"Kuhook" Point-of-Sale Malware

Sylvia Auyeung, Director, VISA, NA Merchant Risk
Erik Rasmussen, Director, VISA, Cyber Intelligence and Investigations
Jason Rebholz, Manager, MANDIANT, a FireEye Company
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

• Global Payment Card Compromise Landscape

• “Kuhook” Overview

• “Kuhook” Capabilities

• “Kuhook” Detection Strategies

• Questions and Answers
Global Payment Card Compromise Landscape

Sylvia Auyeung, Director, VISA, NA Merchant Risk
Payment System Risk Landscape

Data Security

• Frequency of data breaches is increasing
• Large merchant breaches account for the majority of ‘known’ compromised accounts
• Emphasis on cyber intelligence information sharing is growing

Fraud Trends

• Fraud levels and accounts are increasing
• Fraud is concentrated in markets/channels that rely on static authentication data
• CNP fraud is disproportionately high

New Players in the Eco-system

• Proliferation of third party agents and nontraditional players is increasing security risks
• Visa is focusing on its leadership role in payment system security

Regulatory Attention

• Governments and regulators are paying more attention to fraud and data security
• Opportunities for public-private collaboration on payment security are expanding

“Kuhook” Point-of-Sale Malware | 27 January 2016
Global Data Compromises

2011-2015 Compromise Cases by Region

- Global data compromise events are slightly higher in 2015 over those managed in 2014.
- 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 comprising a quarter of the total.
- Breaches in VE and AP are primarily CNP.
Global Data Compromises
Breach trends by merchant level

<table>
<thead>
<tr>
<th>Entity Type</th>
<th>2012</th>
<th>2013</th>
<th>2014</th>
<th>2015</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>%</td>
<td>%</td>
<td>%</td>
<td>%</td>
</tr>
<tr>
<td>Level 1</td>
<td>&lt;1%</td>
<td>1%</td>
<td>1%</td>
<td>&lt;1%</td>
</tr>
<tr>
<td>Level 2</td>
<td>&lt;1%</td>
<td>1%</td>
<td>1%</td>
<td>&lt;1%</td>
</tr>
<tr>
<td>Level 3</td>
<td>1%</td>
<td>4%</td>
<td>4%</td>
<td>5%</td>
</tr>
<tr>
<td>Level 4</td>
<td>95%</td>
<td>92%</td>
<td>93%</td>
<td>92%</td>
</tr>
<tr>
<td>Agent</td>
<td>&lt;1%</td>
<td>1%</td>
<td>1%</td>
<td>2%</td>
</tr>
<tr>
<td>Other</td>
<td>2%</td>
<td>&lt;1%</td>
<td>0%</td>
<td>0%</td>
</tr>
<tr>
<td>Total</td>
<td>100%</td>
<td>100%</td>
<td>100%</td>
<td>100%</td>
</tr>
</tbody>
</table>

- As a proportion of the total number of breach events, L4s remain the vast majority of compromise cases (93% in 2014-2015)
- At-risk accounts in 2015 were largely attributed to L4 merchants
- Level 4 merchants outnumber L1s in the US

Large breach events (levels 1 & 2)

- Fewer level 1 and 2 breaches in 2015
- Threat actors are targeting smaller interconnected merchants in large numbers
- Restaurants and “other retail” make up the biggest portion of total known breaches
- Quick service restaurants, supermarkets, and lodging make up the other top MCCs
“Kuhook” Overview

Erik Rasmussen, Director, VISA, Cyber Intelligence and Investigations
Kuhook Overview: Distinctions

Why is this malware interesting?

1. Output file encryption...with unique keys!
2. Unconventional device driver modules
3. Possible exploitation of symmetric keys vulnerability
4. Victim merchant sample dataset is extremely small
PoS Malware Behavior

Malware exfiltration methods:

NOTE: Malware in this presentation communicated via C&C servers
PoS Malware Types

Malware will often fall into one of these categories:

NOTE: This malware exhibits all 4 characteristics.

1. File scraper
2. Network sniffer
3. Keylogger
4. Memory Scraper
Kuhook Tools Selection

• “Hacker” Tools
  – cain.exe
    • Network password scanner
    • Password cracking capability
    • “recovery” tool
  – mimikatz.exe
    • Password dumper tool
    • Plaintext passwords
    • Not just hashes

• “Dual Use” Tools
  – psexec
    • Microsoft remote/local administration cmd line utility
  – sdelete.exe (aka SDelete)
    • Microsoft cmd line utility for wiping
    • Replaces each character of the file's name with a successive alphabetic character. For instance, the first rename of "foo.txt" would be to "AAA.AAA".

“Kuhook” Point-of-Sale Malware | 27 January 2016
Visa Public
Kuhook Tools Selection

Note: These screenshots are demonstrative only and not from actual Visa or Mandiant investigations.

"Kuhook" Point-of-Sale Malware | 27 January 2016
“Kuhook” Capabilities

Jason Rebholz, Manager, MANDIANT, a FireEye Company
How Compromises Are Being Detected

31% victims discovered the breach internally

69% victims notified by an external entity
Anatomy of a Targeted Attack

- Initial Compromise: Gain Initial Access Into Target
- Establish Foothold: Strengthen Position within Target
- Escalate Privileges: Steal Valid User Credentials
- Internal Recon: Identify Target Data
- Complete Mission: Package and Steal Target Data
Packed device driver that targets the Windows XP operating system

- Identified five variants
  - All packed with the same packer and contained nearly identical driver payloads
  - Primary difference was the functionality of the shell code
  - Variants identified by file size

- Persistence is maintained through a Windows service
  - Randomly generated service name
  - Easy to find if you know what you’re looking for!
Malware Variants

- Card data harvester
  - Injects malicious code into the POS process that handles card holder data
  - Searches process memory for track 2 data
  - Writes stolen card data out to files that were encrypted with a unique key per host!
- Keystroke logger
  - Injects shell code into “explorer.exe” that enumerates all input devices
  - Intercepts data from devices (keyboard, mouse, etc.)
  - Data is output to a file that is encrypted with unique AES key per host
- Backdoor
  - Downloads and executes shellcode
  - Communicates to hard-coded IP address using HTTP POST requests
What happens when it loads?

- Driver unpacks itself and starts a new system thread
  - Reports back to the system that the original driver failed to load
  - Does not appear to be loaded but is actually running separate from the original driver
- Unpacked driver decodes and injects shell code into user space
  - Initially targets “csrss.exe”
    - Becomes main broker of future user-space processes
  - Additional shell code deployed that is specific to the variant
  - Variants are able to communicate with each other
“Kuhook” Detection Strategies

Erik Rasmussen, Director, VISA, Cyber Intelligence and Investigations
Breach prevention and detection strategy
Defense-in-depth, preparation, vigilance

- Adopt data devaluation technology
- PCI DSS as baseline controls
- Have a breach preparedness plan
- Monitor for known POS and other malware
- Know your environment
- Know the warning signs

Note: IOC = Indicators of Compromise

"Kuhook" Point-of-Sale Malware | 27 January 2016
Mitigation
Best Practices**

- Control the Windows Administrator account
  - Make privilege escalation difficult
- Install application whitelisting on Point of Sale systems
- Closely monitor activity on Point of Sale systems
  - Be aware of anomalous behavior and investigate all suspicious activity on the POS
- Ensure the POS system functions as a single purpose machine.
- Keep operating system patch levels up to date
- Restrict permissions on Windows file sharing or disable file sharing altogether
- Restrict remote access services use
- Promote security awareness

**Source: Visa Publication: New Year's Resolution: Resolve to Fight Malware
Indicators of Compromise (IOCs)

<table>
<thead>
<tr>
<th>IOC</th>
<th>Type</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>91.207.61.208</td>
<td>Destination IP address</td>
<td>Command and control server</td>
</tr>
<tr>
<td>109.72.149.42</td>
<td>Destination IP address</td>
<td>Command and control server</td>
</tr>
<tr>
<td>130.0.237.22</td>
<td>Destination IP address</td>
<td>Command and control server</td>
</tr>
<tr>
<td>5.187.1.198</td>
<td>Destination IP address</td>
<td>Command and control server</td>
</tr>
<tr>
<td>ABA833D11679DFEBC95060BD3C557853</td>
<td>File MD5 hash</td>
<td>Malicious driver file</td>
</tr>
<tr>
<td>215BDF185C0B335503923FCFB872C75PC</td>
<td>File MD5 hash</td>
<td>Malicious driver file</td>
</tr>
<tr>
<td>F9C4E2D13D8A87F545B85BA1F8691B</td>
<td>File MD5 hash</td>
<td>Malicious driver file</td>
</tr>
<tr>
<td>F214036C7516B37F7FC17F401CED6F</td>
<td>File MD5 hash</td>
<td>Malicious driver file</td>
</tr>
<tr>
<td>6FBD31E7B5A315F75BD0D858D332785</td>
<td>File MD5 hash</td>
<td>Malicious driver file</td>
</tr>
<tr>
<td>68F40544ACD5568BD7B2434CA05FAE55</td>
<td>File MD5 hash</td>
<td>Malicious backdoor file</td>
</tr>
<tr>
<td>S40DF64B08393BFA39D2FEDC6C608EA12</td>
<td>File MD5 hash</td>
<td>Password harvesting file</td>
</tr>
<tr>
<td>%SystemRoot%\system32\drivers</td>
<td>Install path</td>
<td>Malware install path</td>
</tr>
<tr>
<td>C:\windows\Installer[random characters].bin</td>
<td>Path to log files</td>
<td>Keystroke logger, track 2 data logs</td>
</tr>
<tr>
<td>C:\windows\TEMP[random characters].bin</td>
<td>Path to log files</td>
<td>Keystroke logger, track 2 data logs</td>
</tr>
<tr>
<td>C:\windows\TEMP[random characters].temp</td>
<td>Path to log files</td>
<td>Encrypted status logs</td>
</tr>
<tr>
<td>HTTP POST /robots.txt</td>
<td>Network indicator</td>
<td>Network traffic to the /robots.txt POST request shows patterns in the request headers and server response that are consistent across all samples.</td>
</tr>
</tbody>
</table>

- The request is to a hard-coded IP address over HTTP
- The user-agent string is consistent throughout the samples previously listed
- The server returns a 405 “Method Not Allowed” response

Following the HTML closing tag is a series of spaces (hexadecimal value, "20") followed by &#60!-- which serves as a marker for where the encrypted data stream begins.
Upcoming Events and Resources

- Visa Data Security Website – www.visa.com/cisp
- Alerts, Bulletins
- Best Practices, White Papers
- Past Webinar Presentations

- 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...