CASE STUDY

Gartner

COOL
VENDOR
2020™

Obfuscated JavaScript

Delivering Card-Skimming Exploit with Obfuscated JavaScript

In December 2019, Trinity Cyber thwarted a sophisticated attempt to steal credit-card information via an attempted JavaScript exploit. We took six different actions against card-skimming JavaScript that had been served up to both Chrome and iOS Safari browsers. The delivery mechanism was through a legitimate e-commerce site that had been previously and unknowingly compromised. A small piece of code had infected the site with the intention of stealing credit-card information and redirecting it to an attacker's listening web server.

These defensive events were unique because they took place without our client knowing anything was amiss while also preserving the browsing session. These factors enabled us to neutralize the threat surgically without the intended victim noticing anything unusual had happened.

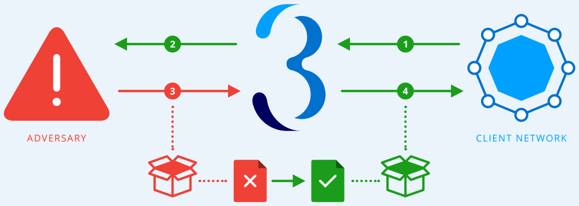
In this instance, our client was exposed to a compromised vendor website while researching WiFi cameras. This employee had no way of knowing their sensitive data was at risk had it not been for Trinity Cyber's advanced threat prevention. Because we neutralized the exploit code instantly, the only work left was for our SOC to dig deeper into the attack, verify the presence of the malicious JavaScript on the site, and alert the owner of the site.

Upon inspection, our teams found this exploit was designed to POST back credit-card information when someone tried to buy a WiFi camera from the vendor site. This was accomplished using corrupted Google Analytics, which processed and served web pages—commonly known as "obfuscated script"—that had been heavily modified to host malicious content that could skim sensitive information from every tab in a victim's browser. The exploit was very sophisticated. It was not a first-stage JavaScript payload; it went through a legitimate Google Analytics decoding process before it was delivered to the browser, which is why the initial scan for malicious code, as verified by several public URL-scanning websites, came back as clean. In many ways, what we detected (and neutralized in flight) was a second-stage exploit, meaning one designed to survive even after a legitimate service such as Google Analytics had done its job.

Identifying and Neutralizing a Well-Hidden Threat

With the infected payload hosted on a "spoofing" site that tried to mimic the legitimate Google Analytics, this threat possessed an additional layer of sophistication. But despite these details, the key takeaway is not what was discovered about the exploit afterward, but that Trinity Cyber defeated the malicious JavaScript in every network session where it was encountered. Leveraging a unique defense-in-the-middle position and using a capability designed to root out various types of obfuscated JavaScript, this well-hidden threat was identified and neutralized without disrupting or alerting the intended victim.

Unlike typical cybersecurity solutions, we didn't identify the threat by its signature, but by its characteristics—like stopping a burglar before he even has a chance to enter the building, rather than waiting for him to trip an alarm. Our advanced technology finds and removes or alters malicious JavaScript obfuscation regardless of the source IP or the domain from which it is served.



sales@trinitycyber.com • (240) 842-9900 • trinitycyber.com

Trinity Cyber was named a Cool Vendor in Gartner's Cool Vendors in Network and Endpoint Security, Mark Harris, Rob Smith, et al., 30 September 2020.

The GARTNER COOL VENDOR badge is a trademark and service mark of Gartner, Inc., and/or its affiliates, and is used herein with permission. All rights reserved. Gartner does not endorse any vendor, product or service depicted in its research publications, and does not advise technology users to select only those vendors with the highest ratings or other designation. Gartner research publications consist of the opinions of Gartner's Research & Advisory organization and should not be construed as statements of fact. Gartner disclaims all warranties, expressed or implied, with respect to this research, including any warranties of merchantability or fitness for a particular purpose.

Trinity Cyber