Monthly Research

Survey of POS Malware

FFRI, Inc.
http://www.ffri.jp

Ver 1.00.01

Agenda

- A case study of POS malware
- Security research of POS system
- Why is a POS system attacked by malware?
- Examples of POS malware; BlackPOS, Backoff
- Measures to POS malware
- Summary

A case study of POS malware

- A Large-scale information leakage incident on Target Corporation which is a retail giant in the United States
  - Time of occurrence
    - Until Christmas from autumn of 2013
  - Leaked Information
    - Credit card information: 40 million
    - Personal information: 70 million
  - This cyber attack is called “Kaptoxa”
  - Trojan.POSRAM was used
    - It is a variant of the POS malware called “BlackPOS”
    - Another 6 companies have been affected by this malware
  - As a result, the CEO of Target resigned in May 2014

Security research of POS system

- Security researchers have also focused on POS system
- At BlackHat USA 2014, there were 3 research presentations of POS system security as a new topic
  - POINT OF SALE SYSTEM ARCHITECTURE AND SECURITY
    - Dataflow analysis and typical attack vectors of POS system
  - A JOURNEY TO PROTECT POINTS-OF-SALE
    - Typical vulnerability of POS systems
    - Memory scraping technique
    - How to protect POS system
  - MISSION MPOSSIBLE
    - Vulnerability of mobile POS system
    - Demonstration of attack that malicious credit card drops a remote shell

Why is a POS system attacked by malware?

- OS for POS terminals
  - 8 suppliers of POS terminals adopt Windows OS
    - Those suppliers occupy about 97% of new sales shares of POS terminals (DSS Institute investigation)
    - We confirmed spec of some products of each supplier
  - Windows Embedded POSReady is used primarily
    - It is based on Windows Embedded Standard
    - It may have vulnerabilities just like PC
    - POS malware is developed using technique just like Windows malware
- Network environment
  - POS terminal may be connected to vulnerable network

An example of POS malware; BlackPOS

- BlackPOS
  - It is sold in underground hacking forum
  - The author is estimated to be the residence by Russia
  - Trojan.POSRAM was not detected by latest antivirus software at it was discovered
  - Technical information of Trojan.POSRAM have been described in the report "POS Malware Technical Analysis" by DHS and Multiple agencies
    - Following slides cite information contained in this report

Behavior of Trojan.POSRAM

- The attacker intrude the internal network in some way.
  Then, he was infected with POSRAM to POS terminal.
- Trojan.POSRAM is RAM Scraper
  - It steals decrypted authentication data (card number, CVV, etc.) by the following behavior:
    - Hooks process of payment application to extract data
      - pp.exe, PosW32.exe, pos.exe, epsenginesrv.exe
    - Saves authentication data to .dll file
    - At every 7 hours, checks to see at if time is between 10 a.m. and 5 p.m.
      If so, attempts to send the .dll to temporary share folder on an internal host (over TCP port 139, 443 or 80)
    - This step allows the attacker to remotely steal data from POS terminals

Combination Malware with Trojan.POSRAM

- ICMP Listener
  - Listens for custom ICMP packets to log dump transfers from a POS scraper to an internal LAN dump server
- Shellcode Loader
  - Receives raw commands across the network to be loaded and executed on a compromised host
  - Covertly subverts network controls and forensic to conceal all data transfers and executions
- Hacking Tools
  - Tools for network discovery, credential compromise, database operations and port forwarding

Concern about POS malware

- Leak of the source code of BlackPOS
  - The Report has warned POS malware will increase explosively soon because the source code of BlackPOS became easily available
  - In the future, custom made POS malware will be created, detection will be more difficult
- Another POS malware
  - The US-CERT warned about the new POS malware "Backoff" at July 31, 2014
  - It seems not a variants of BlackPOS
  - 7 POS system vendors have confirmed infection of this malware
  - The Secret Service estimates that over 1,000 U.S. businesses are affected

Another example of POS malware; Backoff

- The following information is shown in the report of US-CERT
- Backoff was not detected by latest antivirus at it was discovered
- There are 3 variants (ver. 1.4, 1.55, 1.56)
  - Change has been confirmed in October 2013 to July 2014
- Functions
  - RAM Scraping
  - Key Logger (exclude 1.4)
  - C&C(C2) communication by HTTP POST
  - Code injection into explorer.exe (exclude 1.55)

Measures to POS malware

- Present survey
  - Refer to technical information that has been published from security vendors and US-CERT
    - Investigate whether there is any suspicious files and processes in POS terminal and surrounding system
    - Investigate whether suspicious communication does not occur from POS terminal and surrounding system
    - Perform vulnerability assessment
- Precaution
  - Isolate network between POS terminal and office PC
  - Restrict IP address that can communicate with POS terminal
  - Apply security updates to POS terminal
    - Windows Update

(FYI) Detection of the POS malware by FFR yarai

- We got the POS malware samples by searching file hash

- The FFR yarai detected 6 samples by static scan
  - FFR yarai ver. 2.5.1192 on Windows 7

SHA-1	Family
332548d0bc638c8948f3a429e79053003b4f6261	BlackPOS
9d99a2446aa54f00af0b049f54afa52617a6a473	BlackPOS
11b7430026c82097657c145dcedfa818bf1032d3	Backoff
98dbaeb6d46bd09eca002e1f2b6f3e76fd3222cd	Backoff
a6eb86b55148a7a491093f1f6af6a15c4b44b96c	Backoff
ab354242992af39f93520ac356ec12796e119151	Backoff

Summary

- The Large-scale incident by POS malware occurred last year in the United States
- Security researchers have also focused on the POS system
  - New vulnerability of POS system may be discovered in future
- POS system is targeted by malware
  - Many POS systems are working on Windows
  - Multiple POS malware were found
  - The source code of BlackPOS was leaked
  - There is a risk that similar incidents also occur in Japan
  - Preventive measures and investigation of POS system are recommended

References 1

- レジやPOSを狙うマルウェア
  - http://blog.kaspersky.co.jp/ram-scrapers-and-other-point-of-sale-malware/
- 米小売業者のカード情報流出、Target以外にも6社が被害に
  - http://itpro.nikkeibp.co.jp/article/IDG/20140121/531183/
- 7000万件に及ぶ情報漏洩事件の「その後」、株価復調もCEOの辞任に発展した米Target
  - http://it.impressbm.co.jp/articles/-/11538
- Point of Sale System Architecture and Security
  - https://www.blackhat.com/docs/us-14/materials/us-14-Zaichkowsky-Point-Of-Sale%20System-Architecture-And-Security.pdf
- A Journey To Protect Points Of Sale
  - https://www.blackhat.com/docs/us-14/materials/us-14-Valtman-A-Journey-To-Protect-Point-Of-Sale.pdf
- Mission mPOSsible
  - http://www.youtube.com/watch?v=iwOP1hoVJEE
- 平成25年度・POSシステム販売状況調査結果
  - http://dssr.jp/news.html

References 2

- KAPTOXA Point of Sale Compromise
  - http://www.securitycurrent.com/resources/files/KAPTOXA-Point-of-Sale-Compromise.pdf
- POS Malware Technical Analysis
  - http://artemonsecurity.com/20140116_POS_Malware_Technical_Analysis.pdf
- Alert (TA14-212A) Backoff Point-of-Sale Malware
  - https://www.us-cert.gov/ncas/alerts/TA14-212A
- Backoff: New Point of Sale Malware
  - https://www.us-cert.gov/sites/default/files/publications/BackoffPointOfSaleMalware_0.pdf

Contact Information

E-Mail ：research—feedback@ffri.jp
Twitter：@FFRI_Research