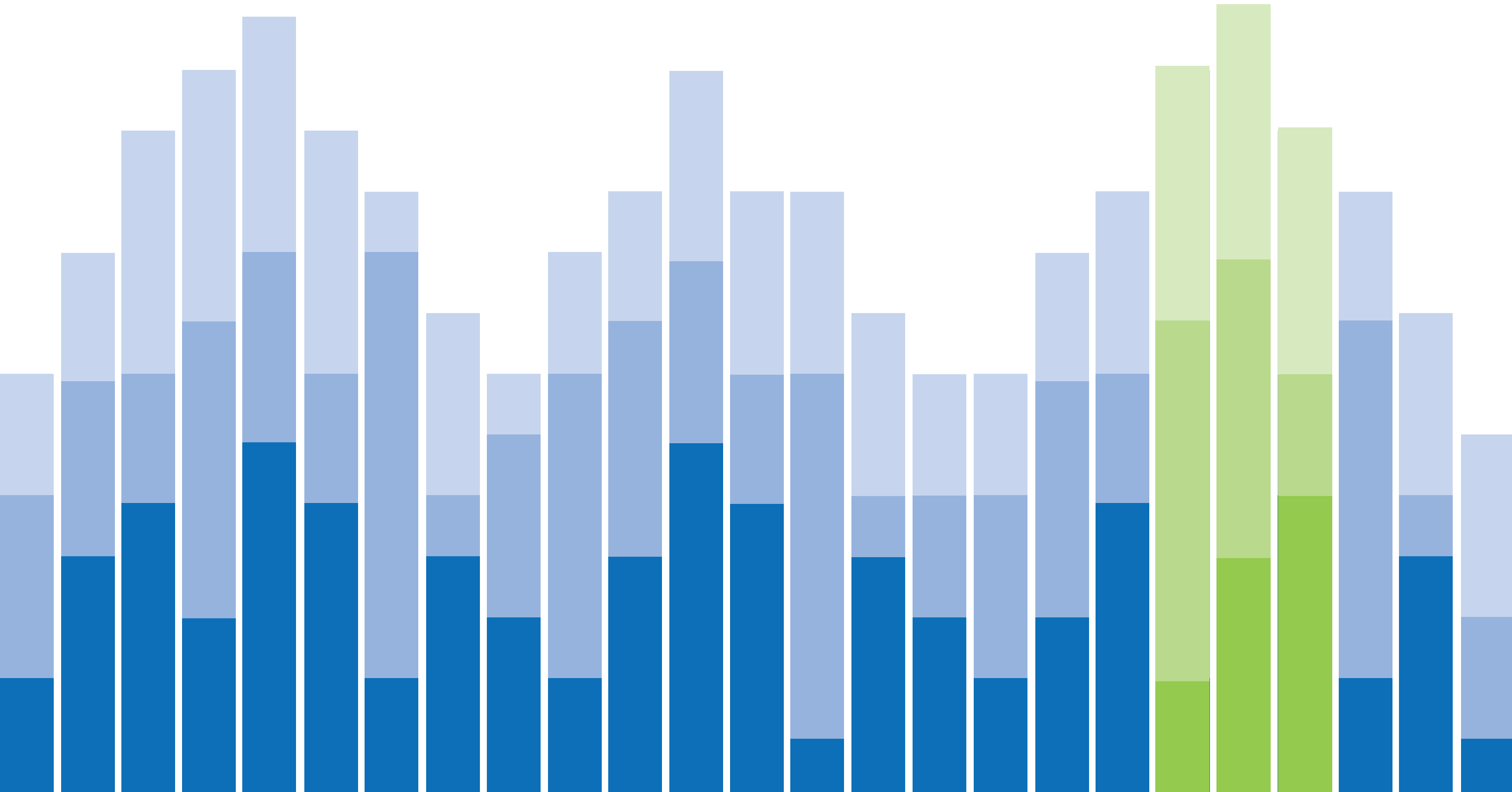
WEBROOT®
Smarter Cybersecurity™

SEPTEMBER 2017

QUARTERLY THREAT TRENDS

Phishing Attacks Growing in Scale and Sophistication



Introduction

The last several years have seen a dramatic evolution in the sophistication of phishing attacks. While antiquated phishing tactics consisted of crudely constructed mass emails trying to snare as many victims as possible, today's attacks are highly targeted, difficult to detect, and just as difficult to evade. Even more important, they're pervasive.

According to the latest Webroot data, an average of 1.385 million unique phishing sites are created each month, with an astonishing high of 2.3 million in May of 2017. The vast majority of phishing sites use domains associated with benign activity, tricking users into thinking they are clicking through to legitimate sites and increasing the likelihood that the attacker will succeed.

Phishing attacks are the number one cause of breaches, and are a growing threat to organizations around the world. According to an FBI Public Service Announcement[i] from May 4, 2017, phishing scams have cost American business nearly $500 million a year over a three year period between October 2013 and December 2016.

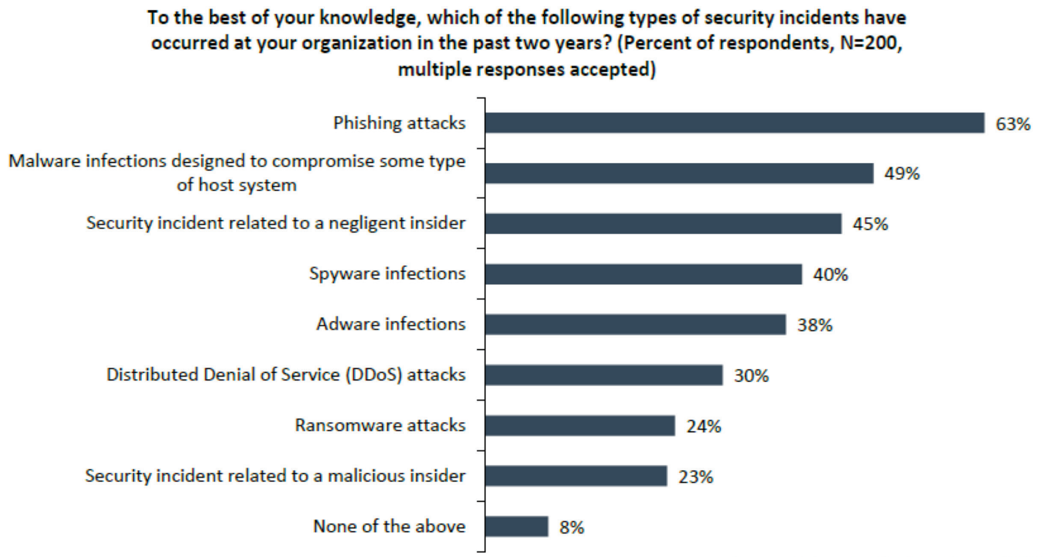
Phishing emails see increased impact by using social media to tailor their attacks to the individual target—sometimes even senior executives—with messages that are likely to resonate with the individual. They employ remarkably realistic web pages that are difficult, if not impossible, to find using web crawlers. They trick victims into providing credentials that can compromise their accounts, then access other accounts where credentials have been re-used.

This report provides details on recent and recurring trends to help you provide accurate detection and prevention of phishing attacks, and gain deeper insight into the characteristics of attacks to prevent future harm. Analysis of data collected and tracked by the Webroot Threat Intelligence Platform and BrightCloud® Real-Time Anti-Phishing Service form the basis for the data presented in this report.

[i] FBI Warns of Dramatic Increase in Business E-Mail Scams. FBI Phoenix, April 2016.

Continued Upsurge in Phishing Attacks

Phishing is one of the most widespread threats facing both businesses and end-users today. A recent report by ESG[ii] showed that 63% of surveyed security and network influencers and decision makers say they've suffered from phishing attacks in the past two years. In the same report, 35% of respondents predict that they will suffer phishing attacks in the next two years, and 29% predict ransomware attacks.



Source: Enterprise Strategy Group, 2017

Figure 1: Types of Security Incidents in the Past Two Years

[ii] 2017 Business Cybersecurity Trends, ESG Research Insights Report, 2017, commissioned by Webroot.

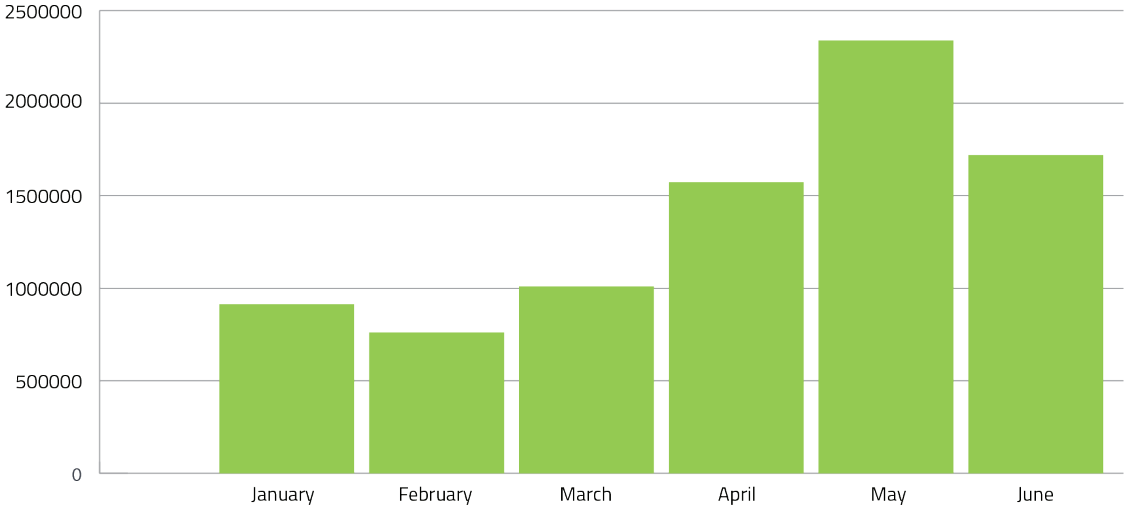


Figure 2: Unique Zero-Day Phishing URLs per Month

Phishing is the number one cause of cybersecurity breaches. According to Verizon[iii], phishing was found in 90% of security breaches and incidents. The magnitude of the problem is demonstrated by the number of unique (zero-day) phishing sites discovered by Webroot businesses and home users during the first six months of 2017, as shown in Figure 2.

Phishing sites amount to an astounding average of 1.385 million sites per month, ranging from a low of just over 761,000 in February to 2.3 million in May. In the past, hackers typically created one new site to use for an entire campaign. This made it feasible to effectively block that domain by entering its name onto a block list. Today, it's clear that putting together a list of bad URLs and blocking them will no longer work. No list, even if updated hourly, can hope to keep up with this volume of new sites.

[iii] Verizon 2017 Data Breach Investigations Report. Verizon, 2017.

Trends in Phishing Attack Sophistication

In the past, phishing attacks targeted as many people as possible—often in the thousands or millions with a single campaign. The hope was that a sufficient number of people would open an infected attachment or click on a link to a malicious web page, allowing the thief to install malware, harvest user credentials, and/or exfiltrate sensitive information.

Today's phishing has become much more sophisticated. Webroot data for the first six months of 2017 indicates three important trends: attacks are highly targeted, they carry advanced payloads, and they use a sense of urgency to impel reckless response.

Highly Targeted Emails

As opposed to outdated phishing campaigns which cast a wide net to catch many victims at once, today's attacks employ spear phishing to target an individual or a small group of carefully selected people. Utilizing social media profiles such as LinkedIn, Facebook, and Twitter, attackers can learn about likes, dislikes, interests, and concerns, then craft emails that appeal very specifically to the individual. Because the message is targeted, and the recipient believes that it comes from a trusted sender, the target is much more likely to open the email and click on a link or attachment.

A variant of this is "whaling", or business email compromise, which targets top-level executives such as CEOs, CFOs, and other decision-makers. The FBI says that more than 22,000 people have reported whaling phishing incidents (Business e-mail compromise or BEC) worldwide.

The 2017 Business Cybersecurity Trends report by ESG, released in August 2017, confirms these findings. In this survey of perimeter security and network influencers and decision-makers, 46% of respondents said malware attacks have become more targeted over the past two years, and 45% said that there is a greater volume of malware than in the past two years.

Advanced Payloads

Phishing has expanded its goal beyond stealing credentials and personal information. Today's attacks are intended to implant malware and set up command-and-control communication with servers to send malicious commands to compromised devices, or to exfiltrate data. These extended capabilities have increasingly made phishing a vector for advanced threats.

Recent examples illustrate the scope of the problem. Locky ransomware infected more than 400,000 victims in 2016, and the WanaCrypt0r attack used a combination of phishing, ransomware, and a fast-moving worm to spread rapidly across hundreds of thousands of computers around the globe. These extended capabilities have increasingly made phishing a vector for advanced threats: some 93% of all phishing emails now lead to ransomware.[iv]

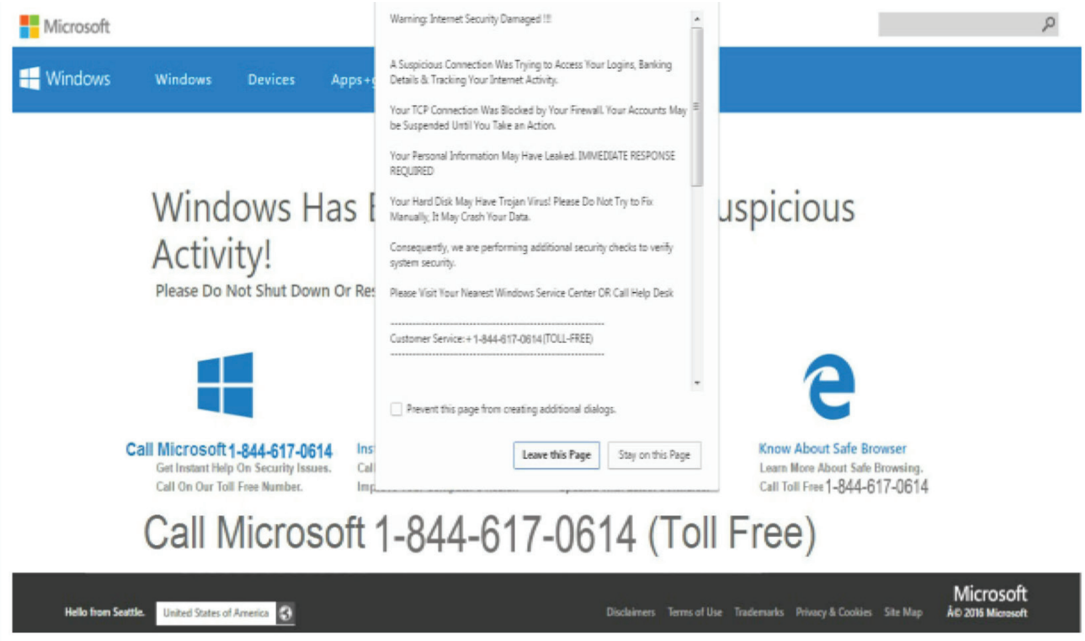
[iv] Kevin Lonergan, Information Age, June 2016.

Sense of Urgency

Webroot analysis in the first half of 2017 shows that phishing emails frequently play on fear and emotion, impelling the recipient to take quick action without taking normal precautions. Whether the urgency is implied in the subject line or in the fake URL of the phishing site, fear is being used to spur recipients to act before thinking.

Typical subjects may imply that there has been unusual activity on an account, a recent purchase must be verified, an account is in danger of being closed, or urgent invoices or tax bills are waiting. Often, terms such as “error”, “warning”, “account closed”, “Microsoft-toll-free”, and “official alert” are included in the subject line.

These scare-tactic emails include links that take users to cleverly-executed web pages with the goal of heightening fear, implying that the user will suffer dire consequences unless action is taken immediately. Whether the goal is to coerce the user to disclose credentials or other confidential information, or to implant malware on the endpoint, the urgent nature of the email and phishing site work together to play on the natural human tendency to take immediate action. The example shown below plays up the danger if action is not taken immediately. Instead of asking the user to enter credentials, it asks the user to call in to verify their credentials.



Warning: Internet Security Damaged !!!

A Suspicious Connection Was Trying to Access Your Logins, Banking Details & Tracking Your Internet Activity.

Your TCP Connection Was Blocked by Your Firewall. Your Accounts May be Suspended Until You Take an Action.

Your Personal Information May Have Leaked. IMMEDIATE RESPONSE REQUIRED

Your Hard Disk May Have Trojan Virus! Please Do Not Try to Fix Manually, It May Crash Your Data.

Consequently, we are performing additional security checks to verify system security.

Please Visit Your Nearest Windows Service Center OR Call Help Desk

----

Customer Service:+1-844-617-0614(TOLL-FREE)

□ Prevent this page from creating additional dialogs.

Windows Has E uspicious Activity!

Please Do Not Shut Down Or Res

Call Microsoft 1-844-617-0614
Get Instant Help On Security Issues.
Call On Our Toll Free Number.

Ins
Cal
Imp

Know About Safe Browser
Learn More About Safe Browsing.
Call Toll Free 1-844-617-0614

Call Microsoft 1-844-617-0614 (Toll Free)

Figure 3: Phishing page mimicking Microsoft Windows warning notification

Phishing Attacks Are Getting Harder to Detect

Webroot monitoring of phishing attempts found two important trends in the first half of 2017 that make it increasingly difficult to detect phishing attacks.

1. Hackers are stepping up their use of evasive tactics
2. They are becoming more adept at fooling the victim.

Evade Detection

The most important methods of evading detection are the short lifecycles of phishing attacks, and the use of benign domain names such as PayPal and Google.

Short-Lived Sites

We reported in 2016 that the short lifecycles of phishing attacks has made it increasingly difficult to block email messages or websites associated with attacks. The first half of 2017 shows a continuation of the trend toward very short-lived attacks, with the majority being online and active for only 4-8 hours on average.

Short-lived sites are designed to evade detection by traditional anti-phishing strategies such as block lists. When only active for minutes or hours, they stay far ahead of lists of IP addresses and URLs suspected of malicious activities. Even if the lists are updated hourly, they are generally 3-5 days out of date. The answer to the question "Is this a phishing site" needs to come in milliseconds, not days.

And while a site can be noted as malicious for a short period, it might change back to benign in a matter of hours or days, only to once again be malicious. For these reasons, a static list of malicious sites becomes outdated in minutes, and cannot be depended upon. Each time a URL is requested, it must be evaluated anew.

Benign Domain Names

Another trend from 2016 continues to have troubling effects in 2017: the vast majority of phishing sites are presented as if they're pages on a trusted domain, when instead they are disconnected pages with no inbound or outbound links.

This lack of links makes it impossible for web crawlers to find these pages, so they remain hidden. Pages that use benign domain names make end-users believe they are communicating with a trusted site and disclosing personal information to a trusted party.

Real-Time URL Validation Increases Detection

These advanced deception strategies require superior detection and protection protocols that don't rely on outdated protection tactics. They require an anti-phishing service that performs real-time URL validation rather than relying on inadequate domain crawlers and static phishing block lists.

Real-time validation, in turn, requires an advanced machine learning platform that can evaluate a site's risk and return a verdict in milliseconds, providing supplementary information such as a snapshot of the site while it is still live. These details help security teams understand the severity of the attempt and prioritize their response.

43% of respondents to a recent ESG study plan to invest in new threat-detection technology, perhaps as a result of machine-learning advances that improve accuracy, reduce false positives, and accelerate threat detection and remediation.

Machine Learning for Real-Time Anti-Phishing

1 To combat zero-hour attacks, every web page must be verified at the time the request is made, and a verdict must be delivered in milliseconds. The only effective way to do this is through advanced machine learning, delivered on a massive scale through a cloud-based infrastructure.

2 A machine-learning model uses advanced heuristics to evaluate requested URLs instantly, taking into consideration hundreds of site attributes, as well as correlated intelligence from a contextual analysis engine that accounts for web and IP reputation, the site's lifespan, recent threat history, and more.

3 Input sources can include active scanning and third-party lists. Importantly, human threat researchers and security analysts provide feedback to the model, leading to iterative adjustment, which improves the algorithms and functions over time.

4 A machine learning-based, anti-phishing solution provides immediate value for security providers. It detects phishing sites three to five days ahead of any other method—a necessity when sites are only active for a short time.

5 When speed and accuracy are everything, machine learning delivers highly accurate, real-time protection against phishing attacks, as well as contextual threat insights that drive strategic intelligence.

Fooling Victims

Phishers are becoming more adept at fooling the end-user. Throughout the first half of 2017, Webroot saw a continued use of realistic websites and other tools intended to fool even security-savvy users.

Hard-to-Spot Fake Sites

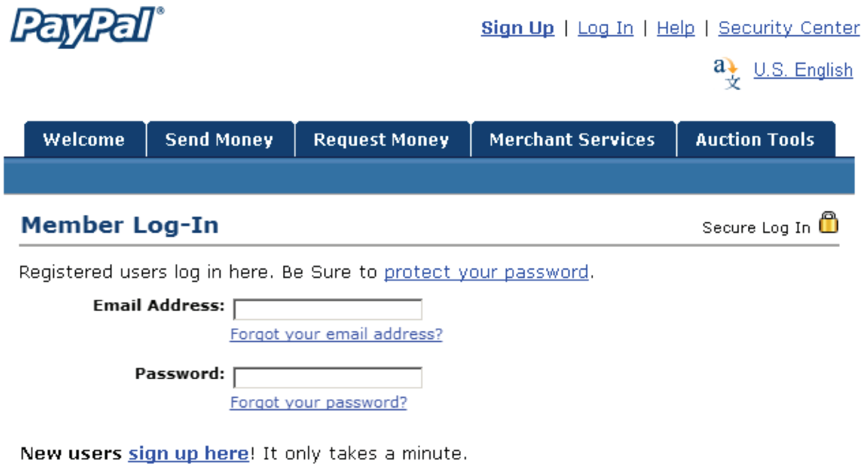
While past efforts to imitate legitimate sites were often crude and easily-spotted, today's sophisticated pages often appear remarkably authentic. They use the same colors, layouts, fonts, and logos as the site's legitimate pages.

The similarlity makes it difficult for end-users, or even security professionals, to decipher whether a phishing site is a fake. This is because attackers often start with a legitimate page from the website and modify it for their own use.

Phishing education programs have taught users to check the browser's address bar for suspicious URLs. Today's phishers know this, and they use scripting to fool the user with a benign address.

See Figure 4 for an example of a phishing site impersonating the PayPal website. outdated protection tactics. They require an anti-phishing service that performs real-time URL validation rather than relying on inadequate domain crawlers and static phishing block lists.

Real-time validation, in turn, requires an advanced machine learning platform that can evaluate a site's risk and return a verdict in milliseconds, providing supplementary information such as a snapshot of the site while it is still live. These details help security teams understand the severity of the attempt and prioritize their response.



Registered users log in here. Be Sure to protect your password.

Email Address:

Forgot your email address?

Password:

Forgot your password?

New users sign up here! It only takes a minute.

Figure 4: Phishing site impersonating PayPal

Graphics Obfuscate Text

Another technique found in Webroot research is the obfuscation of text. In the above example, the user willingly enters credentials, but the login field tags have been replaced by graphics. This technique is difficult for traditional anti-phishing techiniques to detect—since graphics can't be scanned like text, these fields evade web crawlers.

Responding to phishing attacks with credentials may not only jeopardize that account, but may create an information gateway to other accounts if the same password is used elsewhere.

Real-Time Anti-Phishing Solutions Provide Additional Protection

These attempts to fool victims and evade detection call for the immediacy and accuracy of real-time anti-phishing solutions. When clever website reproductions, misleading URLs, and obfuscated text are no match even for phishing-savvy users, a solution that conducts real-time URL assessment based on machine learning can provide "time of need" protection.

This approach is as dynamic as the hackers. Plus, it creates little to no impact on end-user productivity. Providers of safe web browsers and plugins, as well as search engine providers, welcome this real-time capability as a way to provide superior protection to customers, while differentiating their businesses.

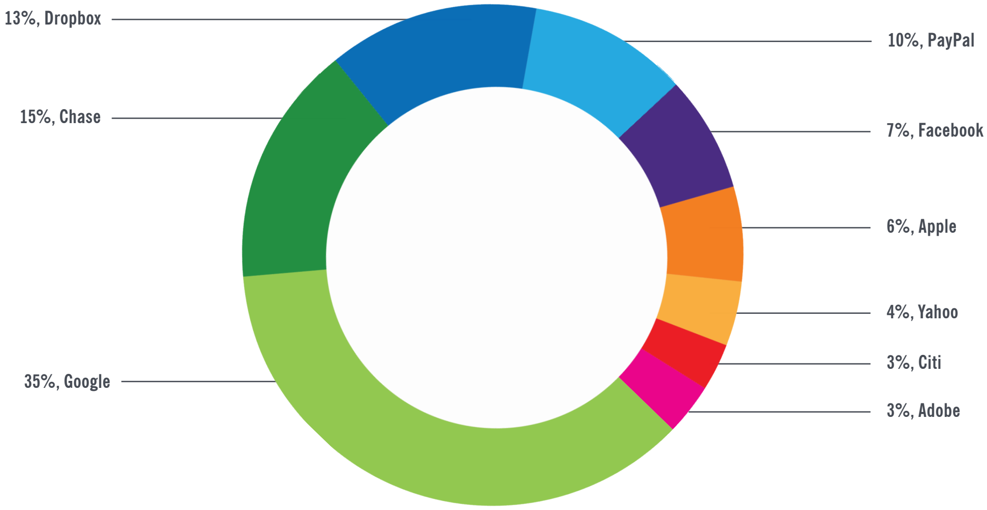


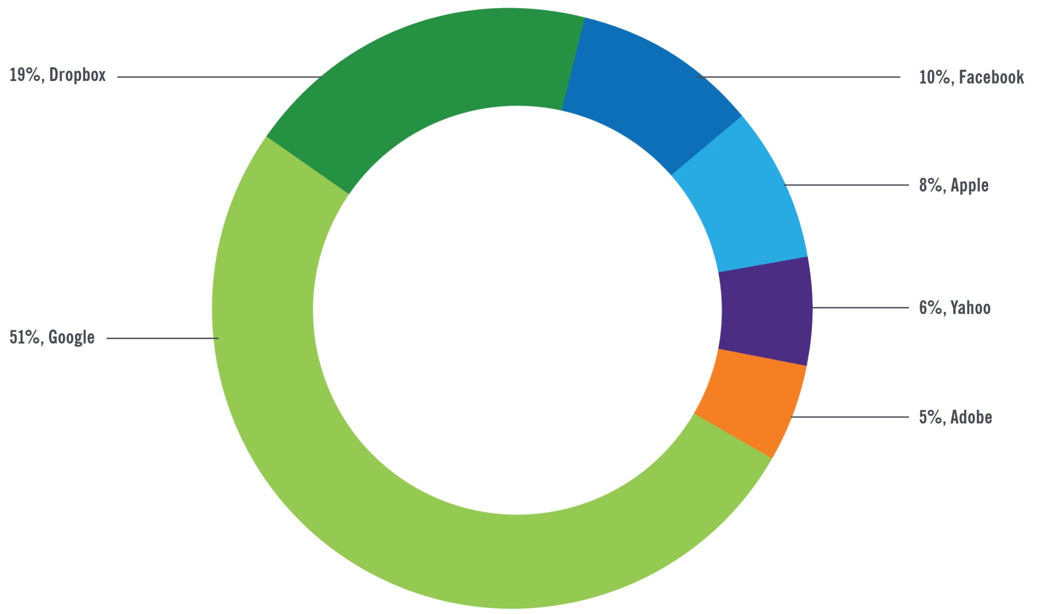
Figure 5: The Top Ten Most Phished Companies

Figure 5 shows that Google snagged the top spot as the company most targeted—almost two and half times as often as the second most phished site, Chase (the largest U.S. bank by assets).

Dropbox was the next most targeted company, at 13%, with PayPal at 10% in the first half of 2017.

Yahoo, Apple, and Wells Fargo were in the top 5 most impersonated companies in the 2016 Webroot report, but this year all have dropped significantly. Yahoo fell from 20% to 4% this year, and Apple from 15% to 6%. Wells Fargo, representing 13% of the most-targeted sites last year, now only accounts for 4%.

For every phishing email impersonating a financial institution, there were two targeting technology companies. Google represented 51% of the technology company targets with Dropbox second at 19%.



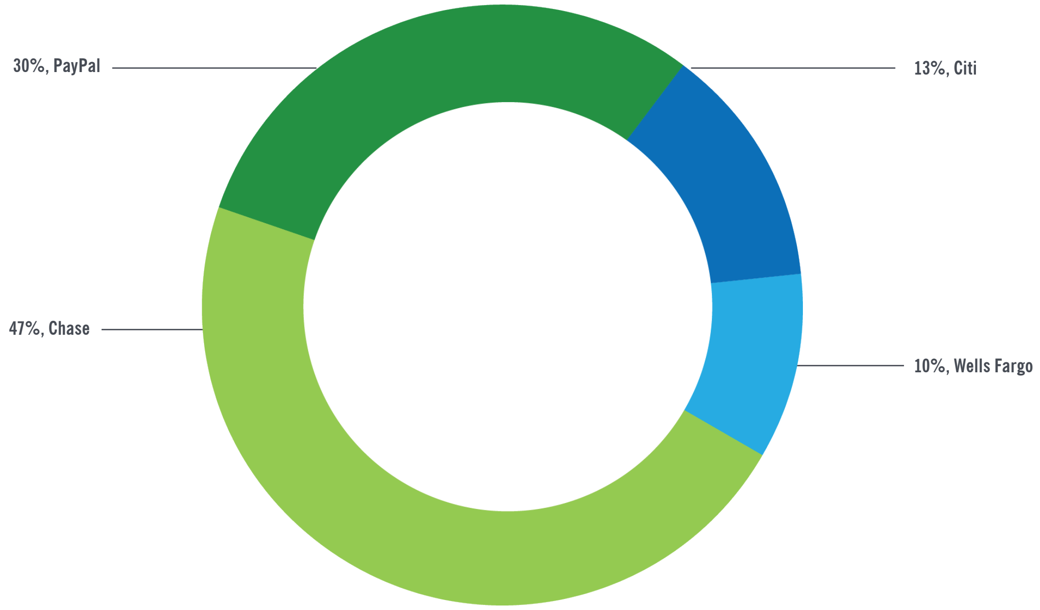


Figure 6: Top Technology (top) and Financial (bottom) Company Phishing Targets

Conclusion

Phishing is not going away. It's more pervasive and more sophisticated than ever before. With bulls-eye targeting of victims, obfuscation of addresses, and realistic impersonated websites, phishing attacks are becoming increasingly difficult to detect using traditional methods. The most important findings from this report:

» The number of new phishing websites has increased dramatically, to an average of more than one million per month, making it impossible to block sites using static block lists.

» The average lifecycle of a phishing website is now 4-8 hours, many with no inbound or outbound links, making web crawlers ineffective at finding such sites.

» Attacks are becoming much more sophisticated, hiding behind benign domains, obfuscating true URLs, carrying more malignant payloads, and fooling even security-savvy users with realistic impersonated websites.

» While Google, Chase, Dropbox, and PayPal are all at high risk of being impersonated, all businesses should be aware of the dire consequences associated with phishing attacks.

With the stakes so high, it's time to move beyond old anti-phishing techniques. Automation based on sophisticated machine learning models is the only effective way to minimize the time between the first sign of a threat, and full protection. By checking each requested page, each time it is requested, the model can make an instant assessment of the probability that it is related to phishing.

Rather than assuming that a previously-benign site is still benign, the model correlates characteristics of the site with contextual information such as recent IP reputation scores, returning a verdict that the organization can use to take automated action. Short-lived sites designed to evade detection are no match for sophisticated machine learning solutions at scale that can prevent phishing—the number one cause of breaches.

About Webroot

Webroot delivers network and endpoint security and threat intelligence services to protect businesses and individuals around the globe. Our smarter approach harnesses the power of cloud-based collective threat intelligence derived from millions of real-world devices to stop threats in real time and help secure the connected world. Our award-winning SecureAnywhere® endpoint solutions, BrightCloud® Threat Intelligence Services, and FlowScape® network behavioral analytics protect millions of devices across businesses, home users, and the Internet of Things. Trusted and integrated by market-leading companies, including Cisco, F5 Networks, Citrix, Aruba, Palo Alto Networks, A10 Networks, and more, Webroot is headquartered in Colorado and operates globally across North America, Europe, and Asia. Discover Smarter Cybersecurity™ solutions at www.webroot.com.

385 Interlocken Crescent Suite 800 Broomfield, Colorado 800.870.8102 webroot.com