SUCEFUL, the first multi-vendor ATM malware

September 14, 2015 By Pierluigi Paganini

According to the malware researchers at FireEye Labs Suceful is the first multi-vendor ATM malware threatening the banking industry.

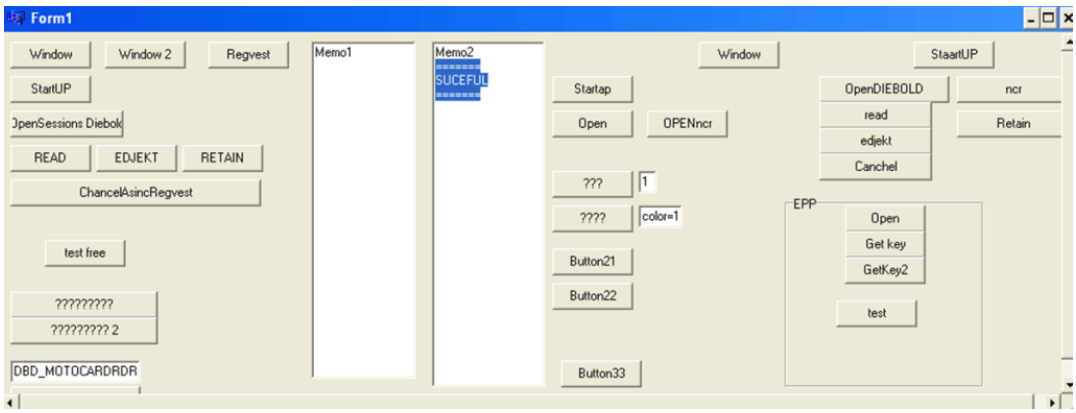
Experts at FireEye have discovered a new strain of malware dubbed Suceful (Backdoor.ATM.Suceful) specifically designed to target ATMs. Malware designed to hack ATMs are not new, in the past security experts have already detected malicious codes used to make ATMs dispense cash, such as Ploutus or Tyupkin.

Why Suceful is singular?

According to the malware researchers at FireEye Labs Suceful is the first multi-vendor ATM malware threatening the banking industry.

The variant detected by FireEye appears to have been created on August 25, it was recently uploaded to VirusTotal from Russia and experts speculate that it could be the result of ongoing development.

"FireEye Labs discovered a new piece of ATM malware (4BDD67FF852C221112337FECD0681EAC) that we detect as Backdoor.ATM.Suceful (the name comes from a typo made by the malware authors), which targets ***cardholders*** *and is able to retain debit cards on infected ATMs, disable alarms, or read the debit card tracks." states the blog post published by FireEye.*



Similar to other ATM malware, SUCEFUL interacts with a middleware called XFS Manager which is the interface between the application (malware in this case) and the peripheral devices (e.g., printer, dispenser, card reader, in pad).

Almost every vendor has its own implementation of the XFS Manager despite they also support the default XFS Manager template.

According to the experts in Diebold or NCR ATMs, SUCEFUL is able to read credit/debit card data, and suppressing ATM sensors to avoid detection.

The SUCEFUL capabilities in Diebold or NCR ATMs include:

1. *Reading all the credit/debit card track data*
2. *Reading data from the chip of the card*
3. *Control of the malware via ATM PIN pad*
4. *Retention or ejection of the card on demand: This could be used to steal physical cards*
5. *Suppressing ATM sensors to avoid detection*

FireEye is still investigating on the case, it has no evidence of how the crooks installed on SUCEF
on the ATMs.

Pierluigi Paganini

(Security Affairs – SUCEFUL , ATM)

ATM | Cybercrime | FireEye | Hacking | malware | SUCEFUL

Breaking News | Cyber Crime | Malware

Pierluigi Paganini

Pierluigi Paganini is Chief Information Security Officer at Bit4Id, firm leader in identity management, member of the ENISA (European Union Agency for Network and Information Security)Treat Landscape Stakeholder Group, he is also a Security Evangelist, Security Analyst and Freelance Writer. Editor-in-Chief at "Cyber Defense Magazine", Pierluigi is a cyber security expert with over 20 years experience in the field, he is Certified Ethical Hacker at EC Council in London. The passion for writing and a strong belief that security is founded on sharing and awareness led Pierluigi to find the security blog "Security Affairs" recently named a Top National Security Resource for US. Pierluigi is a member of the "The Hacker News" team and he is a writer for some major publications in the field such as Cyber War Zone, ICTTF, Infosec Island, Infosec Institute, The Hacker News Magazine and for many other Security magazines. Author of the

Books "The Deep Dark Web" and “Digital Virtual Currency and Bitcoin”.

PREVIOUS ARTICLE
Security Affairs newsletter Round 26 – Best of the week from best sources

YOU MIGHT ALSO LIKE

Vodafone Australia has hacked a Fairfax journalist’s phone

September 13, 2015 By Pierluigi Paganini

Lockerpin, the first known Android lock-screen ransomware

September 13, 2015 By Pierluigi Paganini