Visa Security Alert

DECEMBER 2019

CYBERCRIME GROUPS TARGETING FUEL DISPENSER MERCHANTS

Distribution: Public

Summary

In summer 2019, Visa Payment Fraud Disruption (PFD) identified three unique attacks targeting merchant point-of-sale (POS) systems that were likely carried out by sophisticated cybercrime groups. Two of the attacks targeted the POS systems of North American fuel dispenser merchants. PFD recently reported on the observed increase of POS attacks against fuel dispenser merchants, and it is likely **these merchants are an increasingly attractive target for cybercrime groups. Track 1 and track 2 payment card data was at risk in the merchant's POS environments due to the lack of secure acceptance technology, (e.g. EMV® Chip, Point-to-Point Encryption, Tokenization, etc.) and non-compliance with PCI DSS.**

The activity detailed in this alert highlights continued targeting of POS systems, as well as targeted interest in compromising fuel dispenser merchants to obtain track data.

1. Threat Description

In the first incident, PFD analyzed the compromise of a North American fuel dispenser merchant. The threat actors compromised the merchant via a phishing email sent to an employee. The email contained a malicious link that, when clicked, 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. 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 following indicators of compromise (IOCs) are associated with the attack against this North American fuel dispenser merchant:

Filename	psemon10.dll
Exported DLL Name	psemonitor_x86.dll
Source	Virus Total
MD5	19d38325f715f623bd4b6e819a150cde
SHA1	15f34ce2e4a9c8bbeb6fa243d70d587f7a627ece
SHA256	cc5b3904458b144c5f263f47a3dffc9628ecdccab993bf7e01d345f496692c1a
SSdeep	384:nOZZmnD/R1EuVbtOWm/WzA3eaRrG2b44JR8kFvbWMz1DuDetv8fQYNRcAIoGlRt:OqQuNts3/Rq20s9dWyDPtRYXc1Rb

In a second incident, PFD identified a different compromise of another North American fuel dispenser merchant wherein threat actors targeted the merchant's POS environment. The actors again obtained network access to the targeted merchant, although it is unclear how the actors gained this initial access, and moved laterally within the network to the POS environment. A RAM scraper was injected into the POS environment and was used to harvest payment card data. The targeted merchant accepted both chip transactions at the in-store terminals and magnetic stripe transactions at fuel pumps, and the malware injected into the POS environment appears to have targeted the mag stripe/track data specifically. Therefore, the payment cards used at the non-chip fuel pumps were at risk in the POS environment.

Forensic analysis of the targeted network identified numerous indicators of compromise (IOCs) that can likely be attributed to the cybercrime group known as FIN8. FIN8 is a financially motivated threat group active since at least 2016 and often targets the POS environments of retail, restaurant, and hospitality merchants to harvest payment account data. Among the IOCs recovered are command and control (C2) domains previously used by FIN8 in threat activity. The malware used in the attack also created a temporary output file, wmsetup.tmp, which was used to house the scraped payment data. This file was previously identified in attacks attributed to FIN8 and FIN8-associated malware.

The following IOCs are associated with this attack:

C2s	Troxymuntisex[.]org (162.243.40[.]7) Nduropasture[.]net (192.64.119[.]98) Diolucktrens[.]org (157.230.233[.]65) Fraserdolx[.]org (134.209.78[.]73)

In a third incident, PFD conducted analysis on malware recovered from the network of a compromised North American hospitality merchant. The analysis determined that the compromise was likely the result of an operation conducted by the cybercrime group FIN8. The attack used a FIN8-attributed malware, but also used new malware not previously seen employed by the group in the wild. The new malware is a full-featured shellcode backdoor that is based on the RM3 variant of the Ursnif (aka Gozi/Gozi-ISFB) modular banking malware. While the malware used in this attack was not identified in the attacks against the fuel dispenser merchants, it is possible FIN8 will use this malware in future operations targeting fuel dispenser merchants.

The following IOCs are associated with this compromise:

Filename	mxSlipStream3.exe
MD5	5d4b9106c9911854b59c8891b40f29c0
SHA1	3187aa12119ef31d2f1e03af0adf5d9a9e3c45fd
SHA256	3a934f3cea6f9aff894eafd6e25ed01a93ef7dc4f7a16e2ade2da9f12060908f
SSdeep	1536:6w4fpS/nSciztM74N0DIDidcLbIA97Zn2eZe+1hRMVSsgm5:6w4gnScGuDI2dcjd2efHRuR5
Note	Nullsoft Installer-Based Loader

Filename	631081634
MD5	ede53b0ce6f3f3410b9f9595923fa2d4
SHA1	b038e0518162881af4c2584d8b4967e85bad3a77
SHA256	a7e41affb12e8e5c5e54cf9eb73104fb2069fb020eb2bf741f646f32b04d803a
SSdeep	384:hhicRs1D0pxnVXKmEnRj4gHRF5sQoURZ6qWFFkWoQxqt4CnJmnOjyEPiFa3EXx+H:3i31D0pxnNAnRj3HdsQoUIFF/oMEAOjb
Note	Encoded or Encrypted Data

Source	Virus Total
MD5	30c23ec53a3443b6d53a6c8ad29cbcc8
SHA1	0b18ea041f8b467158b96ab8c655e97329b95a45
SHA256	431f83b1af8ab7754615adaef11f1d10201edfef4fc525811c2fcda7605b5f2e
SSdeep	1536:ih5JdoIB8i6rAsm3m0I1H6WHZR8YTCUz6eIQ+rIvBH2jrz6Q:6jdoUxIg33A6W55TCO6eIQ+rIR2L
Note	Ursnif_Variant

Metasploit Bind TCP Stager	0.0.0.0:8443
TINYMET Meterpreter Stagers	185.159.131[.]11:443 45.77.152[.]39:443 45.77.152[.]39:80

2. Conclusion

PFD reported in February 2019 that an Advanced Persistent Threat (APT) group expanded their operations to eCommerce merchants. While it is expected that APTs and other financially motivated threat actor(s) will continue to target eCommerce environments, the recent attacks display a continued interest in obtaining track data from targeted brick-and-mortar merchants. Additionally, the recent compromises of fuel dispenser merchants represents a concerning trend whereby sophisticated threat groups have identified fuel dispenser merchants as an attractive target for obtaining track data.

It is important to note that this attack vector differs significantly from skimming at fuel pumps, as the targeting of POS systems requires the threat actors to access the merchant's internal network, and takes more technical prowess than skimming attacks. Fuel dispenser merchants should take note of this activity and deploy devices that support chip wherever possible, as this will significantly lower the likelihood of these attacks. PFD assesses that fuel dispenser merchants will continue to be an attractive target for sophisticated threat actors motivated by obtaining track data from POS systems.

Recommendations for Issuers and Acquirers

Visa recommends merchants and acquirers take the following actions to mitigate against these threats:

- **Employ the IOCs contained in this report** to detect, remediate, and prevent attacks using the POS malware variant.
- **Secure remote access** with strong passwords, ensure only the necessary individuals have permission for remote access, disable remote access when not in use, and use two-factor authentication for remote sessions.
- **Enable EMV technologies** for secure in-person payments (chip, contactless, mobile and QR code).
- **Provide each Admin user with their own user credentials**. User accounts should also only be provided with the permissions vital to job responsibilities.
- **Turn on heuristics (behavioral analysis) on anti-malware** to search for suspicious behavior, and update anti-malware applications.
- **Monitor network traffic** for suspicious connections, and log system and network events.
- **Implement Network Segmentation**, where possible, to prevent the spread of malicious software and limit an attacker's foothold.
- **Maintain a patch management program** and update all software and hardware firmware to most current release to limit the attack surface for zero-day vulnerabilities.
- **In the event of a confirmed or suspected breach, refer to Visa's** *What to do if Compromised (WTDIC),* **published October 2019.**

Refer to the following resources for more information on security standards, PCI compliance requirements, and best practices:

- PCI Data Security Standard Quick Reference Guide
- Refer to Visa's Card Acceptance Guidelines for Visa Merchants
- Additional information on PCI DSS can be found at www.pcissc.org

Contact Information

For more information, please contact paymentintelligence@visa.com

Disclaimer:
This report is intended for informational purposes only and should not be relied upon for operational, marketing, legal, technical, tax, financial or other advice. Visa is not responsible for your use of the information contained in this report (including errors, omissions, or non-timeliness of any kind) or any assumptions or conclusions you may draw from it. All Visa Payment Fraud Disruption Situational Intelligence Assessment content is provided for the intended recipient only, and on a need-to-know basis. PFD reporting and intelligence are intended solely for the internal use of the individual and organization to which they are addressed. Dissemination or redistribution of PFD products without express permission is strictly prohibited.