VISA SECURITY ALERT

December 2015

MULTIPLE MALWARE FAMILIES TARGETING LODGING MERCHANTS

Distribution: Merchants, Acquirers

Summary

In 2015, multiple malware families targeted the lodging industry, including casinos and resorts. To name a few, "FindPOS" (or "Poseidon"), "FrameworkPOS", and "rawpos" are confirmed in several Visa investigations, suggesting the industry continues to be attractive to attackers interested in payment card data. Lodging merchants of varying sizes are among the list of compromised entities this year. Visa has witnessed all three malware families infecting merchants as late as November 2015. See http://researchcenter.paloaltonetworks.com/2015/10/understanding-and-preventing-point-of-sale-attacks/#more-10781 for a timeline of POS malware in the payment card ecosystem.

"FindPOS" Malware Family

"FindPOS", one of the most prominent families of POS malware out there and a relative of the "Backoff" malware family, is traditionally introduced via phishing emails. Two sites that explain the behavior of this malware are listed below:

http://researchcenter.paloaltonetworks.com/2015/03/findpos-new-pos-malware-family-discovered/

http://blogs.cisco.com/security/talos/poseidon

Both sites contain numerous helpful indicators of compromise (IOCs). POS integrators and POS vendors who cater to the lodging industry should carefully review these IOCs as part of their general information security practices.

"FrameworkPOS" Malware Family

Like traditional POS malware, "FrameworkPOS" scrapes memory for payment card data and employs encoding of the compromised data (usually a basic substitution cipher). However, the majority of samples analyzed by Visa do not contain exfiltration capabilities. Manual exfiltration or separate processes or files are used to exfiltrate payment card data.

A recent blog about this malware family is available via the link below:

https://www.trustwave.com/Resources/SpiderLabs-Blog/Another-Brick-in-the-FrameworkPoS

"RawPOS" Malware Family

The "rawpos" malware is typically a cluster of files that includes a memory scraper. Variations date as far back as 2008, and it is one of the first known memory scrapers to target Point of Sale (POS) systems. There is no known standard infection method for this malware. Of particular note with recent samples is the existence of a logic bomb that does not function outside the timing parameters, meaning the malware will not function outside of certain times hardcoded into the malware itself.

Trend Micro published an informative technical brief on this family in April 2015. See http://sjc1-te-ftp.trendmicro.com/images/tex/pdf/RawPOS%20Technical%20Brief.pdf for further details. In October 2015, FireEye/Mandiant also presented on this malware family. See http://securityaffairs.co/wordpress/41044/cyber-crime/fin5-hacked-a-casino.html for further details.

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.

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.

All third-party websites, brand names, or logos are the property of their owners and are used in this document for reference purposes only. Visa is not responsible for the content included on non-Visa websites. Such references do not imply an endorsement of any kind.

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