Monthly Research

Latest Trends in Linux Malware

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

Ver 1.00.02

Introduction

- Linux based computing platform has increased
  - Server, mobile and embedded(incl. IoT)

- Malware of target to Linux system becomes too large to ignore
  - In virustotal statistics, 127,385 ELF binaries has submitted during the week of 2015/01/19
  - cf). 2,722,106 Win32 binaries has submitted in the same week
  - Not all ELF binaries are malware

- In this paper, we introduce trends in Linux malware and countermeasure against malware infection

ELF DDoS botnet（Chinese Chicken）

- Large DDoS botnets are widely observed in china since 2011
  - Peter and Jaromír have reported in botconf2014 https://www.botconf.eu/chinese-chicken-multiplatform-ddos-botnets/
  - The series of malware called China DDoS malware

- Botnets are used to real DDoS attacks for threatening in china
  - Targets: online gaming/casinos e-commerce shops and forums

- Typical malware
  - IptabLes/IptabLex
  - XOR.DDoS
  - AES.DDoS
  - ChinaZ

IptabLes/IptabLex (2013~)

- A minute report published by Akamai in 2014
  - Its called IptabLes/IptabLex
  - The malware infect using vulnerabilities of open source software such as Apache Struts, Tomcat and Elasticsearch
  - Exploiting newest vulnerabilities

- Some malware stores itself in /boot with the name “.IptabLes” or “.IptabLex”

References：
"IptabLes and IptabLex DDoS Bots Threat Advisory", September 3, 2014
http://www.stateoftheinternet.com/resources-web-security-threat-advisories-2014-iptables-iptablex-linux-bots-botnet.html

XOR.DDoS (2014~)

- An ELF malware
- The malware contains LKM（Linux Kernel Module）rootkits
  - Based on “Suterusu” open source LKM rootkit
- LKM rootkits hiding processes, files and other malware activity from security services and administrators

References：
"MMD-0028-2014 - Fuzzy reversing a new China ELF "Linux/XOR.DDoS""
http://blog.malwaremustdie.org/2014/09/mmd-0028-2014-fuzzy-reversing-new-china.html

AES.DDoS (2014~)

- An ELF malware is available for several architectures
  - EM_386, EM_x86_64, EM_MIPS, EM_ARM, PE x86
  - A MIPS architecture often used to router

- Targets of this malware are a wide variety of systems such as desktop, mobile, routers and IoT devices.

References：
“MMD-0026-2014 - Router Malware Warning | Reversing an ARM arch ELF AES.DDoS (China malware)”,
http://blog.malwaremustdie.org/2014/09/reversing-arm-architecture-elf-elknot.html

ChinaZ (2015~)

- The ELF malware intrudes into vulnerable host by the Shellshock vulnerability

References：
“MMD-0030-2015 New ELF malware on Shellshock: the ChinaZ”,
http://blog.malwaremustdie.org/2015/01/mmd-0030-2015-new-elf-malware-on.html

Trends in Linux Malware

- ELF malware are not sophisticated yet unlike windows malware
  - Today, antivirus vendor endeavor to raise detection rate of ELF malware
  - “Google's VirusTotal puts Linux malware under the spotlight” http://www.zdnet.com/article/googles-virustotal-puts-linux-malware-under-the-spotlight/

- On the other hand, Several ELF malware has execution portability
  - It is unique perspective in Linux system

References：
“Golangによるマルウェア(Japanese)”,
http://blog.0day.jp/2014/09/linuxgoarmbot.html

Malware Detection and Intrusion Detection in Linux

- Malware Detection
  - ClamAV, Linux Malware Detect etc.

- Intrusion Detection
  - AIDE
    - User-land integrity checker

  - Linux IMA (Integrity Measurement Architecture)
    - Kernel-level integrity measurement

Mitigation Techniques

- **USE SELINUX**
  - Intruder’s activity is limited to an application of attack surface

- Restrict outbound connections
  - Using C&C blacklist

Conclusions

- Linux based platform such as server, mobile and embedded has increased
  - ELF Malware has increased at the same time

- Several malware intrudes vulnerable host using latest vulnerabilities

- Administrators and developers should have control over all system components and response to new vulnerabilities
  - Should be considered anti-malware, intrusion detection and mitigation

References

- “virustotal += Detailed ELF information”
  http://blog.virustotal.com/2014/11/virustotal-detailed-elf-information.html
  (2015/01/26 viewed)
- “VirusTotal/Statistics”
  https://www.virustotal.com/ja/statistics/
  (2015/01/26 viewed)
- “Linux DDoS Trojan hiding itself with an embedded rootkit”
  https://blog.avast.com/2015/01/06/linux-ddos-trojan-hiding-itself-with-an-embedded-rootkit/
- Linux-Malware−Detect
  https://www.rfxn.com/projects/linux-malware-detect/
- Linux-IMA
  http://sourceforge.net/p/linux-ima/wiki/Home/

Contact Information

E-Mail : research—feedback@ffri.jp

Twitter : @FFRI_Research