December 2016

WEBROOT®
Smarter Cybersecurity™

Webroot Phishing Threat Trends

An update to the 2016 Threat Brief

Introduction

"Who would ever fall for that?" That's what many people think when they see a phishing attempt, since less advanced types of phishing often involve laughable requests with terrible grammar and spelling to lure victims. Most of these are sent to a large number of recipients in hopes that a few will respond, as even the smallest margin of return is a success. However, the majority of today's phishing attacks are becoming increasingly sophisticated, carefully crafted to obtain sensitive information from specific organizations, or even a particular person.

Webroot's latest analysis of phishing activity provides clear evidence of its evolution. Almost 100 percent of phishing URLs use domains typically associated with benign activity, making it much harder for people to recognize the URLs as malicious. Another alarming change is that 84 percent of phishing sites exist for less than 24 hours. Traditional security technologies simply can't keep up with that.

Current phishing campaigns can affect just about anyone within any organization. And the losses from successful phishing attacks can be devastating. For example, the FBI recently reported that companies have lost billions of dollars in just the past few years from employees being tricked, often by phishing attacks, into making fraudulent wire transfer payments.[1]

This report reveals information on the latest phishing trends to help you keep your organization up to date with its anti-phishing efforts. The figures presented are based on the latest data collected, tracked, and analyzed by the Webroot® Threat Intelligence Platform, the BrightCloud® Real-Time Anti-Phishing Service, and other Webroot capabilities.

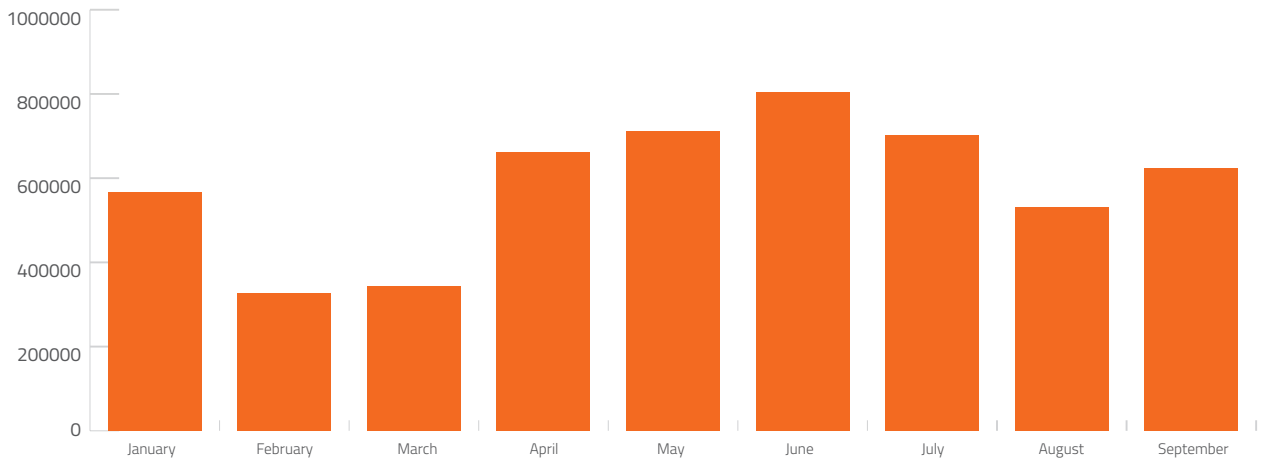

Figure 1: Phishing Sites by Month, 2016 Q1-Q3

[1] FBI, Alert Number I-061416-PSA (2016, June 14). https://www.ic3.gov/media/2016/160614.aspx

Phishing Basics

Phishing *is when an attacker misuses technology to trick someone into divulging sensitive information, such as usernames and passwords or credit card numbers. People often associate phishing with fraudulent email messages—think Nigerian prince scams—but phishing also reaches victims through web pages, documents, text messages, social media content, instant messaging, advertisements, and even phone calls.*

Each phishing attack uses social engineering techniques, exploitation of software vulnerabilities, and other means to attempt to convince internet users to trust what they see or hear and do what is asked of them. In some cases, a phishing attack might request that recipients respond directly with their information, such as giving passwords over the phone to a fake technical support person, or replying to an email from a fake government official to provide financial information. But in other cases, phishing attacks lure victims to a deceptive website.

A phishing website may appear quite convincing. An attacker might duplicate part or all of legitimate websites for financial institutions, technology companies, social media, government agencies, and other commonly visited sites, to the point that even the most diligent user might be unable to identify the sites as fraudulent.

At one time, most phishing attacks were directed at a large number of targets under the assumption that some recipients would fall for the attack and provide their login credentials, credit card numbers, etc. Attackers could reuse that information to conduct identity theft or financial fraud, or they could sell the information to others. In most of these cases, the person was the target of the phishing.

These days, phishing is increasingly taking advantage of individuals in order to target companies. This form of phishing, known as spear phishing, is usually performed to get login credentials for an employee's work account. The attacker can reuse those credentials to infiltrate the organization and install malware, compromise systems, and gain access to the organization's sensitive and proprietary information. Some attackers perform what's called "whaling," which is spear phishing directed at an organization's leadership or other key employees.

Today's news stories have somewhat shifted their focus from phishing to the latest threat: ransomware. Although ransomware is a certainly an important concern, a recent poll of small business owners showed that small businesses are five times more likely to have experienced a phishing attack than a ransomware attack.[2] And susceptibility to phishing is by no means limited to small organizations. Several recent major data breaches, including the Anthem breach of nearly 80 million healthcare records and the theft from Sony Pictures of over 100 terabytes of data, started with a few employees being tricked by phishing attacks. Attackers leveraged that initial access to gain more access and eventually cause hundreds of millions of dollars in damage. Every organization, no matter how large or small, is at immediate and serious risk from phishing attacks.

[2]9 ways Cyber criminals attack small businesses (2016, October 10). https://inthenation.nationwide.com/news/cyber-security-month-2016-survey

Trends in Phishing Attack Blocking

The most troubling trend in phishing is how much the life cycles for an attack have shortened. Back when a single phishing attack lasted for several weeks or months, organizations had time to block the email messages or websites the attack used to prevent more victims from falling prey. Today, attackers have tools that automate the creation of fraudulent sites and the highly customized emails, ads, social media messages, and other phishing content. Figure 2 shows phishing life cycles in hours based on a representative sample of over 800 phishing sites detected by Webroot in September and October 2016. The average life cycle was less than 15 hours. Twenty sites were online for less than an hour, with one lasting just 15 minutes, while the longest-lived site lasted less than two days (just 44 hours).

A common misconception is that each phishing attack uses a new, dedicated domain name. In actuality, very few modern phishing attacks do this because a domain name used only for phishing can be readily identified, enabling organizations to block all communications involving that domain. Blocking phishing attacks has become much more complicated. Webroot analysis shows that almost 100 percent of the latest phishing URLs are using domains typically reserved for benign purposes. For example, an attacker may have compromised a single page on a web server and replaced that page's content with a phishing page. Figure 3 shows an example of a phishing page impersonating Adobe's website. Note that the URL uses a path based on a benign domain name. Additional URLs using other benign domain names may point to the same phishing site.

84% of phishing sites last less than 24 hours.

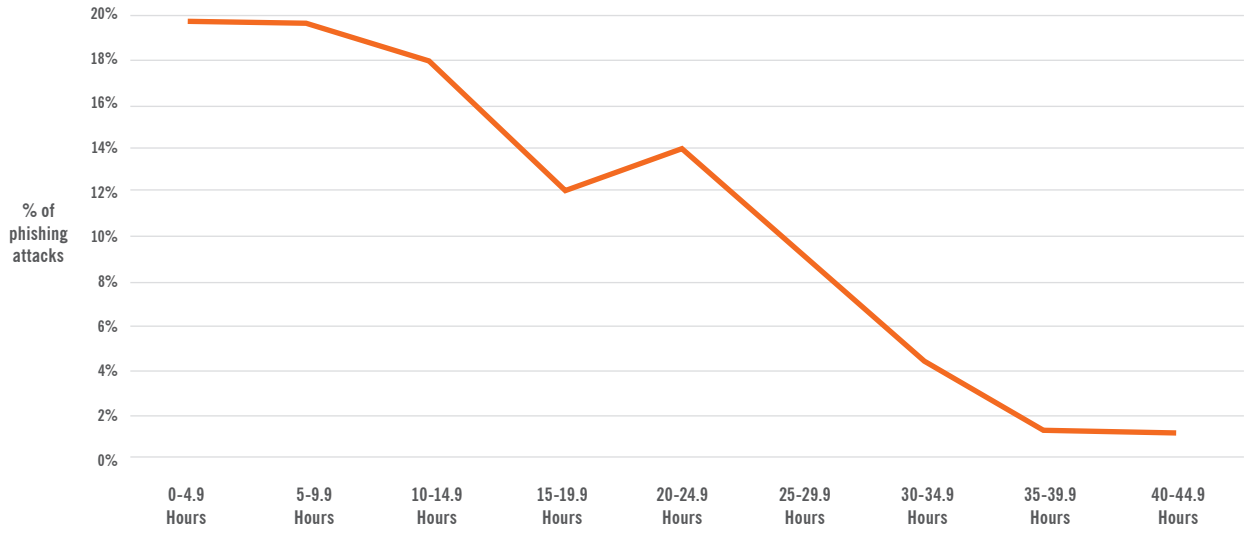

Figure 2: Phishing Attack Life Cycles in Hours

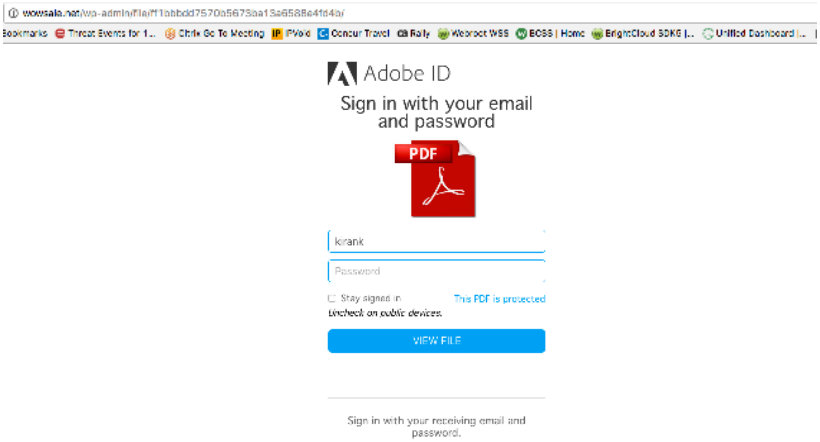

Figure 3: Example of Phishing URL with Benign Domain

Because domain-based filtering is no longer effective at blocking phishing attacks, every URL must be analyzed to look for an individual webpage—especially within otherwise benign domains—that is acting as a phishing site. It is also important that every URL be checked each time it is requested because a page that was benign just seconds ago may have been compromised since the last check. Organizations cannot assume that a URL is safe just because it was safe the last time they checked it.

The data on the volume of new phishing sites is staggering. Throughout 2016, Webroot has monitored attempts to lure people to an average of over 400,000 phishing sites per month. To keep up with the incredibly short phishing life cycles and the sheer volume of phishing sites and URLs, old techniques that use static or crowdsourced blacklists of bad domains and URLs must be abandoned. As malware increases in speed and sophistication, static lists often become obsolete within moments of being published, if not sooner.

To succeed at thwarting ever-changing phishing attacks, organizations must adopt highly automated technologies that leverage the latest machine learning models for identifying threats. These technologies evaluate the page corresponding to each URL request and examine hundreds of characteristics of that page. Machine learning models analyze those characteristics in conjunction with metadata regarding the page, such as how long the domain or website hosting that page has been in existence and what the recent threat reputation scores have been for the IP address hosting the page's website. Ultimately the machine learning model produces a score or rating for the site requested by the URL in just milliseconds. This approach minimizes the time between when the phishing threat is first detected until full protection is achieved.

An organization that uses an anti-phishing technology based on machine learning can achieve highly accurate phishing attack detection. This enables the organization to make automated decisions about whether each page request should be allowed or blocked without causing any perceptible delay for users. The trend toward anti-phishing technology based on machine learning is one that every organization should follow as soon as possible to prevent major breaches.

No matter which anti-phishing technologies an organization adopts, a few types of phishing attacks can still succeed. For example, a phishing attack could start with an attacker asking a user via email for his or her name and phone number. Differentiating such a request from a benign request is extremely difficult, if not impossible, without discussing it with the targeted user. Another example is phishing attacks conducted through phone calls. Phishing attacks may also occur outside the organization's environment, such as an attacker targeting an employee's personal email account in the hopes that the employee uses the same password for work.

A comprehensive approach to anti-phishing requires a combination of technical and non-technical measures. Although technologies can stop most phishing attacks, user awareness and training are the only way to prevent the remaining types of phishing attacks from succeeding.

Trends in Impersonated Companies

One of the most interesting trends in phishing is the specific companies that are impersonated most often. Webroot took a closer look at the companies for which impersonation would likely cause the largest negative impact: the "high-risk" companies. Of the high-risk companies being targeted, Figure 4 shows the companies with the highest number of phishing sites impersonating them between January and mid-October 2016 (Google, Yahoo, Apple, PayPal, and Wells Fargo). The percentages reflect the share of phishing sites targeting the high-risk companies; for example, the chart shows that 21 percent of all phishing sites targeting high-risk companies during that time period were impersonating Google.

At first glance, the top five high-risk companies for 2016 are strikingly similar to those from 2015, which were (in order) Google, PayPal, Dropbox, Yahoo, and Apple. But the relative percentages for the top impersonated targets have changed a great deal.

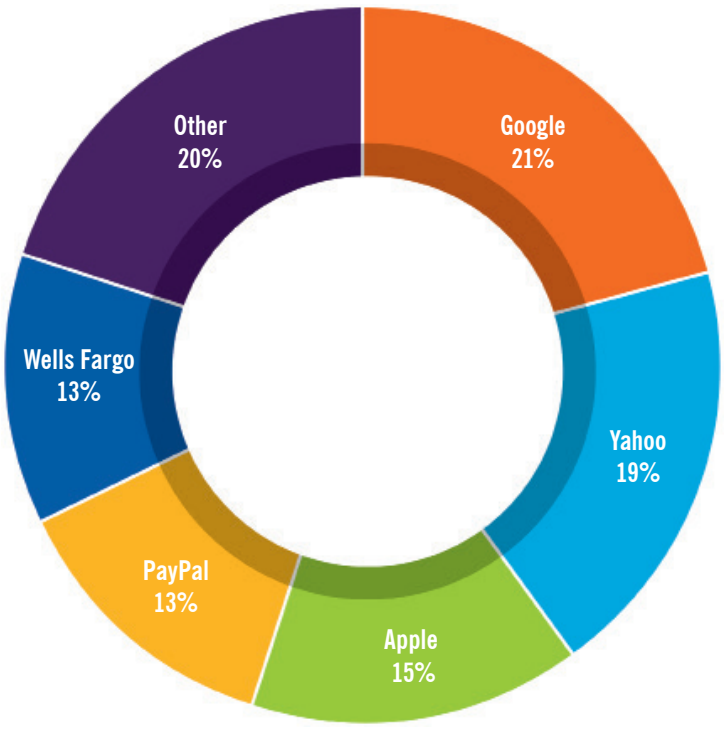

Figure 4: Relative Share of Phishing Sites for Highest-Risk Companies

Figure 5 shows these changes for the four companies that appeared as top targets in both 2015 and 2016. In 2015, Google had over twice as many phishing sites impersonating it as the next highest on the list, PayPal. In 2016, Google's relative share of the phishing sites has sharply dropped from 30 percent to 21 percent, while Yahoo's relative share has nearly doubled, from 10 percent to 19 percent, almost matching Google's share. Apple's relative share has also risen from 9 percent to 15 percent. In short, phishers are concentrating less on Google, and are impersonating a few other companies nearly as often.

Taking all phishing targets into account, attackers are focusing on the same types of targets in 2016 as they did in 2015. In both years, between 55 and 60 percent of the most frequently impersonated companies were financial institutions and the rest were tech companies. Also in both years, there were far more phishing sites for tech companies than financial institutions, at approximately a two to one ratio.

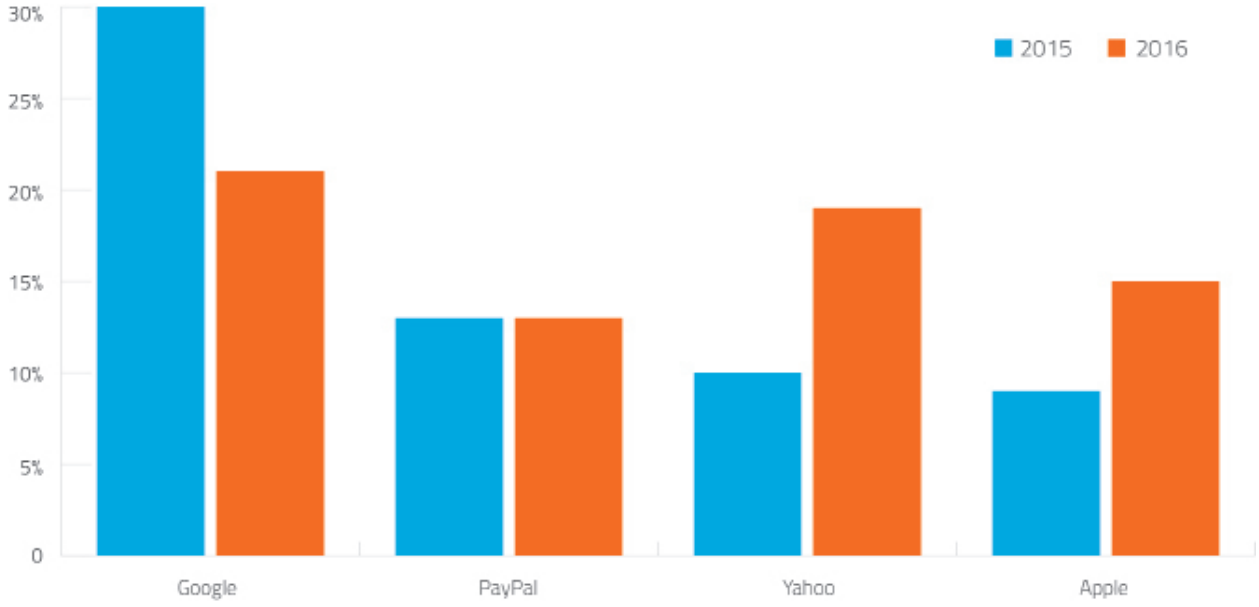

Figure 5: Share of Phishing Sites for Highest-Risk Companies in 2015 and 2016

Conclusion

Despite its humble beginnings, phishing has come a long way since those first crudely constructed phishing emails. The following are the most important findings from this report:

1. The average life cycle for a phishing site is under 15 hours, with some sites lasting just 15 minutes and the longest-lived site lasting less than two days. 84 percent of phishing sites last less than a day.

2. Nearly all of today's phishing URLs are hidden within benign domains. The practice of phishing attacks using dedicated domains has almost disappeared.

3. During 2016, an average of over 400,000 phishing sites have been observed each month.

4. The high-risk companies, i.e. those for whom impersonation would likely cause the largest negative impact, that are most often targeted by phishing are Google, PayPal, Yahoo, and Apple.

Strengthening an organization's anti-phishing strategy means moving beyond old techniques that use static phishing domain or URL lists to highly automated technologies based on sophisticated machine learning methods. These more advanced technologies can quickly check the characteristics and metadata for each requested webpage to look for signs of phishing, then report a score or rating that the organization can use to make automated decisions about allowing or denying access to the page. When phishing sites can appear and disappear in the length of a coffee break, highly automated machine learning solutions are the only way to prevent successful phishing attacks and the major data breaches they facilitate.

About Webroot

Webroot delivers next-generation 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 and BrightCloud® Threat Intelligence Services protect tens of millions of devices across businesses, home users, and the Internet of Things. Trusted and integrated by market-leading companies, including Cisco, F5 Networks, 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

World Headquarters
385 Interlocken Crescent
Suite 800
Broomfield, Colorado 80021 USA
+1 800 772 9383

Webroot EMEA
6th floor, Block A
1 George's Quay Plaza
George's Quay, Dublin 2, Ireland
+44 (0) 870 1417 070

Webroot APAC
Suite 1402, Level 14, Tower A
821 Pacific Highway
Chatswood, NSW 2067, Australia
+61 (0) 2 8071 1900