VISA SECURITY ALERT

6 March 2014

"CHEWBACCA" POS MALWARE

Distribution: Merchants, Acquirers
Who should read this: IT, Information Security, Incident Response

Summary

Chewbacca is a relatively new variation of malware (*Trojan.Win32.Fsysna.fej*) targeting Point of Sale (POS) systems that run on Microsoft Windows. Chewbacca utilizes keylogger and memory scraping/parsing functionality. The malware is privately utilized, meaning that it is not currently distributed through online criminal forums and therefore is not known to be widely available. Since approximately October 2013, the malware has been linked to several dozen merchant compromises.

Distribution and Installation

Since the Chewbacca malware is private at the moment (i.e. being used by a limited number of criminals), it is not yet clear how the malware is disseminated or what the total potential number of victims may be.

Analysis of current samples indicates that the Chewbacca malware installs a copy of itself in the Windows startup folder, as a file named "*spoolsv.exe*." Clearly, the file name disguises the Trojan as a Windows Print Spooler service executable, and placement in the Startup folder causes it to run automatically at Windows startup. It should be noted that unlike some malware, Chewbacca currently has no persistence mechanism and thus deleting the malicious *spoolsv.exe* executable and rebooting the infected machine will remove the malware.

Data-stealing capability

Chewbacca features two distinct data-stealing mechanisms: a generic keylogger and a memory scanner designed to specifically target POS systems. The memory scanner dumps a copy of a running process's memory and searches it using simple regular expressions for credit and debit card magnetic stripe data (track 1 and track 2). If a card number is found, the malware extracts it and enters it into a log. Extracted magnetic stripe data is stored within the "system.log" file inside the user's %temp% folder.

Network traversal and data exfiltration

One of the important innovations associated with the Chewbacca malware is that communication between an infected machine and the Command and Control (C2) server is handled through the TOR (The Onion Router) network. Using a network of encrypted relay systems, it is designed to conceal a user's identity along with the contents of his communications. Tor often communicates over TCP 443 and it can be difficult to distinguish from normal TLS network traffic. All communications are encrypted,

concealing the real IP address of the malware's C2 server(s), which makes network detection more difficult.

For Chewbacca to function properly on the TOR network, it requires a TOR proxy application, which is installed on the infected machine. It is here, on the POS system, where the best opportunity for detection exists. In addition to identifying the TOR client application itself (tor.exe) on a POS system, it is possible to detect TOR running on a Windows system by issuing "**netstat –nt**" from a Windows command prompt. Look for the TOR listener, typically running on TCP 9050.

Mitigation

Visa requires participants in the payment system to comply with all PCI-DSS requirements and we recommend taking the following preventative steps to address this specific threat:

- **Prevent the use of TOR on POS systems**. This can be done by adding TOR and its components (Tor, Vidalia, TOR Browser) to antivirus solutions and application blacklisting controls. Network filtering, particularly outbound traffic from POS systems, can also be used to disable the malware's ability to exfiltrate data.

- **Control the Windows Administrator account.** Data-stealing malware (like Chewbacca) 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.

- **Restrict permissions on Windows file sharing or disable file sharing altogether.** Unless absolutely necessary, 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.

Technical Threat Indicators

IOC	Type	Notes
%ALLUSERSPROFILE%\Start Menu\Programs\startup \spoolsv.exe	Filename	Attempt by the actors to hide the malware as a standard printer spooler application
%TEMP%\system.log	Filename	After installation, the key logger creates this file, logging keyboard events and windows focus changes
ekiga.net	Domain	Spoolsv.exe requests the public IP of the victim via a publicly accessible service at hxxp://ekiga.net/ip (which is not related to the malware)
86.64.162.35	IP	ekiga[.net] resolves to this IP. This is a legitimate service utilized by the malware to request the public IP of the victim
Mozilla / 4.0 (compatible; Synapse)	Non-Standard User Agent	Upon execution Chewbacca performs an external IP lookup by doing a GET request to ekiga[.]net, a legitimate service that replies with the IP address the request is sent from. The GET request is constructed with a non-standard User-Agent.
%TEMP%\tor.exe	Filename	Tor v0.2.3.25 is dropped as "tor.exe" to the user's Temp and runs with a default listing on "localhost:9050"
5ji235jysrvwfgmb.onion	C2	Chewbacca performs a memory scan on running processes with the following regular expressions and uploads the results via hxxp://ji235jysrvwfgmb.onion/recvdata.php
21f8b9d9a6fa3a0cd3a3f0644636bf09	MD5	Chewbacca binary is a PE32 executable compiled with Free Pascal 2.7.1 (the version dated 22.10.2013). The 5 MB file contains Tor 0.2.3.25 as well.
0392f25130ce88fdee482b771e38a3eaae90f3e2	SHA1	Chewbacca binary is a PE32 executable compiled with Free Pascal 2.7.1 (the version dated 22.10.2013). The 5 MB file contains Tor 0.2.3.25 as well.
31d4e1b2e67706fda51633b450b280554c0c4eb595b3a0606ef4ab8421a04dc9	SHA256	Chewbacca binary is a PE32 executable compiled with Free Pascal 2.7.1 (the version dated 22.10.2013). The 5 MB file contains Tor 0.2.3.25 as well.

Additional Resources

This malware targets Windows-based POS systems, including Windows XP. It should be noted that Microsoft's support ends in **April 2014 for Windows XP** and **January 2016 for Windows XP Embedded** operating systems. POS applications built on these platforms will be placed at increased risk.

- Microsoft Windows XP Support lifecycle timeline

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