Trinity Cyber

THREAT MITIGATION AND PREVENTION CASE STUDY:

Obfuscated JavaScript

JavaScript Skimmers Exploit E-Commerce Websites

JavaScript is a fundamental Internet technology used in the development of interactive web pages and present on approximately 95% of all websites. E-commerce websites are common targets for cybercriminals whose attacks implant "skimmers" deep inside JavaScript to intercept customer credit card information. Businesses regardless of size or industry are susceptible; as an example, British Airways was the victim of this type of attack, which resulted in the exfiltration of half a million credit card numbers and shattered public trust and confidence.[1]

From Legitimate Vendor to Financial Attacker

Recently, Trinity Cyber's revolutionary Trinity Cyber Engine technology defeated a sophisticated attempt to steal credit card information from a legitimate e-commerce site that was unknowingly compromised. Attackers infected the e-commerce site with malicious JavaScript with the intent of stealing users' credit card information and redirecting it to an attacker's "listening" web server. While conducting legitimate research on the site, a user was unknowingly exposed, and sensitive data was put at risk. Although this malware successfully evaded detection by the customer's other deployed security technologies, once the Trinity Cyber Engine technology was deployed, it quickly identified and executed six different actions to immediately neutralize the card-skimming JavaScript attack that targeted both Chrome and iOS Safari browsers of unsuspecting visitors to the site. The remediation of this attack occurred automatically, without the user's knowledge, so the interactive experience with the site was preserved and business transactions could continue.

Defeating a Multistage Exploit

The malicious JavaScript used in this attack was very advanced and designed to snatch credit-card information when users attempted to purchase products from the vendor's infected 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 capable of "skimming" sensitive information from every tab in a victim's browser. This exploit was not simply a first-stage JavaScript payload; instead, it went through a legitimate Google Analytics decoding process before being delivered to the user's browser. This exploit was designed to survive and remain effective even after completing Google Analytics security processes. Because the infected payload was hosted on a "spoofing" site that tried to mimic legitimate Google Analytics, this sophisticated threat was missed by traditional security technologies.

KEY TAKEAWAYS

- **Identified and stopped a multistage threat**
- **Delivered protection missed by other technologies in place**
- **Protected credit card information of unsuspecting users**
- **Happy customer, frustrated adversary**

Malicious JavaScript Is No Match for the Powerful Trinity Cyber Engine

The revolutionary Trinity Cyber Engine technology automatically *identified and defeated the malicious JavaScript* in every network session. The Engine is tuned to defeat attacker tactics, techniques and procedures (TTPs) at multiple stages to protect networks against entire classes of malware, ransomware, command and control (C2), remote exploits, drive-by downloads and in-the-wild malicious threats. Its exemplary performance unites near-zero false positive rate accuracy and depth (providing rich contextual application layer fidelity) with automated preventive controls that are executed in less than a millisecond. The Trinity Cyber Engine discovers and neutralizes threats commonly missed by traditional detect-and-respond systems and is unique in its ability to deeply inspect full session Internet traffic —at line rate speed and in both directions—to expose and mitigate threat content inline.

Want to learn more about how you can benefit from this powerful solution? Reach out to Trinity Cyber at info@trinitycyber.com for more information.

1. "JavaScript skimmers: An evolving and dangerous threat," Fabian Libeau, ComputerWeekly.com, April 3, 2020.

Gartner COOL VENDOR 2020