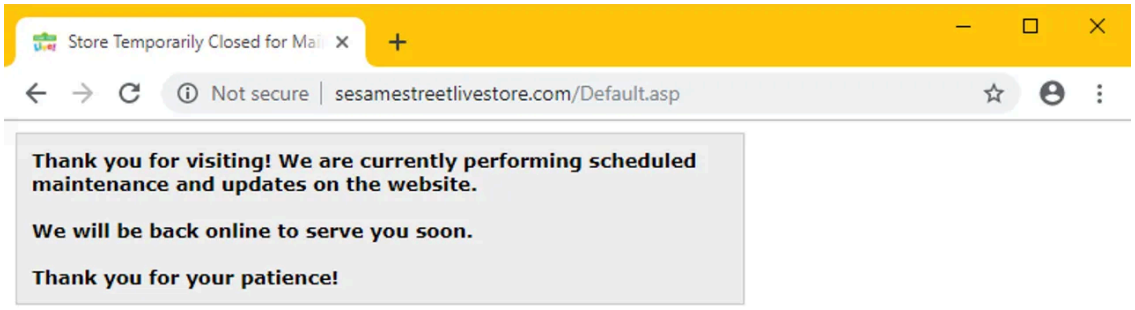
Hackers breach Volusion and start collecting card details from thousands of sites

By Written by Catalin Cimpanu, ContributorContributor Oct. 8, 2019 at 12:38 p.m. PT

Archived: 2026-04-05 14:24:44 UTC



Hackers have breached the infrastructure of Volusion, a provider of cloud-hosted online stores, and are delivering malicious code that records and steals payment card details entered by users in online forms.

See als

-

More than 6,500 stores are impacted, but the number could be even higher. In a press release published last month, Volusion claimed it had more than 20,000 customers.

The most notable compromise is the Sesame Street Live online store, which has been taken down earlier today after another journalist reached out.

At the time of writing, the malicious code is still on Volusion's servers and is still being delivered to all of the company's client stores.

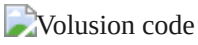
Volusion has not returned emails or phone calls from this reporter, nor from security researchers from Check Point and Trend Micro. Cyber-security firm RiskIQ is also tracking the incident and confirmed the hack to ZDNet.

> @Volusion Hi! We sent you a Direct Message. Looking forward to your reply.
>
> — Trend Micro Research (@TrendMicroRSRCH) October 7, 2019

Compromised Google Cloud infrastructure

The incident took place this week after hackers gained access to Volusion's Google Cloud infrastructure, where they modified a JavaScript file and included malicious code that logs card details entered in online forms.

Volusion is a known Google Cloud Platform customers.


Volusion code

The compromised file is hosted at *https://storage.googleapis.com/volusionapi/resources.js* [copy], and is loaded on Volusion-based online stores via the */a/j/vnav.js* file.

For users interested in the inner workings of this code, Check Point security researcher Marcel Afrahim published an analysis on Medium earlier today.

Classic Magecart supply-chain attack

The incident is what cyber-security experts call a Magecart attack or web card skimming, where crooks steal payment card details from online shops, rather than ATMs. These types of hacks have been happening for years, but they've intensified over the past two.

In a report published last week, RiskIQ said Magecart attacks have reached a peak, with card-stealing scripts (called skimmers) being spotted on more than 18,000 websites over the past few months.

Most Magecart attacks take place when hackers use vulnerabilities in self-hosted stores to plant skimmer code on outdated online shops.

But, sometimes, hackers also manage to breach cloud-based platforms -- like Volusion -- or companies that provide widgets, analytics, ads, or other secondary services to online stores.

Something like the latter case happened in May when hackers breached the cloud infrastructure for seven companies that provided services to online stores -- namely Alpaca Forms, Picreel, AppLixir, RYVIU, OmniKick, eGain, and AdMaxim.

The May incidents were traced to those companies' misconfigured cloud-hosting accounts, which allowed hackers to modify existing files without permission.

Similar attacks followed over the summer, and in most, hackers targeted misconfigured Amazon Web Services accounts. The Volusion incident that's currently underway is the first one traced back to Google Cloud.

Europol’s top hacking ring takedowns

Security
