Hackers abuse Google Apps Script to steal credit cards, bypass CSP

By Sergiu Gatlan

Published: 2021-02-18 · Archived: 2026-04-05 14:01:32 UTC

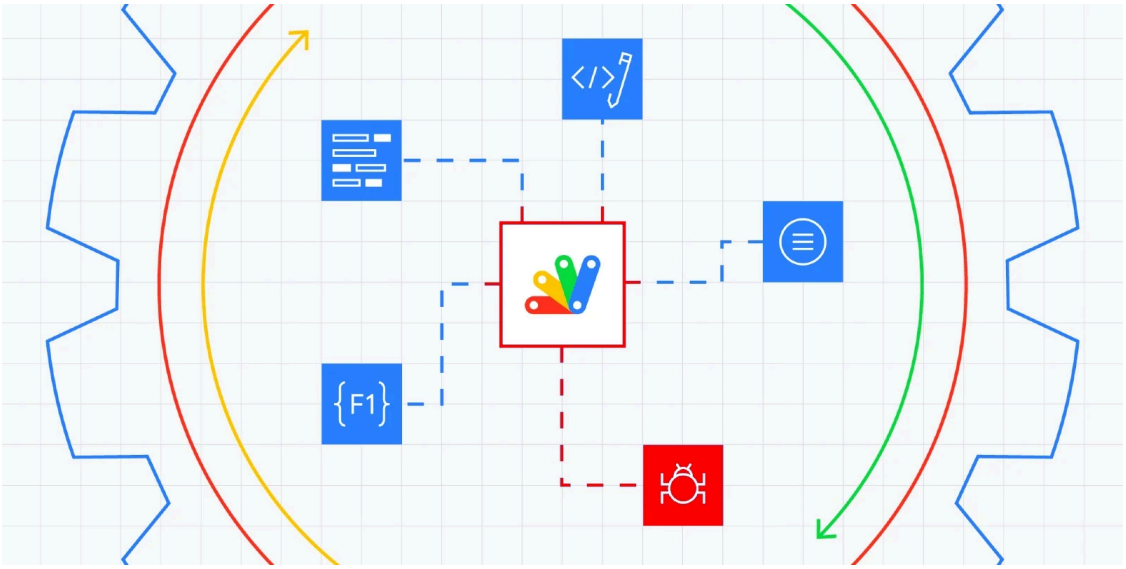
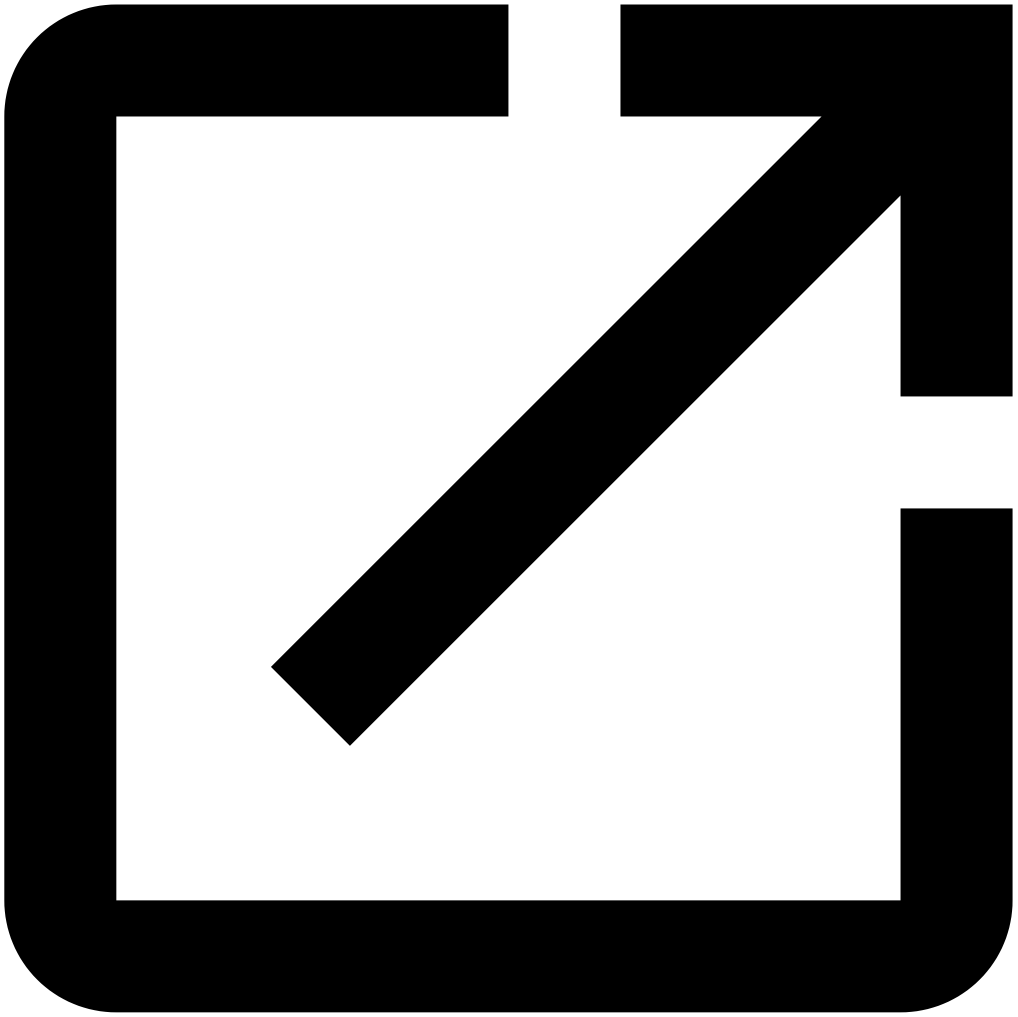


Image: Google

Attackers are abusing Google's Apps Script business application development platform to steal credit card information submitted by customers of e-commerce websites while shopping online.

They are using the *script.google.com* domain to successfully hide their malicious activity from malware scan engines and bypass Content Security Policy (CSP) controls.


DIE LINKE.
0:00



They take advantage of the fact that online stores would consider Google's Apps Script domain as trusted and potentially whitelisting all Google subdomains in their sites' CSP configuration (a security standard for blocking untrusted code execution in web apps).

Credit card skimmers (Magecart scripts or payment card skimmers) are JavaScript-based scripts injected by cybercrime groups known as Magecart groups inject into hacked online stores as part of web skimming (also known as e-skimming) attacks.

Once deployed, the scripts allow them to harvest the payment, and personal info submitted by the hacked shops' customers and collect it on servers under their control.

Google Apps Script domain used as exfiltration endpoint

This new payment info theft tactic was discovered by security researcher Eric Brandel while analyzing Early Breach Detection data provided by Sansec, a cybersecurity company focused on fighting digital skimming.

As he discovered, the malicious and obfuscated skimmer script injected by the attackers in e-commerce sites intercepted payment info submitted by users.

All the payment info stolen from the compromised online shop was sent as base64 encoded JSON data to a Google Apps Script custom app, using script[.]google[.]com as an exfiltration endpoint.

After reaching the Google Apps Script endpoint, the data was forwarded to another server — Israel-based site analit[.]tech — controlled by the attackers.

"The malware domain analit[.]tech was registered on the same day as previously discovered malware domains hotjar[.]host and pixelm[.]tech, who are also hosted on the same network," Sansec said.

Error displayed when accessing attackers' custom Google Apps Script app (*Sansec*)

This isn't the first time this Google service has been abused, with the FIN7 cybercriminal group using it in the past together with Google Sheets and Google Forms services for malware command-and-control.

Since mid-2015, FIN7 (aka Carbanak or Cobalt) has targeted banks and the point-of-sale (PoS) terminals EU and US companies using the Carbanak backdoor.

"This new threat shows that merely protecting web stores from talking to untrusted domains is not sufficient," Sansec added.

"E-commerce managers need to ensure that attackers cannot inject unauthorized code in the first place. Server-side malware and vulnerability monitoring is essential in any modern security policy."

Google Analytics also abused to steal credit cards

Other Google services were also abused in Magecart attacks, with the Google Analytics platform being used by attackers to steal payment info from several dozen online stores.

What made those attacks worse was that by abusing the Google Analytics API, the threat actors could also circumvent CSP, seeing that web stores whitelist Google's web analytics service in their CSP configuration for tracking visitors.

As Sansec and PerimeterX found at the time, instead of blocking injection-based attacks, allowing Google Analytics scripts enabled the attackers to utilize them for stealing and exfiltrating data.

This was done using a web skimmer script specifically designed to encode stolen data and send it to the attacker's Google Analytics dashboard in encrypted form.

Based on stats provided by BuiltWith, more than 28 million sites are currently using Google's GA web analytics services, with 17,000 of the websites reachable via an HTTPArchive scan in March 2020 whitelisting the google-analytics.com domain according to PerimeterX statistics.

"Typically, a digital skimmer (aka Magecart) runs on dodgy servers in tax havens, and its location reveals its nefarious intent," Sansec explained at the time.

"But when a skimming campaign runs entirely on trusted Google servers, very few security systems will flag it as 'suspicious.' And more importantly, popular countermeasures like Content-Security-Policy (CSP) will not work when a site administrator trusts Google."

"CSP was invented to limit the execution of untrusted code. But since pretty much everybody trusts Google, the model is flawed," Sansec CEO and founder Willem de Groot also told BleepingComputer.
