Drive-By Skimming & Supply Chain Attacks Can Affect Your Website

cyber security risk management

Summary: Are you protected against drive-by skimming and supply chain website attacks? These can be hard to detect even with the usual cybersecurity measures such as firewalls, penetration tests, and security assessments. We explain how these attacks happen and what community financial institutions can do to mitigate the risk of these occurring to them.

Tea has been associated with health for over sixteen centuries. In the year 400, tea consumption for medicinal purposes started gaining popularity. While tea demand in Asia continued, it was not until 1589 that tea was recognized for its health benefits in Europe. Studies on the benefits of tea, especially green tea, imply that it can reduce certain types of cancer, decrease blood pressure, assist with weight control, and kill bacteria and viruses.

Unfortunately, there is no “cyber green tea” available to support the health of your website against attacks. So, you’ve implemented numerous cybersecurity measures to protect your website, including performing periodic penetration tests, vulnerability scans, and security assessments to lessen potential harm to your customers. But what about “drive-by skimming” and “supply chain attacks” on the various third-party applications you include on your website? Community financial institutions (CFIs) that operate chatbots, track customer usage, and measure the success of your digital marketing campaigns, among other tasks use third parties. The stakes have been raised in this area of risk management, so CFIs need to be prepared.

Case in point. Take the notorious “Gocgle Campaign,” in 2019 in which hackers placed hidden skimming code on Google analytics products used by eCommerce companies and other businesses to track online traffic. When customers made payments on those websites over the following year, the skimming code was injected onto the websites via the third-party Google analytics application. The hackers then used their code to inject malware onto the websites, subsequently obtaining customer credit card numbers and additional sensitive information.

Vulnerabilities continue. More and more websites are vulnerable to such attacks. According to a PerimeterX survey of more than 500 security professionals and developers, virtually all said their website employs at least one third-party script, and most said that third-party scripts comprise half or even two-thirds of their website’s content. Do you have these on your website? Possibly. Just consider if you have Google Analytics, which is a third-party script, that allows you to track your website analytics. Some financial institutions, including PCBB, have podcasts with a third-party script that plays the episodes. Or maybe your CRM or other payment services are connected to your website, which are also third-party scripts. So, it is very possible to have at least one on your current website and for valid business reasons.

Half of the respondents said such scripts change four or more times each year, yet, only a quarter of the professionals analyze the security of each change. One-third said they had the ability to detect any modifications made to their website that could potentially cause harm, and nearly half of surveyed security professionals could not confirm whether or not their website had been hacked.

How drive-by skimming and supply chain attacks work

The initial attack wouldn't occur on a CFI's website — rather it would first occur on the browser of a user's laptop, tablet, or phone. The hackers place hidden skimming code into a JavaScript file of the third-party web application, impacting all businesses that use the application on their websites, in a "**drive-by skimming**." When a user opens a website that uses the third-party web application, they inadvertently download the skimming code embedded within the third-party code, which then injects malware onto the website, i.e. a "**supply chain attack**," that can collect sensitive information that the hackers subsequently sell on the dark web.

The hackers have found ways to obscure the skimming code and malware, making it harder for CFIs to detect via conventional cybersecurity measures. Some are able to steal sensitive information on websites for weeks, if not months. Several hackers inject ransomware onto websites, in an effort to demand payment or else they'll release sensitive information to the public.

What CFIs can do to lessen potential harm

Traditional cybersecurity measures don't work well in combating drive-by skimming and supply chain attacks. Why? Firewalls are placed on the front of web applications to detect malicious attempts. Yet, drive-by skimming code is embedded within third-party code that firewalls haven't been designed to detect. Moreover, businesses typically whitelist the JavaScript libraries and code of the third-party web applications they use to keep their functionality.

Then, there are the limitations around penetration tests, vulnerability scanning, and security assessments that are typically conducted either quarterly or annually. Namely, hackers will just wait until after the regularly scheduled events to perform their nefarious acts.

CFIs need to implement continuous third-party JavaScript monitoring, to detect real-time attempts of drive-by skimming and supply chain attacks via user browsers. You can employ client-side solutions that provide security permissions and controls to the JavaScript and codes used by their third-party web applications. Such solutions automatically block all unauthorized script and sketchy code behavior.

Cybercriminals are craftily coming up with new ways to breach cybersecurity protections. Drive-by skimming and supply chain attacks are their latest efforts in this game. CFIs can mitigate these risks if they employ continuous monitoring actions along with traditional cybersecurity measures and stay updated on the latest cyber risks. This game is not over yet though.

PCBB NO LONGER USING LIBOR FOR NEW BUSINESS

As of January 1, 2022, in accordance with Fed guidance, PCBB is no longer entering into LIBOR-based transactions. Fed funds and SOFR are available for both scenario planning and transaction execution. Visit our SOFR Resource Center for more information on this new index.

ECONOMY & RATES

Rates As Of: 01/24/2022 02:26PM (GMT-0700)

Treasury	Yields	MTD Chg	YTD Chg
3M	0.17	0.11	0.11
6M	0.35	0.16	0.16

1Y	0.59	0.20	0.20
2Y	0.98	0.25	0.25
5Y	1.55	0.29	0.29
10Y	1.77	0.26	0.26
30Y	2.11	0.21	0.21

FF Market	**FF Disc**	**IORB**
0.08	0.25	0.15

SOFR	**Prime**	**OBFR**
0.05	3.25	0.07