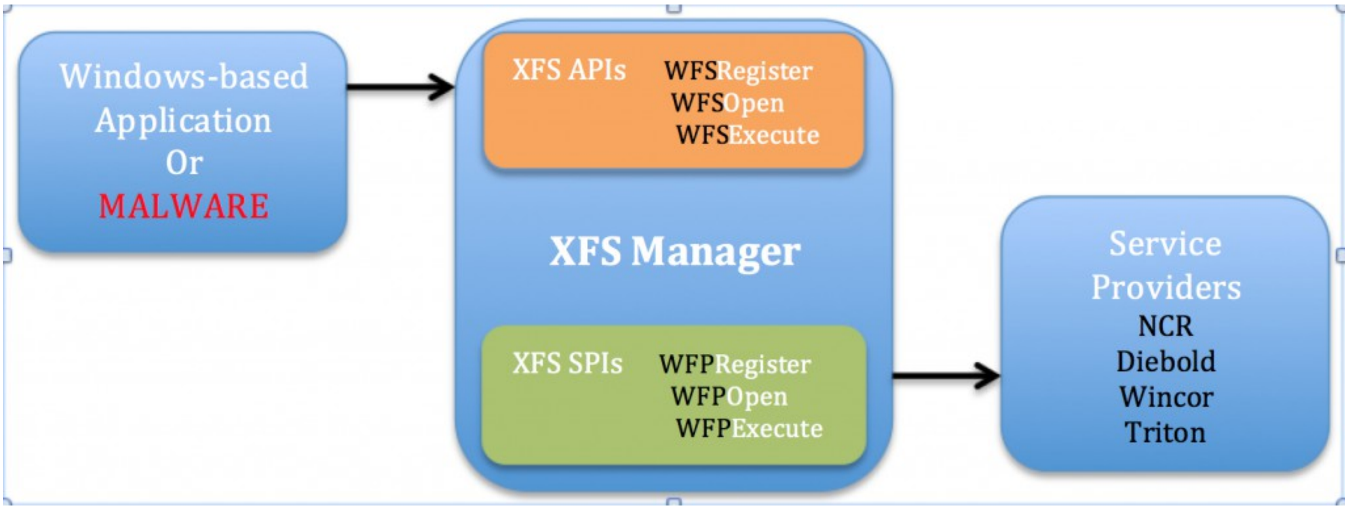
Backdoor.ATM.Suceful – ATM Malware Like No Other

Author: Milena Dimitrova+ | September 15, 2015 | 0 Comments

PC security ATM malware, backdoor, credit card, debit card

Name	Backdoor.ATM.Suceful
Type	ATM Malware, Backdoor
Short Description	Suceful is the first ATM malware to target physical debit and credit cards.
Symptoms	The victim's card can be retained.
Distribution Method	Backdoor.
Detection tool	Download Malware Removal Tool, to See If Your System Has Been Affected By Backdoor.ATM.Suceful

Stealing money online has never been easier. ATM malware, along with other online money theft scams, has been quite popular during the last couple of years. One of the latest ATM 'viruses' enables criminals to physically harvest debit and credit cards inserted into automated teller machines, or as they're known for short – ATMs. The malware is dubbed Suceful and, most likely, has been created on August 25, 2015.



ImageSource: FireEye

The malicious piece has been identified by the research team at FireEye. The malevolent threat was detected as

Backdoor.ATM.Suceful. If you notice something weird about the Suceful name, there is a simple explanation. Its authors made a spelling mistake.

Backdoor.ATM.Suceful Technical Review

We have already written about the various types which enable cyber criminals to steal money online. PoS malware and ATM malware pieces are one of them. What is interesting about Backdoor.ATM.Suceful is it incorporates features never seen in ATM threats before. The new twist, as pointed out by FireEye, is directly targeting the cardholders. Even though Suceful is most likely still in development, its characteristics make it a fearful one.

The malware is smartly designed. It permits the authors to test if it operates properly. When the word Suceful is displayed within the testing interface, it means that the attack was… successful, indeed. Backdoor.ATM.Suceful shares similarities with other ATM threats that have been detected in previous years, such as Ploutus and PadPin. What is common with the three of them is they interact with a middleware called XFS Manager. XFS Manager is a part of the WOSA/XFS[3] Standard used by major vendors.

Suceful may have several malicious capabilities in Debold and NCR ATMs:

- Reading all credit/debit card track data.
- Reading data from the chip of the card.
- Malware control via ATM PIN pad.
- Retention or ejection of the card on demand – this feature could be used to steal physical cards.
- Suppressing ATM sensors to avoid detection.
- XFS Manager.

Backdoor.ATM.Suceful Attack Explained

Once the distribution is initiated and defined as successful, Suceful will establish a connection with the XFS manager. Then, a session with the peripheral devices will be started through the Service Providers and XFS manager. Here, the first parameter is the Logical Device Name.

Once a session has been started, the APIs WFSExecute or WFSAsyncExecute can be applied to request certain operations to the peripheral devices. Here, the second parameter is the command to be executed.

As soon as this is done, the malware is ready to read debit card track data and chip, when a card is inserted. The malware can also wait to read it when the card is inserted or pulled through.

The DLL Hooking Feature

FireEye research indicates that DLL Hooking is also used. Even though the technique is not innovative, the reason it is being applied here is quite intriguing. Backdoor.ATM.Suceful can control and monitor all the commands given to the peripheral devices.

As explained by the FireEye research team, controlling and monitoring is done by changing the first 6 bytes of the

API Entry point with a push , ret instruction to redirect execution.

Backdoor.ATM.Suceful Attack: the Conclusion

Since Suceful is the very first multi-vendor ATM malware aiming at cardholder, it is not easy to presume what might happen. Furthermore, there is no way to determine whether a card is retained because of the malware. Researchers' advice is to have the contact number of your bank and call it, while keeping an eye on the ATM.

Backdoor.ATM.Suceful is not only created to steal the tracks of the card but also to steal the card itself. This is what makes Suceful a unique piece of ATM malware.

How Can I Protect My Banking Information?

Read More about Online Money Theft in 2015

Banking malware is one of the biggest concerns in today's cyber crime. US Intelligence research indicates that more than $1 billion alone were stolen in 2008 in ATM skimming. Cyber crime, as a total, has cost the world economy at least $400 billion. How can users protect their personal information? Even though it is quite difficult to protect one's debit and credit card, users can protect their personal information. Having a strong anti-malware software running in real time and sustaining healthy surfing habits are the best tips in online security today.

Spy Hunter scanner will only detect the threat. If you want the threat to be automatically removed, you need to purchase the full version of the anti-malware tool.Find Out More About SpyHunter Anti-Malware Tool / How to Uninstall SpyHunter

*By: **Berta Bilbao**. If you find this article useful please comment and follow me in G+*

← Previous post Next post →