"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

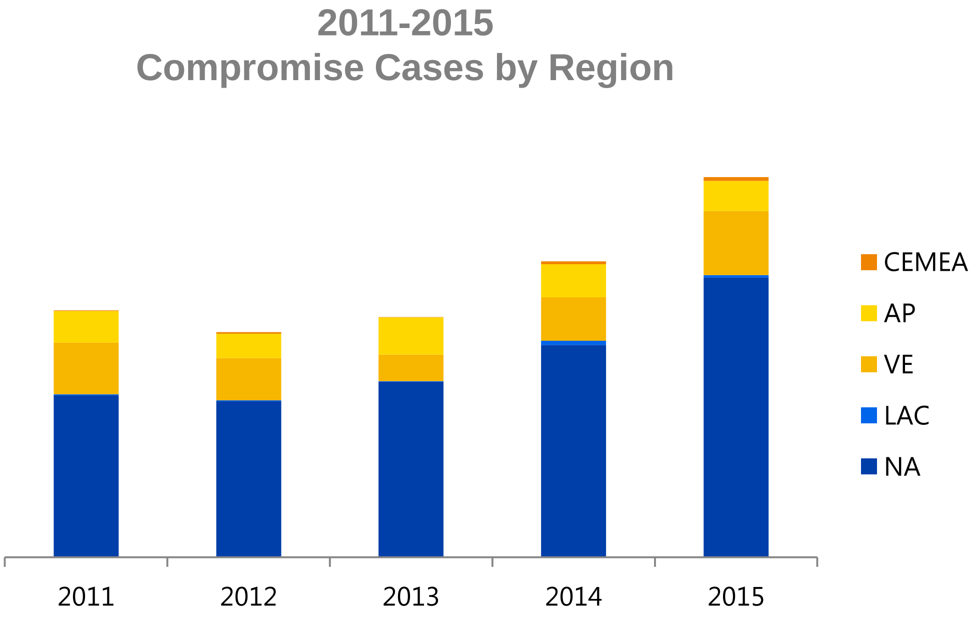
New Players in the Eco-system

- 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

Global Data Compromises



- 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

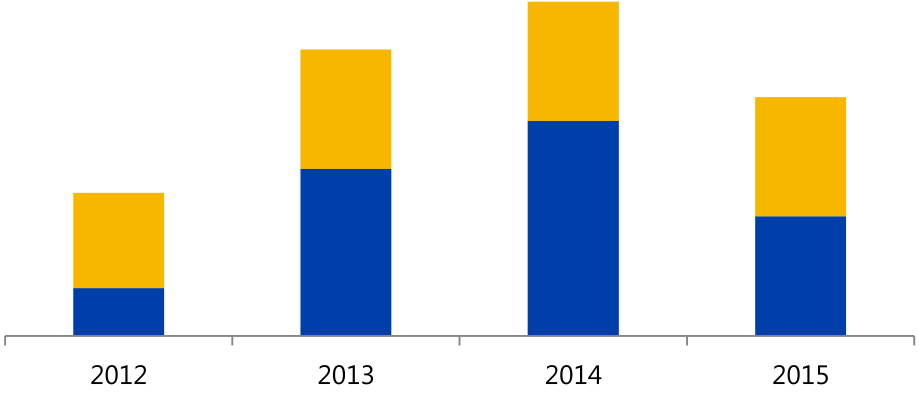
Breach trends by merchant level

Breach events by merchant level

Entity Type		2012	2013	2014	2015
		%	%	%	%
	Level 1	<1%	1%	1%	<1%
	Level 2	<1%	1%	1%	<1%
	Level 3	1%	4%	4%	5%
	Level 4	95%	92%	93%	92%
Agent		<1%	1%	1%	2%
Other		2%	<1%	0%	0%
Total		**100%**	**100%**	**100%**	**100%**

- 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)

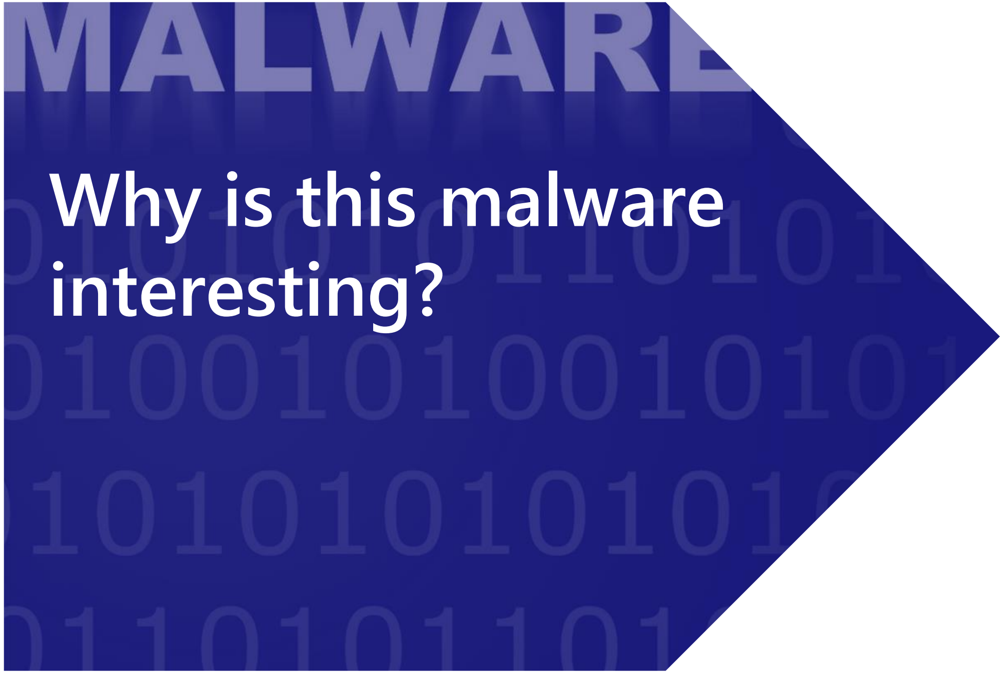


- Fewer level 1 and 2 breaches in 2015
- Threat actors are targeting smaller interconnected merchants in large numbers
- Restaurants and “other retail” make up the biggest portion of total known breaches
- Quick service restaurants, supermarkets, and lodging make up the other top MCCs

“Kuhook” Overview

Erik Rasmussen, Director, VISA, Cyber Intelligence and Investigations

Kuhook Overview: Distinctions



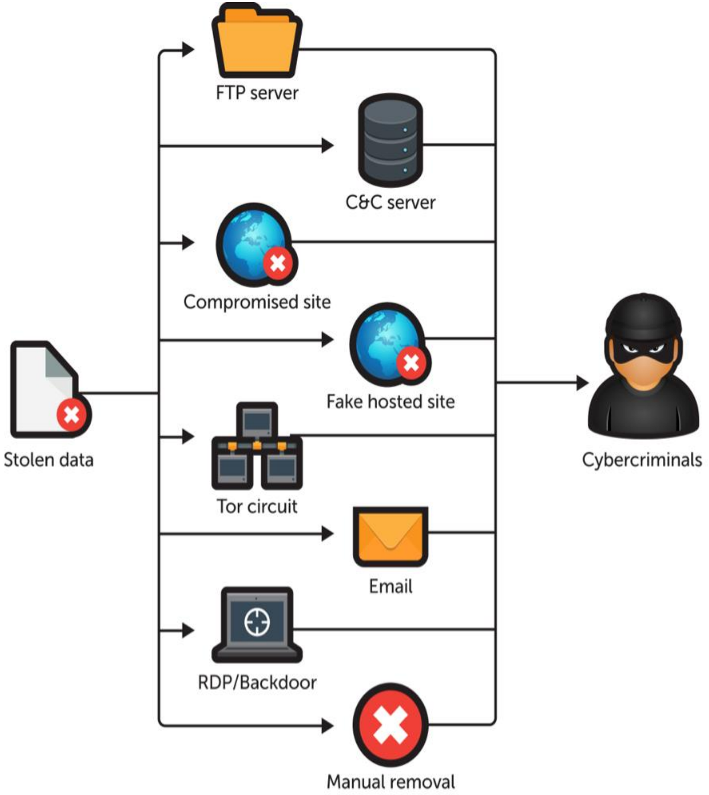
Why is this malware interesting?

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



Graphic courtesy of Trend Micro

PoS Malware Types

Malware will often fall into one of these categories:

NOTE: This malware exhibits all 4 characteristics.

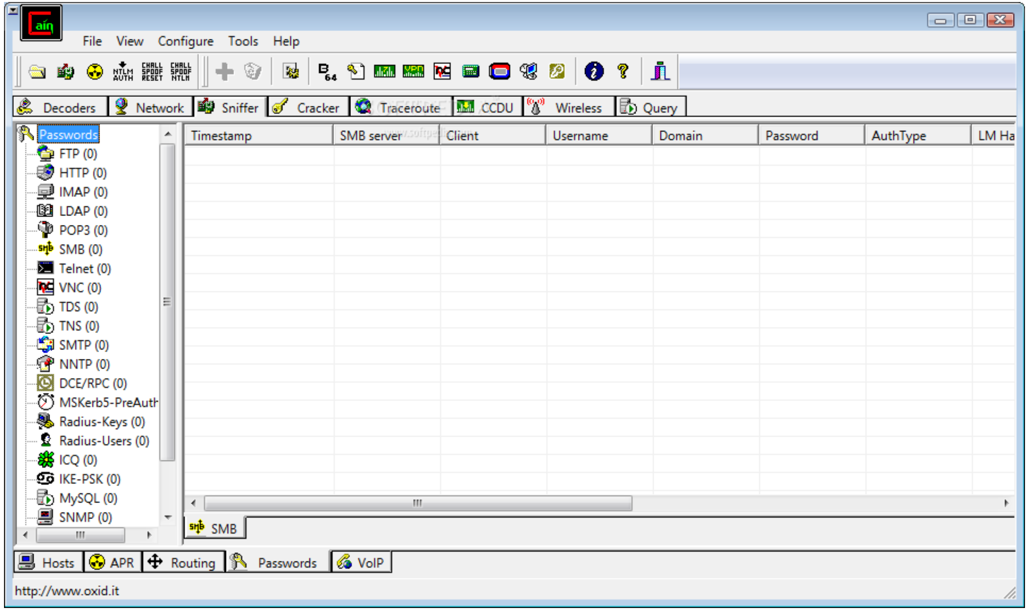
1. File scraper
2. Network sniffer
3. Keylogger
4. Memory Scraper

Kuhook Tools Selection

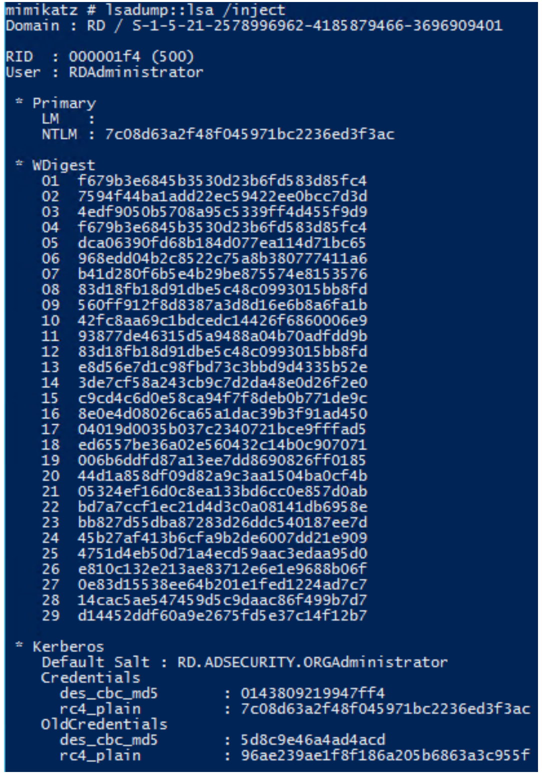
- “Hacker” Tools
  - cain.exe
    - Network password scanner
    - Password cracking capability
    - “recovery” tool
  - mimikatz.exe
    - Password dumper tool
    - Plaintext passwords
    - Not just hashes

- “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 Tools Selection



cain.exe screenshot



```
mimikatz # lsadump::lsa /inject
Domain : RD / S-1-5-21-2578996962-4185879466-3696909401

RID  : 000001f4 (500)
User : RDAdministrator

 * Primary
    LM   :
    NTLM : 7c08d63a2f48f045971bc2236ed3f3ac

 * WDigest
    01  f679b3e6845b3530d23b6fd583d85fc4
    02  7594f44ba1add22ec59422ee0bcc7d3d
    03  4edf9050b5708a95c5339ff4d455f9d9
    04  f679b3e6845b3530d23b6fd583d85fc4
    05  dca06390fd68b184d077ea114d71bc65
    06  968edd04b2c8522c75a8b380777411a6
    07  b41d280f6b5e4b29be875574e8153576
    08  83d18fb18d91dbe5c48c0993015bb8fd
    09  560ff912f8d8387a3d8d16e6b8a6fa1b
    10  42fc8aa69c1bdcedc14426f6860006e9
    11  93877de46315d5a9488a04b70adfdd9b
    12  83d18fb18d91dbe5c48c0993015bb8fd
    13  e8d56e7d1c98fbd73c3bbd9d4335b52e
    14  3de7cf58a243cb9c7d2da48e0d26f2e0
    15  c9cd4c6d0e58ca94f7f8deb0b771de9c
    16  8e0e4d08026ca65a1dac39b3f91ad450
    17  04019d0035b037c2340721bce9fffad5
    18  ed6557be36a02e560432c14b0c907071
    19  006b6ddfd87a13ee7dd8690826ff0185
    20  44d1a858df09d82a9c3aa1504ba0cf4b
    21  05324ef16d0c8ea133bd6cc0e857d0ab
    22  bd7a7ccf1ec21d4d3c0a08141db6958e
    23  bb827d55dba87283d26ddc540187ee7d
    24  45b27af413b6cfa9b2de6007dd21e909
    25  4751d4eb50d71a4ecd59aac3edaa95d0
    26  e810c132e213ae83712e6e1e9688b06f
    27  0e83d15538ee64b201e1fed1224ad7c7
    28  14cac5ae547459d5c9daac86f499b7d7
    29  d14452ddf60a9e2675fd5e37c14f12b7

 * Kerberos
    Default Salt : RD.ADSECURITY.ORGAdministrator
    Credentials
      des_cbc_md5       : 0143809219947ff4
      rc4_plain         : 7c08d63a2f48f045971bc2236ed3f3ac
    OldCredentials
      des_cbc_md5       : 5d8c9e46a4ad4acd
      rc4_plain         : 96ae239ae1f8f186a205b6863a3c955f
```

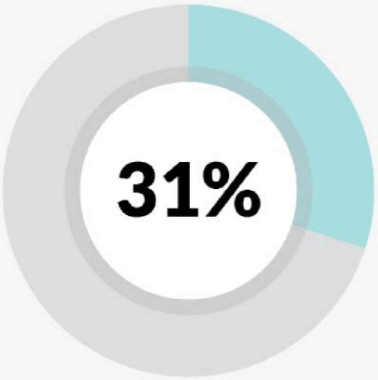
mimikatz.exe screenshot

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

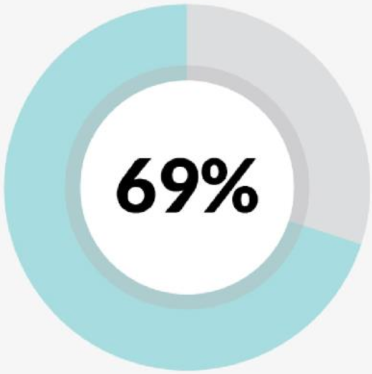
“Kuhook” Capabilities

Jason Rebholz, Manager, MANDIANT, a FireEye Company

How Compromises Are Being Detected



victims discovered the breach internally

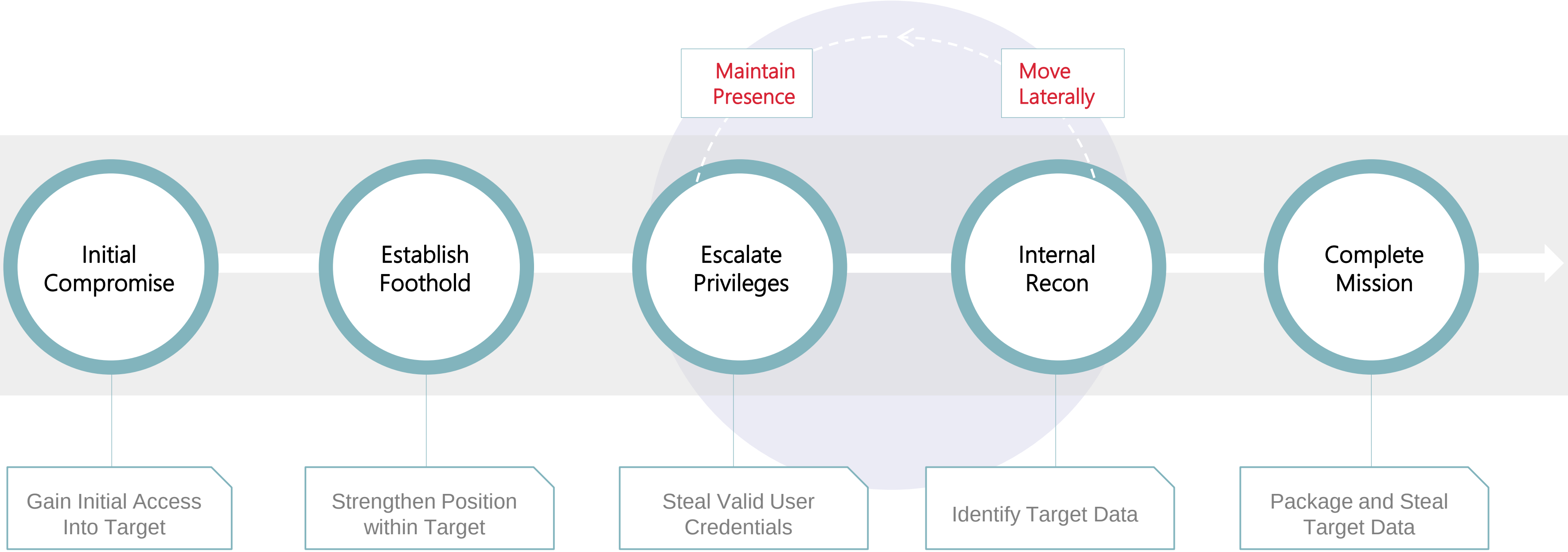


victims notified by an external entity

Anatomy of a Targeted Attack

VISA

MANDIANT
A FireEye® Company



Maintain Presence

Move Laterally

Initial Compromise

Establish Foothold

Escalate Privileges

Internal Recon

Complete Mission

Gain Initial Access Into Target

Strengthen Position within Target

Steal Valid User Credentials

Identify Target Data

Package and Steal Target Data

SOUMAT, MODPOS, Kuhook Malware

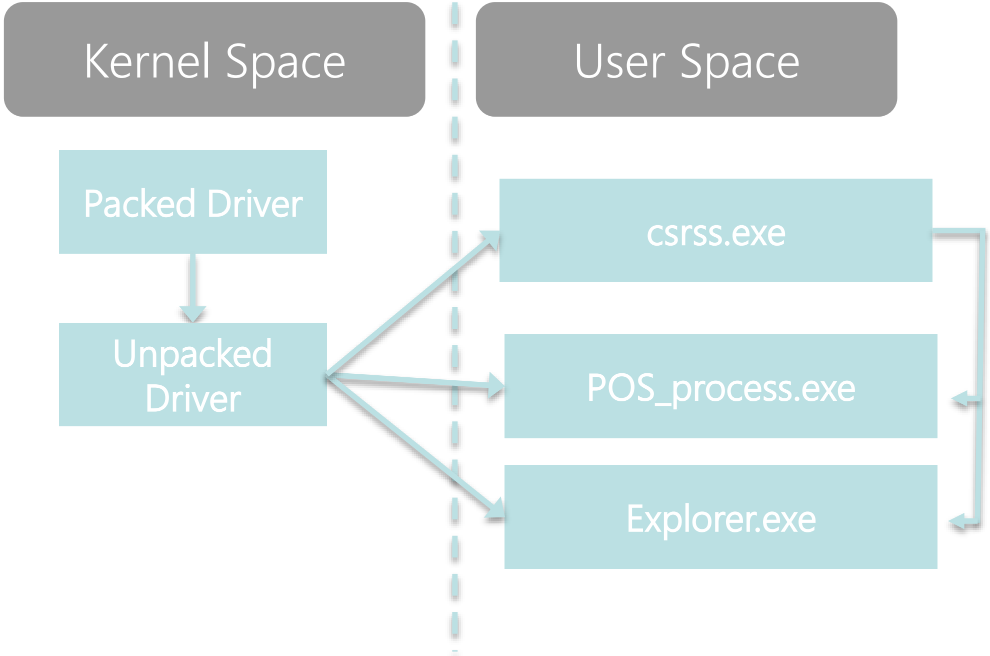
- Packed device driver that targets the Windows XP operating system
- Identified five variants
  - All packed with the same packer and contained nearly identical driver payloads
  - Primary difference was the functionality of the shell code
  - Variants identified by file size
- Persistence is maintained 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



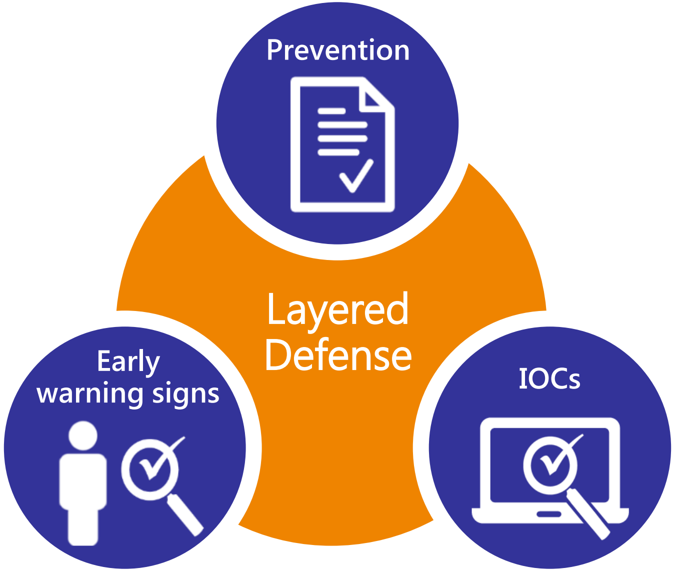
“Kuhook” Detection Strategies

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

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)

IOC	Type	Notes
91.207.61.208	Destination IP address	Command and control server
109.72.149.42	Destination IP address	Command and control server
130.0.237.22	Destination IP address	Command and control server
5.187.1.198	Destination IP address	Command and control server
ABA833D11679DFEBC95060BD3C557853	File MD5 hash	Malicious driver file
215BDF185C3B35503923FCF8872C75FC	File MD5 hash	Malicious driver file
F9C4E2D38DF8A87F545B6F5BA1F8691B	File MD5 hash	Malicious driver file
F21403B6CF7516B37EFFC17F410CED6F	File MD5 hash	Malicious driver file
6FBD31E7B5A31F5F75BD0D858D3327B5	File MD5 hash	Malicious driver file
68F40544ACD5568BD782434CA0F5AEE5	File MD5 hash	Malicious backdoor file
540DF6480B393BFA39D2E7CEC608EA12	File MD5 hash	Password harvesting file
%SystemRoot%\system32\drivers	Install path	Malware install path
C:\windows\Installer\[random characters].bin	Path to log files	Keystroke logger, track 2 data logs
C:\windows\TEMP\[random characters].bin	Path to log files	Keystroke logger, track 2 data logs
C:\windows\TEMP\[random characters].temp	Path to log files	Encrypted status logs
HTTP POST /robots.txt	Network indicator	Network traffic to the /robots.txt POST request shows patterns in the request headers and server response that are consistent across all samples. • 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

- 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?