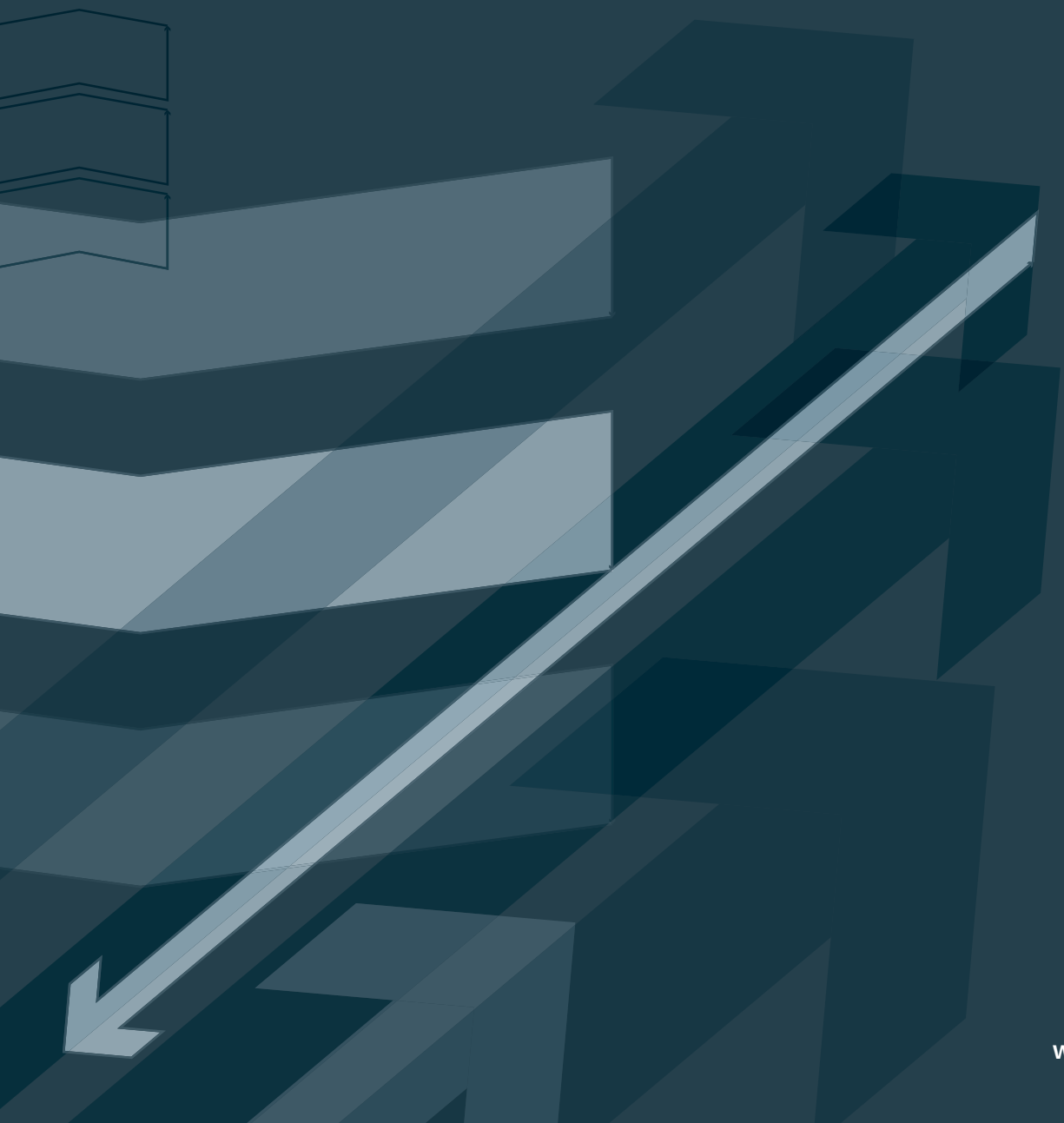
PHISHLABS

2017 PHISHING TRENDS & INTELLIGENCE REPORT

Hacking the Human



www.phishlabs.com

CONTENTS

INTRODUCTION

Welcome to the 2017 Phishing Trends and Intelligence (PTI) Report. The purpose of this report is to not only provide insight on significant trends, tools, and techniques being used by threat actors to carry out phishing attacks, but to also provide context and perspective into why these changes are occurring.

The phishing threat landscape today is astoundingly different than it was at the start of 2016. There were two transformative events that led to fundamental upheavals in the landscape and shape what to expect going forward.

The first of these events is a fundamental shift in who is being targeted by phishing attacks, driven by changing threat actor motivations and the widespread acceptance of email addresses in place of unique usernames.

The second transformative event of 2016 was the rapid rise of ransomware into a public epidemic that claimed victims across the spectrum of society. Phishing was and continues to be, by a wide margin, the most prolific method used to distribute ransomware. Fighting back against ransomware requires fighting back against phishing.

This report provides a first-hand, in-depth view of the these events as well as others that come 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. And we hope that the detailed findings are used to better mitigate that risk.

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 attacks.

To provide context for our intelligence holdings, consider:

- We analyzed nearly one million confirmed malicious phishing sites in 2016.
- These sites resided on more than 170,000 unique domains (23% more than in 2015).
- We investigated and mitigated more than 7,800 phishing attacks every month, identifying the underlying infrastructure used in these attacks and shutting them down.
- We analyzed thousands of unique malware samples from more than 100 ransomware variants and more than 20 banking Trojan families.
- Leading financial institutions, social media sites, healthcare companies, retailers, insurance companies, and technology companies use our services to fight back against phishing threats.
- We've been fighting back against phishing attacks since 2008.

We investigated and mitigated more than 7,800 phishing attacks every month, identifying the underlying infrastructure used in these attacks and shutting them down.

EXECUTIVE SUMMARY

Phishing is the top threat vector for cyberattacks. Exploiting the human vulnerability continues to be the most attractive and successful path for threat actors targeting the assets of organizations and individuals.

The 2017 PTI Report provides analysis of trends in phishing attacks and insight into the techniques being used in those attacks. It attempts to provide clarity on who is being targeted and give perspective into how and why they are being targeted. Those who read this report will have a better understanding of phishing threats and be better equipped to protect against them **(and, ideally, join in efforts to fight back).**

Key findings of the 2017 PTI Report include:

- Cloud storage sites will likely overtake financial institutions as the top targets of phishing attacks, marking a major evolution in phishers' target selection process.
- Broad acceptance of email addresses instead of unique usernames is being heavily exploited to mass harvest credentials, exposing an exponentially greater number of unsuspecting online services to secondary attacks via credential reuse and other methods.
- We identified phishing sites that resided on more than 170,000 unique domains, a 23% increase.
- Phishing volume grew by an average of more than 33% across the five most-targeted industries.
- Attacks targeting government tax authorities have grown more than 300% since 2014.
- There were more IRS phishing attacks in January 2016 than there were in all of 2015.
- In a deviation from prior years, phishing volume peaked mid-year due to the influence of major global events, such as Brexit, and a spike in virtual web server compromises.
- The share of attacks against targets in the United States continues to grow, accounting for more than 81% of all phishing attacks.
- Attacks on Canadian institutions grew 237%, more than any other country.
- Although 59% of phishing sites were hosted in the United States, there was a significant increase in the number of phishing sites hosted in Eastern Europe.
- Although the .COM top-level domain (TLD) was associated with more than half of all phishing sites in 2016, new generic TLDs are becoming a more popular option for phishing because they are low cost and can be used to create convincing phishing domains.
- Of more than 29,000 phish kits collected, more than a third used techniques to evade detection.
- Ransomware attacks, the predominant type of malware being distributed via phishing, are now focusing on organizations that are more likely to pay ransoms, such as healthcare, government, critical infrastructure, education, and small businesses.

KEY FINDINGS

THE PHISHING LANDSCAPE TRANSFORMATION

While it is always shifting, in 2016 we observed significant changes in the fundamental dynamics of the phishing threat landscape. These changes are transforming the landscape in profound ways that will impact organizations for years to come. This section reviews those observations and examines them in detail.

Methodology

The findings detailed in this section are the result of an analysis of nearly one million **confirmed** malicious phishing sites hosted on more than 170,000 unique domains and more than 66,000 unique IP addresses identified by PhishLabs in 2016. Throughout this section, we reference the share and volume of phishing attacks observed throughout the year. In the context of this report, we define a phishing "attack" as a domain hosting phishing content. References to "share" of phishing attacks indicate the percentage of attacks relative to the entire attack population, while "volume" refers to the raw, cumulative number of attacks. This analysis represents our observations and judgements regarding the targets of consumer-focused phishing attacks and the techniques used by phishers.

How phishing works

Generally, after a phisher has compromised a vulnerable website or registered a malicious domain where their phishing content will be hosted, they upload a compressed collection of files containing all of the assets needed to create a phishing site, also known as a "phish kit." By analyzing these kits, we are able to gain a better understanding of phishers' tactics and techniques, as the kits contain the "recipe" for developing a successful phish. Reverse-engineering these kits allows us to learn about a scheme so we can better identify individual phishing sites, neutralize a phisher's data exfiltration infrastructure, and allows us to adapt our mitigation techniques when phishers' modus operandi evolves.

In addition to containing the building blocks for a phishing site, these kits also contain scripts that send any information that is collected during a phishing compromise to the phisher. The compromised information is usually sent to a temporary email account set up by the phisher, known as a "drop email account," but we have also seen instances where information has been forwarded to another domain controlled by the scammer, stored in a file on a compromised server, or even sent via an instant messaging protocol, like XMPP.

In 2016, PhishLabs analyzed nearly 1 million confirmed malicious phishing sites hosted on more than 170,000 unique domains.

1 MILLION

More than 91% of all phishing attacks in 2016 targeted five industries: financial institutions, cloud storage/file hosting services, webmail/online services, payment services, and ecommerce companies.

Who is being targeted?

[TL;DR — Across the five most-targeted industries, attack volume grew by an average of 33% in 2016. By the end of 2017, it is likely that cloud storage services will take the place of financial institutions as the top phishing target. This monumental shift from historical trends marks a significant expansion in how phishers profit from their attacks. In addition to seeking direct profits from phishing financial accounts where funds can be immediately stolen, phishers have adopted more indirect approach to making money. Phishers are exploiting the now-widespread authentication practice of using email addresses in place of unique usernames. By launching phishing attacks targeting popular online services that use this authentication practice, phishers are mass harvesting email address/password credential combinations that can be used to attack secondary targets (often via password reuse attacks).]

In 2016, we identified 976 brands from 568 parent institutions (private companies, government agencies, schools, etc.) that were targeted by consumer-focused phishing attacks. This is an increase from 2015, where phishing attacks targeted 895 different brands from 559 institutions. Of those entities targeted in 2016, 166 had not been targeted the previous year. Conversely, 155 institutions that were targeted by phishers in 2015 were not phished in 2016.

More than 91% of all phishing attacks in 2016 targeted five industries: financial institutions, cloud storage/file hosting services, webmail/online services, payment services, and ecommerce companies. The total number of phishing attacks increased for each of these five industries by an average of 33%.

Financial institutions, the historical target-of-choice for phishers, remained the most popular target in 2016. Although the total number of phishing attacks grew slightly in 2016, the industry's share of phishing attack targets has decreased substantially in recent years. In 2013, attacks targeting financial institutions accounted for more than a third of all phishing attacks. That number has now dropped to represent only less than a quarter of the global phishing volume.

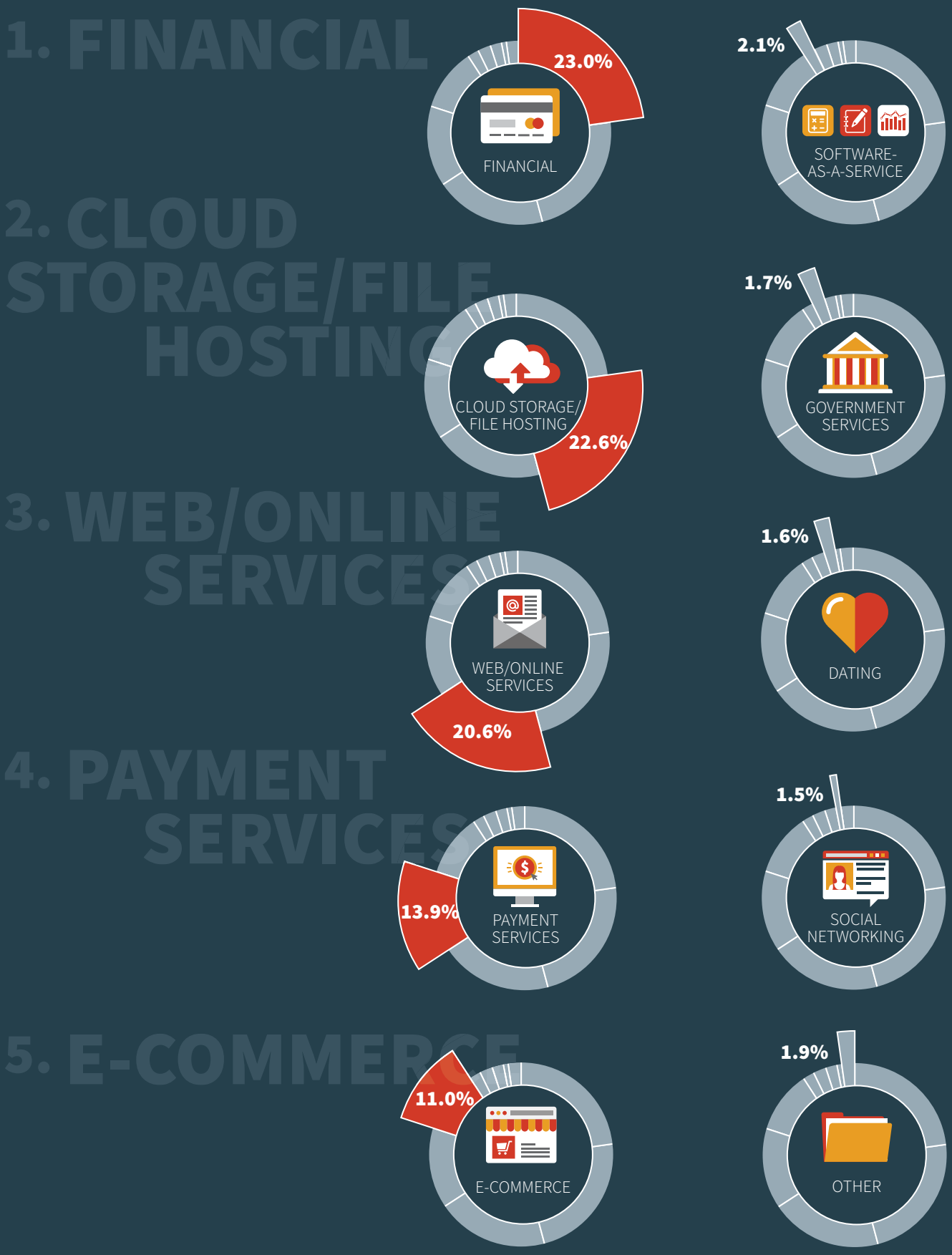
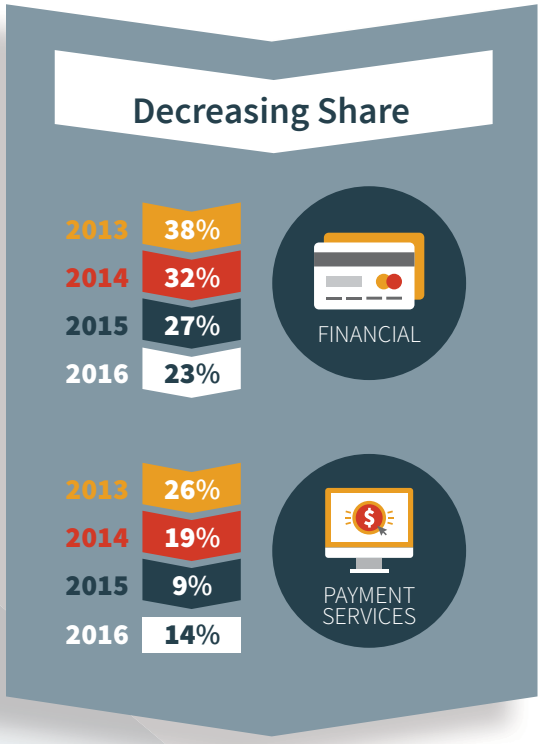


FIGURE 1: Industries Targeted by Consumer-Focused Phishing (2016)

FIGURE 2: Industries With Declining Shares of Phishing Attacks (2013–2016)



As the share of attacks targeting financial institutions has declined, other industries have seen their shares increase substantially. This trend is most pronounced with cloud storage services. In 2013, fewer than one in ten phishing attacks targeted cloud storage services. In 2016, the industry's share was only a fraction of a percent behind financial institutions (22.6% compared to 23%). **If these recent trends continue as we expect, there is a strong likelihood that cloud storage services will overtake financial institutions as the most targeted industry in 2017.** It is also notable that phishing attacks impacting this industry almost exclusively target only two companies: Google (Google Drive/Docs) and Dropbox.

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 nearly tripled in 2016. Although attacks targeting SaaS companies only accounted for slightly more than two percent of global phishing volume in 2016, it's likely that the frequency of attacks targeting these services will continue to increase in the future. As with cloud storage sites, phishing attacks plaguing the SaaS industry primarily target two companies, Adobe (Adobe ID) and DocuSign. (There is a very good reason for this, which we'll explore in just a moment).

Of the top five most targeted industries, only webmail/online services have seen a consistent increase in their share of phishing attacks in each of the last four years. Over this time period, the percentage of phishing attacks targeting webmail/online services has nearly doubled, growing from 11% in 2013, to 21% in 2016.

After seeing decreases in attack volume in 2015, payment service companies and e-commerce sites both saw significant increases in 2016. In 2015, the number of attacks targeting payment service companies fell by more than 28% and was the only industry to see a decrease in total phishing volume. In 2016, however, phishing attacks against payment service companies rebounded and grew by 80%, now accounting for 14% of total phishing activity. This is, however, well below the 26% share the industry had in 2013, when it was the second-most targeted industry. E-commerce companies experienced a surge of 44% in the number of phishing attacks targeting their customers and now account for 11% of global phishing activity.

Although most industries saw increases in the number of phishing attacks in 2016, a few saw a dip in the number of incidents impacting their customers. After seeing a steady increase in phishing attacks from 2013 to 2015, the gaming industry saw a substantial 75% decrease in the number of attacks, by far the most of any industry. Social networking sites, which saw a massive increase in attacks in 2015, also saw a decline in the total volume of phishing attacks in 2016, dropping by 17%.

Phishing attacks targeting government services also increased dramatically in 2016. This growth was almost entirely due to a surge in phishing attacks against government tax collection agencies. Since 2014, attacks targeting these institutions have increased more than 300%. Clearly, phishers have found them to be very attractive targets. Nearly all the attacks targeting tax agencies targeted institutions in four countries: Canada (Canada Revenue Agency), France (Directorate General of Public Finance), United Kingdom (HM Revenue & Customs), and United States (Internal Revenue Service).

FIGURE 3: Industries With Increasing Shares of Phishing Attacks (2013–2016)

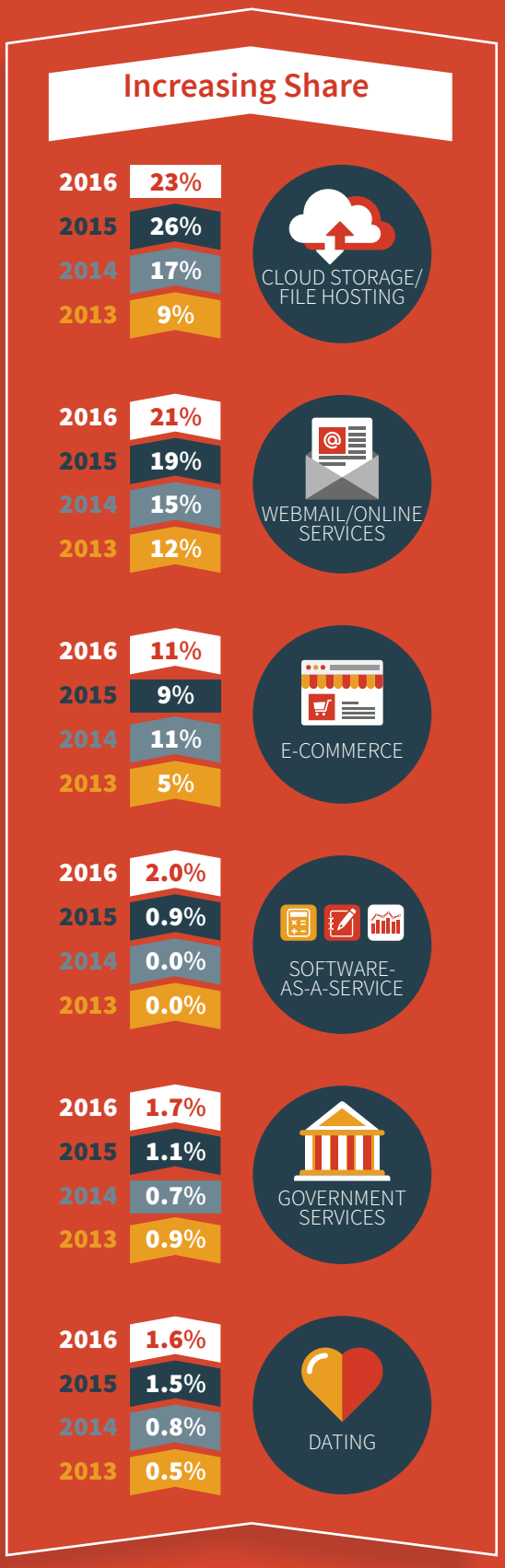


FIGURE 4: Changes in Phishing Volume (2016)

So why are we seeing these changes? Because a fundamental shift is underway in the overall phishing threat landscape. **Phishing threat actors are evolving their tactics to make their jobs easier and take advantage of ease-of-use features built into many websites.** By shifting their targets and techniques, phishers have:

- made credential collection more efficient;
- focused on collecting a wider breadth of information that can be used to facilitate other types of crimes; and
- moved to a more indirect, but likely more lucrative, profit motive.

The shift is driven by a major vulnerability in how many web services, including nearly all of the cloud storage services and SaaS companies that have seen a substantial increase in phishing attacks, allow their users to authenticate into their accounts. Instead of requiring users have a unique username and password, they allow users to log in using their email address in conjunction with a "unique" password. The problem with this method is that many, perhaps a majority, of their users simply reuse their email password instead of creating a new one.

WHAT DRIVES WHO PHISHERS TARGET?

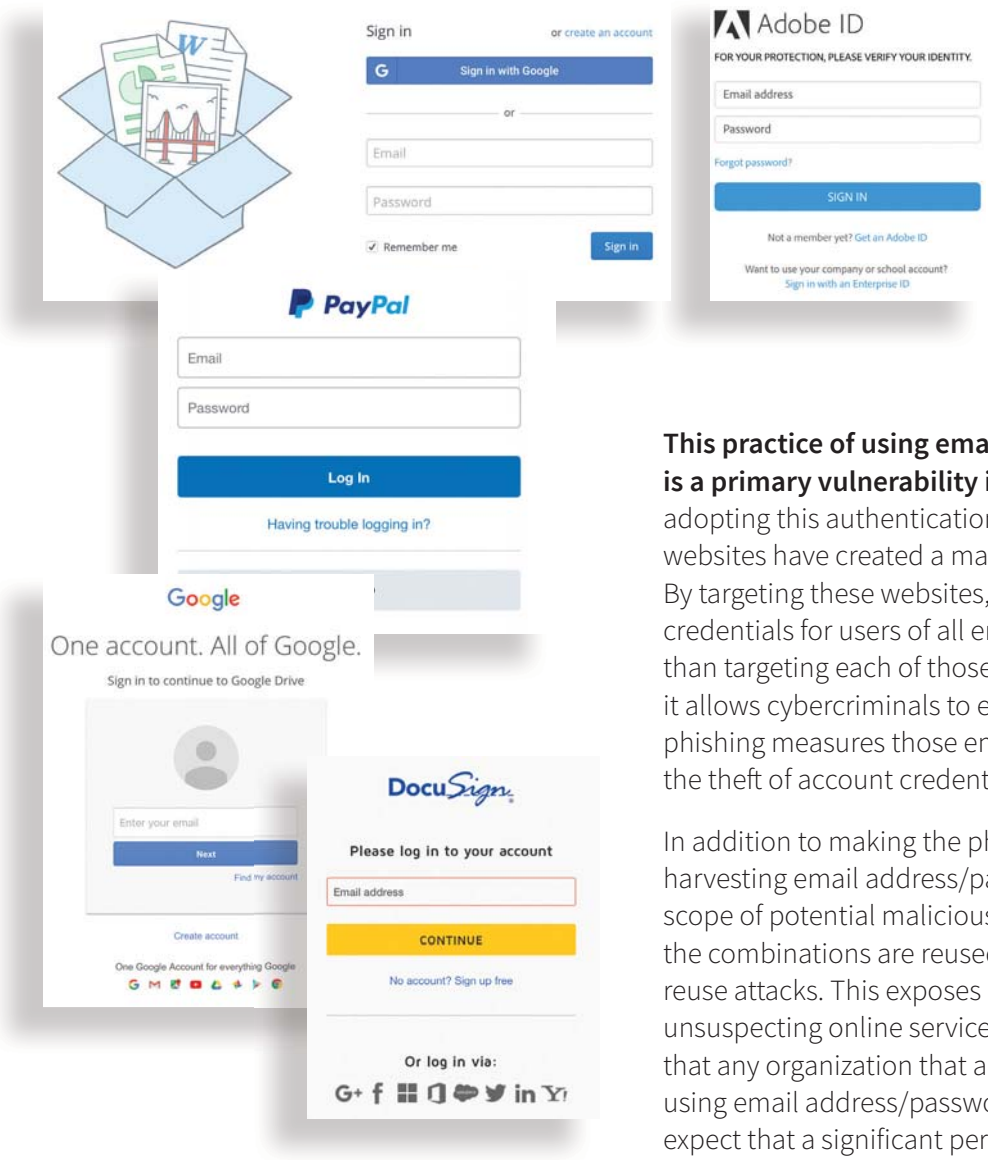
Recent trends indicate phishing threat actors' previously well-established motivations are fundamentally shifting. There are three primary motivations for phishers' selection of targets.

1. Immediate Account Takeover — stealing money from an account or selling access to an account in an underground market

2. Credential Proliferation — attacking targets using generic credentials (e.g., email accounts) that allows for more efficient collection that can be used to attack secondary targets on a larger scale

3. Data Diversification — collecting comprehensive information about a victim that can be used to commit other crimes, such as identity theft or tax fraud, or sold for more money in the underground economy

FIGURE 5: Examples of Websites Using Email Accounts as User Credentials



This practice of using email addresses as account credentials is a primary vulnerability in the phishing ecosystem. By adopting this authentication practice, cloud storage and SaaS websites have created a massive opportunity for cybercriminals. By targeting these websites, cybercriminals can easily harvest credentials for users of all email services. This is far more efficient than targeting each of those email providers individually and it allows cybercriminals to effectively sidestep potential anti-phishing measures those email providers have in place to prevent the theft of account credentials.

In addition to making the phishers' job more efficient, mass harvesting email address/password combinations expands the scope of potential malicious activity to any other accounts where the combinations are reused using techniques like password reuse attacks. This exposes an exponentially greater number of unsuspecting online services to indirect attacks. It also means that any organization that allows account holders to authenticate using email address/password combinations should reasonably expect that a significant percentage of their users are relying on credentials **that have already been compromised elsewhere.**

WHAT IS A PASSWORD REUSE ATTACK?

A password reuse attack is a method used by cyber threat actors that takes previously-compromised user credentials and, relying on frequent reuse, uses them to access a user's account on other websites, generally using an automated tool. This attack vector became a major focus in 2016 as a result of numerous high-profile, massive data breaches. One of the biggest problems with password reuse attacks is that the websites impacted by these attacks are secondary casualties stemming from an initial compromise.

PASSWORD REUSE

SHIFT IN TACTICS

This evolution in the phishing landscape also denotes a changing mindset in how phishers use the information they collect for financial gain (because it's always about the money). Historically, when phishers targeted customers of financial institutions, they would usually immediately use the credentials to break into a victim's account and steal their money. While this method is still being used at historically-consistent levels (the overall number of attacks targeting financial institutions increased in 2016), the 2016 phishing landscape was marked by explosive growth in attacks targeting credentials that cannot be used for an immediate profit.

With the recent shift in tactics, phishers are likely taking a more indirect approach to making money from stolen credentials. There are two basic ways they can do this. The first method involves using password reuse attacks to break into multiple financial accounts to steal money.

This technique gives a threat actor an opportunity to multiply their financial gain by taking over more than one insecure account. The second method involves selling mass harvested credentials on underground forums and Dark Web marketplaces, which was a popular subject in the media in 2016. Although the market for credential dumps has become quite saturated, prices for these collections of compromised credentials have recently ranged from $50–$1,000 USD.

It's worth noting that this means that many cloud storage and SaaS accounts compromised are likely **not** the accounts that the phishers are truly targeting. These accounts are being targeted as an intermediate step in a bigger scheme.

...many cloud storage and SaaS accounts compromised are likely **not** the accounts that the phishers are truly targeting. These accounts are being targeted as an intermediate step in a bigger scheme.

The increase in phishing attacks against industries such as government services, payment services, and e-commerce sites also indicates an expansion in the type and amount of information coveted by phishers.

The increase in phishing attacks against industries such as government services, payment services, and e-commerce sites also indicates an expansion in the type and amount of information coveted by phishers. Historically, information that was primarily targeted in phishing attacks included account credentials and basic personal data. Recent attack trends show phishers are now interested in a much wider variety of personal, financial, employment, and account security information. This information is generally collected in phishing attacks that coerce victims into entering a substantial amount of information needed to "verify" or "reactivate" their online account, one of the most common lures phishers use to trick victims.

Why is the scope of information targeted by phishers expanding? A likely reason is to facilitate more lucrative future phishing and account takeover activities. For example, a growing number of phishing sites collect account security information, such as common challenge/response combinations and mother's maiden name. This information can be used later to bypass verification mechanisms during password reuse attacks.

Another piece of information that has been targeted more frequently is victim phone numbers. Not only can knowing a victim's phone number be used to bypass two-factor authentication, it is likely that this information is also being harvested to deliver subsequent phishing campaigns via SMS, which is quickly becoming a more popular vector of attack (often referred to as SMiShing).

It's also worth noting that the extensive amount of personal information collected by some phishing sites can easily be used for a variety of other criminal purposes, such as identity theft. financial information, a favorite target of phishers, can be used to commit credit card fraud. The explosion of phishing attacks targeting tax agencies in 2016, also shows that phishers are moving toward tax return fraud as a preferred use of compromised data.

INTERNAL REVENUE SERVICE

One of the biggest cybersecurity events at the beginning of 2016 was the massive increase in phishing attacks targeting the Internal Revenue Service. The surge was so substantial that the number of phishing sites observed in January 2016 was greater than the total number of IRS phish seen in all of 2015.

We observed phishing campaigns targeting both taxpayers and tax professionals (those paid to prepare tax returns for others). For most IRS phishing scams, stealing taxpayer information is the objective. These attacks varied in scope, but they generally sought to collect any personal, financial, and employment information needed to file a legitimate-looking fraudulent tax return.

This includes information such as an individual's personally identifying information (PII), filing status, employer information, and income. Some phishing sites went even further and gathered on the victim's spouse and dependents, electronic filing PIN details, and/or complete W2 data.

In 2016, phishers used a variety of different ploys to trick victims into handing over their personal and financial information. For IRS phishing schemes, the most common technique used to scam taxpayers was to claim that a victim needed to update or verify their information in order for their return to get processed.

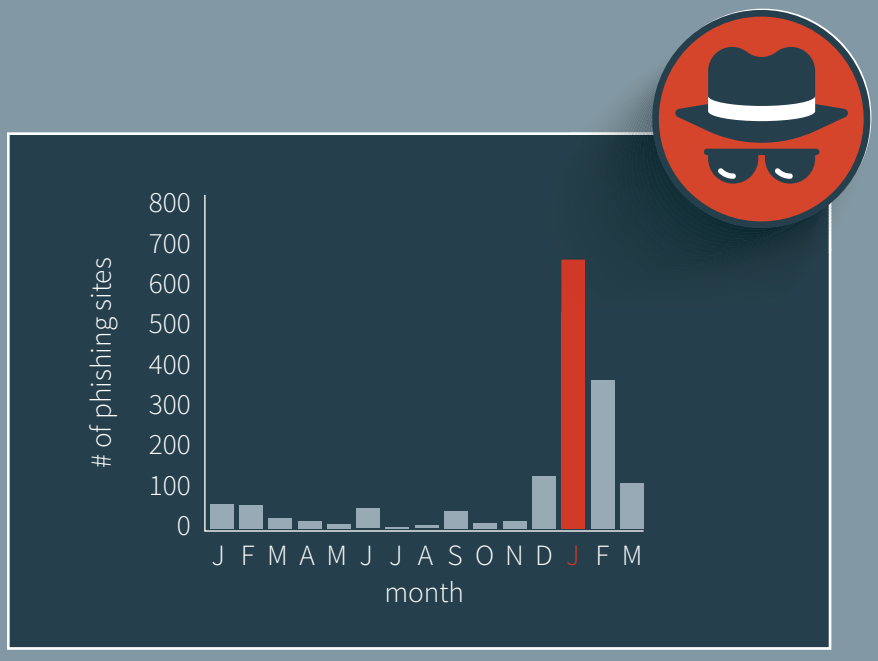
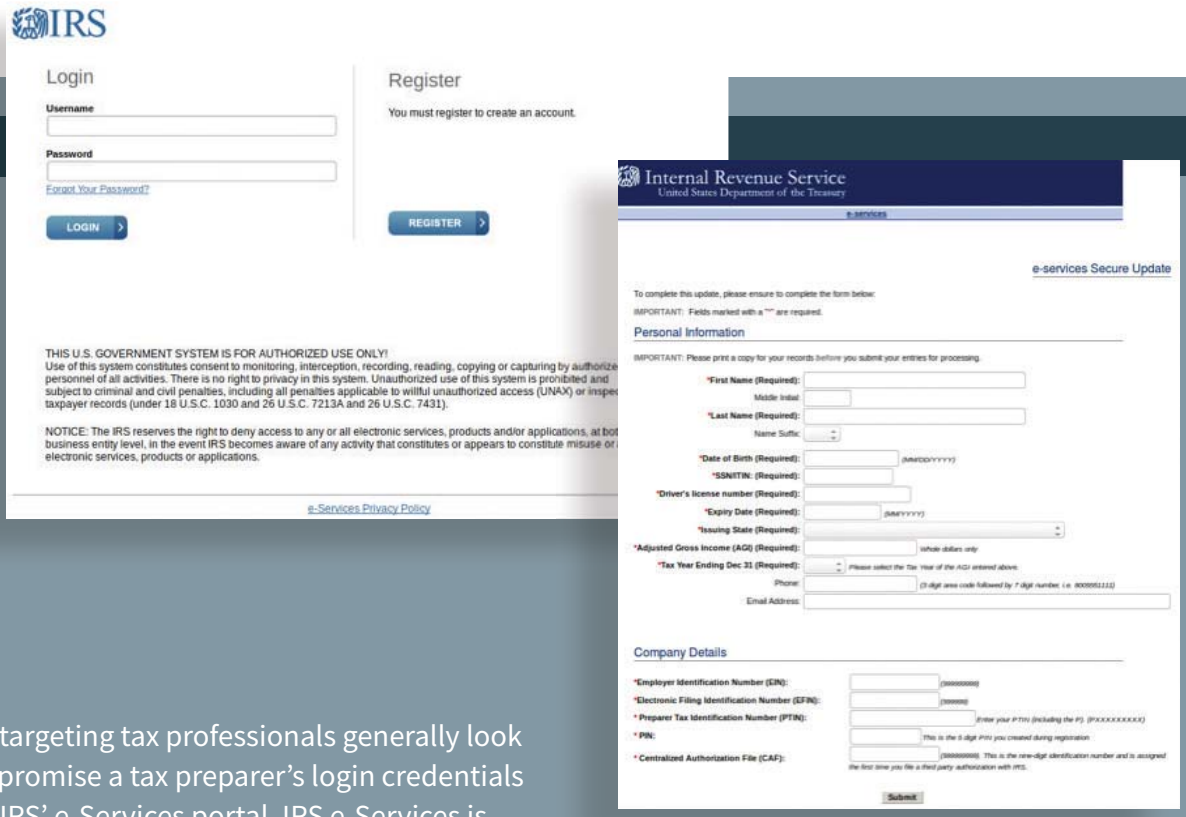


FIGURE 6: IRS Phishing Attacks (2015–2016)

FIGURE 7: Example of IRS E-Services Phishing Pages



Scams targeting tax professionals generally look to compromise a tax preparer's login credentials for the IRS' e-Services portal. IRS e-Services is an online platform that allows tax professionals to request client transcripts and file client returns electronically. Phishing attacks targeting e-Services credentials were so prevalent in early-2016 that the IRS sent out a warning to tax preparers alerting them of the scam.

Although fewer attacks were observed targeting tax preparers, the amount of damage that could be caused by these attacks has the potential to be far greater. Not only would a phisher have the ability to request previous tax information for numerous clients at once, but they could also use the application to electronically file fraudulent returns using a vetted source.

Although we saw a tremendous spike in phishing activity targeting the IRS during the 2016 tax season, our analysis indicated the kits that fuel these attacks were written and distributed by a relatively small number of individuals. Compared to phishing campaigns targeting other industries, most IRS scams were less sophisticated than campaigns targeting other industries. That said, we did observe some phishers including advanced features to enhance the authenticity of their phishing sites and restrict access to the sites to certain visitors. Due to the success of these phishing attacks in 2016, it is likely that we will see a similar spike in IRS phishing activity in early-2017.

When are attacks happening?

[TL;DR — In 2016, phishing volume spiked mid-year and declined in the fourth quarter. This deviated from prior years in which volume steadily increased and peaked at end of each year. This mid-year spike can likely be attributed to phishers capitalizing on major global events (such as Brexit) and an anomalous surge in virtual web server compromises.]

Between 2013 and 2015, the trend of phishing attacks through the year followed a consistent and predictable pattern. During these three years, phishing attacks generally increased throughout the year and surge in the fourth quarter during the holiday season. This was not the case in 2016. Instead of peaking at the end of the year, phishing attacks in 2016 crested in the middle of the year and trailed off during the holiday season. Additionally, December 2016 saw the lowest number of phishing attacks observed in nearly two years.

Instead of peaking at the end of the year, phishing attacks in 2016 crested in the middle of the year and trailed off during the holiday season

This deviation from historical patterns may be attributed to two factors:

1. phishers taking advantage of historic global events and
2. a spike in the number of web server attacks.

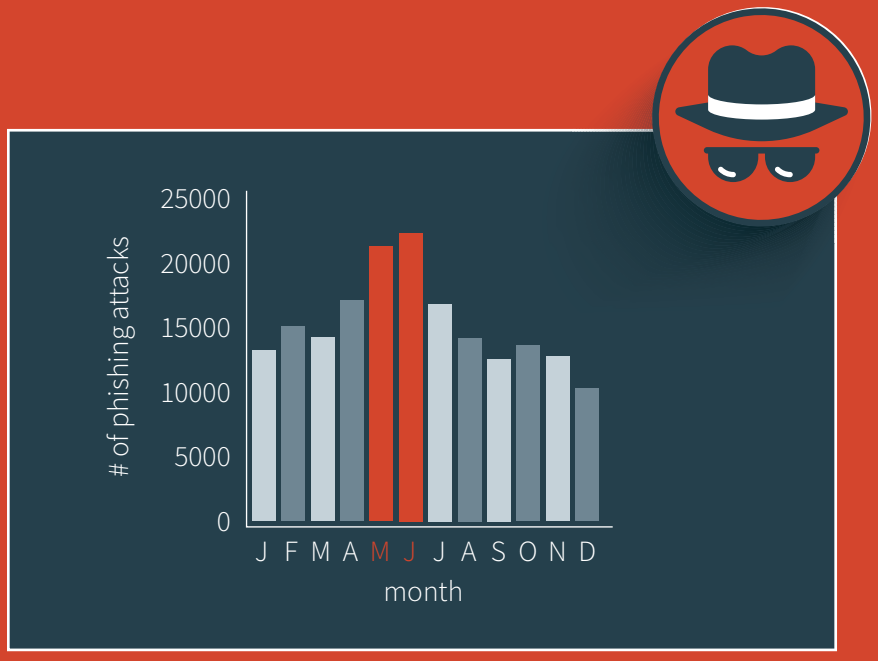


FIGURE 8: Phishing Attacks by Month (2016)

Phishers try to take advantage of potential victims' anxiety and fears caused by major events.

1. The Brexit Effect

As we have seen throughout the years, phishers will always take advantage of temporally relevant events, major incidents, or global crises to exploit potential victims. Therefore, phishing attacks have historically surged during the holiday season and taken advantage of consumers' expectations to receive communications from certain companies during this time of year. Generally, phishing campaigns are more successful when they use contextually relevant lures during timeframes in which the target population is accustomed to receiving legitimate emails of the same nature.

Just as phishers hope to exploit human complacency during certain time periods, they also try to take advantage of potential victims' anxiety and fears caused by major events. The uncertainty and anxiety surrounding the United Kingdom's referendum vote to leave the European Union ("Brexit") likely contributed to some of the increased phishing activity observed in the middle of the year. Evidence of the impact of Brexit on phishing volume can be clearly seen when looking at phishing attacks targeting British institutions. Over the course of the year, the total volume of attacks against British targets saw a decrease of 23% compared to 2015; however, in May and June, leading up to referendum vote, there was a massive spike in phishing attacks targeting British organizations. This surge in attacks primarily focused on payment service companies and government agencies. The average number of phishing attacks in these two months was more than double the average number of attacks throughout the rest of the year. In July, immediately following the Brexit vote, the number of phishing attacks targeting British entities plummeted.

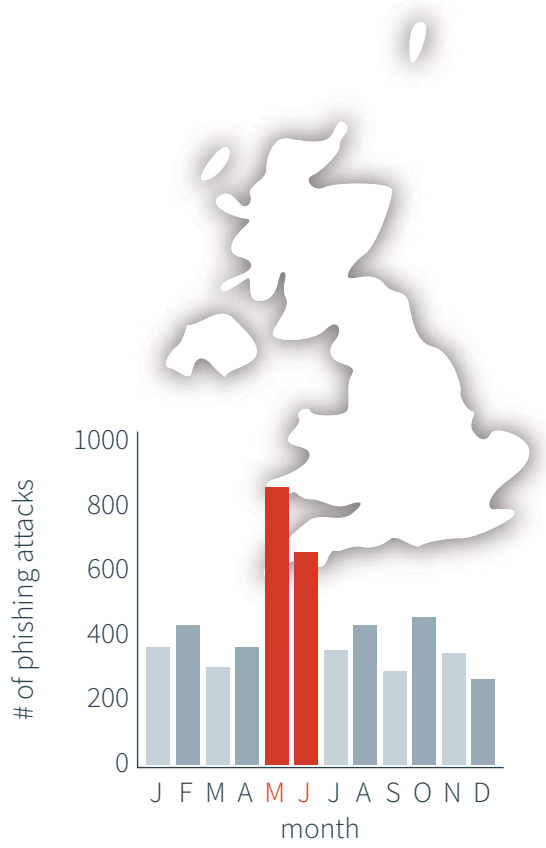
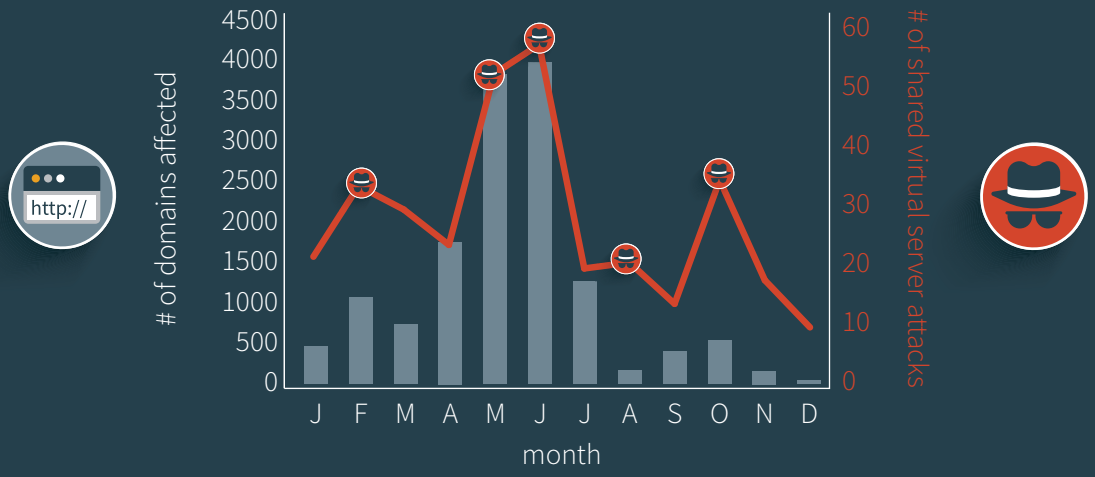


FIGURE 9: Phishing Attacks Targeting British Institutions in 2016

FIGURE 10: Number of Shared Virtual Server Attacks and Number of Domains Affected in 2016



2. Surge in Shared Virtual Server Attacks

Another factor contributing to the mid-year spike in phishing attacks was an unexpected increase in the number of shared virtual server attacks. While this technique is not new, its use has not been widespread in recent years. In 2016, we observed more than 300 incidents involving the compromise of a virtual web server that impacted more than 14,000 domains. This represented 10% of the overall phishing attack volume for the year. A third of these attacks occurred during two months, May and June, which affected nearly 8,000 domains.

While the overall trend in phishing volume deviated from previous years, most industry-specific trends stayed true to their historical norms. E-commerce sites, social networking sites, and SaaS companies saw an increase in phishing activity as the year progressed. Conversely, cloud storage sites, financial institutions, and government services saw a decrease in phishing activity as the year came to a close. These findings support the hypothesis that, although financial institutions and cloud storage sites are the two most commonly targeted industries overall, phishers choose to target other industries at significant times (such as e-commerce sites during the holiday season) to maximize the possibility of success.

WHAT IS A SHARED VIRTUAL SERVER ATTACK?

Instead of compromising a single domain, a shared virtual web server attack is when a phisher breaks into a web server that hosts dozens, or sometimes hundreds, of separate domains. Once the phisher has compromised the web server, he can then create a user directory or utilize an existing user directory on the server to upload their malicious phishing content. Once the content has been uploaded, the phisher can then use automated tools to quickly add the phishing site to every host on the server. This amplifies the attack by creating a large number of pathways to get to the same destination.

FIGURE 10: Industries With Increasing Phishing Volume Throughout Year (2016)

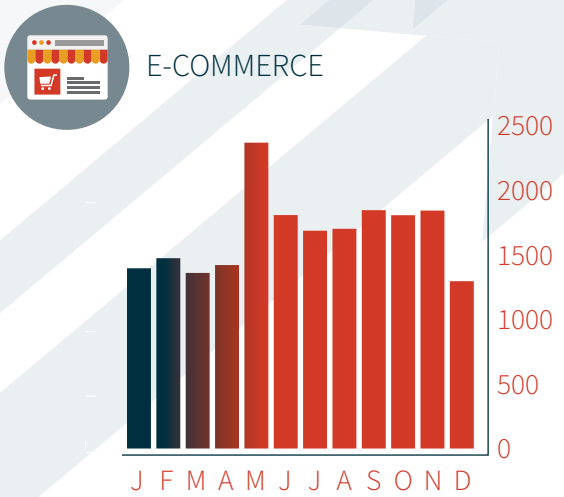


FIGURE 11: Industries With Decreasing Phishing Volume Throughout Year (2016)

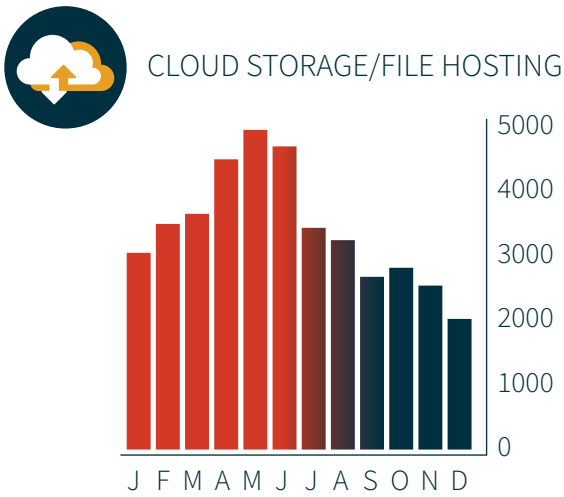
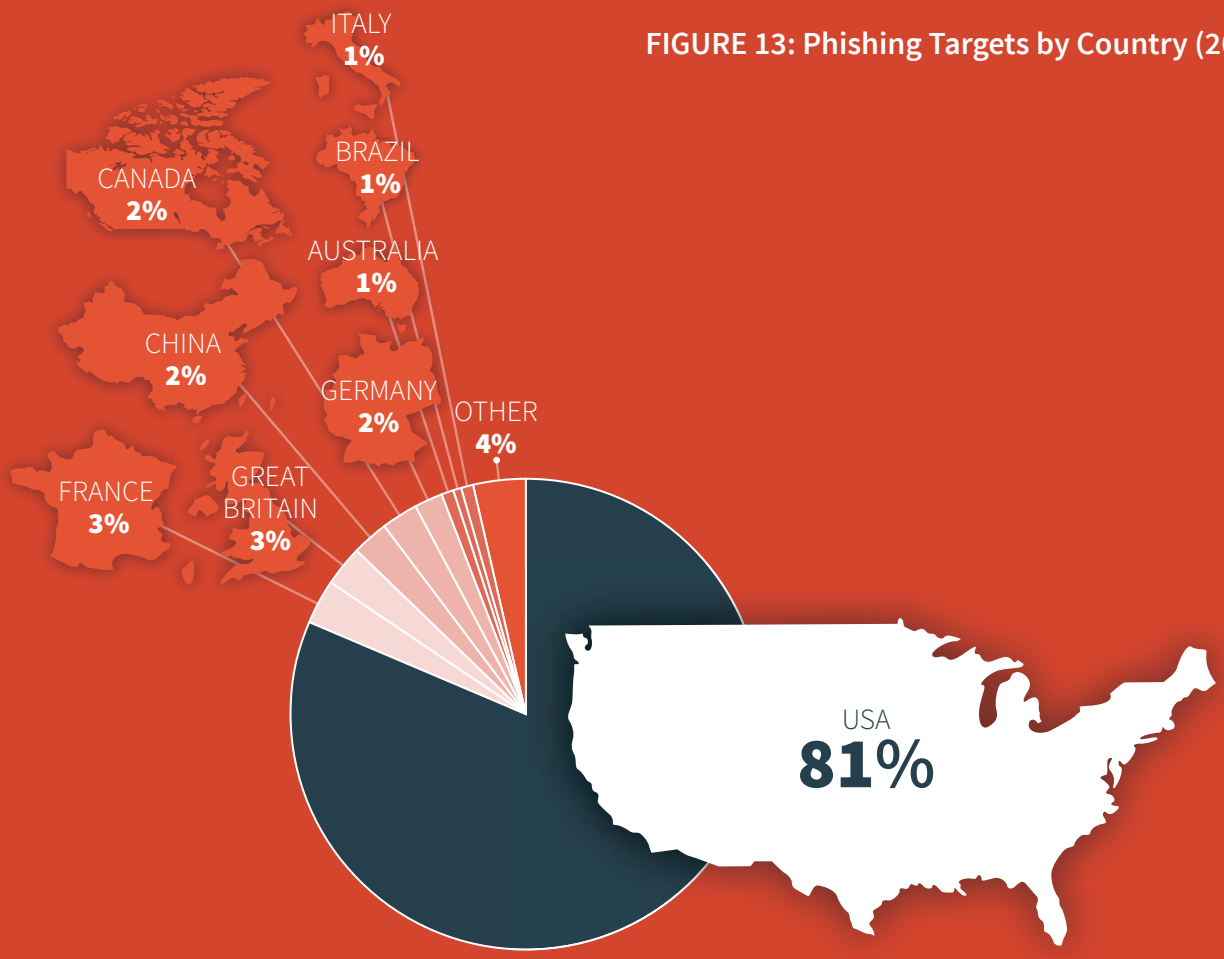


FIGURE 13: Phishing Targets by Country (2016)

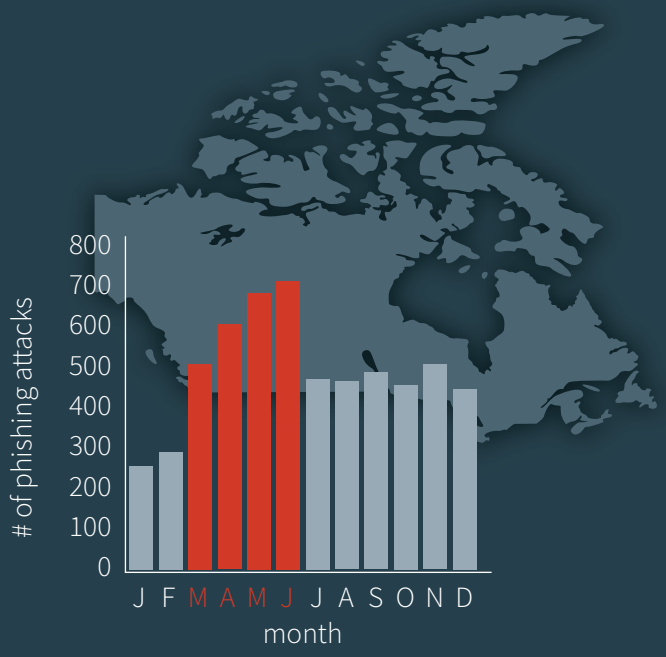


Where are the attacks happening?

[TL;DR — The share of phishing against U.S.-based targets continues to grow and now accounts for 81% of global phishing volume. There was a massive, sustained surge in phishing attacks targeting Canadian companies in 2016, primarily attributed to attacks against financial institutions, indicating Canada may be becoming a preferred target for phishers. Targets in France and Switzerland also saw significant increases in phishing attacks in 2016, while British, Chinese, and South African companies were targeted substantially less.]

Consistent with prior years, institutions in the United States were by far the most popular targets of phishing attacks in 2016. Not only were entities in the United States the top choice for phishers, but compared to other countries, the share of phishing attacks targeting U.S. organizations continued to grow. In 2014, 71% of all phishing attacks targeted institutions in the United States. In 2016, the share of global phishing volume targeting U.S. entities grew to more than 81%. Over this three-year period, the total number of phishing attacks against targets in the United States has doubled.

FIGURE 14: Phishing Attacks Against Canadian Targets in 2016



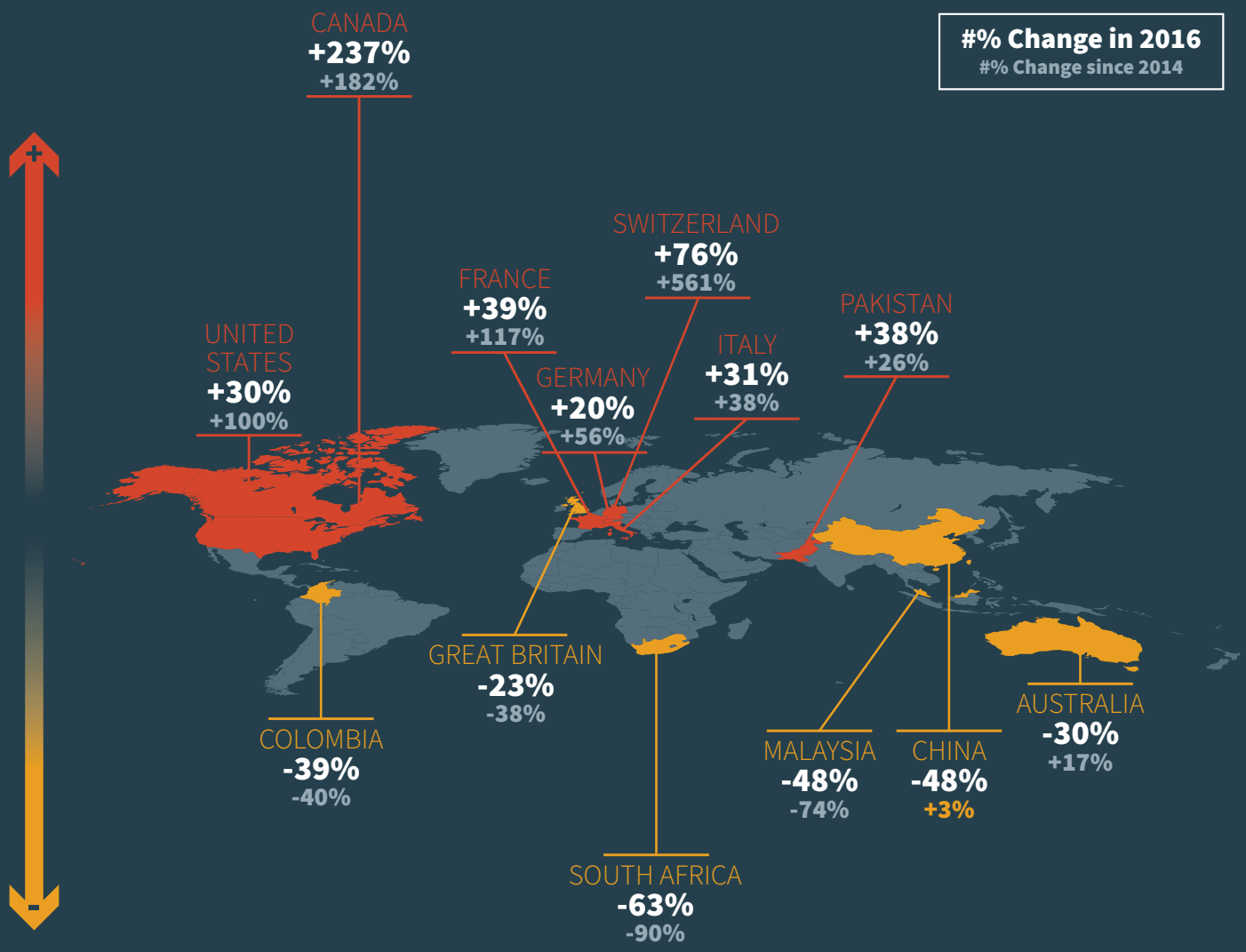
Canadian companies saw the biggest growth in phishing volume in 2016, with a 237% increase from 2015. Interestingly, this increase was not caused by a single, isolated spike in phishing activity at one or two points during the year. Instead, attacks targeting Canadian institutions rose in March 2016 and remained at elevated levels throughout the rest of the year. This increase is primarily attributed to attacks targeting Canadian financial institutions, which grew by 444% in 2016. The sustained nature of this trend through the year suggests that Canadian financial institutions have become more attractive targets to phishers.

Switzerland and France also saw substantial increases in phishing attacks in 2016. Switzerland's phishing volume grew 76% due to a surge in attacks targeting their e-commerce and telecommunications companies. Attacks targeting French institutions rose 39% in 2016, which is attributed to a sharp increase in attacks targeting the country's banks and government services. France's phishing volume has more than doubled since 2014, and it is now the second-most targeted country behind the United States.

A handful of countries saw notable decreases in phishing activity targeting their institutions. After the number of phishing attacks nearly doubled in 2015, attacks against Chinese targets fell 48% in 2016. Phishing attacks targeting British entities have been in steep decline in recent years, falling 23% in 2016, and 38% since 2014.

One of the most interesting changes observed recently is the massive decline in phishing attacks targeting South African companies. In 2014, businesses in South Africa were the sixth-most popular targets of phishing attacks. Over the past two years, though, there has been a 90% reduction in the number of phishing attacks targeting the country's institutions, placing them 22nd in total phishing volume.

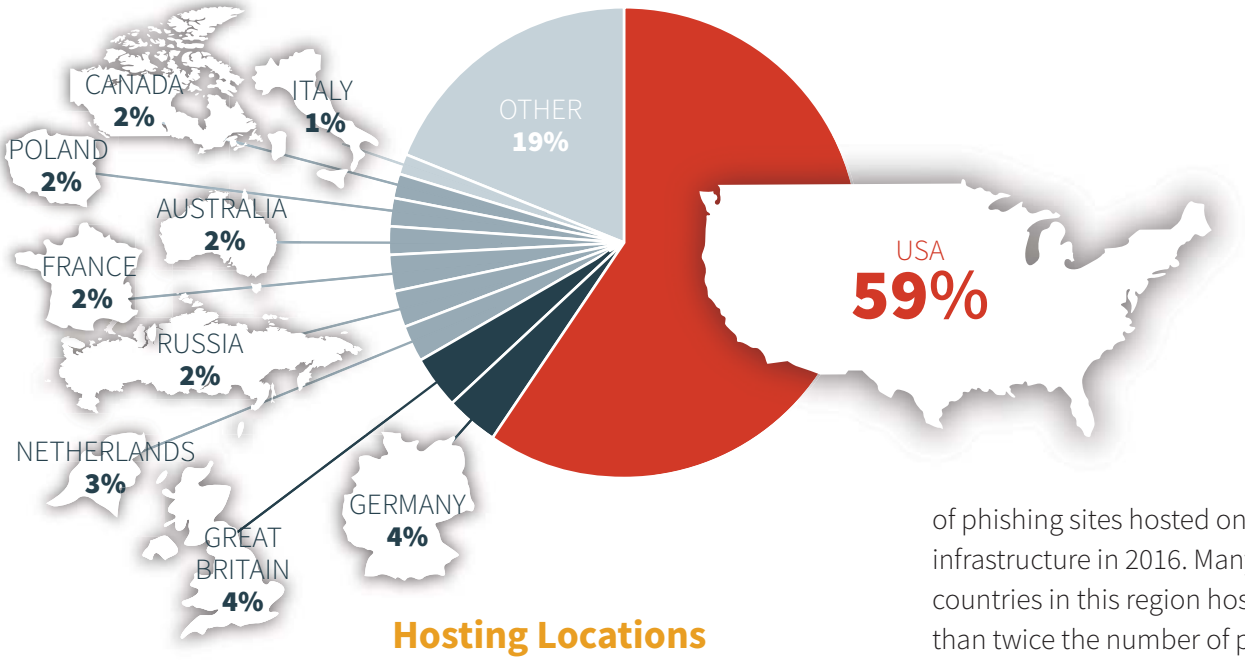
FIGURE 15: Notable Country-Specific Trends in Phishing Volume



How are phishing attacks being carried out?

This section of the report provides analysis and insight into the tactics, techniques, and procedures (TTPs) used to carry out consumer-focused phishing attacks. These underlying components are uncovered through the course of investigating and mitigating phishing attacks. By identifying, analyzing, and shutting down these components we make it more difficult for phishers to stage attacks, collect stolen information, and profit.

FIGURE 16: Phishing Site Hosting Locations (2016)



Hosting Locations

[TL;DR — In 2016, 59% of phishing sites were hosted in the United States. In contrast with 2015, there was a sharp increase in phishing sites hosted in Eastern European countries, and a decline in phishing sites hosted in East Asian countries.]

Most phishing sites are located on compromised web hosting networks, exploited by phishers using a variety of different tools and techniques. In 2016, more than 80% of all phishing sites were hosted in only 10 countries, including 59% that were hosted in the United States, easily making it the most popular choice for phishers. After the United States, the next most common countries hosting phishing infrastructure were Germany (4%), Great Britain (4%), Netherlands (3%), and Russia (3%).

Countries in Eastern Europe saw a tremendous growth in the number of phishing sites hosted on their infrastructure in 2016. Many of the countries in this region hosted more than twice the number of phishing sites than in 2015, including Latvia (+360%), Serbia (+152%), Poland (+123%), Lithuania (+116%), Bulgaria (+112%), Czech Republic (+111%), and Russia (+110%). Other countries that saw a significant uptick in phish hosting included Panama (+657%), Italy (+98%), Netherlands (+88%), Australia (+86%), and Indonesia (83%).

In contrast to the Eastern European increase, many East Asian countries saw a notable decline in the number of phishing sites hosted there. These countries included Taiwan (-43%), Hong Kong (-38%), South Korea (-34%), and Japan (-30%). China, which actually saw a net increase in the number of phishing sites hosting in the country in all of 2016, saw a nearly 50% decrease in the number of phish hosted in the second half of the year when compared to the first six months. Other countries where the volume of hosted phishing sites decreased include Chile (-50%), India (-33%), Turkey (-24%), and South Africa (-23%).

FIGURE 17: Change in the Number of Phishing Sites Hosted (2016)

+657%	PANAMA
+360%	LATVIA
+152%	SERBIA
+123%	POLAND
+116%	LITHUANIA
+112%	BULGARIA
+111%	CZECH REPUBLIC
+110%	RUSSIA
+98%	ITALY
+88%	NETHERLANDS
+86%	AUSTRALIA
+83%	INDONESIA
+47%	GERMANY
+43%	UNITED STATES
+32%	BRAZIL
+31%	GREAT BRITAIN
+27%	CHINA
-23%	SOUTH AFRICA
-24%	TURKEY
-30%	JAPAN
-33%	INDIA
-34%	SOUTH KOREA
-38%	HONG KONG
-43%	TAIWAN
-50%	CHILE

Top-Level Domains (TLDs)

[TL;DR — While newly-available generic top-level domains (gTLDs) were associated with a small percentage of phishing domains (2%) in 2016, the volume of attacks hosted on new gTLDs grew by more than 1000%. This suggests new gTLDs are becoming 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, slightly more than 51% of all phishing sites were hosted on domains registered with the .COM top-level domain (TLD) in 2016, which was the exact same percentage of phish found on .COM domains observed in 2015. After .COM domains, the most common TLDs found in phishing sites were .BR, .NET, .ORG, .RU, .UK, .AU, .INFO, .IN, and .PL. These ten TLDs were associated with more than three-quarters of all phishing sites.

Because a 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 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 that met these criteria in 2016 included .COM, .BR, .CL, .TK, .CF, .ML, and .VE.

FIGURE 18: Top TLDs Hosting Phishing Sites in 2016

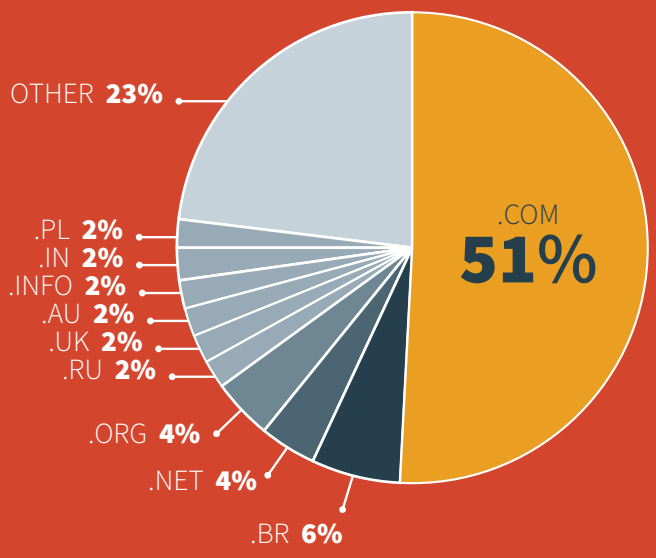
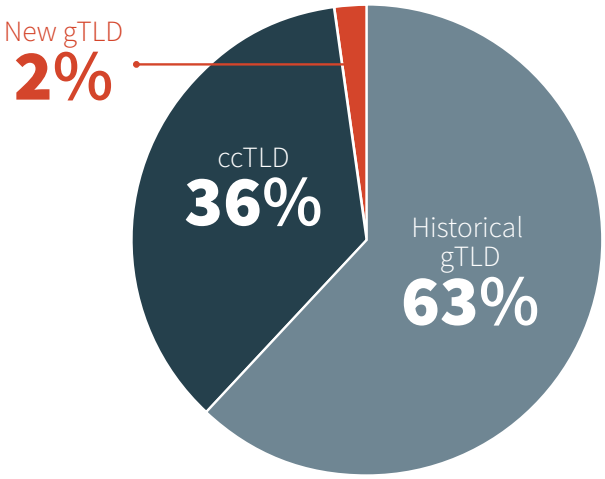


FIGURE 19: TLDs Over-Represented in Phishing Sites

TLD	Phishing Sites	General Population
.COM	51.1%	48.4%
.BR	5.7%	1.8%
.CL	0.8%	0.2%
.TK	0.7%	0.1%
.CF	0.4%	<0.1%
.ML	0.4%	<0.1%

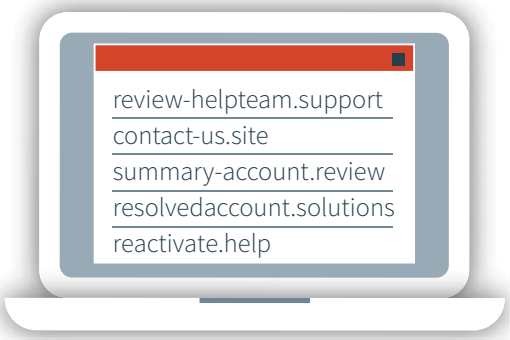
FIGURE 20: Type of TLD Associated With Phishing Sites (2016)



In 2016, we identified phishing sites hosted on 432 different TLDs, a significant increase from the 280 TLDs we observed in 2015. A primary reason for this increase seems to be that phishers are starting to host more phishing sites on recently created generic TLDs (gTLDs). These new gTLDs are ones that have been approved since ICANN launched its most recent gTLD expansion program in 2011. Last year, 220 new gTLDs were found hosting phishing content, more than three times the amount that were associated with phishing sites in 2015 (66). The most common new gTLDs used to host phishing content last year were .TOP, .XYZ, .ONLINE, .CLUB, .WEBSITE, .LINK, .SPACE, .SITE, .WIN, and .SUPPORT.

Although new gTLDs were used in only 2% of phishing domains, the overall number of phishing sites hosted on new gTLD domains grew by more than 1,000% in 2016, evidence that they are beginning to evolve as a more popular option for phishers when constructing their phishing schemes.

There are a few reasons new gTLDs are gaining traction in the phishing ecosystem. For one, some new gTLDs are incredibly cheap to register and may be an inexpensive option for phishers who want to have more control over their infrastructure than they would with a compromised website. Secondly, phishers can use some of the newly developed gTLDs to create websites that appear to be more legitimate to potential victims. For example, the following domains were found to have hosted a variety of phishing content in 2016:



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

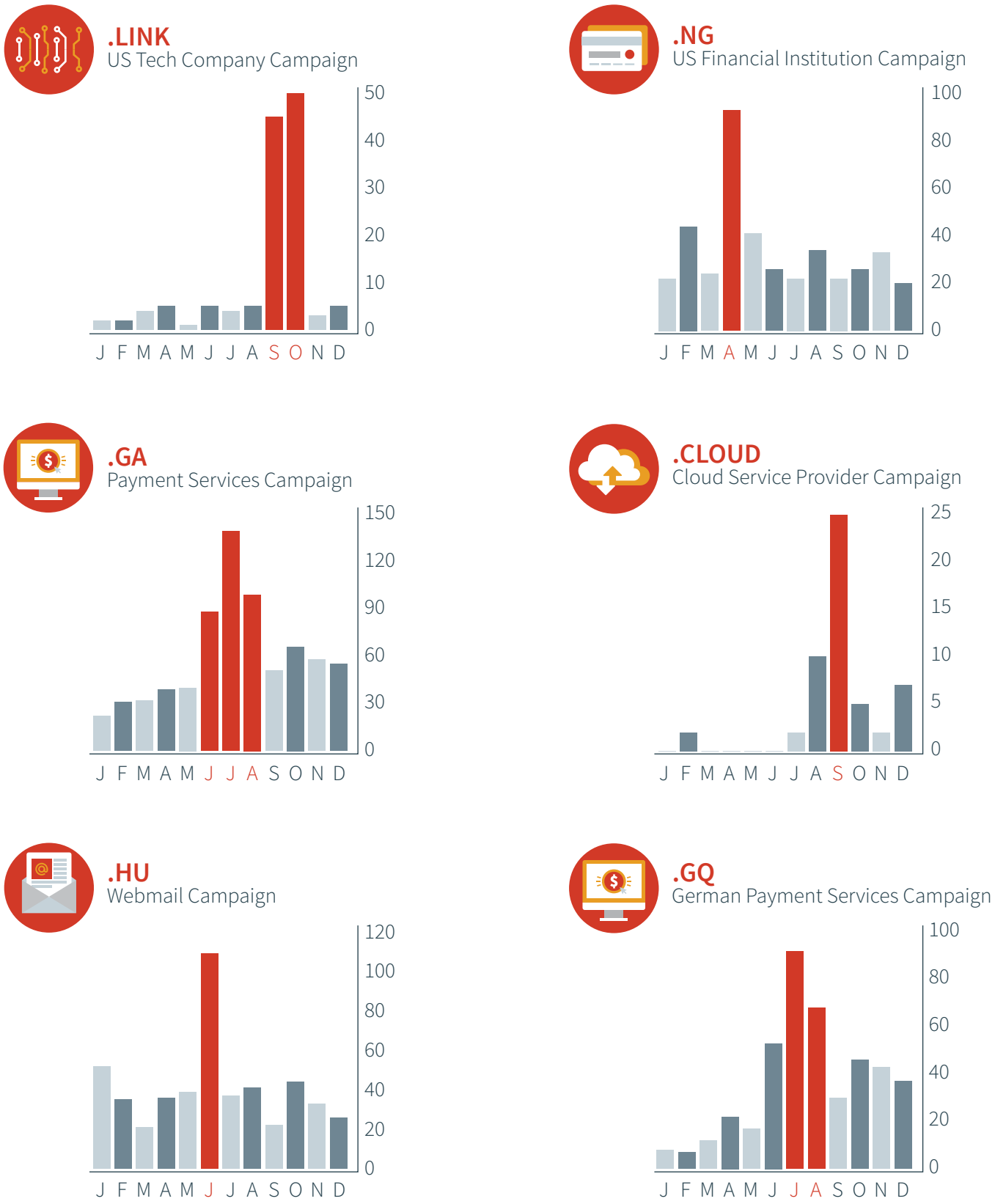
Analyzing TLDs can also be a useful tool in identifying possible phishing campaigns targeting a company or industry, particularly when a spike is observed in phishing sites using a TLD that is rarely associated with phishing sites. From an analytical perspective, it is important to note that all of the domains identified in campaigns using this technique were maliciously registered rather than compromised by a phishing actor, so when one of these spikes is identified, valuable intelligence can generally be collected on the domain's registrant.

Examples of these TLD spikes include:

- A spike in .LINK phishing sites in the Fall of 2016 was directly attributed to a phishing campaign targeting a U.S.-based technology company.
- A sharp rise in the use of .GA phishing sites in the summer of 2016 identified a campaign targeting a major payment service company.
- A campaign targeting multiple webmail providers was identified as a result of a spike in phishing sites using the .HU TLD in June 2016.
- In April 2016, a spike in the number of phishing sites hosted on .NG TLDs was associated with a campaign targeting a large U.S.-based financial institution.
- A spike in the use of .CLOUD domains to host phishing content, which was rarely observed throughout the rest of the year, identified a phishing campaign against a U.S.-based cloud services provider in August/September 2016.
- A significant increase in the number of .GQ phishing sites in July/August 2016 was correlated with a campaign focused on a German payment services target.

...when one of these spikes is identified, valuable intelligence can generally be collected on the domain's registrant.

FIGURE 21: Examples of TLD Spikes Used to Identify Phishing Campaigns



29,000 PHISH KITS

Phish Kits

[TL;DR — We collected more than 29,000 phish kits targeting more than 300 different organizations in 2016. More than a third of these kits used anti-detection techniques, including 22% that utilized mechanisms to restrict access and 29% that used techniques to evade browser-based blocking. Instead of selling kits in underground markets for a direct profit, phish kit authors are more commonly distributing their kits for free on social media and file sharing sites.]

Phish kits are collections of files, usually contained in an archive file, such as a ZIP file, that include all the components necessary (HTML/PHP page templates, scripts, images, etc.) to create a working phishing site. In 2016, we collected more than 29,000 unique phish kits containing the components to create phishing sites targeting more than 300 different companies.

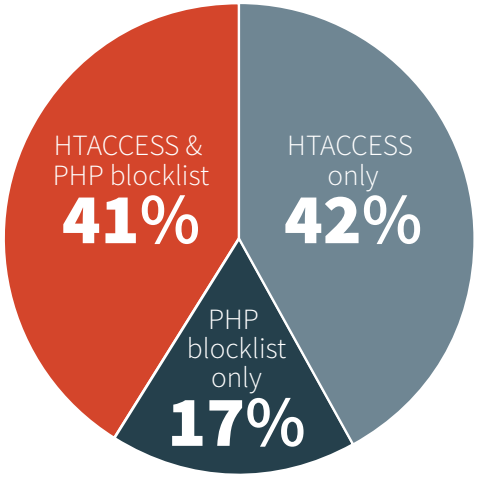
Because kits are essentially the "recipe" used by most scammers to create phishing sites, by collecting and analyzing phish kits found in the wild, we are able to get a more in-depth understanding of the techniques phishers use to carry out their scams. By analyzing these kits, we can identify any anti-detection mechanisms that may be deployed, so we can better enact countermeasures to prevent these strategies from being successful. Using a combination of artifact analysis and behavioral analysis, we can link kits to the individual phishing sites that they create and get a better sense of what kits are primarily being used by phishers. We can then identify the distribution mechanisms of these kits (social media, file hosting sites, underground forums, vendor websites, etc.) and attempt to disrupt the kit supply chain by taking down the distribution points.

To prevent their phishing sites from being detected and taken down, phishers sometimes try to restrict access to their sites using different techniques. One of the ways phishers attempt to prevent unwanted visitors to their phishing sites is to employ some type of access control, which blocks access to the site based on certain characteristics, such as IP address, user agent string, hostname, or HTTP referrer. Generally, these access controls are found in the form of HTACCESS files or blocklists in PHP scripts. Although rare, we have also observed phish kits that contain access whitelists, which, instead of blocking visitors based on certain characteristics, only allow visitors to the site that meet specific criteria. These whitelists are usually used in phishing campaigns targeting a specific region or country where visitors can be filtered out based on geo-locating their IP address.

Of kits analyzed in 2016, 22% used some sort of access control mechanism. Of these, 42% blocked visitors using HTACCESS files and 17% controlled restricted access by using PHP blocklists. For more comprehensive control over a phishing site's visitors, 41% of these kits used combination of both HTACCESS files and PHP blocklists.

We collected more than 29,000 phish kits targeting more than 300 different organizations in 2016...by collecting and analyzing phish kits found in the wild, we are able to get a more in-depth understanding of the techniques phishers use to carry out their scams.

FIGURE 22: Access Controls Used by Phish Kits (n = 6511)



Another technique used by phishers to attempt to evade detection is by dynamically altering the phishing site's URL for each visitor, making browser-based blocking (presumably) less effective. There are two primary techniques phish kit authors use in their attempts to evade browser-based detection: directory generation and randomized URL parameters.

A directory generating phish generates a new directory on the server with a randomized name for each potential victim that visits the initial phishing page. All of the original components that make up the phishing site are then copied into this directory. Thus, the initial URL for each person who visits the page will be different (the root path where the phish kit is located, though, will remain the same). Of the phish kits we collected in 2016, 15% of them used directory generation techniques.

Of the phish kits analyzed in 2016, 14% contained scripts that were used to generate random parameters that were appended to the end of a phishing page's URL. Like directory generating phish, the resulting URL is unique each time the phishing page is loaded. Although URL parameters have legitimate uses, their purpose when used in phishing sites is usually benign (although some sophisticated kits have been found that require specific parameters for a phishing site to load). The purpose of this technique is the same as directory generators; however, the main difference is that this method does not create or copy new files on the server.

FIGURE 23: Example of PHP Script Used to Dynamically Generate a New Directory for Each Visitor

```
<?
$random=rand(0,100000000000);
$md5=md5("$random");
$base=base64_encode($md5);
$dst=md5("$base");
function recurse_copy($src,$dst) {
$dir = opendir($src);
@mkdir($dst);
while(false !== ( $file = readdir($dir)) ) {
if (( $file != '.' ) && ( $file != '..' )) {
if ( is_dir($src . '/' . $file) ) {
recurse_copy($src . '/' . $file,$dst . '/' . $file);
}
else {
copy($src . '/' . $file,$dst . '/' . $file);
}
}
}
closedir($dir);
}
$src="signin";
recurse_copy( $src, $dst );
header("location:$dst");
?>
```

```
<?php

header("location:
log.php?cmd=_account-details&session=".md5(microtime())."&dispatch=".sha1(microtime()));
exit;

?>
```

FIGURE 24: Example of PHP Script Used to Generate Random URL Parameters

One of the interesting facets of the phishing ecosystem is that there is a large number of actors committing attacks, but only a small number of phishers that are sophisticated enough to write a phish kit from scratch. Because of this, kit authors seek to profit from their creations by distributing their kits to less sophisticated users. There are two ways kit authors make money in the phishing economy: selling kits for profit or freely distributing kits containing backdoors.

Phish kits used to be most commonly sold on underground forums, vendor websites, or Dark Web marketplaces. Most kits are sold for between $1 USD and $50 USD, depending on the target and sophistication of the kit. Some kits, however, are bundled with other features, such as campaign tracking control panels, and are sold for hundreds of dollars. This is the easiest and most direct way for a phishing kit author to make money; however, because there is a cost associated with the kit, it may limit the number of phishers who want to spend money to use their kit.

This is why a growing number of phish kit authors are choosing to freely distribute their kits to potential users. These kits are sometimes circulated in underground hacking forums, but many of them are openly distributed via social media and free file hosting sites.

Using this business model, kit authors insert "backdoors" in their kits that, in addition to forwarding phished information to the kit's user, send all compromised data to a facility controlled by the kit's creator. These backdoors are generally obfuscated within the kit and usually go undetected by the kit's unsophisticated users. So instead of directly profiting from the sale of a kit, by freely distributing kits, a phish kit author makes money by selling the extensive amount of personal and financial information they secretly collect from all the kit's users as a result of these backdoors.

...a growing number of phish kit authors are choosing to freely distribute their kits to potential users... many of them are openly distributed via social media and free file hosting sites.

SECRET BACKDOORS

EPIDEMIC
YEAR OF RANSOMWARE

THE RANSOMWARE EXPLOSION

[TL;DR — Phishing is, by far, the most prevalent delivery mechanism of ransomware. Overall, ransomware attacks have had a high infection rate, but a low rate of success with only a small fraction of victims paying ransoms. In 2016, threat actors evolved their tactics from targeting individual victims to companies that were more likely to view paying a ransom as their best option. This includes small businesses, schools, government agencies, critical infrastructure facilities, and medical facilities.]

Malware trends in late-2015 and early-2016 hinted that a ransomware epidemic was just around the corner. Before the first quarter of 2016 was over, analysts and industry insiders branded it the "Year of Ransomware." Fast forward a year and the term has become cliché, but no less true. Undoubtedly, 2016 will be remembered as the year ransomware became the most pervasive and profitable threat in the malware landscape.

Although ransomware has been a threat in the cyber landscape for decades, the sinister nature of this year's ransomware wave captured the attention of those outside of the IT Security industry. Popular media reported daily about businesses that had fallen prey and detailed the costs and consequences of such infections. Consumers were not spared, either. The net effect is that a vast number of users throughout the world have come to understand that the term "ransomware" refers to software that restricts access to a computer and requests a ransom from the victim in exchange for restored access. This simple awareness has not yet equated to an ability to prevent infection and ransomware has continued to grow in popularity with malware authors and malicious actors.

All your important files are encrypted.

FIGURE 25: Images Like This Became all too Common for Computer Users in 2016

Why is ransomware so popular?

The popularity of ransomware among attackers is the result of many factors, including profitability, simplicity, and viability. The most important factor for any financially-incentivized criminal activity is profitability. The success of ransomware campaigns at the beginning of 2016, magnified by constant media coverage about these successes, drew other cybercriminals away from their various ventures to try their hand at ransomware. The simplicity of ransomware made this transition easy.

Ransomware allows attackers to effectively utilize one configuration for all targeted users. It also allows for instant monetization — there are no credentials to sell, no fraudulent transactions to initiate, and no further social engineering is required. Monetization by anonymous attackers is made viable by the injection of cryptocurrency into the mainstream economy. Ransomware attackers, who formerly risked being exposed by relying upon credit cards or pre-paid money cards, now had a reliable way to collect large ransoms anonymously. These factors combined to make ransomware an increasingly attractive venture.

FIGURE 26: Ransomware Actors Utilize Bitcoin for Anonymous Transactions

Who are the actors?

The number of actors involved in the creating and distribution of ransomware has expanded significantly over the past year. Established ransomware families like Cryptolocker and Cryptowall continued to evolve by releasing stronger, more refined versions. The effectiveness of these well-known families spawned new variants, imitators, and look-alikes hoping to capitalize on the success of their predecessors. Perhaps the best example of this is Locky, one of the most successful families of ransomware in 2016, which has been linked to the same actors responsible for the Dridex banking Trojan.

CRYPTOLOCKER
CRYPTOWALL

SMALL BUSINESSES SCHOOLS MEDICAL

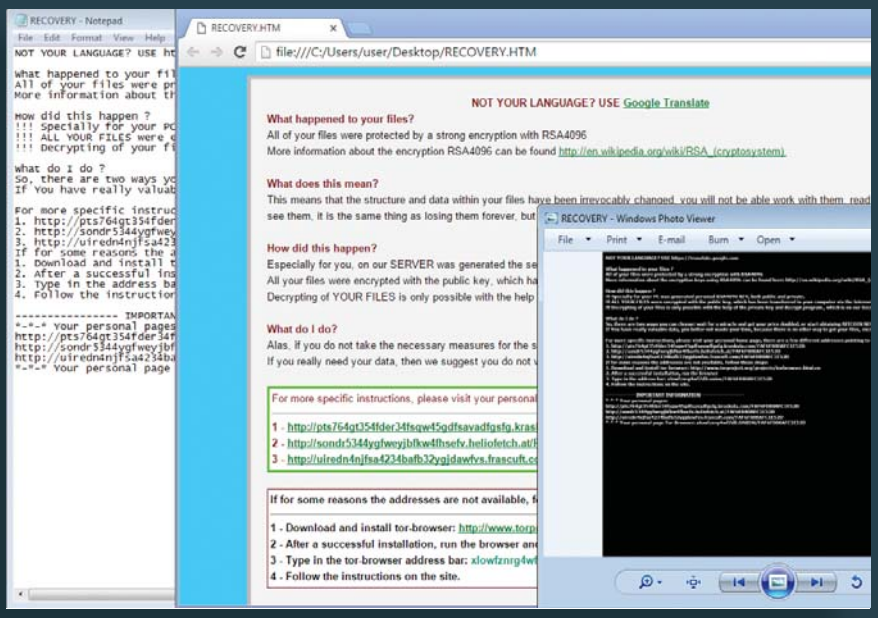
This year also saw the expansion of the ransomware-as-a-service model. Families like Cerber and Petya/Mischa allow technically unsophisticated actors to get involved in the ransomware trend by authoring malware, providing it for distribution, and splitting the profits with affiliates. In some cases, these less technical actors are also attempting to write their own malicious software, leading to a scourge of low-quality ransomware that is often more destructive than intended. The overall success of ransomware in the past year has emboldened and energized actors targeting a wide range of consumer and commercial targets.

Who is being targeted?

One of the most interesting trends in ransomware over the past year is the maturation of its targeting scheme, particularly by the more successful families. Historically, ransomware has been distributed in broadcast attacks, where attackers were attempting to net the largest number of victims possible. This was the same strategy used by many ransomware families at the beginning of 2016. As the year went on, however, there was a notable shift away from the targeting of individual consumers, who began paying ransom to regain access to their files less frequently.

Instead, ransomware campaigns evolved into targeted spear phishing campaigns, focused on small businesses, schools, government agencies, critical infrastructure facilities, and medical facilities. Several factors make these organizations prime targets. First, they have valuable data. Data availability is paramount to the day-to-day operations of these organizations and in many cases, they are willing to pay a ransom to restore access quickly. Second, they often have small budgets for IT staffing and may not be adequately prepared to protect their IT assets or respond to an incident. Finally, these organization are often subject to regulations that can complicate their ability to create and store backups. In such cases, paying a ransom may be the only means to recover the encrypted data.

FIGURE 27: Established Malware Authors Launched Successful Ransomware Campaigns in 2016



Why is ransomware successful?

Modern ransomware is successful in infecting their targets for a variety of reasons. Perhaps foremost is the fact that the delivery methods utilized exploit the weakest link — humans. By far, the most prevalent delivery method for ransomware is phishing emails. Unwary users fall prey to social engineering tactics, navigate to malicious URLs, download malicious files, and execute malicious programs.

Other infection vectors include exploit kits, malicious advertisements, drive-by downloads, and scanning networks for vulnerable software. These methods still rely on the humans, though, to fail to keep software up-to-date or to utilize unknown/untrusted software.

Beyond the delivery methods, the success of ransomware lies in the use of strong encryption methods and sound key management. High-quality modern ransomware samples utilize well-established cryptographic algorithms and store decryption keys securely in a location accessible only to the attacker, thereby decreasing the chances that a security researcher can reverse-engineer the sample or that a victim can decrypt files without payment.

FIGURE 28: Phishing Emails Remain the Top Attack Vector for the Distribution of Ransomware

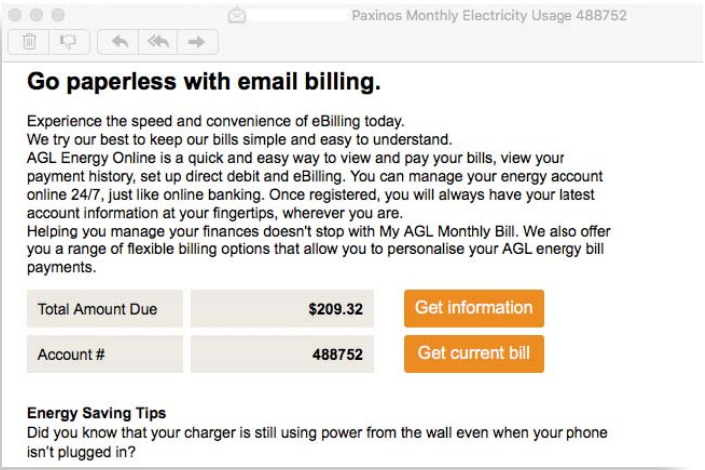


FIGURE 29: Successful Campaigns Often Include Convincing Social Engineering Elements

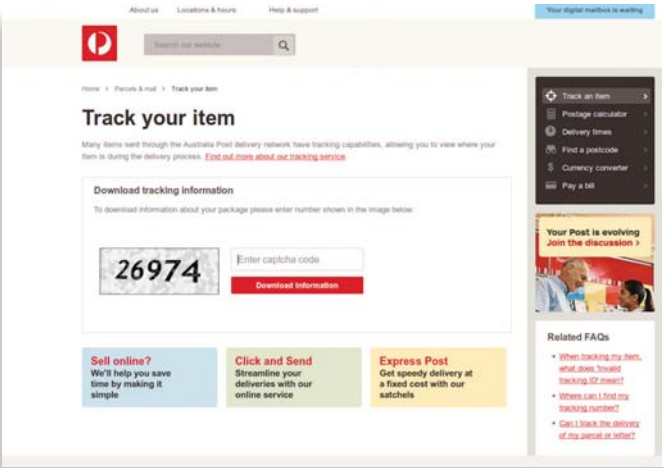
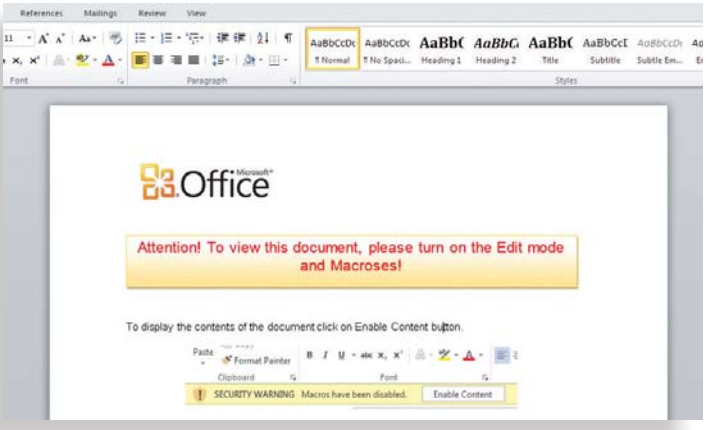


FIGURE 30: Malicious Office Documents Were a Popular Delivery Method for a Variety of Malware Types in 2016



NATION-STATE USE OF SPEAR PHISHING

Historically, the use of spear phishing by nation-states has mostly been hidden from public view. In 2016, however, spear phishing campaigns orchestrated by foreign governments to infiltrate high-level targets and exfiltrate data for non-monetary gain made headlines. The continuing revelations and controversy surrounding Russian intelligence infiltration of the Democratic National Committee through spear phishing shows the method's potency and effectiveness in both gaining access and obscuring attribution.

Spear phishing, most often associated with threat actors seeking quick financial gain, is commonly leveraged by intelligence agencies seeking access to the networks of their adversaries. These groups use spear phishing to deliver a range of malware that allows for remote code execution and file transmission.

Like spear phishing scams targeting businesses, lures are crafted and targets selected specifically to ensure a high rate of compromise. An advanced persistent threat (APT) will spoof the sender's email address to make the message appear to be from a legitimate and high priority sender, include a subject to draw the victim's attention, and contain a body that reinforces the legitimacy of the email and gets the user to open an attachment that will deliver a malicious payload needed to accomplish the objective.

Finally, successful ransomware is functionally sound and delivers on its promise to decrypt files upon payment. Malicious actors know they will be unable to monetize infections if word spreads that payment does not result in decryption.

While modern ransomware is very effective in terms of infection volume, it is not as effective in terms of conversion rate. Only a small percentage of infected users pay the ransom requested of them. For many, data loss has become a fact of life. Having experienced data loss previously, they take a ransomware infection in stride and start over again. Others are too unfamiliar or uncomfortable with cryptocurrency to make a purchase and follow through with payment. Still others feel a civic duty to avoid funding a criminal enterprise. Despite the low conversion rate, the number of infected users who do pay is more than enough to make ransomware a perpetually attractive attack vector in the coming years.

FIGURE 30: Well-Written Ransomware Utilizes Strong Cryptographic Algorithms

The future of ransomware

After a banner year for ransomware, what is next? Some trends have already begun to develop that help to answer this question. While a large percentage of ransomware targets Windows users, some malware authors have begun to create samples targeting other platforms. This trend is likely to continue with more sophisticated malware targeting OS X, Linux, server operating systems, and mobile platforms.

Additionally, ransomware actors are likely to attack Internet of Thing (IoT) devices, as recent non-ransomware attacks have demonstrated a significant level of vulnerability in this area. In addition to expanding targeted platforms, attackers are likely to seek expanded functionality. Ransom messages have long included threats of public disclosure, but only recently have ransomware samples included exfiltration functionality to allow such threats to be acted upon. Samples from the past year have also been observed enrolling computers in botnets, stealing bitcoin wallets, purposefully destroying data, and harvesting email addresses and login credentials. Authors will continue to expand functionality as ransomware targeting evolves.

As noted earlier, attackers have honed in on certain businesses and industries as prime ransomware targets. Over time, the organizations that are currently being targeted will harden their defenses. However, this won't be the end for ransomware. Rather, attackers will continue their successful strategy of seeking out organizations and industries which have a combination of high-value data and a weak information security posture. This tried and true formula will ensure that targeted ransomware attacks will continue to proliferate.

FIGURE 32: Windows Is not the Only Platform Being Targeted by Ransomware Authors

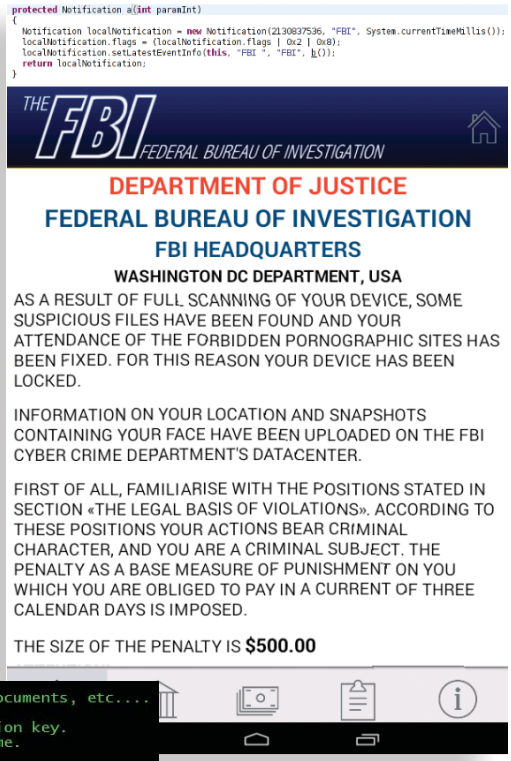


FIGURE 33: Destructive Ransomware Families Raise the Stakes by Purposefully Destroying Data Until the Ransom Is Paid

CONCLUSION

Phishing is the primary method of attack, whether the objective is to steal credentials or to deliver ransomware. To survive in today's threat landscape, organizations must make defending against phishing attacks a top priority.

The phishing threat landscape changed course in profound ways in 2016, breaking from historical trends and painting a future path that is substantially different than what was expected years prior. The year is even more compelling when considering the two transformative events that shaped it are essentially unintended consequences of changes that cybercriminals have heavily exploited.

Cloud storage, SaaS, and other online service providers have broadly adopted the user-friendly practice of substituting email addresses for unique usernames. This practice makes it far easier to collect username/password credential pairs via phishing attacks. Threat actors have seized this opportunity and credential pairs are being mass harvested at unprecedented scale. There were nearly as many phishing attacks targeting cloud storage providers in 2016 as there were targeting financial Institutions, even as attacks against financial Institutions grew. The widespread adoption of this authentication practice has triggered a ripple effect that is driving waves of change throughout the cybercrime ecosystem that will be felt for years to come.

While ransomware existed for decades, the advent of cryptocurrency was the spark that took it from a novelty to Public Enemy #1. Of course, it was a reasonable expectation that cryptocurrency would provide opportunities for cybercriminals by offering a global online currency with true anonymity and legitimate monetary value. What was not expected, however, was that it would lead to a new, more streamlined cybercrime business model focused on collecting cryptocurrency ransoms from victims instead of (or in addition to) stealing valuable data. This business model fueled ransomware's rapid ascension to the top of the malware landscape, where it will continue to shape the cybercrime world for years to come.

The trends and information presented in this report help to show security leaders, practitioners, and others in the community the impact of these two events as well as the many other changes that were observed in 2016. And while these trends were and continue to be truly transformative, it is critical to understand that the prevalence and effectiveness of phishing remains constant. Phishing is the primary method of attack, whether the objective is to steal credentials or to deliver ransomware. To survive in today's threat landscape, organizations must make defending against phishing attacks a top priority.

PHISHLABS

Thank you for reading the 2017 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/