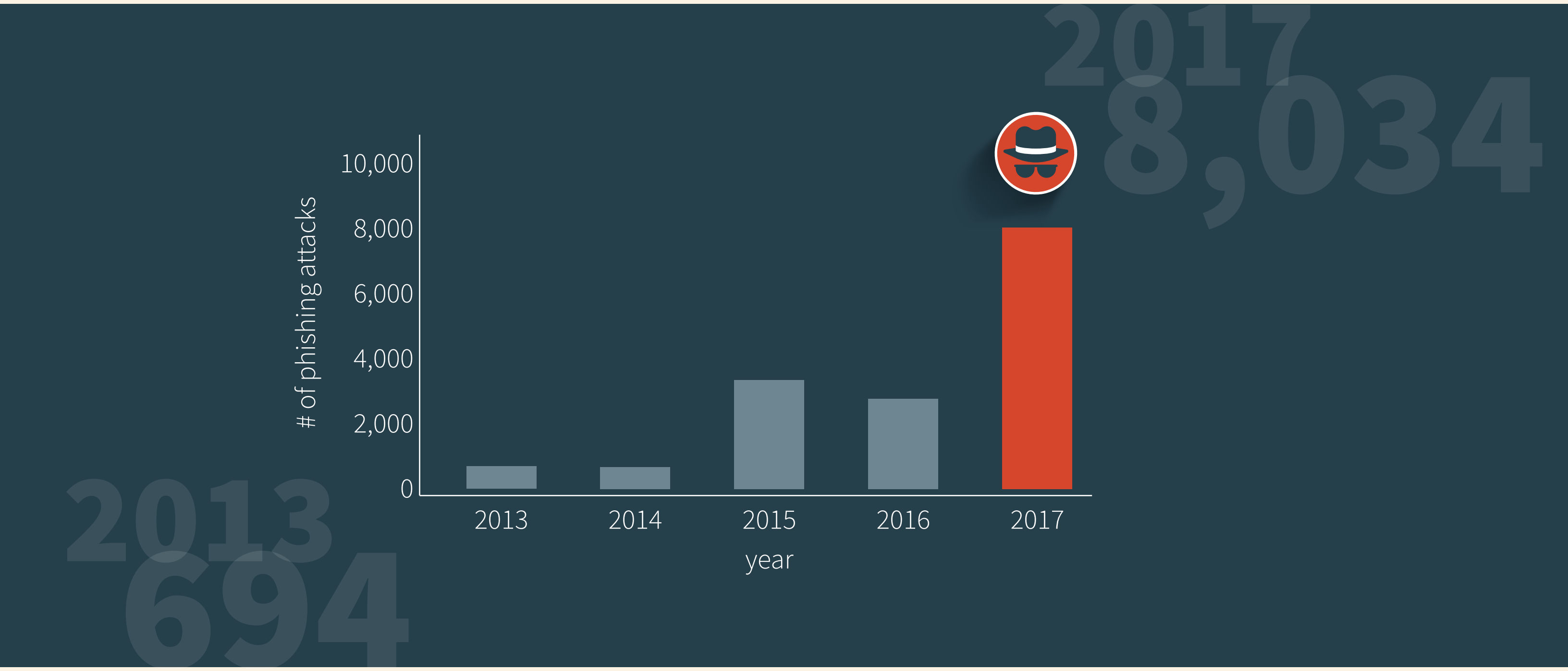
2017 was a big year for social media based phishing campaigns, and if current trends continue, social platform providers will need to take drastic action to protect users. During 2017 phishing of social media users tripled; the number of attacks in Q2 alone exceeded the total for the entirety of 2016. Why? Because users inherently trust social media platforms, and aren't conditioned to act cautiously when using them. As a result, campaigns targeting individuals through social media platforms are often more effective than those relying on traditional email lures.

Like many other web services, social media platforms have become a prime target for threat actors. While there are a number of potential explanations for this shift, the method of authentication used by social platforms is particularly relevant; social platforms allow users to use their email address in place of a unique username. This, when combined with the tendency for most people to reuse the same password across multiple services, has opened up a substantial opportunity for threat actors: The so-called "password reuse" attack.

Password reuse attacks capitalize on use of identical login credentials across multiple accounts. Threat actors simply take compromised credentials and use them to access accounts across a range of websites, typically using an automated tool. Along the same lines, threat actors can also conduct "reset attacks" after gaining access to a victim's email, by using the ubiquitous "forgot password" function to gain entry to any account that doesn't employ two-factor authentication.

Just like email, any compromised social media account can be used to further propagate a phishing campaign, and due to the trust placed in social media this tactic is often highly effective. For example, a compromised Twitter account could be used to spread malicious links via automated direct messages or public tweets, and any user who follows that link and enters their information will provide yet more fuel for the campaign.

FIGURE 30: Trends in Social Media Phishing Attacks (2013–2017)



WHAT IS A PASSWORD REUSE ATTACK?

A password reuse attack is a technique used by cyber threat actors that uses previously compromised user credentials to access accounts on other websites, generally using an automated tool. This attack vector became a major focus in 2016 due to a torrent of massive, high profile breaches. One of the biggest problems with password reuse attacks is that the websites affected are secondary casualties stemming from an initial infection — They fall victim to countless account compromises through no fault of their own.

One of the greatest challenges faced by phishing threat actors is creating trust in a potential victim; for a well-crafted spear phishing attack, threat actors often go to extreme lengths to spoof the email address of a senior executive within a target organization in order to generate the level of trust necessary to inspire action. But unlike corporate email accounts, which are typically guarded by firewalls and other security measures, communications from social media platforms designed for business provide the illusion of authenticity while being far easier to compromise. For threat actors aiming to steal private information or credentials, then, social media accounts used for business could be a quick way to open Pandora’s box.

Though still in their infancy, volume of social media attacks will likely continue to rise in the coming months, exposing the public to an increasing number of cyber vulnerabilities. Why? Because while security technologies continue improve, people are seen as the easiest route to compromise. Ultimately, the combination of social media trust and mass-harvested credentials offers threat actors a clear route to financial return, particularly when password reuse and reset attacks are considered, and that isn’t likely to change in the near future.

CONCLUSION

During 2017, PhishLabs observed a major shift in the threat landscape as threat actors turned their attention from consumers to enterprise targets. This was primarily executed via phishing attacks designed to exploit brands and tools commonly used by businesses, including email services and SaaS providers. The reason behind the shift is simple: By targeting businesses, threat actors have more opportunities to generate revenue from stolen information, i.e., by selling credentials, gaining access to sensitive or proprietary information for espionage, or individual exploitation.

While attack methods continue to evolve, reliance on social engineering and human error is a consistent theme each year. During 2017, threat actors increased their adoption of SSL certificates for maliciously registered websites, taking advantage of the misconception that HTTPS websites are inherently secure or safe. Unfortunately, as more legitimate webmasters adopt HTTPS, we can anticipate a further increase in compromised HTTPS websites in addition to a continued rise in maliciously registered HTTPS sites. The false sense of security surrounding HTTPS is highly likely to result in a further rise in phishing attack victims.

Over time, individuals have become more aware of email-based threats, forcing threat actors to adopt alternative mediums. Correspondingly, we observed a substantial increase in attacks targeting social media accounts during 2017, as well as the appearance of new mobile-specific tactics such as URL padding. As social media and mobile device usage increases, we can expect to see a steady and persistent evolution in the number and sophistication of attacks exploiting vulnerabilities in these platforms.

After exploding in 2016, the ransomware landscape stabilized last year despite several new families entering circulation. Ransomware is by no means a thing of the past, however, and it did take its toll on a variety of hospitals, local authorities, and end users throughout 2017. Over the next year, we anticipate further growth in ransomware attacks targeting mobile users.

The trends and information presented in this report are intended to help security leaders and practitioners understand the impact of changes in the phishing landscape. While social media and mobile attacks are on the rise, traditional phishing is an ever-present threat to corporate networks, and will remain the primary attack vector for the foreseeable future. As the phishing landscape evolves, organizations must continue to invest in proactive defense in order to avoid falling prey to the latest phishing tactics.

> As social media and mobile usage increases, we can expect to see a steady and persistent evolution of attacks exploiting vulnerabilities offered through each. More education of email-based phishing attacks has resulted in user suspicion, forcing threat actors to pivot to the next medium.

PHISHLABS

Thank you for reading the 2018 Phishing Trends and Intelligence Report. We hope you found the information to be useful. If you would like to discuss it, contact us at **info@phishlabs.com**.

For more information on PhishLabs and how we help organizations fight back against phishing, visit **www.phishlabs.com**.

For more research and commentary, sign up for our blog at **blog.phishlabs.com.**

You can also follow us social media:

@PhishLabs

www.linkedin.com/company/phishlabs

https://www.facebook.com/PhishLabs/

PHISHLABS™