POS and Credit Cards: In the Line of Fire with “PunkeyPOS”

pandasecurity.com/mediacenter/malware/punkeypos/

June 23, 2016

PandaLabs, Panda Security’s anti-malware laboratory, has been working on an in-depth investigation since May related to Point of Sale terminals (POS) in restaurants across the United States. A new malware sample was discovered during this investigation called **PunkeyPOS, a malware variant that is able to access credit card data**. PandaLabs left this information at the disposal of American law enforcement so they can take the appropriate actions. Let’s see what this is and how it operates.

How can they steal your card without touching your wallet?

PunkeyPOS runs seamlessly in all Windows operating systems. The cyber-criminal’s plan is to install the malware in POS terminals in order to steal sensitive information such as account numbers, magnetic strip contents (tracks) from bank cards, etc.

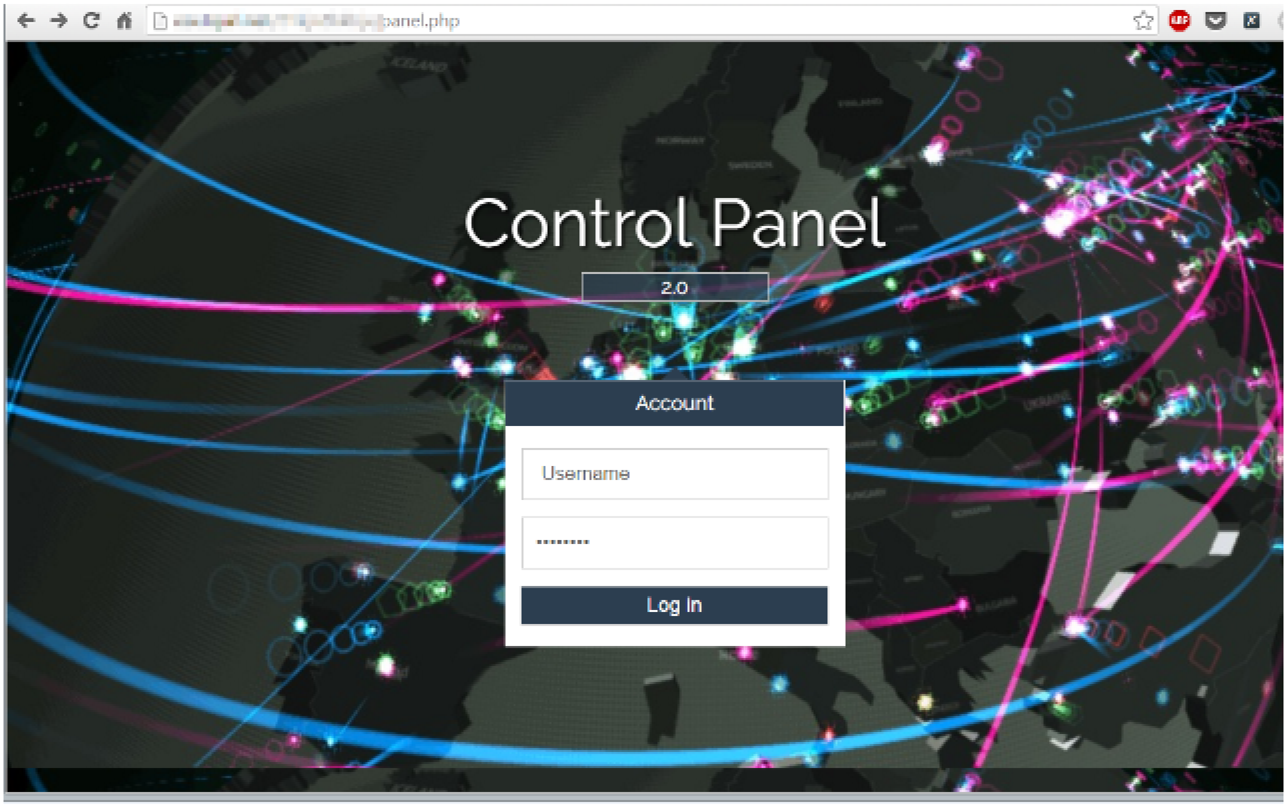
PunkeyPOS seems simple:

It installs a *keylogger* that is responsible for monitoring keystrokes, then it installs a *RAM-scraper* that is responsible for reading the memory of all processes running on the system.

Based on the information it captures, the malware performs a series of controls to determine what is valid and what isn't. Regarding the keystrokes, PunkeyPOS ignores all information other than credit card data. It is mostly interested in *tracks1/2* from the process memory that is obtained from *RAM-scraping*. The POS terminals read this information from the bank cards' magnetic strips and then can use this data to clone the cards at a later time.

Once the relevant information has been obtained, it is encrypted and forwarded to a remote web server which is also the *command and control (C&C)* server. In order to avoid the detection of the card information in case somebody is scanning the network traffic, it is encrypted before it is sent using the AES algorithm.

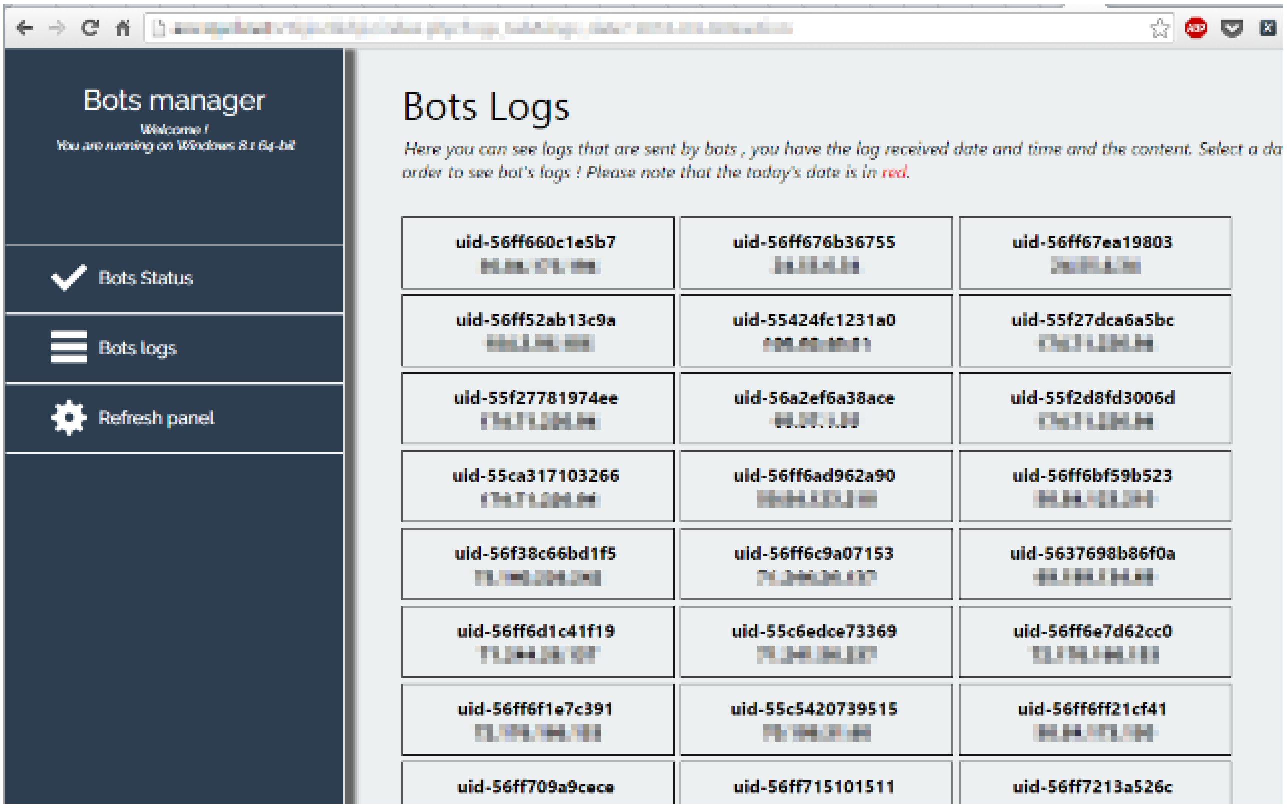
The *command and control (C&C)* server address can be easily obtained based on this malware sample through reverse engineering or analyzing their communications. This is the main page of the control panel; it requires a username and password to get access:



Follow the Trail to the Digital Pickpocketers

The cyber-criminals behind this attack haven't been very careful. Since the server was not configured correctly, PandaLabs was able to access it without credentials.

Because of their neglect, PandaLabs was able to see where PunkeyPOS sends the stolen information. In addition to being in front of a panel that is used to access the stolen data, from this panel cybercriminals can reinfect or update current clients (POS bots).



[redacted]

Bots manager

Welcome !
You are running on Windows 8.1 64-bit

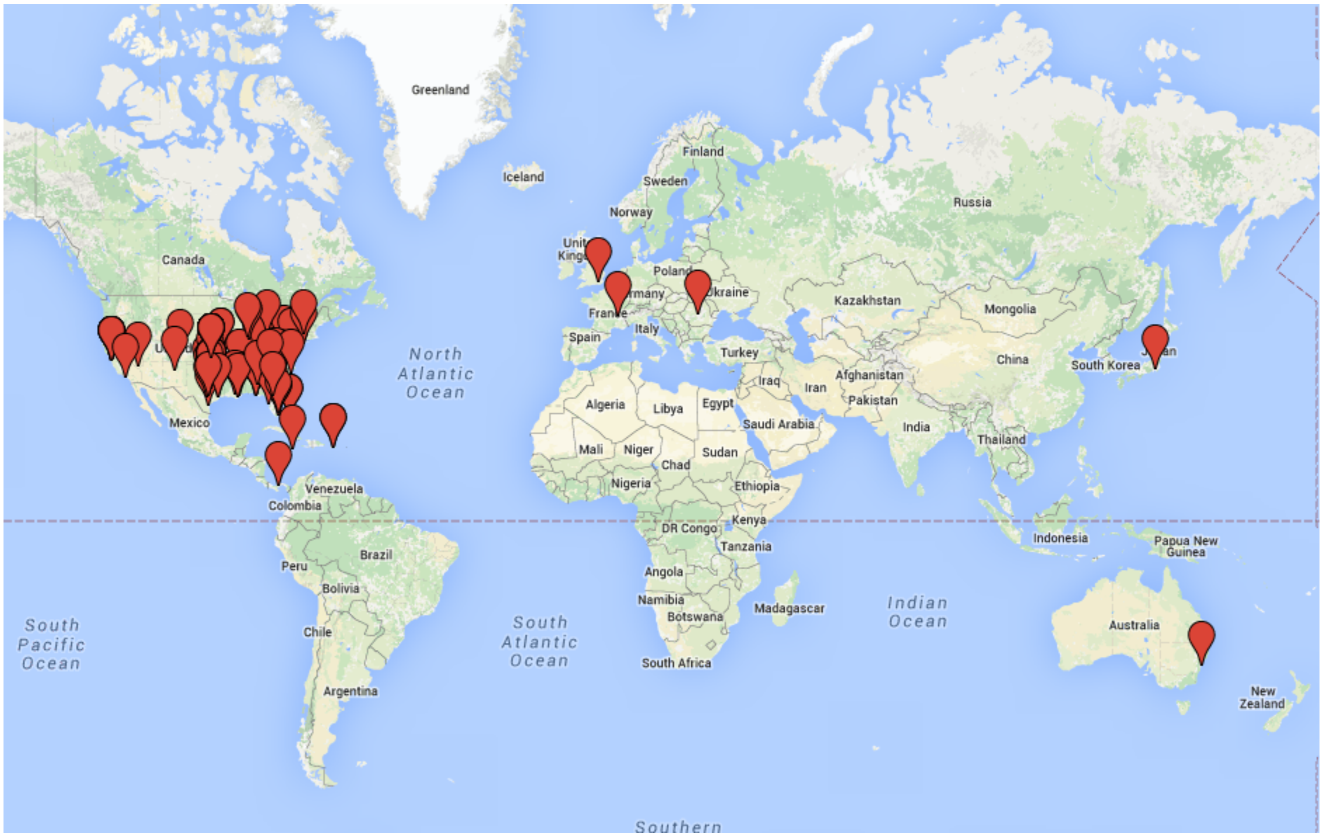
Bots Logs

Here you can see logs that are sent by bots , you have the log received date and time and the content. Select a da
order to see bot's logs ! Please note that the today's date is in red.

uid-56ff660c1e5b7 [redacted]	uid-56ff676b36755 [redacted]	uid-56ff67ea19803 [redacted]
uid-56ff52ab13c9a [redacted]	uid-55424fc1231a0 [redacted]	uid-55f27dca6a5bc [redacted]
uid-55f27781974ee [redacted]	uid-56a2ef6a38ace [redacted]	uid-55f2d8fd3006d [redacted]
uid-55ca317103266 [redacted]	uid-56ff6ad962a90 [redacted]	uid-56ff6bf59b523 [redacted]
uid-56f38c66bd1f5 [redacted]	uid-56ff6c9a07153 [redacted]	uid-5637698b86f0a [redacted]
uid-56ff6d1c41f19 [redacted]	uid-55c6edce73369 [redacted]	uid-56ff6e7d62cc0 [redacted]
uid-56ff6f1e7c391 [redacted]	uid-55c5420739515 [redacted]	uid-56ff6ff21cf41 [redacted]
uid-56ff709a9cece	uid-56ff715101511	uid-56ff7213a526c

The version of the analyzed PunkeyPOS sample is hardcoded: “2016-04-01”. If we compare this sample with older versions, some from 2014, we can barely see any difference in the way it operates (in the References section of this article you can find links that will go further into detail about how it works.)

PandaLabs has been able to gain access to the control panel of PunkeyPOS, and has geolocated around 200 Point of Sale terminals that were compromised by this specific malware variant. We can see that virtually all the victims are in the United States:



Taking into account how easy it is to sell this information on the black market, and how convenient it is to compromise these POS terminals anonymously through the internet, we are certain that cyber-criminals will be increasingly drawn to these terminals.

Protect your devices proactively from these types of attacks with an **advanced cyber-security solution** like Adaptive Defense. Real-time control of all inappropriate user operations is in your hands.

References:

http://krebsonsecurity.com/2016/06/slicing-into-a-point-of-sale-botnet/

https://www.trustwave.com/Resources/SpiderLabs-Blog/New-POS-Malware-Emerges—Punkey/

Panda Security

Panda Security specializes in the development of endpoint security products and is part of the WatchGuard portfolio of IT security solutions. Initially focused on the development of antivirus software, the company has since expanded its line of business to advanced cyber-security services with technology for preventing cyber-crime.

2 comments

Leave a Reply

Your email address will not be published. Required fields are marked *

*

*

*