Cyber - Security and Investigations

Ingrid Beierly
August 18, 2008
Agenda

• Visa Cyber - Security and Investigations
• Today’s Targets
• Recent Attack Patterns
• Hacking Statistics *(removed)*
• Top Merchant Vulnerabilities
• Visa’s “What To Do If Compromised” procedures
• Payment Card Industry Data Security Standards (“PCI DSS”)
• Questions and Answers
Visa Cyber - Security and Investigations

• Provide fraud control support, direction and assistance
  – External and internal stakeholders
  – Publish fraud alerts and best practices
• Identify and actively investigate fraud incidents
  – Intake / triage point for all reported fraud incidents
• Other activities
  – Investigate global fraud affecting multiple members
  – Share intelligence across all Visa regions
  – Collaborate with high-tech private / public fraud groups
  – Represent U.S. on regional fraud working groups
  – Gather “carder” intelligence from various sources
Visa Cyber - Security and Investigations

- Ensure immediate containment of external Visa cardholder account security breaches
- Coordinate appropriate forensic response globally
- Provide technical support to Investigations, Incident Management and CISP / PCI DSS teams
- Review forensic reports
- Identify and communicate vulnerabilities exposing Visa data
- Oversee remediation of high-risk vulnerabilities
Law Enforcement Support

• Act as liaison with all federal, state and local law enforcement agencies
  – Coordinate compromise investigations
  – Provide critical fraud loss information to support criminal indictments
  – Gather “carder” intelligence from law enforcement
  – Participate in United States Secret Service (“USSS”) Electronic Crime Task Forces
  – Provide education and training to prosecutors

• Provide law enforcement investigative support on a global basis

• Coordinate research and response to law enforcement subpoenas
Today's Targets

• Hackers are attacking:
  – Brick-and-mortar merchants
  – Issuers
  – E-commerce merchants
  – Processors and Agents

• Hackers are looking for:
  – Software that stores sensitive cardholder data
  – Personal information to perpetrate identity theft
  – Track data and payment account numbers
  – PINs
  – Malware customized to steal cardholder data
Other Target Areas of Interest

• Log in credentials for online banking and networks
• Vulnerable public facing websites (SQL attacks)
• Targeted phishing or spear phishing attacks against issuers
• Fraudulent purchase of gift cards with counterfeits
• ATM skimming on the increase
• Automated Fuel Dispenser ("AFD") skimming
Recent Attack Patterns

Based on high-profile compromises YTD, Cyber - Security and Investigations has identified the following malware:

• **BP0.exe** is a remote command shell “backdoor.” It allows remote attackers use of the windows command shell to run commands and interact with the compromised server. Malware is hard-coded with a fixed IP address. A new version of BP0.exe has been identified with a new IP address.

• **Wiadebyls.dll** is a password collector that gathers credentials as they are used. It then transmits them to a hard-coded IP address using the HTTP protocol.

• **Sp.exe** extracts and runs the wiadebyls.dll malware. It uses a technique known as “process injection” to cause the winlogon process to forcibly load the DLL.
Recent Attack Patterns

- Wininet.exe is a packet sniffing program which can be configured to capture payment data on the network

- Wuauclt.exe is a key logger program and can be configured to capture keystrokes and payment data on the Point-of-Sale ("POS") terminal

Note: Visa shares new malware with security product vendors to ensure vendors develop signature files to detect malware
Top 5 Merchant Vulnerabilities

1. Storage of Track Data
2. Insecure Remote Access
3. Insecure POS Systems
4. Vendor - Supplied Default Settings and Passwords
5. Insecure Network Configuration
Top 5 Merchant Vulnerabilities

Storage of Track Data Mitigation Strategy

• Contact your POS vendor or reseller to validate whether the applications and versions in use are storing full track data or other sensitive information
• Perform a secure delete of sensitive cardholder from the POS system
• Merchants must use a payment application that has been validated against PCI Payment Application Data Security Standards (“PA-DSS”)

Insecure Remote Access Mitigation Strategy

• Contact your POS vendor, reseller, or IT staff to ensure secure configuration of remote access. For example:
  – Enable remote access port only when needed
  – Upgrade to latest version of remote access management
  – Allow connection from trusted IP addresses
  – Enable strong encryption
  – Enforce use of strong password
Top 5 Merchant Vulnerabilities

Insecure POS Systems Mitigation Strategy

- Use latest operating system
- Install critical patches
- Disable unnecessary ports and services
- Disable Internet access (inbound and outbound)
- Use POS system only for business purposes (e.g., do not allow personal use, such as email, browsing the Internet, downloading music)
- All users must have a unique ID and password to access the POS system
- Implement anti-virus software with latest signature files
- If POS system is running a database server (such as SQL or MySQL), protect the Administrator account by issuing a strong password and remove unnecessary stored procedures
- Enforce use of strong password
- Enable logging for forensic purposes
Top 5 Merchant Vulnerabilities

Vendor - Supplied Default Settings and Passwords Mitigation Strategy

• Change default or blank settings and passwords prior to deployment. This includes operating systems, firewall devices, routers, wireless access points, etc.

Insecure Network Configuration Mitigation Strategy

• Implement a stateful inspection firewall
• Direct Internet access to the POS system should not exist. This can be addressed using a firewall device separating the Internet and the POS system
• Enable logging on remote access and firewall
• Monitor logs periodically to detect unknown activity
• Implement network segmentation to separate payment processing systems from non-critical systems.
  – Separation is key to limiting the extent of a compromise that may originate in another segment of the network
• Any wireless network must be segmented from the wired network where the POS system resides
Visa’s What To Do If Compromised Procedures

Compromised entities must:

• Immediately contain and limit the exposure
• Notify their merchant bank
• Notify law enforcement
• Work with Visa on forensic investigation
• Provide compromised Visa, Interlink, and Plus accounts to your merchant bank
• Provide an incident report to your merchant bank

For more info go to www.visa.com/cisp
Visa’s What To Do If Compromised Procedures – Continued

Acquirers must:

- Ensure compromised entity cooperates with Visa on the investigation
- Perform an initial investigation and provide documentation to Visa
- If Visa deems necessary, an independent forensic investigation must be conducted by a Qualified Incident Response Assessor ("QIRA")
Visa’s What To Do If Compromised Procedures – Continued

Acquirers must:

- Perform a PIN security assessment (if PINs are at risk)
- Provide forensic report to Visa
- Provide at-risk account numbers to Visa
- Ensure the compromised entity has contained the incident
- Ensure the compromised entity achieves PCI compliance

For more info, please refer to the What To Do If Compromised document available at www.visa.com/cisp
Industry Collaboration

- PCI Security Standards Council (“SSC”), launched in September 2006, is a global forum for the ongoing development and enhancement of security standards for account data protection

- Security standards managed by the council include the PCI Data Security Standard (“DSS”), Payment Application Data Security Standard (“PA-DSS”) and PIN Entry Device (“PED”) program

- Visa, Amex, Discover, JCB and MasterCard are founding members

- Payment card industry stakeholders are invited to join as Participating Organizations and can be elected to an Advisory Board

  - Participating organizations are invited to attend community meetings, comment on DSS revisions and future security standards and participate in implementation "best practice" discussions
## PCI DSS

### PCI DSS is based on fundamental data security practices

<table>
<thead>
<tr>
<th>Build and Maintain a Secure Network</th>
<th>1. Install and maintain a firewall configuration to protect data</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>2. Do not use vendor - supplied defaults for system passwords and other security parameters</td>
</tr>
<tr>
<td>Protect Cardholder Data</td>
<td>3. Protect stored data</td>
</tr>
<tr>
<td></td>
<td>4. Encrypt transmission of cardholder data and sensitive information across public networks</td>
</tr>
<tr>
<td>Maintain a Vulnerability Management Program</td>
<td>5. Use and regularly update anti-virus software</td>
</tr>
<tr>
<td></td>
<td>6. Develop and maintain secure systems and applications</td>
</tr>
<tr>
<td>Implement Strong Access Control Measures</td>
<td>7. Restrict access to data by business need-to-know</td>
</tr>
<tr>
<td></td>
<td>8. Assign a unique ID to each person with computer access</td>
</tr>
<tr>
<td></td>
<td>9. Restrict physical access to cardholder data</td>
</tr>
<tr>
<td>Regularly Monitor and Test Networks</td>
<td>10. Track and monitor all access to network resources and cardholder data</td>
</tr>
<tr>
<td></td>
<td>11. Regularly test security systems and processes</td>
</tr>
<tr>
<td>Maintain an Information Security Policy</td>
<td>12. Maintain a policy that addresses information security</td>
</tr>
</tbody>
</table>
# Visa Merchant Compliance Validation

<table>
<thead>
<tr>
<th>Level</th>
<th>Validation Action</th>
<th>Scope</th>
<th>Validated By</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>• Annual On-site Security Audit</td>
<td>• Authorization and Settlement Systems</td>
<td>• Qualified Security Assessor or Internal Audit if signed by Officer of the company</td>
</tr>
<tr>
<td></td>
<td>• Quarterly Network Scan</td>
<td>• Internet Facing Perimeter Systems</td>
<td>• Approved Scan Vendor</td>
</tr>
<tr>
<td>2 and 3</td>
<td>• Annual Self-Assessment Questionnaire</td>
<td>• Any system storing, processing, or transmitting Visa cardholder data</td>
<td>• Merchant</td>
</tr>
<tr>
<td></td>
<td>• Quarterly Network Scan</td>
<td>• Internet Facing Perimeter Systems</td>
<td>• Approved Scan Vendor</td>
</tr>
<tr>
<td>4</td>
<td>• Annual Self-Assessment Questionnaire Recommended</td>
<td>• Any system storing, processing, or transmitting Visa cardholder data</td>
<td>• Merchant</td>
</tr>
<tr>
<td></td>
<td>• Network Scan Recommended</td>
<td>• Internet Facing Perimeter Systems</td>
<td>• Approved Scan Vendor</td>
</tr>
</tbody>
</table>
Level 4 Small Merchant Initiatives

Executing a plan to address small merchants in the U.S.

- Level 4 merchants account for more than 85% of all compromises identified since 2005, but less than 5% of potentially exposed accounts
  - Most small merchant compromises involve vulnerable payment applications
- Outreach to all active acquirers to promote small merchant security
- Education and awareness campaign including a webinar series, regular data security alerts and bulletins
- Publish list of vulnerable payment applications quarterly and promote use of PA-DSS validated applications
- 100% of 231 acquirers provided Visa with Level 4 compliance plans
  - Updated progress reports due from acquirers by June 30, 2008
Payment Application Security

Drive the adoption of secure payment applications that do not store prohibited data

- Visa PABP published in 2005
  - Provide vendors guidance to develop products that facilitate PCI DSS compliance
  - Minimize compromises caused by insecure payment applications with emphasis on track data storage

- List of validated payment applications published monthly since January 2006
  - 348 products across 157 vendors independently validated by a Qualified Security Assessor
  - List of validated applications published on www.visa.com/cisp

- List of vulnerable payment applications published quarterly since February 2007

- PABP adopted by PCI SSC as an industry standard, Payment Application Data Security Standard (“PA-DSS”) in April 2008

www.visa.com/pabp
Level 4 Merchant Security Best Practices

Understand PCI DSS Requirements:

- Use online resources
  - The PCI SSC website contains the standards and other supporting documentation (e.g. self-assessment questionnaires) – www.pcisecuritystandards.org
  - The Visa website has an array of helpful security and compliance information – www.visa.com/cisp

- Partner with your merchant bank
  - Utilize resources offered by your merchant bank such as alerts, bulletins and training
  - Understand the compliance validation required by your merchant bank

- Understand PCI PIN Security Requirements:
  - The www.visa.com/pin website has an array of helpful PIN security and compliance information for Interlink accepting entities
  - The PCI SSC website contains the Approved PIN Entry Devices list and other supporting documentation – www.pcisecuritystandards.org/pin
Level 4 Merchant Security Best Practices

Adopt Payment Application Best Practices:

• Vet Point-Of-Sale (“POS”) applications with Visa’s list of validated payment applications
  - List available at [www.visa.com/pabp](http://www.visa.com/pabp)
• Confer with payment application vendors (or reseller / integrator) to ensure their software does not store prohibited data (e.g., magnetic-stripe, CVV2 or PIN data)
• Partner with merchant bank to obtain a list of vulnerable payment applications
  - If payment application deficiencies are identified, merchants should work with their acquirer to immediately upgrade to a compliant version
  - In addition to upgrading the application, any historical storage of prohibited data must be securely wiped from all systems immediately!
Questions or Comments?
Thank You!