Inspired eLearning July Newsletter

NEW WORKING SECURELY FROM HOME COURSE

This new course teaches employees how working outside of an organization's secured facilities can expose a remote worker and his/her workplace's assets to additional cyber threats. This course will provide best practices for working securely from home and help defend against these threats.

LEARN MORE

COMMON TYPES OF MALWARE AND PREVENTION

In 2019, Kaspersky's web antivirus platform identified more than 24 million "unique malicious objects". This number will only continue to increase in 2020, and with it, our need to learn more about potential threats. This blog will define some of the most common types of malware and how to prevent them.

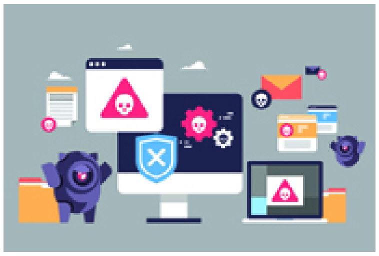
READ BLOG

99% of Websites at Risk of Attack Via JavaScript Plug-ins

Third-party programs such as Google Analytics and other plug-ins expose websites to Magecart, form jacking, cross-site scripting, and credit-card skimming, and other attacks, new research shows.

A report released today by Tala Security found that these kind of attacks exploit vulnerable JavaScript integrations that run on some 99% of the world's websites. And while 30% of the websites analyzed implemented new security policies – a 10% increase over 2019 – only 1.1%

of websites were found to have effective security in place, an 11% decline from 2019.



"This indicates that while deployment volume went up, effectiveness declined steeply," says Aanand Krishnan, founder and CEO of Tala Security. "The attackers have the upper hand largely because we are not playing effective defense."

Krishnan adds that without effective policy controls, every piece of code running on most websites can modify, steal, or leak information via client-side attacks executed by JavaScript. These attacks are powerful for hackers because once they attack a third-party tool, they can exploit it on any other website where that tool gets deployed.

"In many cases, this data leakage takes place via whitelisted, legitimate applications, without the website owner's knowledge," Krishnan says. "Our report found that data risk is everywhere and effective controls are rarely applied. But just like the security business fixed network security issues with SSL and TLS, we'll do the same with these third-party integrations by deploying better security controls and working with the industry to develop standards-based solutions."

The report, which tracked the security posture of the Alexa top 1,000 websites, found that the average website includes content from 32 different third-party JavaScript programs, up slightly from 2019.

Of great concern: despite increasing numbers of high-profile breaches, the forms used to complete orders on 92% of websites expose data to an average of 17 domains.

"So this means that data doesn't just get exposed on the main website, the shipper's site, or at the payment clearing house, an average of 15 other domains are exposed, which dramatically exposes risk," says Mark Bermingham, vice president of marketing at Tala. "We've seen cases where the hackers have changed code and even taken down entire websites."

The nature of the threat underscores that third-party JavaScript vendors are open to attack, he says, and these same third-party vendors have been very aggressive collecting user data - something that should concern major e-commerce companies because they are now subject to the General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA) and could get hit with a hefty fine.

Hank Schless, senior manager of security solutions at Lookout, notes that the data shows that opening a company's platforms to third parties introduces more risk, especially in terms of exposure to GDPR and CCPA.

"With privacy being the main focus these days, security teams need to properly evaluate the security posture of any third-party integrator before giving them access to customer data," Schless says. "On the flip side, integrators understand that they need proper security controls in place if they want to succeed in such a climate."

Thomas Hatch, co-founder and CTO of SaltStack, says he's concerned about the reported declines in effective security management. "When we see declines of this nature, it highlights that there are fundamental issues with how cybersecurity is being managed today," Hatch says. "These types of attacks and vulnerabilities are not new, yet they are more present than ever. If we want to overcome these issues we need to rethink how we deploy our applications, rethink how we secure our applications, and rethink how we manage, contribute to, and support the vast array of open source projects that the modern Web is built on top of."

This article was originally posted by Dark Reading. Read the full article here.

Coronavirus scams: How to protect yourself from identity theft during COVID-19

The ongoing spread of the coronavirus continues to create new crops of hackers, targeting people who are working from home, still awaiting stimulus or benefit checks, or just trying to stay healthy at home or on a socially distanced vacation. Scammers are even pretending to be government officials, so it's important to be on guard against online misinformation in your inbox and in your text messages.

A March release from the FBI's Internet Crime Complaint Center offers some solid advice on what to watch out for.

"Scammers are leveraging the COVID-19 pandemic to steal your money, your personal information, or both. Don't let them," the FBI said. "Protect yourself and do your research before clicking on links purporting to provide information on the virus; donating to a charity online or through social media; contributing to a crowdfunding campaign; purchasing products online; or giving up your personal information in order to receive money or other benefits."

An April report from Next Caller found that about 32% of 1,000 surveyed Americans believe they had already been targeted by fraud or scams related to COVID-19. Next Caller also found that fraud concern is increasingly on consumers' minds, with 52% of Americans saying they're more worried about being victimized by fraud than normal. 44% of respondents said they've noticed an increase in phone calls and texts from unknown numbers, and emails from unknown sources.

Meanwhile, researchers at Trustwave found that ransomware attacks amounted to 18% of overall breach incidents observed in 2019, up from 4% in 2018. Researchers also found the amount of malware in traditional spam email declined to 0.2% from 6% the previous year, as attackers look for more effective infection vehicles. The biggest rise was in social engineering attacks, like phishing. In 2018, Trustwave analysts found 33% of all data breach incidents were the result of phishing or social engineering attacks. In 2019, that number rose to half.

Here phishy, phishy

Unsolicited emails that prompt you to click on an attachment should always raise a red flag when you're checking your inbox. But these classic email phishing scams still lure unsuspecting people into downloading malicious items and giving up their login information every day.

When news first broke back in March that the government would issue payments of up to $1,200 in coronavirus relief to US taxpayers, the FBI issued a warning to be on alert for attackers masquerading as the agency and asking for personal information supposedly in order to receive your check. "While talk of economic stimulus checks has been in the news cycle, government agencies are not sending unsolicited emails seeking your private information in order to send you money," the Bureau said.

As the nation waits to see if Congress will approve a second stimulus payment this month, the US Federal Trade Commission warned consumers about scammers pretending to be government officials in order to get victims' bank account information. If people share that information, the scammers claim in an email, they'll get money from a COVID-19 "Global Empowerment Fund."

Calling it a scam, the FTC warned that there's no money or fund. The agency urged recipients not to respond to messages like these, and to instead report them to the FTC at ftc.gov/complaint.

Among other steps to create a safer inbox, the US Cybersecurity and Infrastructure Security Agency recommends turning off your email client's option to automatically download attachments. Not all email clients offer this and each client is different, but some do. Because social engineering attacks -- scams designed to persuade you to hand over your sensitive information by targeting specific information about you -- have become increasingly common in times of crisis, it's also a good idea to read up on how to identify these security risks.

And remember, never reveal personal or financial information in an email, or respond to requests for it.

Mobile malware

If you're looking to track COVID-19 news with an app, it's a good idea to keep an eye out for malware traps. In March, a malicious Android app called CovidLock claimed to help users chart the spread of the virus. Instead, it led to a slew of Android phones being locked and held for ransom by hackers.

Researchers at Check Point discovered 16 malicious apps posing as legitimate coronavirus-related apps in a bid to steal users' sensitive data or generate fraudulent revenues from freemium services. Among them, a notorious strain of banking trojan known as Cerberus, which can log all of your keystrokes and let someone command your device remotely.

Meanwhile, Reason Labs recently discovered hackers were using coronavirus-tracking map sites to inject malware into people's browsers. As reported by MarketWatch, coronavirus-related website name registrations are 50% more likely to be from malicious actors.

As Android Authority points out, setting a password on your phone can help protect you from a lock-out attack if you're using Android Nougat. It's also a good idea to stick to the Google Play store for any coronavirus-related apps to better your odds of installing benign software. None of the 16 malicious apps spotted by Check Point were found on an official app store, but were offered on new coronavirus-related websites which the researchers believe were specifically set up to lure new users.

How common are these new coronavirus-related domains? Check Point said it tallied more than 30,103 new coronavirus-related site registrations. Some 131 of those were considered malicious and 2,777 were "suspicious and under investigation."

Charity checkout

During a disease outbreak or natural disaster, the better angels of our nature compel us to open our wallets to the less fortunate through charitable giving and donation. Before we follow that impulse, we need to take an extra few moments to make sure the charity isn't a funnel into the bank account of a predatory impersonator.

Taking a few moments to review the FTC's Charity Scams page could save you the heartbreak of an emptied checking account. You can also improve your odds by searching sites such as guidestar.org and give.org for the name of your charity before donating.

Legit sources
Random Facebook groups offering supposed home cures for COVID-19, long Twitter threads from self-appointed health experts and cleverly designed websites -- there are dozens of ways misinformation can lure unsuspecting victims into a position of vulnerability. While it can be hard to sort the solid information from the scam-baiting, here are a couple of ways:

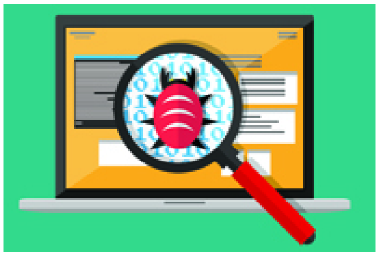
- By clicking the "about" section of a Facebook group, you can see whether that group has changed its name multiple times to reflect new national crises -- a sure sign that the group is trawling for an audience rather than promoting reliable news.
- Keep an eye on official sources on Twitter, including the accounts of trusted news sites and their news reporters, and avoiding political operatives where possible.
- If a site claims to be an official government publication, check the URL to see if it ends in .gov.

This article was originally posted by cnet.com. Read the full article **here**.

Critical SAP Bug Allows Full Enterprise System Takeover

A critical vulnerability, carrying a severity score of 10 out of 10 on the CvSS bug-severity scale, has been disclosed for SAP customers.

SAP’s widely deployed collection of enterprise resource planning (ERP) software is used to manage their financials, logistics, customer-facing organizations, human resources and other business areas. As such, the systems contain plenty of sensitive information.



According to an alert from the Department of Homeland Security, successful exploitation of the bug opens the door for attackers to read and modify financial records; change banking details; read personal identifiable information (PII); administer purchasing processes; sabotage or disrupt operations; achieve operating system command execution; and delete or modify traces, logs and other files.

The bug (CVE-2020-6287) has been named RECON by the Onapsis Research Labs researchers that found it, and it affects more than 40,000 SAP customers, they noted. SAP delivered a patch for the issue on Tuesday as part of its July 2020 Security Note.

“It stands for Remotely Exploitable Code On NetWeaver,” Mariano Nunez, CEO of Onapsis, told Threatpost. “This vulnerability resides inside SAP NetWeaver Java versions 7.30 to 7.50 (the latest version as of [our analysis publication]. All Support Packages tested to date were vulnerable. SAP NetWeaver is the base layer for several SAP products and solutions.”

An attacker leveraging this vulnerability will have unrestricted access to critical business information and processes in a variety of different scenarios, according to the firm.

NetWeaver Java Woes

The bug affects a default component present in every SAP application running the SAP NetWeaver Java technology stack, according to Onapsis. This technical component is used in many SAP business solutions, such as SAP S/4HANA, SAP SCM, SAP CRM, SAP CRM, SAP Enterprise Portal, SAP Solution Manager (SolMan) and many others, the researchers said.

According to DHS, the vulnerability is introduced due to the lack of authentication in a web component of the SAP NetWeaver AS for Java, allowing for several high-privileged activities on the SAP system. A remote, unauthenticated attacker can exploit this vulnerability through an HTTP interface, which is typically exposed to end users and, in many cases, exposed to the internet.

“If successfully exploited, a remote, unauthenticated attacker can obtain unrestricted access to SAP systems through the creation of high-privileged users and the execution of arbitrary operating system commands with the privileges of the SAP service user account (<sid>adm), which has unrestricted access to the SAP database and is able to perform application maintenance activities, such as shutting down federated SAP applications,” according to the alert.

Impact

Put another way, an unauthenticated attacker could create a new SAP user with maximum privileges, bypassing all access and authorization controls (such as segregation of duties, identity management, and governance, risk and compliance solutions) and gaining full control of SAP systems, Nunez said.

“With SAP NetWeaver Java being a fundamental base layer for several SAP products, the specific impact would vary depending on the affected system,” according to Onapsis, in a technical analysis released on Tuesday. “In particular, there are different SAP solutions running on top of NetWeaver Java which share a common particularity: they are hyper-connected through APIs and interfaces. In other words, these applications are attached to other systems, both internal and external, usually leveraging high-privileged trust relationships.”

And while this is bad enough, the RECON vulnerability’s risk increases when the affected solutions are exposed to the internet, to connect companies with business partners, employees and customers. These systems – Onapsis estimates there are at least 2,500 of them – have an increased likelihood of remote attacks, researchers said. Out of those vulnerable installations, 33 percent are in North America, 29 percent are in Europe and 27 percent are in Asia-Pacific.

“Because of the type of unrestricted access an attacker would obtain by exploiting unpatched systems, this vulnerability also may constitute a deficiency in an enterprise’s IT controls for regulatory mandates—potentially impacting financial (Sarbanes-Oxley) and privacy (GDPR) compliance,” according to the writeup.

Patch Available

SAP's patch should be applied immediately, researchers recommended. While for now there is no indication that this has been exploited yet, Nunez told Threatpost that SAP customers should be on high alert now that the vulnerability has been announced and the DHS has sent out its US CERT alert warning.

"Now that the vulnerability and patch have been released, skilled hackers can quickly develop exploit code," he said. "Because there are many vulnerable Internet exposed SAP systems, the complexity of the attack is significantly less."

That said, because of the complexity of mission-critical applications and limited maintenance windows, organizations are often challenged to rapidly apply SAP security notes, the Onapsis team acknowledged.

"It's difficult to patch mission-critical applications such as those from SAP because they need to be constantly available," Nunez told Threatpost. "Testing can take a long time depending upon complexity and customization of the apps. Also, there are limited maintenance windows available to apply the patches."

He added, "For SAP customers, critical vulnerabilities such as RECON highlight the need to protect mission-critical applications, by extending existing cybersecurity and compliance programs to ensure these applications are no longer in a blind spot. These systems are the lifeblood of the business and under the scope of strict compliance requirements, so there is simply nothing more important to secure."

For the full article and more tips, check out the original posting **here**.

Product Updates

We have exciting new updates to share! Click below to learn more about what Inspired eLearning is doing to better our product experience for our customers.

LEARN MORE