Visa Security Alert

JULY 2020

NEW MALWARE SAMPLES IDENTIFIED IN POINT-OF-SALE COMPROMISE

Distribution: Public

Summary:

In late April 2020, Visa Payment Fraud Disruption (PFD) analyzed malware samples recovered from the compromise of a North American merchant. The malware variants were identified as Alina POS, Dexter POS, and TinyLoader. These malware variants were deployed on the merchant network in an effort to harvest track 1 and track 2 magstripe payment card data from the merchant's point-of-sale (POS) environment. However, **the targeted merchant had EMV® Chip enabled point-of-sale terminals.** The implementation of secure acceptance technology, such as EMV® Chip, significantly reduced the usability of the payment account data by threat actors as the available data only included personal account number (PAN), integrated circuit card verification value (iCVV) and expiration date. Thus, provided iCVV is validated properly, the risk of counterfeit fraud was minimal. Additionally, many of the merchant locations employed point-to-point encryption (P2PE) which encrypted the PAN data and further reduced the risk to the payment accounts processed as EMV® Chip.

The technique used to gain initial access into the merchant network was not determined. However, after gaining initial network access, the actors deployed keylogging malware to harvest credentials and facilitate privilege escalation and lateral movement within the corporate network. Eventually, one of the aforementioned POS malware variants was deployed in the POS environment and harvested track 1 and track 2 payment account data. Multiple merchant's store locations were affected by the attack, and the malware variant used differed depending on the store location. The merchant locations employed distinct network architecture at each respective location, which likely explains the use of different malware variants as the attack had to be customized for each location. Again, it should be noted that all locations had EMV® Chip enabled POS terminals.

It is unclear how and when each of the three malware variants were deployed, and if they were deployed as part of the same criminal operation. However, since each malware family was identified in the environment and presented a potential risk to payment account information, PFD is providing the indicators of compromise for merchant network security purposes. The indicators of compromise (IOCs) associated with the analyzed malware samples are included below.

1. Indicators of Compromise (IOC) associated with the merchant compromise:

File #1

Filename	JackPOS.exe
MD5	76c43f82d84507efdfce17d00af81e18
SHA1	57365211c36be10449995cfcdce93d28334bd556
SHA256	f389ba6f9abe0f81b67ed6909524c1e721fc2af9676b1005d40375a0484b5f5c
SSdeep	3072:HAaoC8UzGgGETkE+nIAN0GZgGtDBF2gnizfGumud:kVUzGgBUnrTDpn4fG/ud
Note	Alina POS Malware

During execution, the malware creates a copy of itself at one of the following locations:

- %APPDATA%\usercache\jusched.exe
- %APPDATA%\usercache\jucheck.exe
- %APPDATA%\usercache\desktop.exe
- %APPDATA%\usercache\adobeflash.exe
- %APPDATA%\usercache\win-firewall.exe
- %APPDATA%\usercache\dwm.exe
- %APPDATA%\usercache\testing.exe
- %APPDATA%\usercache\userinit.exe
- %APPDATA%\usercache\windefender.exe
- %APPDATA%\usercache\svchost.exe

Named Pipe:
\\.\pipe\Katrina

Process Blacklist

During execution, the Alina POS Malware scans running processes and blacklists applications that would typically not contain credit card track data. This specific variant of Alina POS Malware contains 22 different processes in its process blacklist

DNS Request(s)	mycookingshow[.]lt (91.216.163[.]138)
HTTP Request(s)	hxxp://mycookingshow[.]lt/xxx/settings.php

- **User-Agent**: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:5.0) Gecko/20100101 Firefox/5.0
- **XOR Key**: 0xAA

File #2

Filename	POSGrabber.exe
Source	Virus Total
MD5	92fd5cad15dd2d6536d393c18b487948
SHA1	af874031311f9cd56b32d37607d3981933a574eb
SHA256	517fa2f87489a49e5dc741f92c0dbc4c9923e91c70132727159939c212f2ddc6
SSdeep	768:d3bZiyINpCsoZK1/5TXweYspiWiXJELaOidf9g:d3b4xU/0/GspivJJdfS
Note	Dexter POS Malware

During execution, the malware creates a copy of itself at the following location:

- %APPDATA%\Java Security Plugin\javaplugin.exe

Persistence - Registry Run Keys / Startup Folder (T1060)

Adding an entry to the "run keys" in the Registry or startup folder will cause the program referenced to be executed when a user logs in. These programs will be executed under the context of the user and will have the account's associated permissions level. In this case, the malware makes changes to the registry which will cause the program referenced to be executed when a user logs in.

- **Key**: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run\
  - **Name**: Sun Java Security Plugin
    - **Value**: %APPDATA%\Java Security Plugin\javaplugin.exe
- **Key**: HKEY_USERS\.DEFAULT\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\
  - **Name**: Sun Java Security Plugin
    - **Value**: %APPDATA%\Java Security Plugin\javaplugin.exe
- **Key**: HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Run\
  - **Name**: Sun Java Security Plugin
    - **Value**: %APPDATA%\Java Security Plugin\javaplugin.exe

DNS Request(s)	gastomix[.]com
HTTP Request(s)	hxxp://gastomix[.]com/abc0c4b847c1e79506b0f48d931e1375/gateway.php

- **XOR Key**: jptyt

File #3

Filename	TinyPOS.exe
MD5	f6f6626cccb5ee54b63268877a7b5e9e
SHA1	f9e9447df9c2f7206e49a77cffa1134bf12fab7e
SHA256	85837f254ca126aa96ae2c8b46ba7304929e8a4313c91dcb2d57f418a03503bc
SSdeep	48:ZvtzNplRZfJIm5Imqm5poo8SSpuxlwM/:Z1zrlthd5ioApuxlj/
Note	TinyLoader Malware

TCP Activity	193.142.30[.]201:4401 46.161.40[.]145:4401 91.92.137[.]40:4401

2. Recommendations for Issuers, Acquirers and Merchants

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

- **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.**

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