Menlo Security

TRUST HACKING

Cybercriminals Are Exploiting Traditional Measures of Trust on the Web

STATE OF THE WEB 2017

KEY FINDINGS

For this report, our researchers analyzed the top 100,000 domains as ranked by Alexa to understand the risks inherent in using the world's most popular websites. We found widespread evidence that cybercriminals are successfully exploiting long-held measures of trust, such as a particular site's reputation or the category in which the site is included, to avoid detection and increase the effectiveness of their attacks.

OF ALEXA'S TOP 100,000 SITES WERE RISKY

We consider a site risky if any one of these three criteria is met:

- The site, either the homepage or associated background sites, is running vulnerable software.
- The site is "known bad," meaning it has been used to distribute malware or launch attacks.
- The site has suffered a security breach in the past 12 months.

4,600 PHISHING SITES USED LEGITIMATE HOSTING SERVICES

Phishing attackers are using well-known, popular hosting services to help avoid detection.

Typosquatters camp out in trusted categories such as **Financial Services, Local Information, Travel,** and **News and Media.**

BUSINESS AND ECONOMY EXPERIENCED THE MOST SECURITY INCIDENTS

In 2017, Business and Economy sites were particularly risky. This category:

- Hosted more phishing sites than any other category.
- Contained more sites running vulnerable software, such as PHP 5.3.3, than any other category.
- Had more "known bad" sites than the Gambling category.
- Experienced the most security incidents in the last 12 months.

WEAPONIZING TRUST

3 Ways Cybercriminals Can Weaponize Your Trust

Trusted Websites May Not Be as Safe as You Think

Page 4

Phishing Sites Leverage New Tricks to Win Your Trust

Page 11

Typosquatting Lives On

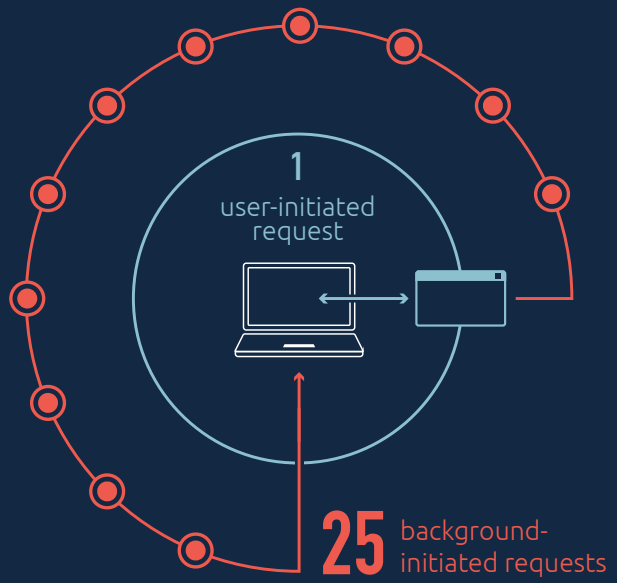
Page 13

Trusted Websites May Not Be as Safe as You Think

The web has become an integral part of our daily routines. From the time we wake up in the morning, to the time we go to bed at night, many of us have spent hours on the web doing our jobs, or simply checking stocks, weather, and news. When we visit well-known sites, as we've done for many years without issue, we have an underlying belief that these sites are safe. After all, these are reputable brands. What could possibly go wrong?

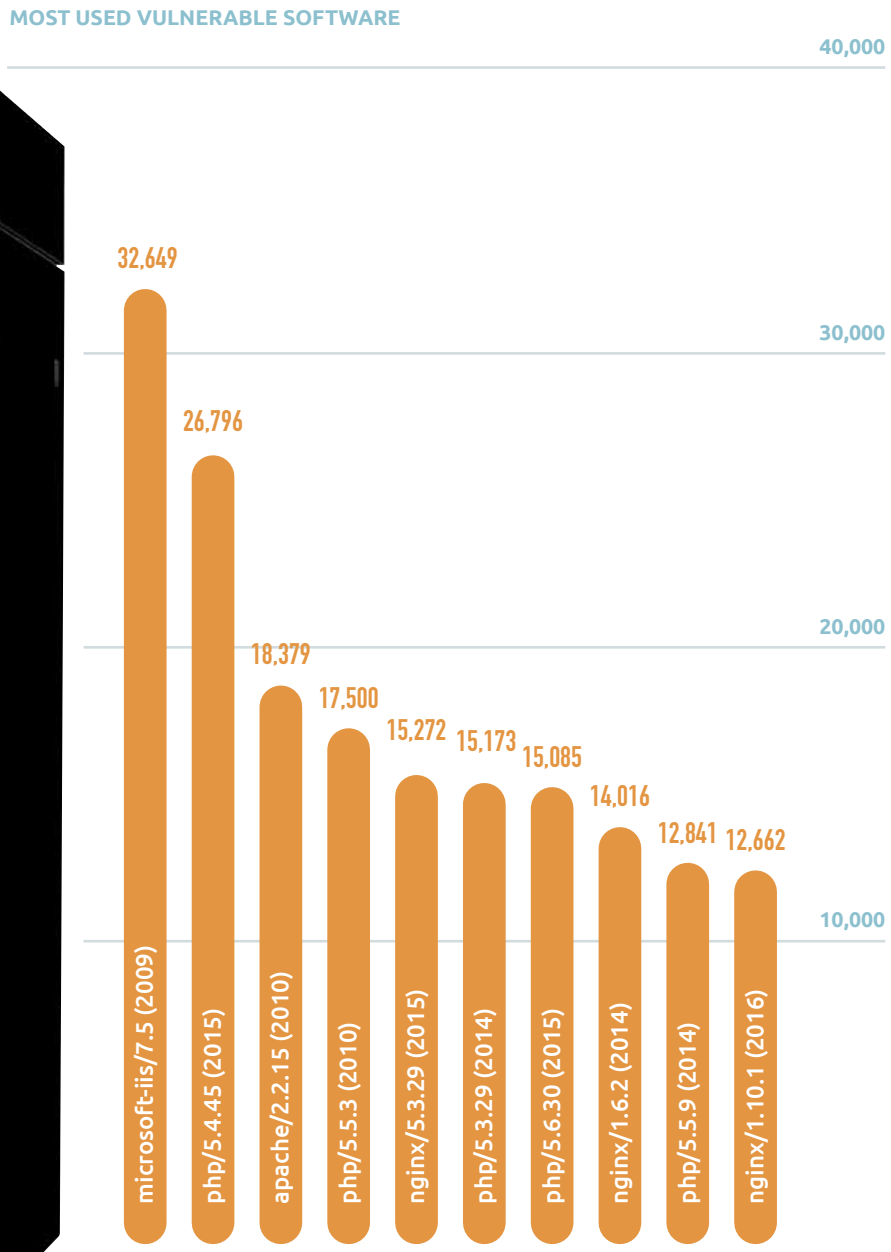
Unfortunately, attackers are taking advantage of the ubiquity of the web and people's trust to infect users' devices and propagate malware.

> Some of the most notorious attacks in 2017, including the WannaCry and NotPetya ransomware attacks, leveraged the web to ensure the widest impact and do the greatest harm.



Background Radiation

Much of the security industry is focused on monitoring and controlling the online behavior of visitors to websites. But much of the damage wrought by cybercriminals happens behind the scenes, as websites connect with so-called "background sites" to carry out a user's requests. Our researchers found that every time a user visits a website, that site calls on an average of 25 background sites for content—say, to fetch the latest viral video from a content delivery server or grab ads to display from an ad-delivery network. The vast majority of malware prevention products, from simple antivirus and web filtering packages to sophisticated approaches such as behavioral modeling, focus on the domains that users click on each day—but ignore these calls to background sites.



Widespread Use of Vulnerable Software

Menlo Security was able to passively fingerprint the script origin servers (website software) for primary and background sites, and correlate the CVE-IDs (documented vulnerabilities) of these sites. We found that many companies use aging software technologies to run their sites—technologies that have been around long enough to have been repeatedly compromised over the years.

> More than 32,000 of the sites we studied rely on Microsoft IIS 7.5, which was released in 2009

In fact, many sites use software that is no longer fully supported. Microsoft's Internet Information Services (IIS) 5 was released in 2000, and reached "mainstream support end" in 2005.

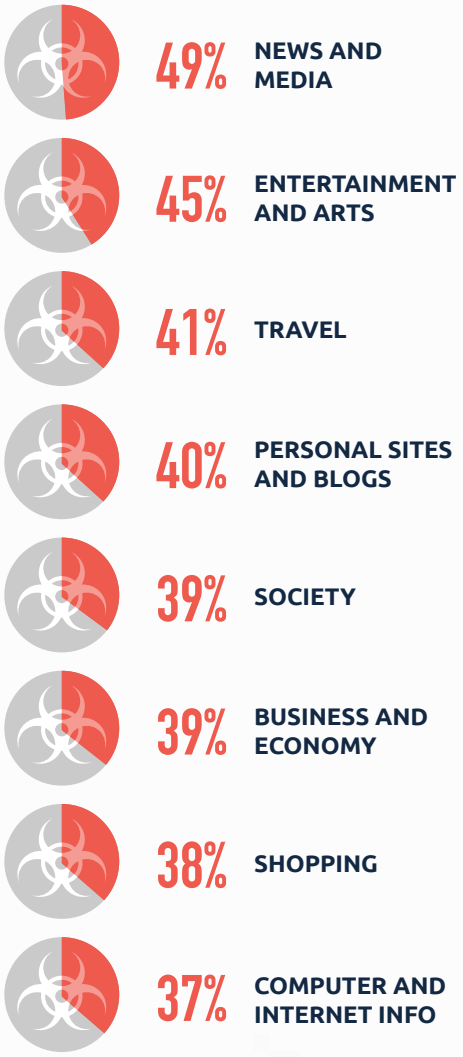
All software has vulnerabilities, and credible vendors, including Microsoft, work diligently to provide patches to close them as soon as they are discovered. It is incumbent on administrators to apply all patches in a timely manner.

What's in a Label? Not Much

For decades, web security vendors have gone to great lengths to segment the world's websites into logical categories, such as Business and Economy, Shopping, News and Media, and Malware. Many companies have used these categories to help set security policy. Unfortunately, it's no longer advisable to consider any category as inherently "safe." According to our research, more than a third of all sites in categories including News and Media, Entertainment and Arts, Shopping, and Travel were risky.

Overall Risk

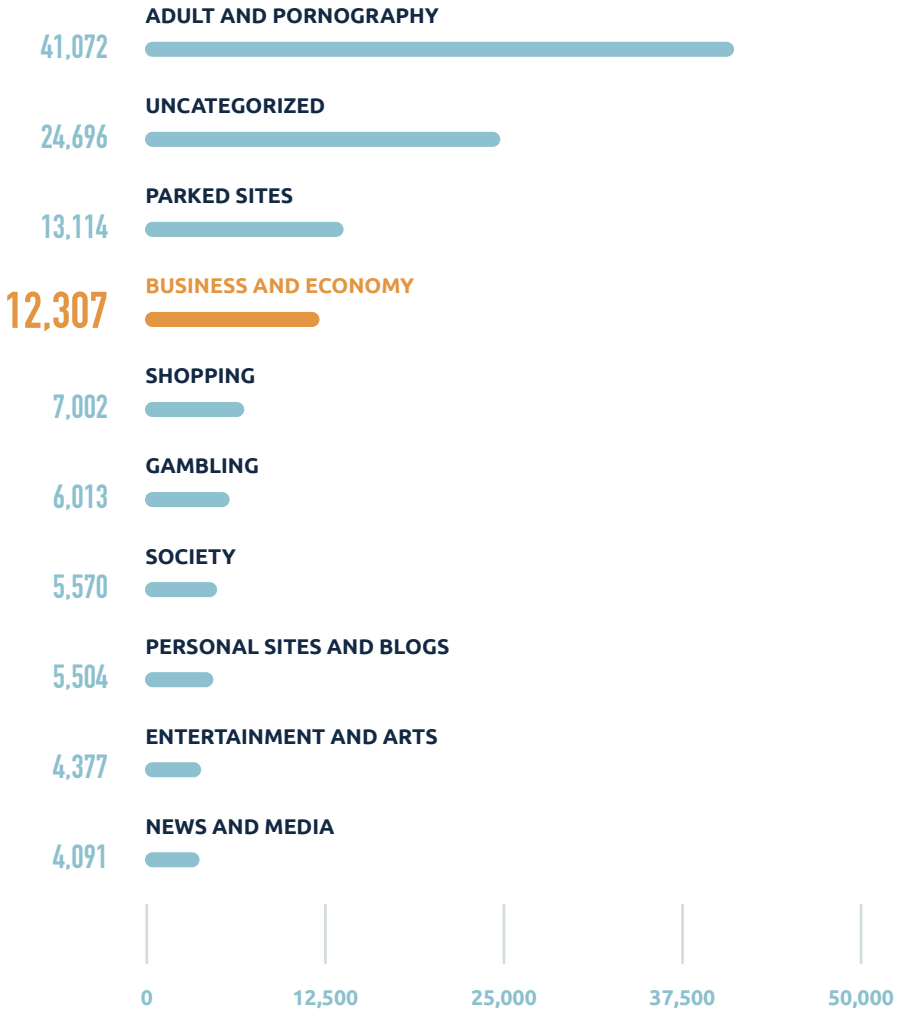
Percentage of sites in categories that satisfied one of our three criteria of riskiness



Consider Business and Economy. It had more “known bad” sites than any other traditionally trusted category, with more than 12,000. That’s fewer than in Adult and Pornography, but more than in Gambling.

Known Bad Sites

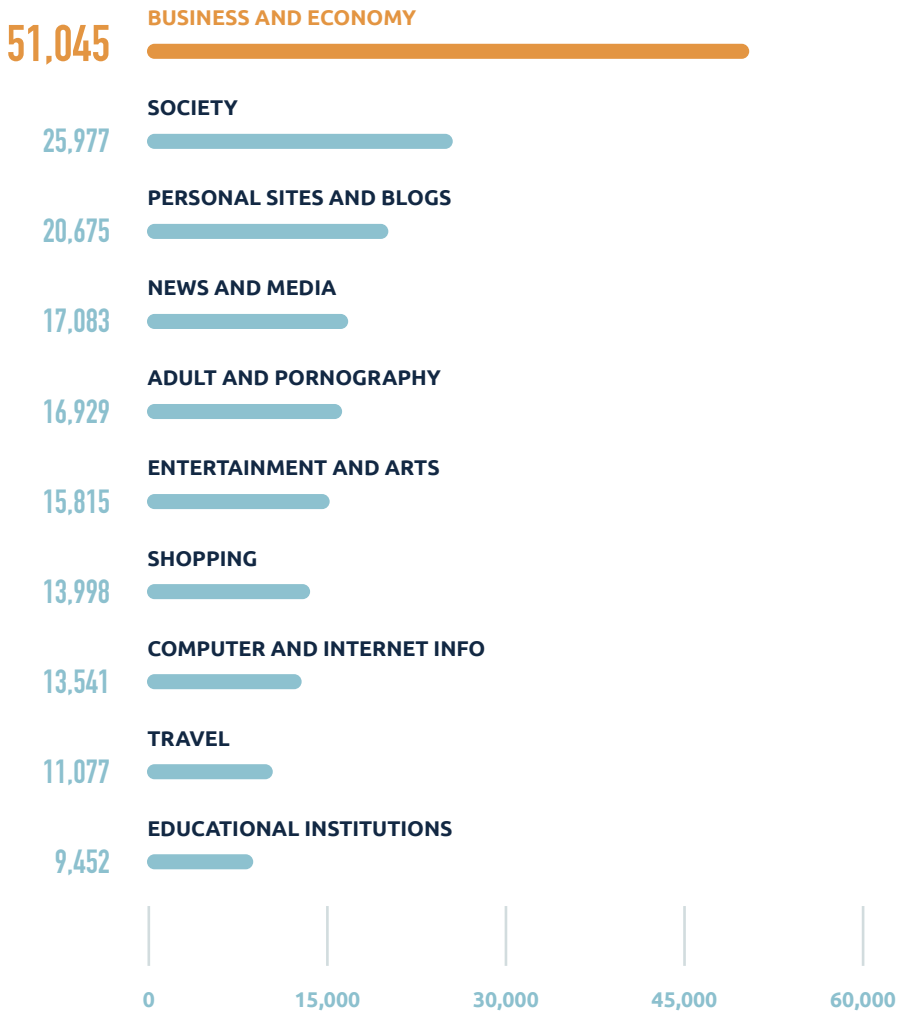
These categories had the most sites that have been used to make attacks or deliver malware.



More sites in Business and Economy relied on vulnerable software than in any other category, for the second year in a row. Many of these sites still use Microsoft's IIS 5 web server, which the company stopped supporting 12 years ago.

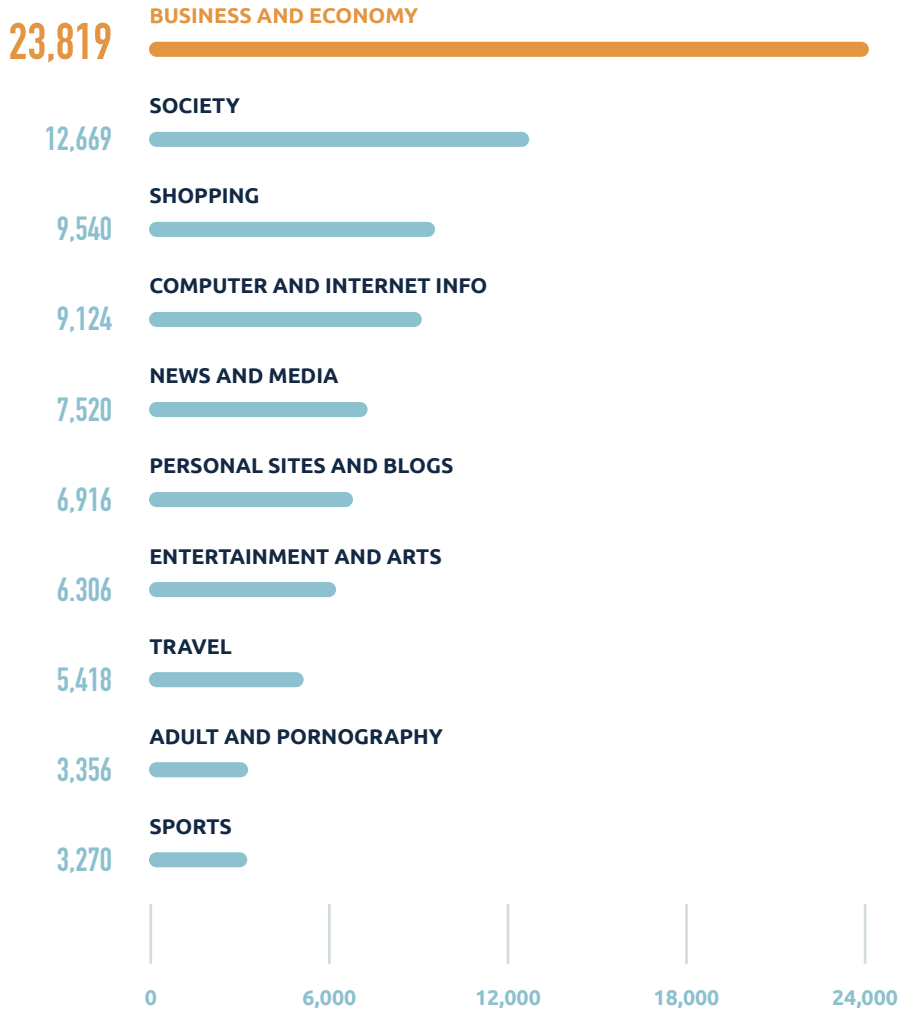
Top Categories of Vulnerable Sites

These categories had the most sites that have been identified as relying on vulnerable software.



Business and Economy sites also suffered more breaches and other successful attacks than any other category.

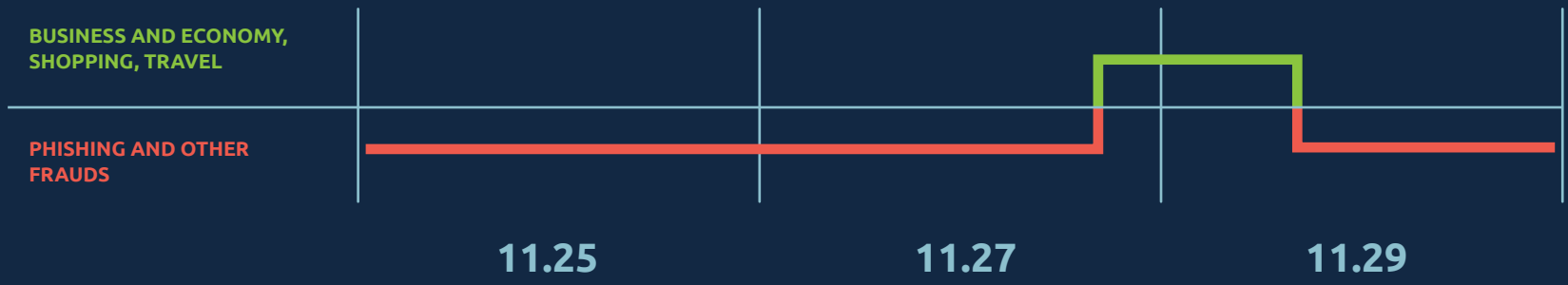
Top Categories with Threat History in the Last Year



One of the most dangerous assumptions about categorization is that once a website has been assigned to a category, it will remain there. The reality is that websites can transition in and out of trusted and untrusted categories. Using our cloud-based isolation platform, we monitored thousands of sites visited by Menlo Security users over a 30-day period. During that time, researchers observed nearly 1,000 sites that were re-categorized at least once by a web security firm. In the example below, a website that had been assigned to the Phishing and Other Frauds category was briefly re-assigned to Business and Economy, Shopping, Travel. While the web security firm later decided the site was once again bad, any visitors to email.complianceonline.com while it was classified in a benign-sounding category may have been unwittingly visiting a phishing site.

So Is This Site Safe or Not?

One reputation service rightly identified email.complianceonline.com as malicious—except for a brief period when it didn't.



CATEGORIES CHANGE

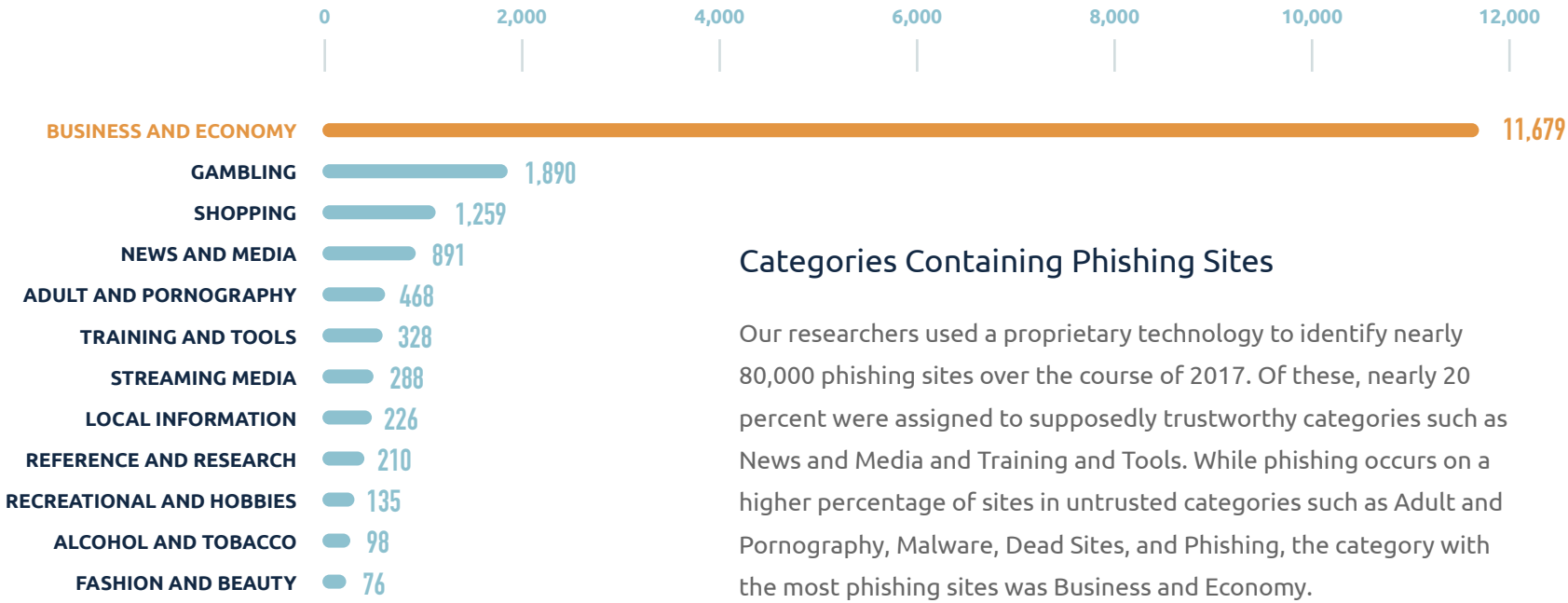
Phishing Sites Leverage New Tricks to Win Your Trust

Most high-profile breaches result from phishing attacks, or sometimes "spear-phishing" attacks designed to compromise a particular individual or organization. Clicking on what appears to be a perfectly legitimate link within a phishing email can expose a user to credential theft or a drive-by malware exploit that could deliver ransomware or command-and-control software, marking the beginning of a larger breach that can result in financial theft, the loss of valuable personally identifiable information (PII), or the loss of intellectual property.

In 2017, we discovered 4,600 phishing sites using legitimate hosting services.

There are other benefits to hiding a phishing site on a widely trusted hosting service. It is far easier to set up a subdomain on a legitimate hosting service than use other alternatives—such as trying to hack a popular, well-defended site or to set up a brand-new domain and use it until it is blocked by web security firms. Legitimate domains are often whitelisted by companies and other organizations out of a false sense of security, giving cover to phishing sites. Also, hosting services typically allow customers to set up multiple subdomains. For example, researchers found 15 phishing sites hosted on the world's 10 most popular domains.

It is important to note that we did not uncover any evidence that anyone was successfully attacked from any of these subdomains. But clearly, attackers are taking advantage of readily available hosting services these sites offer.



Categories Containing Phishing Sites

Our researchers used a proprietary technology to identify nearly 80,000 phishing sites over the course of 2017. Of these, nearly 20 percent were assigned to supposedly trustworthy categories such as News and Media and Training and Tools. While phishing occurs on a higher percentage of sites in untrusted categories such as Adult and Pornography, Malware, Dead Sites, and Phishing, the category with the most phishing sites was Business and Economy.

Typosquatting Lives On

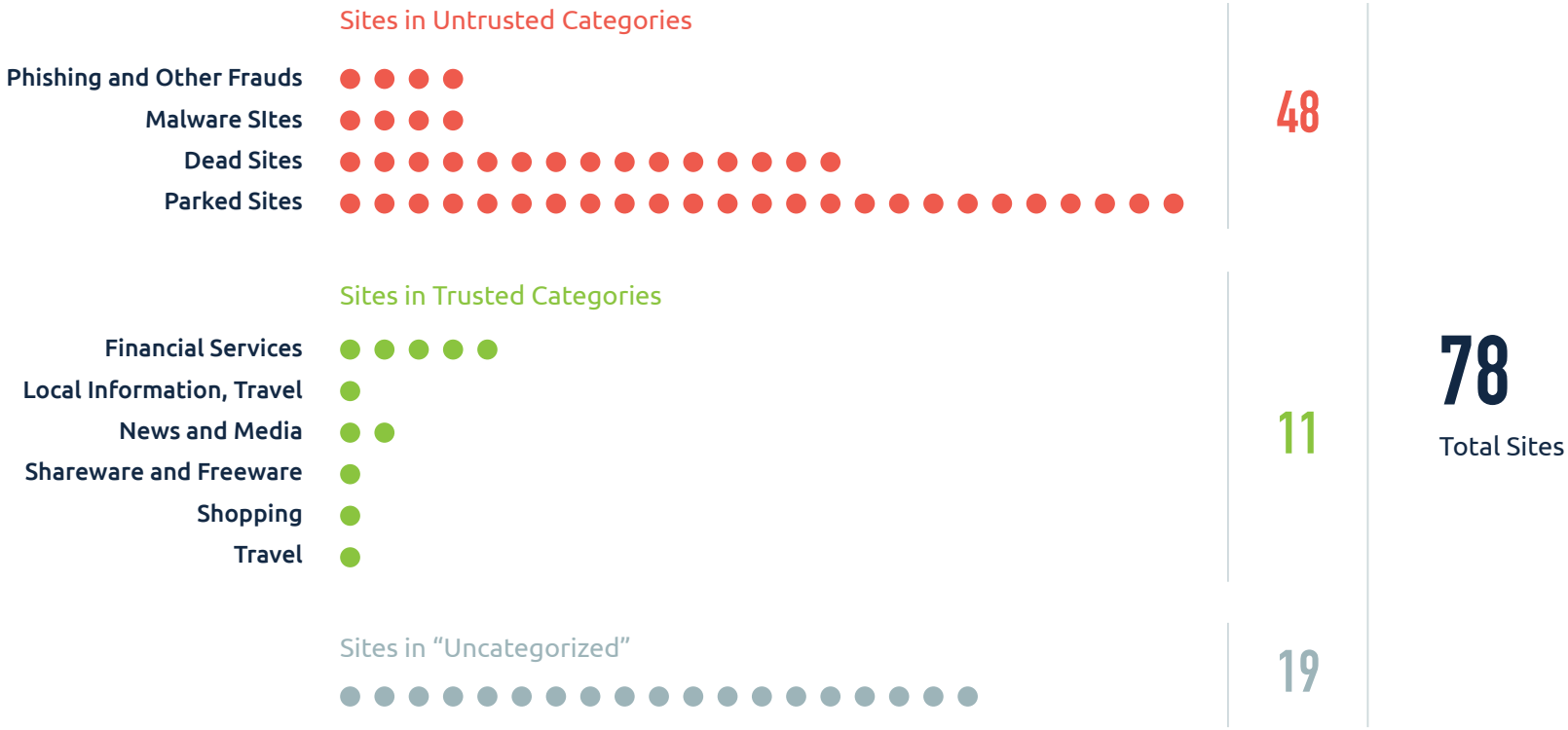
Typosquatting is the act of setting up fake domains containing intentional misspellings that can be used for phishing and malware delivery. For example, millions of Anthem health insurance subscribers provided personal information to typosquatting sites such as we11point.com, because they didn't notice the difference from Anthem's actual URL, which is wellpoint.com (using the letter "l" instead of the number "1"). Although legitimate sites will sometimes register frequently misspelled variants of their domain in an effort to protect visitors, there is no guarantee this is always the case.

Wellsforgo.com
Yotuube.com
Yaoo.com

Typosquatters Play the Categorization Game

To prepare this report, we tracked the web activity of our users over a 30-day period. During that time, we saw traffic to 78 malicious sites that had been misspelled to deceive people trying to visit Alexa's top 1,000 domains. To reduce the odds of detection, more than a third of the sites had found a way to be classified as either Uncategorized or in a generally trusted category, such as News and Media.

Without some proactive effort on the part of the operators of these sites, they would likely have been identified as a Phishing or Other Fraud category, and would therefore have been blacklisted by most companies' web-filtering systems. For example, we found a site called "yotuube.com" that our URL categorization service pegged as a low-risk "shareware" site rather than flag it as something more ominous.



When Is Web Security an Oxymoron? When You're Expecting Legacy Products to Spot and Thwart Never-Before-Seen Attacks

It is extremely difficult for any company to achieve perfect security these days, given the skyrocketing variety and sophistication of cyberattacks—in part because the detection-based products in wide use today too often fail to spot these threats. The insights in this report, gathered in part by tracking our users' web usage over a 30-day period, did nothing to dampen our confidence. But to further test our thesis, we wanted to run a real-world test of these legacy defenses. So we commissioned MRG Effitas, a U.K.-based security research company, to create a malicious website which was registered to appear as if it belonged in a trusted category. The site was designed to deliver phishing attacks, as well as a variety of zero-day web threats including:

- HTML exploits, including delivered through fonts, images, and CSS
- Other browser-based exploits, such as Visual Basic code, including the IronSquirrel exploit delivery method
- Browser plug-in-based exploits, such as Adobe Flash, Java, and Silverlight
- Document-based exploits, such as MS Office and Adobe Reader

MRG Effitas then accessed the malicious site from a test workstation that was protected by a state-of-the-art advanced threat protection appliance that uses content analysis to identify and thwart attacks. As expected, the appliance failed to identify or stop any of these attacks. Because the phishing site was new and was registered in a commonly trusted category, the appliance allowed the workstation to connect directly to the site. In the real world, this would have resulted in a malware infection or stolen credentials.

Similarly, the appliance failed to thwart distribution of any of the malware to the test workstation. Because the URL was newly created, it had not yet been classified as malicious by any public reputation database or assigned to an untrustworthy category, a scenario that happens often in the real world as attackers spin up new websites to launch attacks. In this test, the content analysis appliance, which relies largely on reputation and categorization services to identify risky sites, failed to protect the workstation. The website successfully delivered all of the zero-day exploits listed above.

CONCLUSION

It's more important than ever to have a healthy distrust for the web. Regardless of your company's security strategy, we hope this study makes clear that it is difficult to guarantee security when browsing the web, using attachments, or opening unrecognized emails.

Best practices can lower the odds of being victimized. Website owners need to make sure their servers run the latest software updates, and should investigate technologies such as Content-Security-Policy (CSP), which can reduce introduction of malicious code via background sites.

Consumers should download software updates religiously, avoid vulnerable technologies such as Adobe Flash, and use the Chrome browser when possible. Still, even the best detection-based tools and security policies cannot guarantee security on the web today. Companies must consider new technologies.

One such technology is isolation, which protects users by moving the execution of web content to the cloud. Since malware and malicious code never reaches users' devices, it can't infect them. Isolation isn't new, but its widespread adoption has been hindered by a suboptimal user experience such as latency, choppy scrolling, jittery video, and similar impediments.

Until now.

Menlo Security's patented Adaptive Clientless Rendering completely preserves the user experience, while providing the strongest web security available today. This combination of transparency and efficacy sets Menlo Security apart, and is leading our momentum in the market. We know of no other technology with the potential to protect against known and unknown threats, and take issues of trust off the table.

With isolation, cybercriminals can no longer weaponize your trust.

METHODOLOGY

To analyze the overall risk of the top Alexa websites, Menlo Security developed a distributed Chrome-based browser farm to load the homepage of each of the Alexa listed websites. The Chrome browser was further instrumented with a proprietary Menlo Security Risk Analyzer extension that could monitor the loading and execution of JavaScript. Using a real browser to load the webpage was critical to the page loading in the same manner as it would for an end user. This also triggered software execution in the form of scripts, as well as the dynamic loading of ads, beacons, trackers, and other content.

In addition to tallying up the number of scripts in each page, the Menlo Security Risk Analyzer was also able to passively fingerprint the script origin servers (website software), categorize these background sites, as well as correlate the CVE-IDs of these sites based on the website software. Menlo Security also leveraged readily available threat intelligence feeds to determine whether sites were categorized as "known bad," or had security incidents in the last 12 months. Based on this information, Menlo Security classified sites as risky if one or more of the following statements was true:

- Homepage or background site was running software with known vulnerabilities (CVEs).
- Homepage or background site was categorized as "known bad," such as a phishing website, malware website, etc.
- Homepage or background site has had a security incident in the last 12 months.

Menlo Security also utilized its cloud-based isolation platform to obtain additional insights into typosquatting sites, phishing sites, and user behavior.

Menlo Security

2300 Geng Rd Ste. 200

Palo Alto, CA 94303

Tel: 650 614 1795

info@menlosecurity.com

menlosecurity.com