Webinar

Top 10 Signs Your Payment Network is Breached

Nov 16, 2016

Glen Jones
Senior Director, Visa

Forward-looking statements and disclaimer

This presentation may contain forward-looking statements within the meaning of the U.S. Private Securities Litigation Reform Act of 1995. These statements can be identified by the terms “objective,” “goal,” “strategy,” “opportunities,” “continue," “can,” "will," and other similar references to the future. Examples of such forward-looking statements may include, but are not limited to, statements we make about our corporate strategy and product goals, plans, and objectives. By their nature, forward-looking statements: (i) speak only as of the date they are made, (ii) are neither statements of historical fact nor guarantees of future performance, and (iii) are subject to risks, uncertainties, assumptions, and changes in circumstances that are difficult to predict or quantify. Therefore, actual results could differ materially and adversely from those forward-looking statements for a variety of reasons, including macroeconomic and industry factors such as currency exchange rates, global economic, political, health and other conditions, competitive pressure on customer pricing and in the payments industry generally, and material changes in our customers' performance compared to our estimates; systemic developments such as disruption of our transaction processing systems or the inability to process transactions efficiently, account data breaches involving card data stored by us or third parties, and increased fraudulent and other illegal activity involving our cards; and other factors discussed under the heading "Risk Factors” in our most recent Annual Report on Form 10-K and our most recent Quarterly Reports on Form 10-Q. You should not place undue reliance on such statements. Unless required to do so by law, we do not intend to update or revise any forward-looking statement because of new information or future developments or otherwise.

Studies, survey results, research, recommendations, and opportunity assessments are provided for informational purposes only and should not be relied upon for marketing, legal, regulatory, or other advice. Recommendations and opportunities should be independently evaluated in light of your specific business needs and any applicable laws and regulations. Visa is not responsible for your use of any studies, survey results, research, recommendations, opportunity assessments, or other information, including errors of any kind, or any assumptions or conclusions you might draw from their use. Except where statistically significant differences are specifically noted, survey results should be considered directional only.

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

- Payment System Compromise Trends
- The Top 10 Signs
- Best Practices for Breach Prevention
- Improved Threat Intelligence
- Questions

Payment Data Compromise Trends

VISA

Card Present

- ATM & POS skimming attacks on the rise
- Fewer large merchant breaches
- Most breaches (by %) involve unprotected small merchants
- Fewer breaches detected by conventional methods
- Repeat compromises and "re-breaches"

Other Fraud

- Increase in CNP merchant compromises
- Vulnerable web commerce applications being exploited
- Application fraud losses trending up
- Account takeover losses trending up
- CNP data contributing to other fraud types

The Top 10

10 – Login patterns outside normal activity

- Activity during off hours
- User login to resource with access to payment data from unexpected source
- Remember: anyone can be a phishing victim, so **look for the activity**, not the user
- Look for users abnormally accessing a device or system they normally would have a need to

9 – Lateral Movement Tools

- Sysinternals psexec is the tool of choice for hackers
- PsExec is an extremely powerful tool and is used commonly in enterprise networks, for remote system management
- It's not malware
- Alternate names FRAMEPKG.EXE, psex.exe
- Common component in many retail, restaurant, hospitality merchant breaches

8 – Credential Harvesting Tools

- Used to advance the attack beyond the first system
- Collect usernames and passwords
- Used for “privilege escalation”
- Record keyboard activity
- Examples are:
  - Windows Credential Editor
  - CAIN and Abel
  - Pass the hash

7 – Public-facing Network Connections to Internal Payment systems

- Connections from VPN network to a POS network
- Connections from a public-facing Citrix environment to payment / PCI networks
- Should be no direct connections from un-trusted networks to the PCI segment
- Very common attack scenario: VPN remote access

6 – Evidence of Anti-forensic Tools

- Sysinternals sdelete.exe and variations: “wipes” files
- Also not considered malware
- “Timestomp”: fake time & date stamp on files
- Log clearing & deletion of logs
- Occasional deception involving other activity like file-sharing used to mask hacker activity

5 – Data Staging / Preparation

- New files appearing on POS, base64 encoded
  - Database tools
  - Windows batch files
- Temporary local storage and consolidation of CC data (DLLs are a popular format)
- Hijacking of systems with broad access to PCI network to disseminate malware, collect and consolidate logs
  - Log servers
  - Windows SCCM servers
  - Anti-virus servers!

4 – Data Exfiltration Signs

- Outbound FTP connections
- Odd looking DNS requests
- Outbound connections to Ukraine, other foreign IP addresses (yes, this is obvious, but it still happens)
- Communication with "known bad" IP addresses

3 – Signs of Remote Access "backdoors"

- Reverse tunnel utility installed
- Recent cases involved Ukraine IPs, German IP addresses as sources of the attack
- Usage of VNC, RDP, TeamViewer, LogMeIn or other remote access utilities
- Connections from remote IP addresses using remote access tools
- “Persistent” connections from PCI network to external networks

2 – Memory Scraping Malware

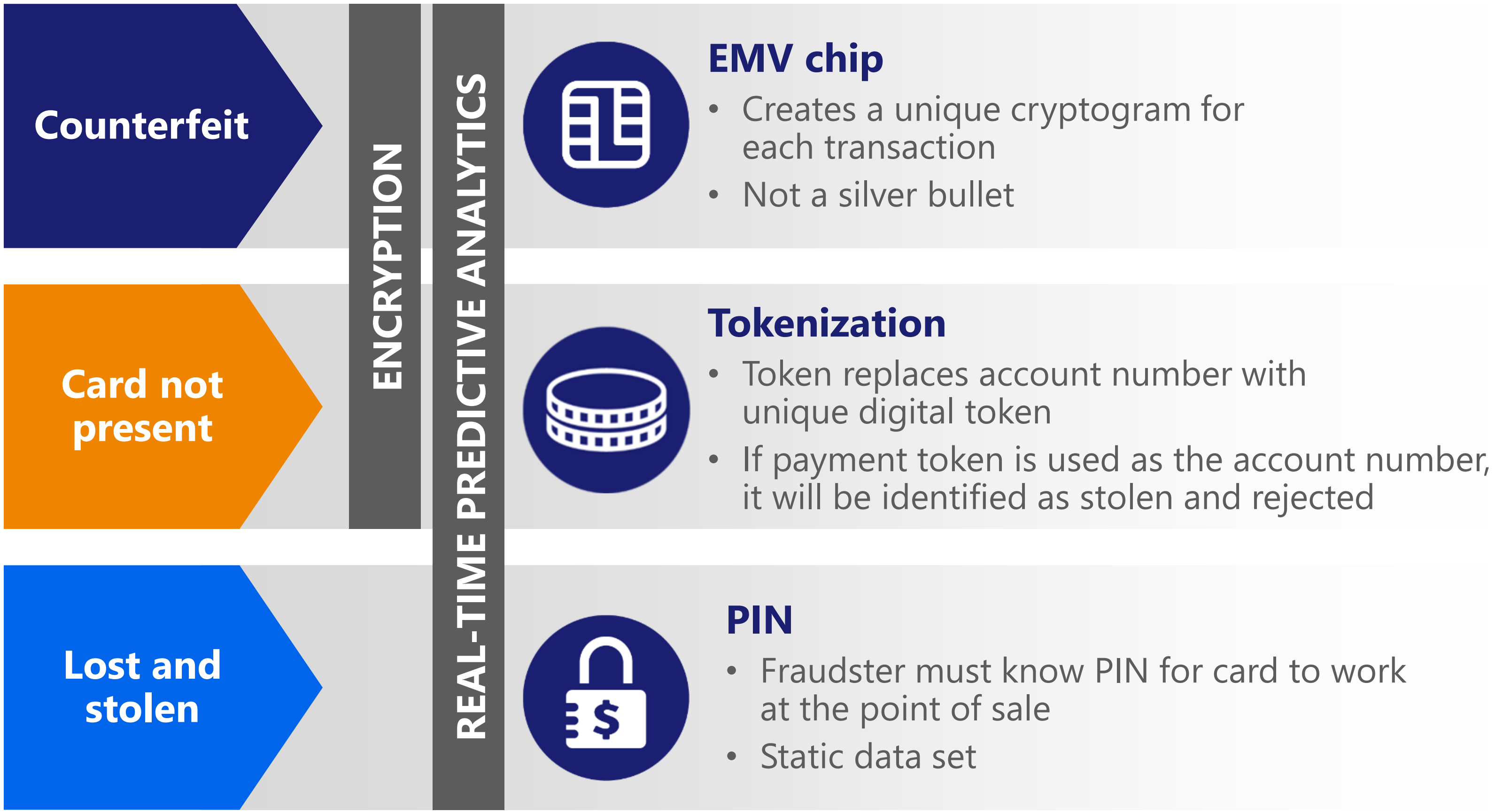
- Criminals have to get to payment data where it's vulnerable (not encrypted)
- Malware has to be installed onto systems that process or store payment cards
- Almost always Windows systems that process payment (POS devices, payment switches, payment applications)
- Look for new processes, executables, scheduled tasks
- Look for POS systems slowing down and/or crashing

1 – Unusual Running Processes or New Scheduled Tasks

- Processes, services or applications set to run on system start-up
- Usually on Point of Sale devices
- Modify the registry keys so the service is started at boot
- One type of unusual process name to look for is a common system process name that has been misspelled
- Spelling is close, so will usually go unnoticed
- Also process with misspelled description or missing description

Best Practices for Breach Prevention

Fighting Fraud With Layers of Security



Counterfeit

Card not present

Lost and stolen

ENCRYPTION

REAL-TIME PREDICTIVE ANALYTICS

EMV chip

- Creates a unique cryptogram for each transaction
- Not a silver bullet

Tokenization

- Token replaces account number with unique digital token
- If payment token is used as the account number, it will be identified as stolen and rejected

PIN

- Fraudster must know PIN for card to work at the point of sale
- Static data set

Source: Visa Fraud Reporting System (FRS) and Enterprise Data Warehouse (EDW); CY 2013; U.S. domestic Visa debit and credit

Strategies for Small Merchants

Merchants with limited resources

- Protect Point of Sale at all costs
- Disallow remote access unless absolutely necessary
- Do not use Point of Sale devices for email, Web
- Install anti-virus **and anti-malware**

Threat Intelligence - Indicators of Compromise

How important are IOCs to your business?

- More reliable and earlier breach detection
- Higher fidelity intelligence
- Streamlining incident management
- Operationalizing cyber intel and automation
- Reducing impact of a breach
- Proactive cyber defense

Improved Threat Intelligence

Anticipate

Anticipate attacks based on a deep understanding of who is attacking you

Intel briefings

Detailed, curated, current and expert intelligence regarding key cyber and payment threats, what they mean and how to take action

Act

Take action to prevent and prepare for known and emerging threats

Indicator fields

Up-to-date and comprehensive intelligence on both established threats and high-risk behavior patterns. **85%** of our indicators are not available from other sources[1]

Respond

React and prepare for threats, reducing the danger of breaches

Community circles

Controlled, invite-only platform for company alliances and partnerships to share knowledge on threats and collaborate to better defend against attackers

[1] *Source: Visa. Based on a sample of Visa Threat Intelligence Indicators compared against four commercial threat intelligence sources (2016)*

Upcoming Events and Resources

Upcoming Webinars

https://visa.com/cisp

December 8th, 2016 – Preventing CNP Fraud and Compromise

Visa Data Security

https://visa.com/cisp

PCI Security Standards Council Website

https://pcissc.org

Visa Threat Intelligence, Powered by FireEye

https://usa.visa.com/visa-everywhere/security/visa-threat-intelligence.html

See a demo:

https://www.youtube.com/watch?v=mqSx_6B18x0

Speaker contact information:

Glen Jones, Visa
gljones@visa.com

Michelle Levin, Visa
cisp@visa.com

Questions?