The Importance of Containment and Remediation of Compromised Payment Processing Environments

Glen Jones – Cyber Intelligence & Investigations

September 2, 2015

Notice of Disclaimer

The information, recommendations or “best practices” 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, programs or “best practices” 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

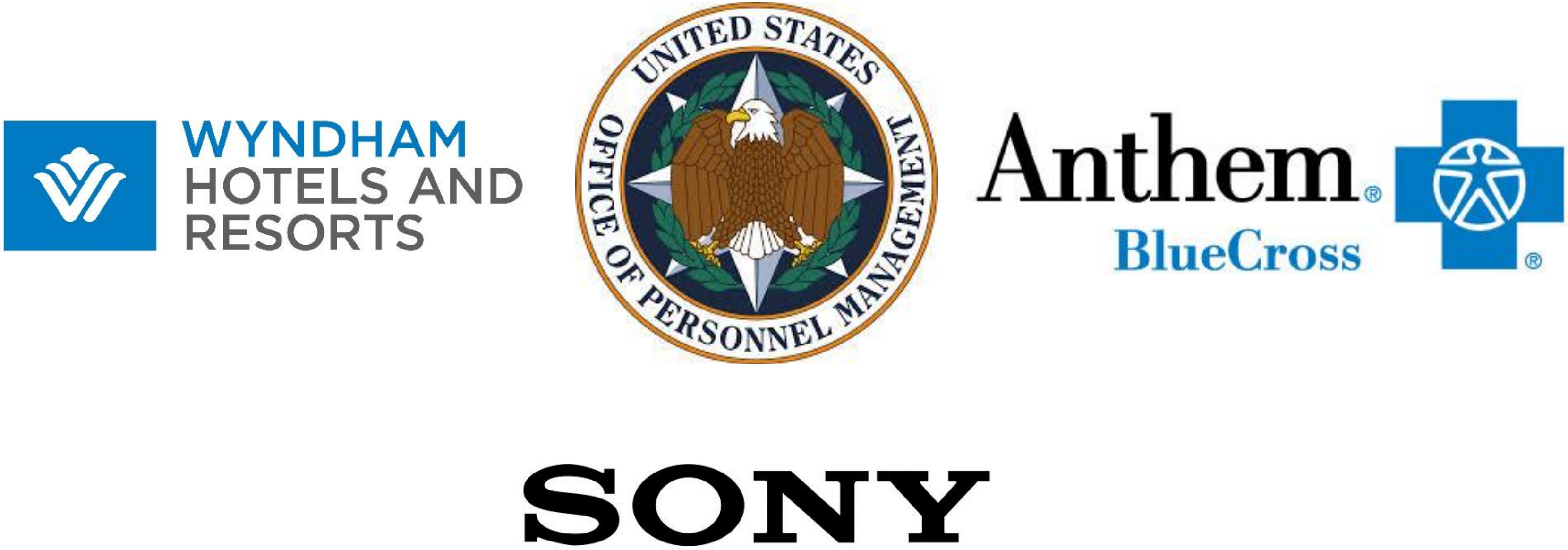
- Global data compromises
- Importance of containment & eradication
- Case study: improper containment & eradication
- Cyber attack kill chain
- Importance of proper scoping investigative response
- Proper containment – short & long term
- Effective eradication
- Containment versus eradication
- Key takeaways

Global Data Compromises

- A compromise is not a matter of "if," it's a matter of "when"
- Global data compromise events grew 23% in 2014 over those managed in 2013
- The average total cost of a data breach is now up to $3.79 million
- The U.S. is the largest contributor, mainly due to its large mag stripe infrastructure and an increase in successful attacks on third party service providers
- VE and AP represent the next largest contributors to known breach events, together compromising a quarter of the total
- Emerging Trend: Recurring compromises

Examples of entities experiencing multiple breaches

Suffered multiple compromises


WYNDHAM HOTELS AND RESORTS
UNITED STATES OFFICE OF PERSONNEL MANAGEMENT
Anthem. BlueCross
SONY

Importance of Containment and Eradication

Risks of not containing and eradicating the first time

- Large merchants can spend significant resources on multiple compromises
  - Multiple forensic investigations
  - Multiple QSAs, since you cannot use the same one as before
  - Money spent on professional security services
  - Time and effort by staff responding and reacting to multiple compromises
- Loss of patience by management
- Loss of consumer confidence in brand
- Could impact shareholder value
- Better to properly contain and eradicate once

Case Study: Improper Containment and Eradication

Based on a payment card forensic investigation

- Retail merchant with over 1,000 locations in the United States and Canada
- Forensic Findings:
  - Cause of breach was undetermined by the forensic investigators
  - Not properly scoped
  - Hosts were not identified
  - Backdoors were left open by cyber thieves
  - After initial clean-up, experienced another breach
  - Significant resources were expended

Cyber Attack Kill Chain

Breaking down elements to contain and remediate

1 Reconnaissance – harvesting emails, personal and company information, etc.

2 Weaponization – exploit vulnerability and gain backdoor access

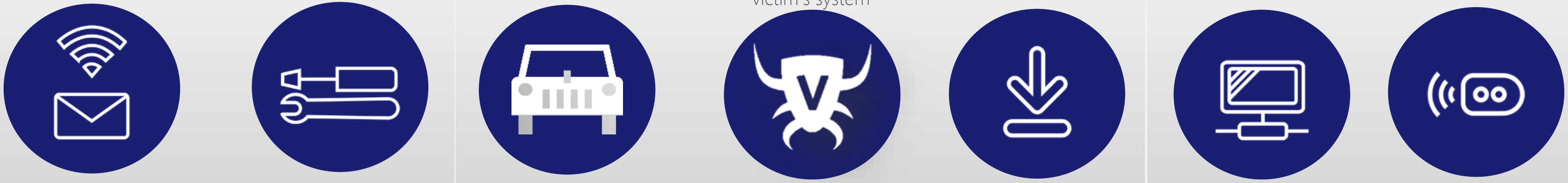
3 Delivery – weaponized payload to victim

4 Exploitation – exploiting a vulnerability to execute code on victim's system

5 Installation – malware on assets

6 Command & Control – remotely operate and control victim's systems

7 Action – commit harvesting and exfiltration



Attackers perform research on potential victims and develop a methodology, including the tactics, techniques, and procedures they will use. Weaponization is the act of developing a set of weapons typically comes prior to an actual attack.

Attackers then select the type of method and delivery to the victim such as spear phishing or social engineering. The victim is sent an attachment such as buffer overflow attack and a backdoor is opened on the victim's workstation. Or login credential is phished providing remote access to the attacker then POS malware is installed on the victim's workstations.

Backdoors are open on the victim's environment and the attacker can remotely control system to commit harvesting and exfiltration of payment card data.

Preparation | Intrusion | Active Breach

* Based on Lockheed Martin Cyber Kill Chain

Importance of complete scoping

Identify all hosts

- Gather events from all sources
- Log files, error messages, IDS/IPS, and firewall logs
- Super hackers do not exist, they always leave a trace
- Document cleanly and completely
- Risk of missing just one host
- Should not proceed until scoping is complete
- Investigation is a marathon, not a sprint

Proper Containment

Short Term

- Goal is to limit and prevent further damage
- Isolate network segments impacted
- Perform system backups before re-imaging
  - Preserve evidence for forensics and investigations
- Gather evidence
  - Identify hosts, IP, MAC, model, etc.
  - Date and time

Long Term

- Ensure accounts and/or backdoors are removed left by attackers
- Root cause analysis
- Rebuild impacted systems
  - Malware persistence
  - System re-imaging
  - Patching systems
- Assess authentication strategy
  - Inventory business partnership and remote access connections
  - Remote access authentication

Effective Eradication

Removal and restoration of affected systems

- Malware removal is addressing the symptom, not the cause
  - Don’t clean, rebuild
  - Determine **how** the malware got installed in the first place
- When in doubt, tear it down and rebuild
- Blocking is good, but not enough
- Rip off the bandage, don’t peel
- Scan affected systems to ensure latent malware is removed
- Ensure affected systems are secure after rebuild
  - Systems patched and hardened
- Consider the use of red team/blue teams

Containment versus Eradication

Containment

- An incident is “contained” when cardholder data is no longer being breached
- The Window of Intrusion starts from the first date that the intruder or malware entered the system and ends at the Date of Containment
- The Date of Containment is the date at which no further data loss can occur because measures have been put in place to address the compromise
  - Measures may be short-term; however, are not the final solution

Eradication

- Fixing what led directly to the compromise
  - Removal of malware or rebuilt of compromised systems
  - Compromised system removed from the network
  - Blocking of malicious IPs on the firewall
  - Rotation of compromised passwords
- Eradication is alleviating symptoms, not tackling the root cause

Remediation

- Remediation is the term used to describe the end of the **Window of System Vulnerability**
- The **Window of System Vulnerability** is the time frame in which a weakness(s) in an operating system, application or network could be exploited by a threat to the time that weakness is properly remediated i.e. the weakness no longer exists.
- This is the desired end result, the compromise has been investigated, the root cause determined and addressed and all corrective actions are in place.
  - Failure to identify root cause can lead to vulnerabilities continuing and, then what no-one wants....a second breach.
  - Identifying the root cause of a breach could easily involve looking beyond the cardholder data environment.
  - PFIs and their customers must be prepared to widen the scope of the investigation if necessary to achieve root cause identification.

Key Takeaways

Lessons Learned

1. **Understand why the breach occurred** – People, process, technology failures
2. **Properly scope the account data compromise –** Ensure all affect hosts are identified
3. **Short term containment – L**imit and prevent further damage
4. **Long term containment –** Backdoor removal, root cause analysis and rebuild
5. **Do not clean, rebuild –** Malware removal is addressing the symptom, not cause
6. **Effective eradication** – Rebuild affected systems, patch and harden system
7. **Understand lessons learned** – Why breach occurred, people, process, and technology failures

Additional Resources

Guidance and standards on incident response and handling

- Review Visa’s “What To Do If Compromised” guide
  - http://usa.visa.com/download/merchants/cisp-what-to-do-if-compromised.pdf
- SANS Incident Handler’s Handbook
  - http://www.sans.org/reading-room/whitepapers/incident/incident-handlers-handbook-33901
- NIST 800-62 Revision 2 – Computer Incident Handling Guide
  - http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf
- For further information on these terms and on PFI investigations please consult the PCI PFI Program Guide:
  - https://www.pcisecuritystandards.org/documents/PFI_Program_Guide.pdf
  - Contact the PFI Program Manager via pfi@pcisecuritystandard.org

Upcoming Events and Resources

Upcoming Webinars – Under Merchant Resources/Training on www.visa.com

Visa Online Merchant Tool Kit provides helpful information to make a seamless EMV transition

- Streamline your chip migration – www.VisaChip.com/businesstoolkit

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, QIR Listing
- Fact Sheets –Mobile Payments Acceptance, Tokenization, and many more…

Thank you for attending!

Questions? Comments?

VISA