HaboMalHunter

An Automated Malware Analysis Tool for Linux ELF Files

{Jingyu YANG, Zhao LIU}@Tencent
Agenda

- Introduction
- Background
- Architecture
- Implementation
- Demonstration
- Conclusion
Introduction

**Habo Analysis System**

- https://habo.qq.com/en
  - Username: BlackHatAsia17
  - Password: Habo@BlackHat17
  - expired on May, 2017

- The Project
  - https://github.com/Tencent/HaboMalHunter
Habo Analysis System

File name: ca38391f0eb69e8e355b385...3e94fb5bff5db7351014886
MD5: 2adf8194c30f3638152f1635096cfdc8
File type: ELF64
Upload time: 2017-03-21 15:11:06
Copyright: N/A
Version: N/A
Shell or compiler: N/A

Key behaviour

Behaviour: Lock file itself
Detail info: process=/usr/sbin/dropb, user=root, access=...e.

Process

Behaviour: Execute a file
Detail info: execve:/tmp/bin/****.elf
Behaviour: Process exit
Background

- Dose Linux virus exist?
- Difference between Windows Malware
  - quantity
  - categories
- Impact
- Related Works
Categories

• Windows
  • Downloader
  • RAT
  • Backdoor
  • Keylogger
  • PUA
  • Ransomware
Architecture

VM Scheduler

Analyze Controller
- Static Analyzer
- ELF Loader
- Dynamic Analyzer

Log Processor
Implementation

- Static Analysis
  - ELF formats
  - Interesting strings
- ELF Loader
- Dynamic Analysis
  - Process
  - I/O
  - Network
  - System Calls
  - Memory Forensics
Demonstration

- Linux.Gafgyt
  - 2adf8194c30f3638152f1635096cfdc8
- Linux. Gates
  - foeacba95df5e796114a930b97b33053
YARA Rules
Linux.Gafgyt

```python
rule Linux_Gafgyt
{
  //Unix.Trojan.1;Engine:51-255,target:6;(0&l&2&3&4&5&6&7
meta:
  Author  = "Jingle"
  Date    = "2016/11/21"
  Description = "Linux/Gafgyt malware"
strings:
  $s0 = "%d.%d.%d.%d"
  $s1 = "PING"
  $s2 = "PONG"
  $s3 = "PROBING"
  $s4 = "KILLATTACK"
  $s5 = "JUNK"
  $s6 = "CNC"
$elf = {7f 45 4c 46} // ELF header
condition:
  $elf in (0..4) and all of ($s*)
}
```
rule Linux_Gates
{
    meta:
    Author = "Jingle"
    Date = "2016/11/10"
    Description = "Linux/Gates malware"
    Reference = "http://www.freebuf.com/articles/system/117823.html"
    strings:
    $s0 = "libamplify.so"
    $s1 = "AttackSyn"
    $s2 = "AttackDns"
    $elf = { 7f 45 4c 46 } // ELF
    condition:
    $elf in (0..4) and all of ($s*)
Conclusion

• Linux Malware
• Benefits of HaboMalHunter
  • Automated
  • Malware Report
  • YARA Rules
• Malware Research
  • https://github.com/Tencent/HaboMalHunter
References


