Skimer Malware Targets ATMs

This is a security alert for all TruShield clients, the financial services industry, and the community at large. We have learned of a recent wave of threats targeting the financial service industry. The threat is a malware known as Skimer that targets ATMs.

About the malware

Skimer is a malware that was discovered by Kaspersky Lab in 2009 and it was the first malware to attack ATMs. Kaspersky Lab identified 49 variations of the malware and 37 of them are aimed at ATMs. In May, a new and improved version of Skimer was discovered and is challenging to evaluate. This is because the malware is concealed with a packer called Themida. According to Kaspersky researchers, Themida is a genuine packer that has been abused by many malware developers and it packs both the infector and the dropper. A malicious actor may use this malware at ATMs to dispense money and steal credentials from the card such as pin numbers and card numbers of victims.

How it works?

In action, the malware drops a file named netmgr.dll. Then, depending on whether the file system is FAT32 it will drop the file in the folder System32, or if it is NTFS it will be dropped in the NTFS data stream corresponding to XFS, an executable name SpiService.exe. According to the Kaspersky researchers, the part where the malware is dropped within the NTFS data stream makes it difficult to evaluate.

After the malware enters the system successfully it reboots the ATM and the malicious library uses a new LoadLibrary call to load into the SpiService.exe. The malware is then able to interact with the device by gaining total access to XFS. The attackers control the malware by using two types of cards with specially crafted track 2 data. “One of the cards is designed for executing commands hardcoded in Track 2, while the other allows attackers to launch one of 21 predefined commands using the PIN pad and the malware interface,” As stated by Kovacs from SecurityWeek.

Then a malicious actor may use this malware at ATMs to dispense money and steal credentials from the card such as pin numbers and card numbers of victims. They can also utilize the interface to erase the malware, troubleshoot it, and upgrade it with code saved on the special card.

Conclusion

ATMs machines are accessible to anyone and it takes one malicious actor to compromise such systems to wreak havoc. As ATM malware advance it will become harder to detect, but the right security controls will prevent it.

Kaspersky researchers recommended mitigation steps below:

- Detect infected ATM systems by observing within processing systems for card numbers that are in the Track2 IOCs below
- Regular AV scans
- Use whitelist technologies
- Device management policies
- Full disk encryption
- Protection of ATM BIOS with a password
- Only allowing HDD booting
- Isolating ATM network from any other internal bank networks

Indicators of Compromise

Hashes
F19B2E94DDFCC7BCEE9C2065EBEAA66C
3c434d7b73be228dfa4fb3f9367910d3
a67d3a0974f0941f1860cb81ebc4c37c
D0431E71EBE8A09F02BB858A0B9B80380
35484d750f13e763eae758a5f243133
e563e3113918a59745e98e2a425b4e81
a7441033925c390ddfc360b545750ff4
Filenames
C:\Windows\Temp\attrib1
C:\Windows\Temp\attrib4
C:\Windows\Temp\mk32
C:\Windows\Temp:attrib1
C:\Windows\Temp:attrib4
C:\Windows\Temp:mk32
C:\Windows\Temp:opt
C:\Windows\System32\netmgr.dll
Track 2 Data
******446987512*=**********
******548965875*=**********
******487470138*=**********
******487470139*=**********
******000000000*=**********
******602207482*=**********
******518134828*=**********
******650680551*=**********
******466513969*=**********

References

https://securelist.com/blog/research/74772/atm-infector/

http://www.securityweek.com/atms-targeted-improved-skimer-malware

https://www.youtube.com/watch?v=hOcFy02c7x0

http://krebsonsecurity.com/all-about-skimmers/

TruShield Security Solutions

TruShield is a leading provider of Managed Security Services across the globe. We are dedicated to helping companies achieve success by making sure they are properly prepared against the current and emerging threats in today's digital world. Our service offerings include: Continuous, 24/7/365 Monitoring, Penetration Testing and Vulnerability Assessments, Audit and Compliance, and many other Managed Services such as Managed Firewalls and Hosted Log Management. We also offer Security Awareness Training and Management Consulting services.
Contact us today to find out how we can help you protect your organization and safeguard your information.

Contact Information:

Email: support@trushieldinc.com
Web: www.trushieldinc.com
Phone: (877)-583-2841

Follow us on:

Twitter: @TruShield
LinkedIn: https://www.linkedin.com/company/trushield-security-solutions
Facebook: https://www.facebook.com/trushieldinc