Visa Warns of Point-of-Sale Attacks from FIN8 Hackers

by Silviu STAHIE on December 16, 2019

Criminal hacking group FIN8, known for a flurry of attacks in 2017 followed by a period of silence in 2018 until re-emerging earlier this year, has recently carried out three attacks against point-of-sale (POS) systems, including two against North American fuel dispenser merchants, Visa Payment Fraud Disruption said.

Visa said the attacks on fuel dispenser merchants aimed to steal credit card data directly from the POS systems. As is usually the case, the hacker's success was due to a mix of human mistakes and lack of proper security protocols.

To steal credit card data, hackers need to go through a number of steps. In the FIN8 attack, it started with an employee opening a phishing email, which installed a Remote Access Trojan (RAT) on the merchant network and granted the threat actors network access.

"The actors then conducted reconnaissance of the corporate network, and obtained and utilized credentials to move laterally into the POS environment," reads the Visa Payment Fraud Disruption report.

"There was also a lack of network segmentation between the Cardholder Data Environment (CDE) and corporate network, which enabled lateral movement. Once the POS environment was successfully accessed, a Random Access Memory (RAM) scraper was deployed on the POS system to harvest payment card data."

The RAM scraper is a piece of software that can be used in a variety of ways, depending on what it's designed to do. It can be used as a keylogger and can even send the data collected directly to the hackers.

A third attack against the network of a compromised North American hospitality merchant was also attributed FIN8, which is known for spearphishing attacks against the restaurant, hotel and hospitality sectors. The third attack used most of the same techniques, including a new shellcode backdoor based on the RM3 variant of the Ursnif (aka Gozi/Gozi-ISFB) modular banking malware.

Besides the improper employee training which lead to the one of them falling for phishing email, the hack was successful because the merchants lacked secure acceptance technology (e.g. EMV Chip, Point-to-Point Encryption, Tokenization, etc.) and didn't comply with PCI DSS.

Visa warns any merchant that uses POS systems to secure their networks, to install and update security solutions, and most importantly, to pay close attention to phishing emails.

Recent Articles By Author

- Latest Firefox Version Unveils and Fixes an AirPod Vulnerability
- Two-Thirds of Healthcare Organizations Have Suffered a Security Incident
- Some VPN Apps Secretly Gather Anonymized User Data

More from Silviu STAHIE

*** This is a Security Bloggers Network syndicated blog from HOTforSecurity authored by Silviu STAHIE. Read the original post at: https://hotforsecurity.bitdefender.com/blog/visa-warns-of-point-of-sale-attacks-from-fin8-hackers-21938.html

FIN8, FIN8 phishing, Industry News, POS hack, POS malware, Visa, VISA POS

← Security Analytics and Big Data: 4 Keys To An Effective Approach

NIST 800-171: Change of Characters in Passwords →

Most Read on the Boulevard

7 Linux Distros for Security Testing
Why Traditional Security Is Failing Us
ZeroNorth Raises $10M to Advance Risk Orchestration
Storage Is Your Data Lifecycle Weak Spot
Supply Chain Security Amid Coronavirus Fallout
Nine Network Security Topics Grabbing Headlines in Q1 2020
COVID-19 Cybersecurity Impact, Hacking the Hackers, Whisper App Data Leak

Upcoming Webinars »

MON 23 — The State of Open Source Security — March 23 @ 1:00 pm - 2:00 pm
TUE 31 — Protect Yourself from Cyber Attacks Through Proper Third-Party Risk Management — March 31 @ 11:00 am - 12:00 pm
APR 09 — Integrate Security Early and Often For Successful DevSecOps — April 9 @ 1:00 pm - 2:00 pm

Recent Security Boulevard Chats

Cloud, DevSecOps and Network Security, All Together?
Security-as-Code with Tim Jefferson, Barracuda Networks
ASRTM with Rohit Sethi, Security Compass
Deception: Art or Science, Ofer Israeli, Illusive Networks
Tips to Secure IoT and Connected Systems w/ DigiCert

Industry Spotlight »


The Coronavirus Pandemic and the Death of the VPN


Top 5 Open Source Serverless Security Tools


5 Good Reasons to Outsource Security Testing

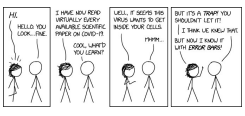
Top Stories »


Report: 97% of Firms Compromised Right Now. Really?


COVID-19 Fears Bring Google Chrome Dev to Screeching Halt


Contrast Security Advances DevSecOps

Security Humor »


XKCD 'Coronavirus Research'