FBI FLASH

FEDERAL BUREAU OF INVESTIGATION, CYBER DIVISION

27 May 2015

Alert Number

MC-000060-MW

Please contact the FBI with any questions related to this FLASH Report at either your local **Cyber Task Force** or **FBI CYWATCH**.

Email:
cywatch@ic.fbi.gov

Phone:
1-855-292-3937

Local Field Offices:
www.fbi.gov/contact-us/field

FBI Liaison Alert System

This product is released at TLP: GREEN. The information in this product is useful for the awareness of all participating organizations as well as with peers within the broader community or sector. Recipients may share this information with peers and partner organizations within their sector or community, but not via publicly accessible channels.

The FBI is providing the following information with **high confidence**:

Summary

Cybercriminals continue to deploy Point of Sale (PoS) malware[1] due to the number of targets connected to the Internet and large potential profits. In the past year, there has been an increase in restaurants, casinos, hotels, and resorts targeted by PoS malware. Cybercriminals infect victim networks to extract credit card information and quickly monetize it within cybercriminal forums.

Technical Details

The FBI is providing PoS malware indicators regarding a recent network intrusion against a restaurant chain. The FBI is distributing these indicators to enable network defense activities and to reduce the risk of similar attacks in the future. The FBI has **High Confidence** that these indicators were involved in past network intrusions and will continue to be utilized in the future by cybercriminals. The FBI recommends that organizations help victims identify and remove the malicious code.

An ongoing FBI investigation revealed the following indicators:

- Analysis of the suspected malware files found the text strings "C:\Users\Bosko\Desktop\jusched-full\dllx64.pdb" and "dllx64.dll.InstallHooks.RemoveHooks" within the memory

[1] PoS malware scans for and scrapes unencrypted, plaintext credit card data (Track 1 and Track 2) found in RAM of the PoS system PoS System refers to the payment process computer and card reader/terminal that end users interact with by sliding their credit card to make a payment transaction.

process space.

- The FBI believes with **High Confidence** the behavior of this PoS malware is consistent with prior reporting on a new family of malware identified as Punkey by Trustwave.[2] The malware in this case appears to exfiltrate data through POSTs to a server with variable “unkey=”, as seen in the prior Punkey variant.
- The infected computer also had a rogue remote access tool (RAT) “\svchost.exe” (MD5: e72b313d807a536d45b68e52c1257996), which launched with parameters "-service" and "-nogui”. VirusTotal showed the file is a renamed version of Amyy Admin, a known RAT. The FBI has no current indication that the installation of Amyy Admin is connected to the use of this PoS malware.

[2] See https://www.trustwave.com/Resources/SpiderLabs-Blog/New-POS-Malware-Emerges---Punkey/ for the full report.

Federal Bureau of Investigation, Cyber Division

Flash Notification

File Name	Dllx64.dll
MD5:	5df3a909bb3e8f71ca11f376581f921e
SHA-1:	1e0febe55d1b4069ba2c30838e77d44d4c9cd7fd
SHA-256:	bc07262b062e6a4b5b9f38d71a961299a014c4da6c7d63c91dd285994fb3d790
Filetype:	PE32 executable for MS Windows (DLL) (GUI) Intel 80386 32-bit
Filesize:	34304
SSDeep:	384:onkkqmFM2bHOvdjDiWuxg6j5hI/Orj+iDXIJ5Z3JlhR/EDHvW50nucMxr7C9NuZZ:okk76YlhXeizIJr/EDPWunaq9N

File Name	jusched.exe
MD5:	be46b05244db7f51fc6d19019e12f04a
SHA-1:	4c1b05a294e41077c835516096da178691046189
SHA-256:	6d78550d140061607557bac7c9ba70787e9589b200758f4ab8d59f6504bb7563
Filetype:	PE32 executable for MS Windows (GUI) Intel 80386 32-bit
Filesize:	370208
SSDeep:	6144:V8ctX4jJ+5VUY6ZA3Vul0C1rv5c3Oan00hhG2jdqwLoOpsDXB:VkcVUXAlioOan00i2jsMoOps9

Administrative Note

This product is marked TLP: GREEN. The information in this product is useful for the awareness of all participating organizations as well as with peers within the broader community or sector. Recipients may share this information with peers and partner organizations within their sector or community, but not via publicly accessible channels. No portion of this product should be released to the media, posted to public-facing Internet Web sites, or transmitted over non-secure, external communications channels.