Menlo Security

MENLO SECURITY LABS REPORT

STATE OF THE WEB

FIRST HALF 2018

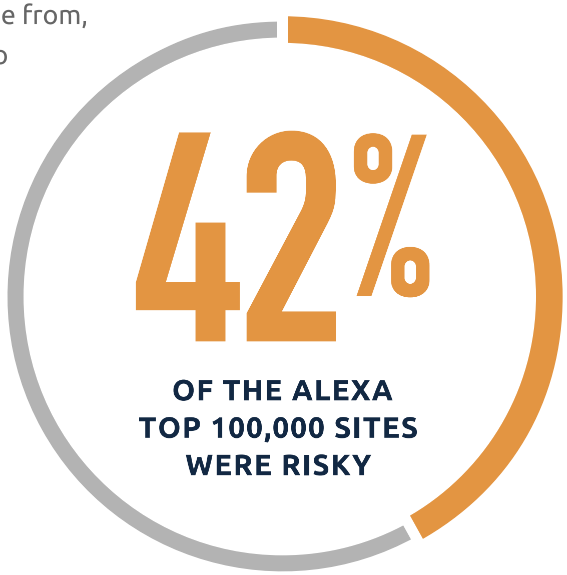
KEY FINDINGS

In our annual State of the Web report for 2017, “Trust Hacking: Cybercriminals Are Exploiting Traditional Measures of Trust on the Web,” we explained why nearly half of the world’s most popular websites are risky places to visit. Specifically, 42 percent of the Alexa Top 100,000 sites were “risky” because they met one of these three criteria: They were built on or routinely connected to sites that used server software known to be vulnerable to cybersecurity attack; the site was “known bad,” meaning it has been used to distribute malware or launch attacks at some point in the past; or the site had suffered a security breach within the past 12 months.

People in different countries prefer different websites, and the risks associated with using the most popular sites in those countries varies accordingly. In this mid-year update to our State of the Web report, we take a deeper look at six specific countries: the United States, Australia, France, Japan, Singapore, and the United Kingdom.

To get this snapshot, we looked at the Alexa Top 50 websites for each country and analyzed how much code was fetched and executed by those sites on July 10, 2018. We analyzed the type of code, where it came from, how many of the sites used or connected to sites that used server software that was vulnerable to compromise by cyberattackers, and more.

The overall conclusion remains the same: It pays to have a healthy distrust of even the most popular, trusted websites on the Internet.



THE RISKS OF THE WEB

Risks Associated with the Use of “Known Bad” Categories

Many companies use website categorization services offered by security technology vendors that assign individual websites to general categories, such as “Business and Economy,” “News and Media,” or “Shopping.” That way, the companies can deny or manage user access to sites in categories with objectionable or productivity-sapping content, such as “Adult and Pornography” or “Gambling.” These website categorization services have some utility in keeping employees from falling victim to cyberattacks, as almost every site in these categories meets our criteria for the “risky” designation. But sites that are categorized as “Malware” (obviously), “Parked Sites” (sites that have been registered, but have not yet been created), or “Uncategorized” (typically, new sites that have not yet been categorized) can also be risky. Because website categorization services may or may not have deemed certain categories to be risky, users and companies are potentially left vulnerable.

In our snapshot update, we found that the popularity of risky categories differed significantly between the six countries. For example, the UK and France had the most porn sites among their Alexa Top 50, with seven and six, respectively; while Japan, Singapore, and the U.S. had just three.

Note that sites in more benign-sounding categories are not safe by definition. For example, we revealed in our 2017 State of the Web report that 49 percent of “News and Media” websites in the Alexa Top 100,000 sites met our criteria for risky.

Risks Associated with Background Websites

In our State of the Web 2017 report, we revealed that whenever a user visits a website, that site calls an average of 25 background sites to fetch various types of content, such as the latest viral video from a content delivery network (CDN) server or ads from an ad-delivery network. So, today more than ever, when a user clicks on a web link to open a website, they are really opening not just a single website, but at least 25 websites at one time.If any of these background sites are themselves risky, they could be used by cyberattackers to compromise the site being visited.

Risks Associated with Use of Active Content

Active content is software that web developers use to make websites dynamic and personalized. By using JavaScript and Flash, active content allows stock tickers to continuously update, for example, and animated images, streaming video and audio, maps, and even drop-down boxes to function.

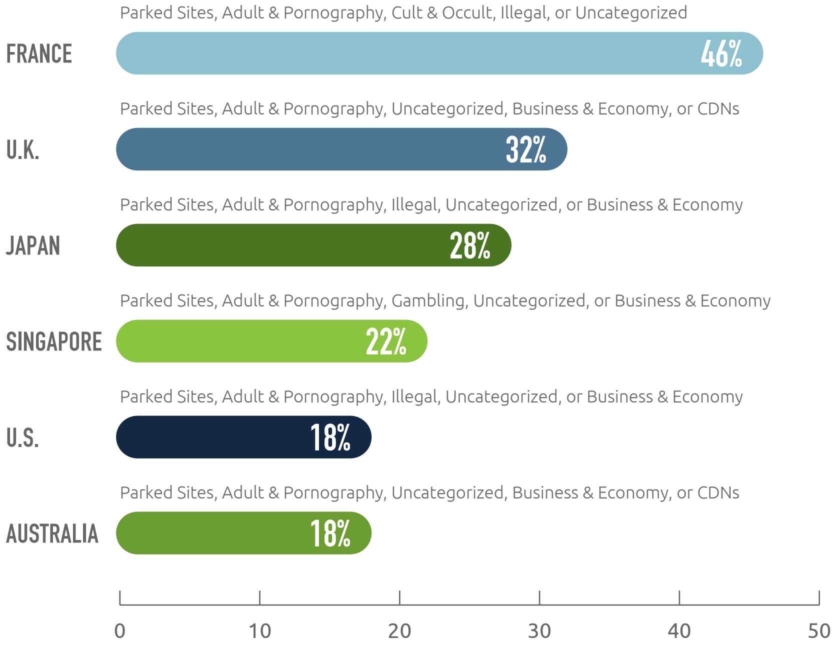
Unfortunately, active content also deprives website operators of control when it comes to securing their sites. Cyberattackers often use active content delivered from background sites to surreptitiously deliver malware, ransomware, and other malicious payloads. There have been a number of recent breaches in which a background site was breached and a visit to a top-ranked, popular website resulted in malware being downloaded onto a user's device, starting a serious organizational infection, credential theft, or data breach.

Our snapshot update found that the percentage of Alexa Top 50 sites that were distributing active content from risky background sites ranged from nearly 50 percent in France to less than 20 percent in Australia.

The fact that these risky websites are providing potentially malevolent active content in the background, unbeknownst to most users and beyond the control of the owner of the website the user visited, should be of great concern to organizations everywhere. All it takes is for one user to visit a popular website and click on one source of contaminated active content, and your organization is infected—and susceptible to a wide range of possible cyberattacks or data breaches.

TOP 50 MOST POPULAR WEBSITES BY COUNTRY

% Serving Active Code from Risky "Background Sites"

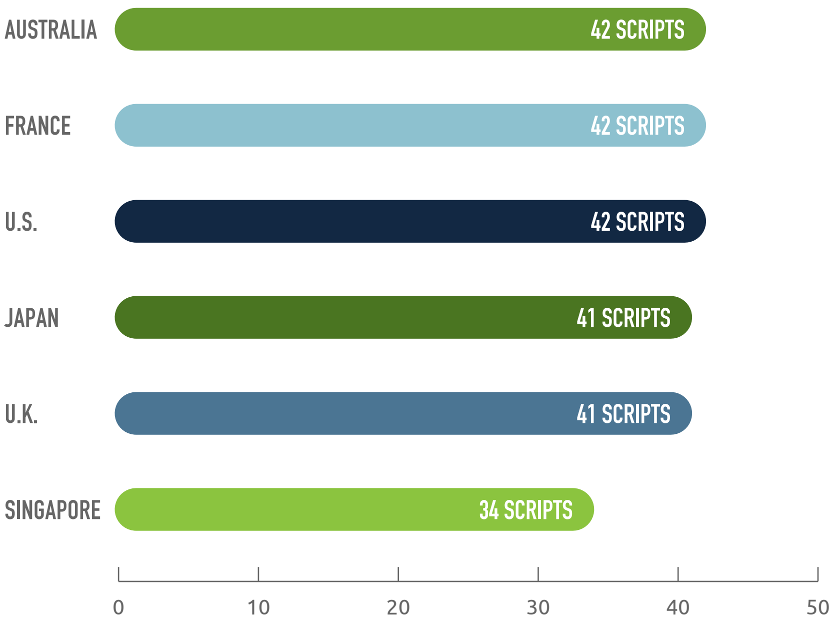


Risks Associated with Use of Scripts

Developers use scripts in many legitimate ways to enhance the user's experience of their websites. But attackers can also use those same scripting capabilities for IFrame redirects and malvertising links to compromise web browsers.

TOP 50 MOST POPULAR WEBSITES BY COUNTRY

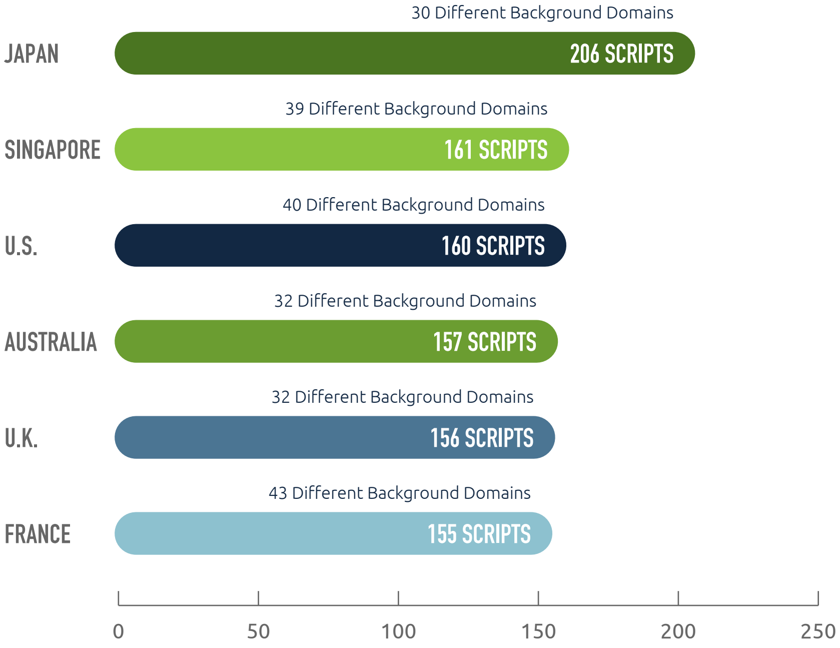
Average # of Scripts Executed per Website



The threat risk increases as the number of scripts delivered from background sites increases.

TOP 50 MOST POPULAR WEBSITES BY COUNTRY

Website with Highest # of Scripts Executed from Background Domains

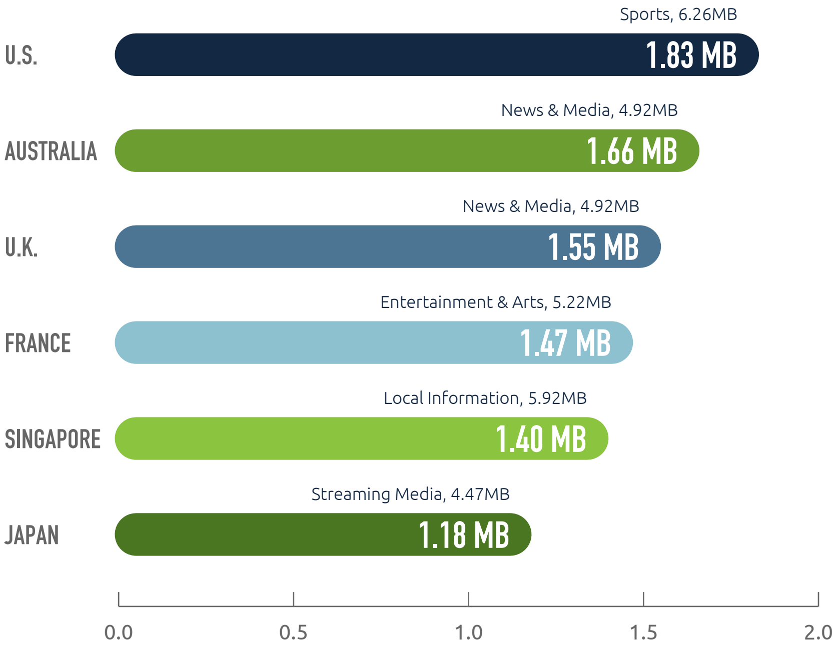


Risks Associated with Downloaded Code

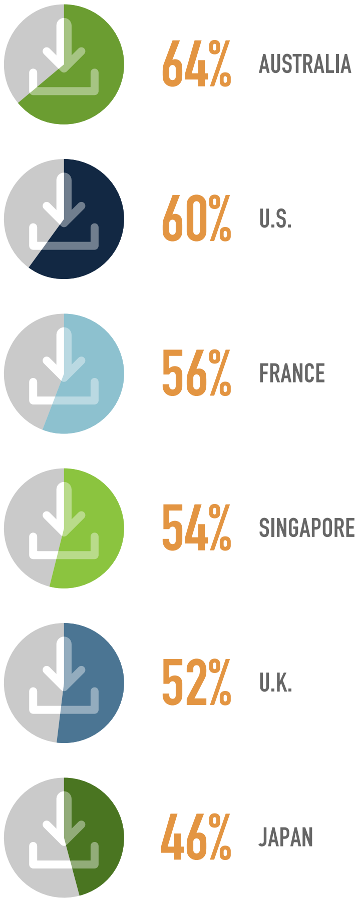
The more active code a site downloads, the greater the risk. Here is a look at the average payload of code downloaded from the Alexa Top 50 sites in each country analyzed, as well as the category of the popular website that downloaded the most code for that nation, and the amount of code the website downloaded.

TOP 50 MOST POPULAR WEBSITES BY COUNTRY

Average Amount of Code Downloaded while Web Browsing



The following pie charts illustrate the percentage of websites downloading to and executing more than 1MB of code on a user's on-device web browser. Australia and the United States are the biggest offenders of website code downloads, while Japanese websites download significantly less code to a user's web browser.



Risk Associated with Use of Vulnerable Web Software

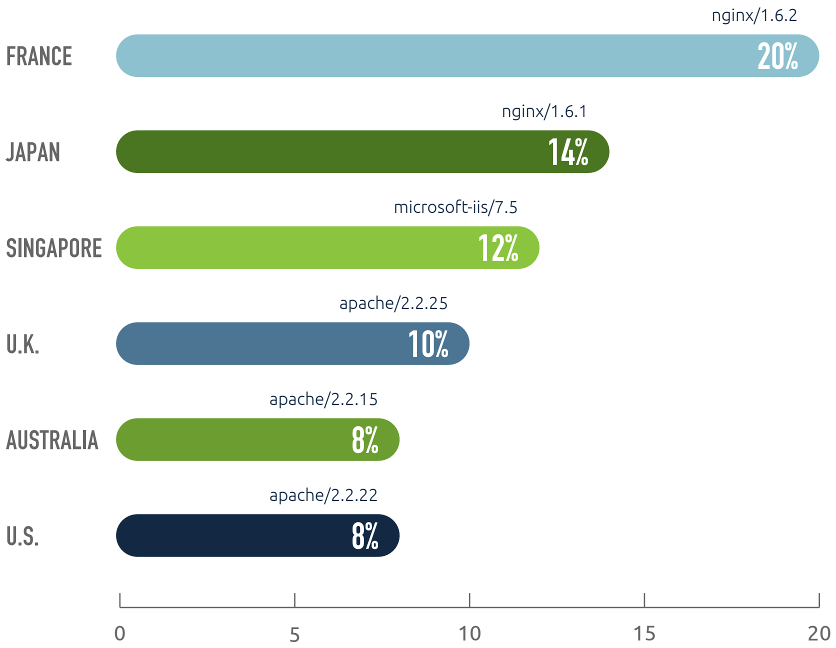
Many of the world's most popular websites run on back-end web servers that are outdated, including some that have not been updated for years or even decades. This leaves those websites extremely vulnerable to web-borne malware, exposing site visitors to possible infections, incursions, or breaches. Use of outdated server software also threatens any site to which it serves as a "background website." Simply put, the older the software, the higher the risk. We identified the software versions being used by the Alexa Top 50 sites in each country by fingerprinting each site against the National Vulnerability Database. A site was marked as "vulnerable" if either it or one of its "background sites" was running vulnerable software. Vulnerable software in this case includes aging software technologies, many of which have been repeatedly compromised over the years or have reached the end of mainstream support—including updates and patches—from their developers.

According to Menlo Security Labs' analysis of data collected from our customers around the world, 7.6 percent of web domains found to be delivering malware or providing safe haven for phishing operations were hosted on vulnerable servers, such as running outdated versions of Apache, nginx, Microsoft IIS, Drupal, and more.

The following chart shows the percentage of Alexa Top 50 sites in each country that used vulnerable web server software, or connected to a background site that did. The chart also lists the most frequently used type of vulnerable software being run in that country.

TOP 50 MOST POPULAR WEBSITES BY COUNTRY

% Running Vulnerable Versions of Web Software



Note that Microsoft IIS version 7.5, which is prominently run on 12 percent of the most popular websites in Singapore and is also the oldest vulnerable back-end software run on websites in Australia, was released in 2009, almost a decade ago. And, the oldest back-end web server software being operated on a top 50 website in the U.S.—PHP version 5.2.3—was released in 2007, *more than* a decade ago.

CONCLUSIONS

Our mid-year drill-down into the relative risk postures of six major countries reinforces what we found last year: The web remains a dangerous place for users to work and play. Strong precautions are needed to ensure that users, their devices, and the networks, apps, and clouds used by organizations aren’t infected and infiltrated by attackers.

Active content downloads and scripts running in the background will continue to be essential to providing a great, dynamic web experience, but there is no excuse for popular websites to use vulnerable server software. Doing so creates a clear and present danger to the sites’ visitors and to the websites to which it serves background content.

So, think about the risk every time a user in your organization—an employee, a contractor, even a visitor—visits an Alexa Top 50 site. According to this study, their browser is likely to be exposed to 160 scripts, and nearly 50 percent of the active content on that Alexa Top 50 site would have been sent from background websites in “risky” categories. There’s a smaller, but still significant, chance the site will be running web server software that is known to be vulnerable to compromise.

If this concerns you, and makes you think twice about your existing security solutions, isn't it time you began looking for a new approach to web and email security?

2300 Geng Rd Ste. 200
Palo Alto, CA 94303
Tel: 650 614 1795
info@menlosecurity.com

menlosecurity.com