Visa Security Alert

JANUARY 2019

Same “PwnPOS” File Identified in Multiple Point-of-Sale Breaches in North America

Distribution: Issuers, Acquirers, Processors and Merchants

Summary

Visa’s Payment Fraud Disruption (PFD) team was the first to link the exact same PwnPOS malware file hash across seven recent point-of-sale breaches reported since March 2018 in North America. PwnPOS is a point-of-sale (PoS) malware first identified in 2015, but potentially active as early as 2013. The use of this malware in recent breaches is notable. In 2016 and 2017 combined, there were only a few reported PwnPOS infections. Whereas in 2018 the number of reported infections greatly increased. PFD also found that each of the PwnPOS malware files recovered from the 2018 breaches were the same across all compromises, rendering PwnPOS an easily identifiable malware family. PFD is providing the indicators of compromise (IOCs) below for mitigation and detection.

1. Threat Description

PwnPOS has the following attributes:

- A component that adds or removes itself from a list of system services
- This component enables the malware to avoid detection and persist on a targeted machine
- The malware installs a RAM scraper that monitors for keyboard inputs containing a string of numbers
  - It checks the string against the Luhn algorithm to determine if it is a credit card number
  - If the check passes, the malware exfiltrates the data with an installed binary

2. 2018 PwnPOS Activity

In the majority of recent cases, the attackers exploited vulnerabilities in unsecured remote access, such as weak passwords or permanently enabled remote access, which allowed infiltration of corporate systems and the subsequent execution of the PwnPOS malware. Additionally, a legitimate remote access application was used as a malicious install to persist in targeted systems. This remote access application was also identified as installing a number of additional compromises. However, these were not attributed to the PwnPOS malware family.

PFD assesses that fraudsters will continue to leverage the PwnPOS malware, given the number of recent successful compromises attributed to this malware family. PFD will further analyze the use of PwnPOS by cybercriminals, which currently appears to be highly active. The common malware hash and characteristics of the criminal campaigns provide organizations with direct indicators of compromise (IOCs) to help mitigate this threat.

3. Best practices and mitigation measures

1. To identify PwnPOS, scan networks for the following IOCs that correspond to the RAM scraper component of PwnPOS:

Filename	wnhelp.exe / dx_PE_ (602).exe
Source	Virus Total
MD5	c86327222d873fb4e12900a5cadcb849
SHA1	b1983db46e0cb4687e4c55b64c4d8d53551877fa
SHA256	088f40a7a52635ff19e80c62883977d94dd5835e85739e19504f7437d296760b
Ssdeep	6144:5GM9f8BHPlmg2XR2j0mYHLptiVK0LZV3C5:5x98HPlmg6R2j0mYF4VRLZtq

PFD identified this file with exact hash matches in seven recent breaches affecting point-of-sale devices of North American hospitality entities. The seven 2018 cases had additional PwnPOS file attributes; however, the RAM scraper component was consistently present in all seven. The above IOCs are also included in a corresponding .csv file, available on Visa Online.

2. Visa recommends the following best practices to reduce the risk of exposure:

- **Secure remote access** with strong passwords, ensure only the necessary individuals have permission for remote access, and disable remote access when not in use.
- **Enable EMV** on all point-of-sale devices.
- **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.
- **Refer to Visa's *What to Do If Compromised (WTDIC)* document**, published August 2016:
  - https://usa.visa.com/dam/VCOM/download/merchants/cisp-what-to-do-if-compromised.pdf

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

a. PCI Data Security Standard Quick Reference Guide

b. Refer to Visa's Card Acceptance Guidelines for Visa Merchants

c. Additional information on PCI DSS can be found at www.pcissc.org

If a merchant suspects a compromise, they should contact their acquiring bank immediately for guidance on next steps and to ensure compliance with all Visa investigation and compliance guidelines. For more information, refer to the What to Do If Compromised (WTDIC) guide.

Contact Information

For more information, please contact paymentintelligence@visa.com.

To report a data breach, contact Visa Fraud Control:

- Asia Pacific Region, Central Europe/Middle East/Africa Region: VIFraudControl@visa.com
- Europe: Datacompromise@visa.com
- Latin America & Caribbean: LACFraudInvestigations@visa.com
- U.S. and Canada: USFraudControl@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.