“BlackPOS” Malware Revisited

Webinar

17 December 2015

Disclaimer

The information or recommendations contained herein are provided "AS IS" and intended for informational purposes only and should not be relied upon for operational, marketing, legal, technical, tax, financial or other advice. When implementing any new strategy or practice, you should consult with your legal counsel to determine what laws and regulations may apply to your specific circumstances. The actual costs, savings and benefits of any recommendations or programs may vary based upon your specific business needs and program requirements. By their nature, recommendations are not guarantees of future performance or results and are subject to risks, uncertainties and assumptions that are difficult to predict or quantify. Assumptions were made by us in light of our experience and our perceptions of historical trends, current conditions and expected future developments and other factors that we believe are appropriate under the circumstance. Recommendations are subject to risks and uncertainties, which may cause actual and future results and trends to differ materially from the assumptions or recommendations. Visa is not responsible for your use of the information contained herein (including errors, omissions, inaccuracy or non-timeliness of any kind) or any assumptions or conclusions you might draw from its use. Visa makes no warranty, express or implied, and explicitly disclaims the warranties of merchantability and fitness for a particular purpose, any warranty of non-infringement of any third party's intellectual property rights, any warranty that the information will meet the requirements of a client, or any warranty that the information is updated and will be error free. To the extent permitted by applicable law, Visa shall not be liable to a client or any third party for any damages under any theory of law, including, without limitation, any special, consequential, incidental or punitive damages, nor any damages for loss of business profits, business interruption, loss of business information, or other monetary loss, even if advised of the possibility of such damages.

Agenda

- The Discovery of BlackPOS
- Malware Capabilities
- Attack Characteristics
- BlackPOS Detection Strategies
- POS Malware Prevention
- Questions and Answers

Trends in Data Compromises

Criminals are launching more sophisticated attacks targeting merchants

The Discovery of “BlackPOS”

BlackPOS Background and Discovery

- Initially seen “in the wild” in early 2012
- Dubbed Kaptoxa, pronounced (“Kar-toe-sha”) based on strings found in the malware
- Identified again in late 2013, believed to be found at several retailers
- Linkages found to earlier POS malware
- Source code has been leaked multiple times
- Associated with a number of data breaches reported in recent years

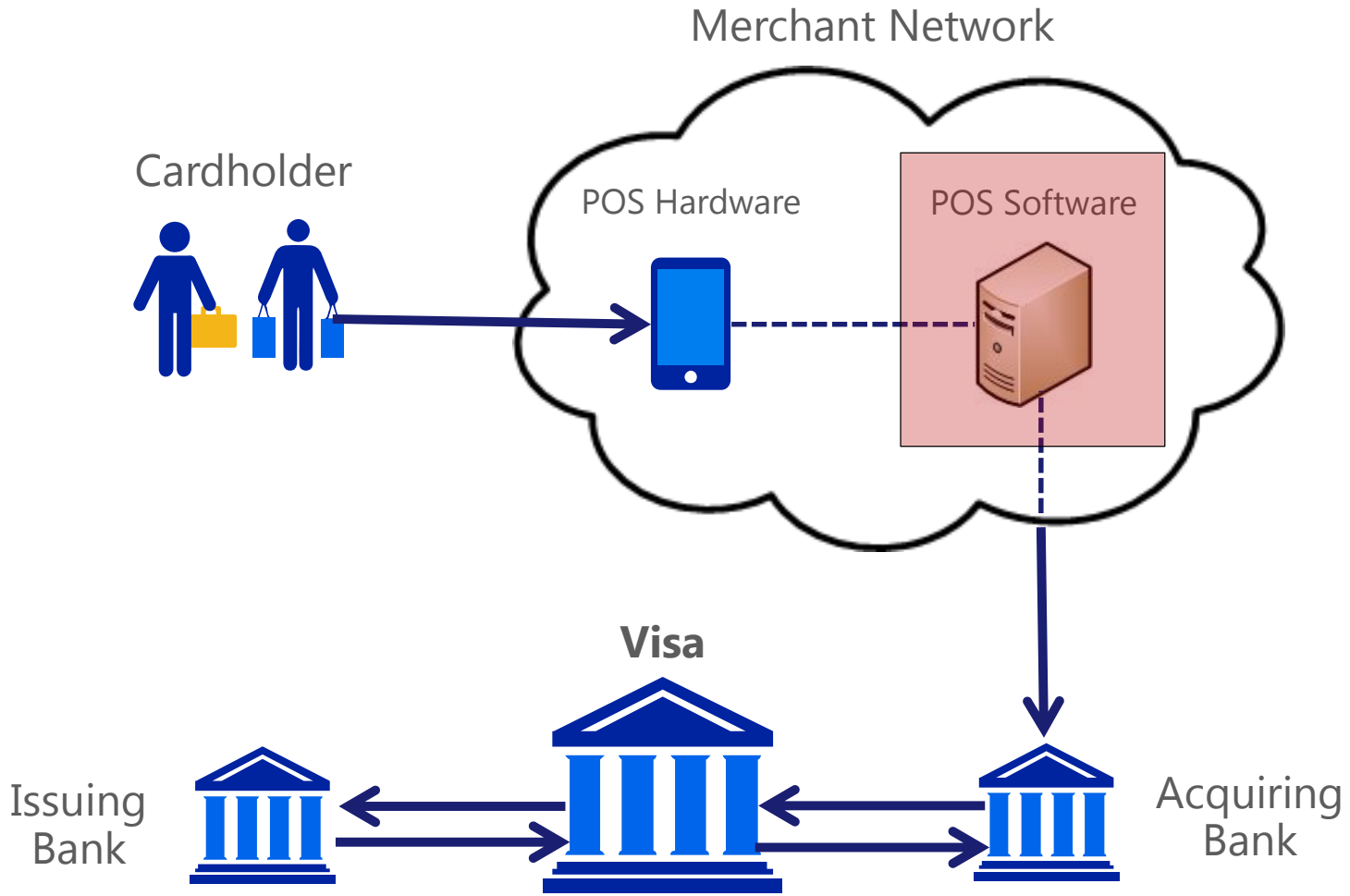
BlackPOS Research and Analysis

- Security researchers are continually reverse-engineering
- String found in one of the earlier versions:

  z:\Projects\Rescator\MmonNew\Debug\mmon.pdb
- Since its discovery, many different versions have been identified –each with new or slightly different characteristics
- Also related to “FrameworkPOS” malware

BlackPOS Malware Capabilities

Point-of-Sale (POS) RAM Scraping



POS RAM Scraping Primer

- Authorization data temporarily stored in clear text system memory
- Cybercriminals attack memory space because it is the easiest path to the data
- RAM scrapers generally use logic to identify track 1 and 2 data
- Some malware known to use Luhn algorithm to validate
- Captured data is pulled out of memory as it passes through
- Data is often briefly stored on the system it was captured

BlackPOS (somewhat) Unique Characteristics

Recent Variations and Functionality

- Additional functionality:
  - Self-deletion capability post exfiltration (reported in recent versions)
  - Not service dependent, so removal is more likely
  - Character shifting obfuscation
  - System level log scrubbing, e.g. Windows Event Log Viewer
  - Data movement timing mechanisms

BlackPOS Capabilities

Core Capabilities With Varying "bells and whistles"

- Different variations each incident (no MD5 match, no A/V detection)
- Installation and persistence mechanisms
- Memory-scraping
- Data encoding and masking
- Data exfiltration
- Self-removal

Attack Characteristics

BlackPOS Attack Characteristics

Initial Attack Vectors

- Common attack scenarios
  - Remote access credentials
  - Internet-facing systems with weak authentication
  - Botnet infection
  - Exfiltration occurs via ports / services commonly associated with data transfer
    - ICMP
    - TLS/HTTPS
    - NetBIOS
    - SSH
    - FTP/SFTP

Post-Attack Infrastructure Setup

Once Inside: Network Exploration and Exploit Tools Accompanying BlackPOS

- Network exploration and system mapping
- Proxies
- Privileged account identification
- Account takeover
- Data aggregation
- Data exfiltration
- Evidence cleanup / anti-forensics

BlackPOS Characteristics

POS Malware Distribution, Data Aggregation, Hiding and Exfiltration

- BlackPOS malware installation
- Data movement timing mechanism
- Aggregation servers
- “Jump” servers for data exfiltration

BlackPOS Detection Strategies

BlackPOS Prevention and Detection Strategies

BlackPOS Warning Signs

- Unexpected Windows services on the POS system
- Unexplained SMB traffic from or from the POS system (possibly encrypted)
- New, unexplained (likely encrypted or encoded) files on the POS
- Newly installed Windows services on POS system
- Outbound FTP traffic to the Internet

BlackPOS Prevention

- Ensure that overall payment processing environment is securely configured and maintained in accordance with the PCI DSS.
    - Ensure that firewall rules only allow remote access from known IP addresses
    - If remote connectivity is required, enable it only when needed
    - Contact your support provider or POS vendor and verify that a unique username and strong password exists for each of your remote management applications
    - Use the latest version of remote management applications and ensure that the latest security patches are applied prior to deployment
    - Plan to migrate away from outdated or unsupported operating systems like Windows XP
- Remote access applications best practices
    - Enable logging and examine logs regularly
    - Do not use default or easily-guessed passwords
    - Restrict access to only the specific IPs and only for established time periods
    - Only use remote access applications that offer strong security controls
    - **Always use two-factor authentication**. If remote access is required by your POS integrator, insist on two-factor authentication

Indicators of Compromise (IOCs)

- Operating system target selection
  - Windows XP, mostly Professional
- Processes activity
  - Searches for *pos.exe* to determine what to scrape
- Exfiltration
  - Creates file *output.txt* which may contain card data
  - Creates *.dll* files (e.g., *twain_32*.dll*) which may contain card data
- File names / MD5 hashes
  - *svchosts.exe* / ce0296e2d77ec3bb112e270fc260f274
  - *bladelogic.exe* / 433a2750429d805907aa4848ff666163
  - *svchosts.exe* / c0c9c5e1f5a9c7a3a5043ad9c0afa5fd
- System Center Configuration Manager (SCCM) manipulation
  - Normal vs. abnormal SCCM behavior

Upcoming Events and Resources

Upcoming Webinars – Training tab on www.visa.com/cisp

- "Kuhook" Point-of-Sale Malware
  - 27 January 2016, 10 am PST

Visa Data Security Website – www.visa.com/cisp

- Alerts, Bulletins
- Best Practices, White Papers
- Webinars

PCI Security Standards Council Website – www.pcissc.org

- Data Security Standards – PCI DSS, PA-DSS, PTS
- Programs – ASV, ISA, PA-QSA, PFI, PTS, QSA, QIR, PCIP, and P2PE
- Fact Sheets – ATM Security, Mobile Payments Acceptance, Tokenization, Cloud Computing, and many more…

Questions?