VISA SECURITY ALERT

March 2015

"RAWPOS" MALWARE TARGETING LODGING MERCHANTS

Distribution: Merchants, Acquirers

Summary

The "rawpos" malware is a memory scraper infecting global lodging merchants at an alarming rate. Variants date as far back as 2008, and it is one of the first known memory scrapers to target Point of Sale (POS) systems. Typically clustered in three files, there is no standard infection method for this malware. Of particular note with recent samples is a logic bomb that does not function outside the timing parameters. Adherence to PCI-DSS 3.0 should mitigate this malware.

Distribution and Installation

Once a vulnerable POS system is identified, various components of the malware are used to discover track data by only targeting the "memdump" portion of a Windows system. A memory dump can be the contents of memory on a system and where cardholder data temporarily resides during a payment transaction. This particular malware piece can be compiled with Perl2Exe. Perl2Exe is a program that takes codes scripted in the Perl language and bundles it into a Windows executable, which hides the Perl code. Numerous directories and file extensions are ignored. Any files not containing the ignored directories and file extensions are searched for track data using a regular expression similar to the format listed below:

```
((B([0-9]{13,16})|([0-9]|\\s){13,25})\\^[A-Z\\s0-9]{0,30}\\/[A-Z\\s0-9]{0,30}\\^(0[7-9]|1[0-9])((0[1-9])|(1[0-2]))([0-9]|\\s){3,50}[0- 9]{1})|([0-9]{15,16}([A-Z]|=)(0[7-9]|1[0-9])((0[1-9])|(1[0-2]))[0-9]{8,30})|(<Field name=\"CardNumber\">[0-9]{15,19}</Field>)|(~CCM[0-9]{15,19}D[0-9]{4}~))
```

Discovered track data is encrypted with an XOR key, such as 'anonymousgroup'. This data is delimited with the '$$$' character combination. Encrypted data can be written to a separate file, sometimes named "dxdiag32.dll". Data is also dumped in clear-text to .dmp files on the victim system in the "memdump" directory. For example:

```
memdump\\<process_name>_<pid>.dmp
```

A second file is also installed as a service by providing the '-install' or '/install' parameter. This creates a persistence mechanism which allows the scraper to continually run so long as the service is running. The sample is installed with the following attributes:

```
Service Name: xxx XXXManager
Display Name: xxx XXXManager
```

Description: [N/A]
Executable Path:
C:\PROGRA~1\xxx\SECURE~1\v1.2.0.3\XXXPrimaryManager\Bin\XXXManagerService.exe
Startup Type: Automatic

Alternatively, the malware removes this service if the '-remove' or '/remove' argument is supplied. In the event the '-debug' or '/debug' argument is provided, the malware will run in standalone mode. By default, the malware will attempt to start the service. When executed, the sample is responsible for executing the following commands on the victim host:

pushd
C:\\PROGRA~1\\xxx\\Secure~1\\v1.2.0.3\\XXXPrimaryManager\\Bin&start /min
xxxprimarymanager.exe&start /min xxxsecondarymanager.exe

The executable can also install itself in the System32 folder.

Additional files and hashes often coupled with “rawpos” include:

mmc.exe

vsssvc.exe

visaudp.exe

psex.exe (aka “psexec”)

sdelete.exe

se.exe

framepkg.exe

spoolsv.chm

While there is no common method of exfiltration associated with this malware family, infected merchants observed payment card data sitting on non-POS systems, suggesting attackers stage the stolen data elsewhere on the network prior to exfiltration.

Best Practices

Visa requires participants in the payment ecosystem to comply with all PCI-DSS requirements and recommends participants implement the following best practices:

- **Control the Windows Administrator account.** Make it more difficult for malware to gain Administrative privileges.
    - Assign a strong password for all accounts on the POS system.
    - Create a unique local Administrator password for each and every POS system.
    - Do not allow users to be local Administrators on a POS system.
    - Change passwords frequently, across the enterprise (at least every 90 days).

- **Ensure the POS system functions as a single purpose machine**. To reduce the risk of malicious software infections, disallow all applications and services (i.e. Internet browsers, email clients) that are not directly required as part of the POS's core functionality in processing payments.
- **Keep operating system patch levels up to date**. For Windows, this means ensuring Windows Update is functioning and automatically applying monthly security patches. For non-supported operating systems like Windows XP, there should be a plan to migrate to a current operating system.
- **Restrict permissions on Windows file sharing or disable file sharing altogether.** Unless absolutely necessary, Visa recommends disabling file sharing on POS systems. Microsoft has published instructions on how to disable simple file sharing and set permissions on shared folders.
- **Restrict remote access services use.** Unless necessary, disable remote access services, ports and accounts. If remote access services are needed, enable only when needed.
- **Promote security awareness.** Design anti-phishing programs, defense in depth strategies, and promote shared responsibility in security awareness.

Indicators

MD5 Hash	Function
bfb0eb8aacbf380cba9beb635557178a	RAM scraper
63b7cad5307a1927e16d7cd096b81831	RAM scraper
52fd283903f0e44e3da3233f7ad894a9	Aggregates and encrypts track data
0a06948f0eb5866216759ec69b315ced	Persistence
20c9388f45ff2d31754812a457ffbb0c	Memory dumper

The following MD5 hashes are also linked to the indicators above:

- 65375c1eb4683cbd2a868f99ac983b03
- 3f66583c8f67e7c255598d9d68394059
- ba9b109d929a643c831867cbc7459c4d
- 0c67494a4019264bceca488253610ef0
- 27d5c5f6f7b921c89ffb860d7e170b29
- 3ba5dafea1c447a2379811996f986006
- 4183e7fc2d9741c6039ba6eb357f57c3
- 5fa64cfcab7f4e95d6a55c2185a0515d
- ce0c7282e9116e1c46ee535c976e676e
- bd6c56097e107d12102c0df1136a96d1
- a3c0c081c4410b8ee1b68f0010ac3e45
- 7b61acc924ba4e5afa32e76afefe1e86
- 6c6de1c1e8e15574cb7e40cc7cc54536
- 65375c1eb4683cbd2a868f99ac983b03
- 19623ea25524a22c70a9b78059eba701
- 0b4b25c328af1fa348b8288043c704b7
- 3d0a57c178977781848533cb3038a087
- 65c44501369650db625043da125a4f0e
- 91c40ca8c3aefa23e12755836220dfad

- 402c8cdb483b1e3e51a7f1e4749f9625
- b075edd7288880e846414736a1f6b124
- 281591ef0fa2ce3536621327d020d23f
- 3004ce6cb7c44605cdf971b74db3a079
- bf27e87187c045e402731cdaa8a62861
- d770adbee04d14d6aa2f188247af16d0
- a63d6203d1d7568868ebe7521406b057
- fb9f8f1bee8b3fb47d7d84bb2286801d

Additional Resources
Microsoft's support for Windows XP ended in **April 2014**and will end in **January 2016** for Windows XP Embedded (XPe). Risk for POS applications built on these platforms will increase. See Microsoft Windows XP Support lifecycle timeline for more details.

To report a data breach, contact Visa Fraud Control:

- Asia Pacific Region, Central Europe/Middle East/Africa Region: VIFraudControl@visa.com
- Canada Region, Latin America Region, United States: USFraudControl@visa.com

For other questions, please contact Visa Risk Management: cisp@visa.com