HaboMalHunter

An Automated Malware Analysis Tool for Linux ELF Files

{Jingyu YANG, Zhao LIU }@Tencent

Agenda

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

Introduction

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

Secure https://habo.qq.com/en/file/detail?md5=2adf8194c30f3638152f1635096cfdc8

Habo Analysis System

File name:	ca38391f0eab69e8e355b385...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.

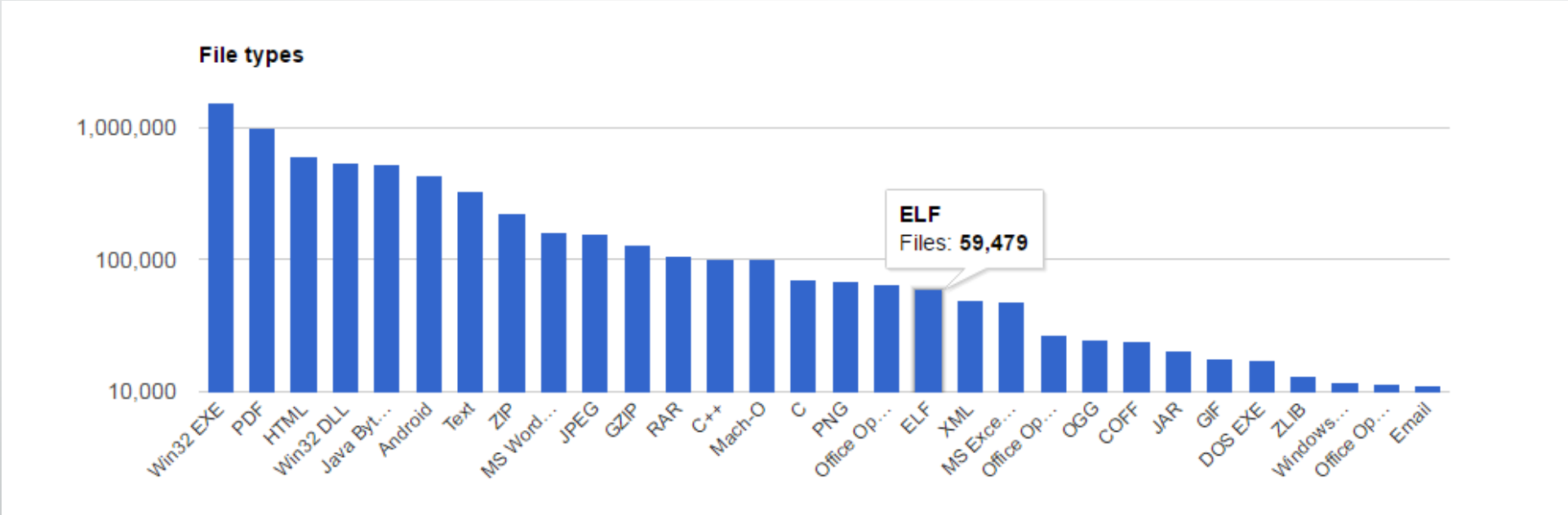
Process

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

Background

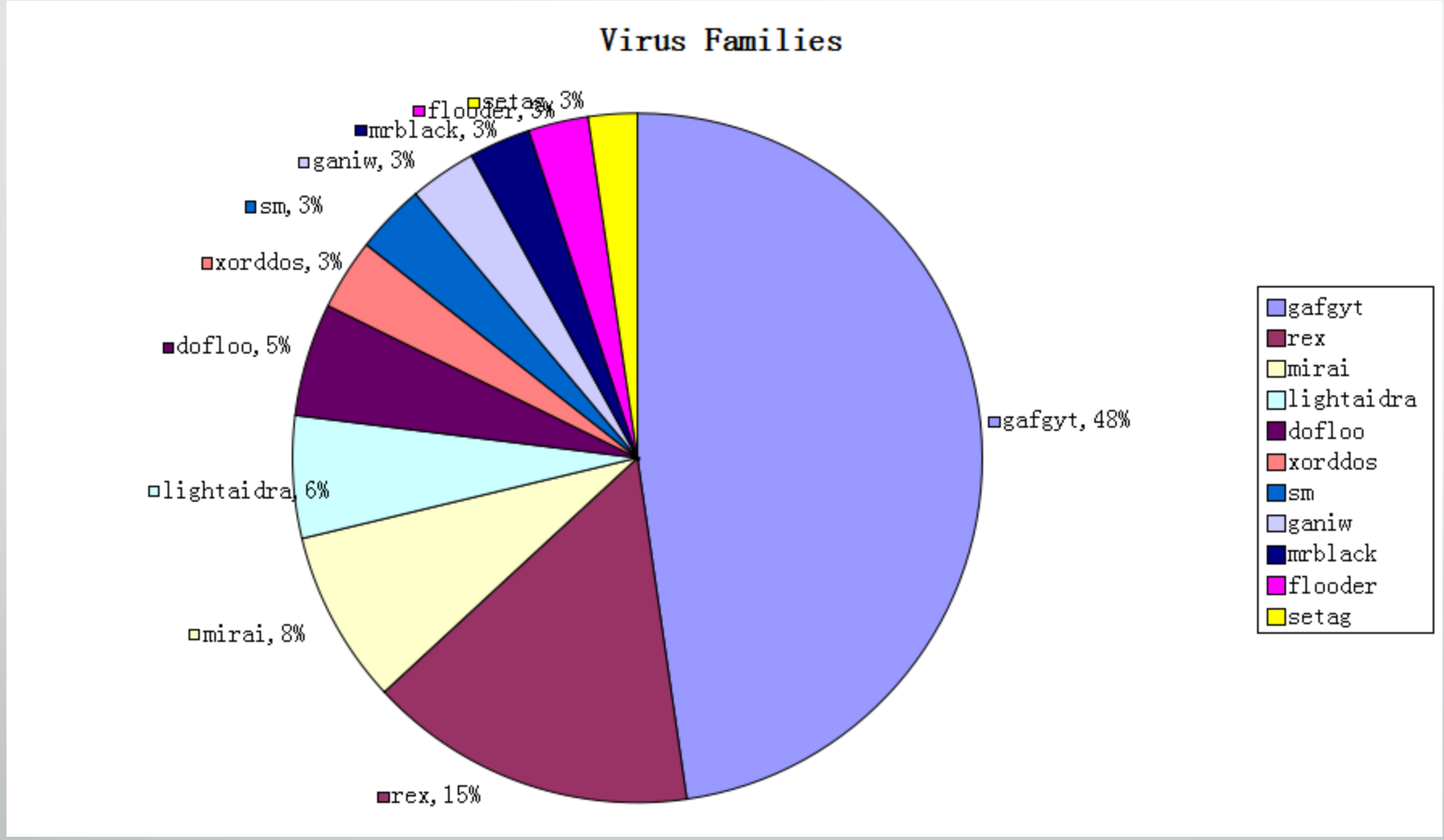
- Dose Linux virus exist?
- Difference between Windows Malware
  - quantity
  - categories
- Impact
- Related Works

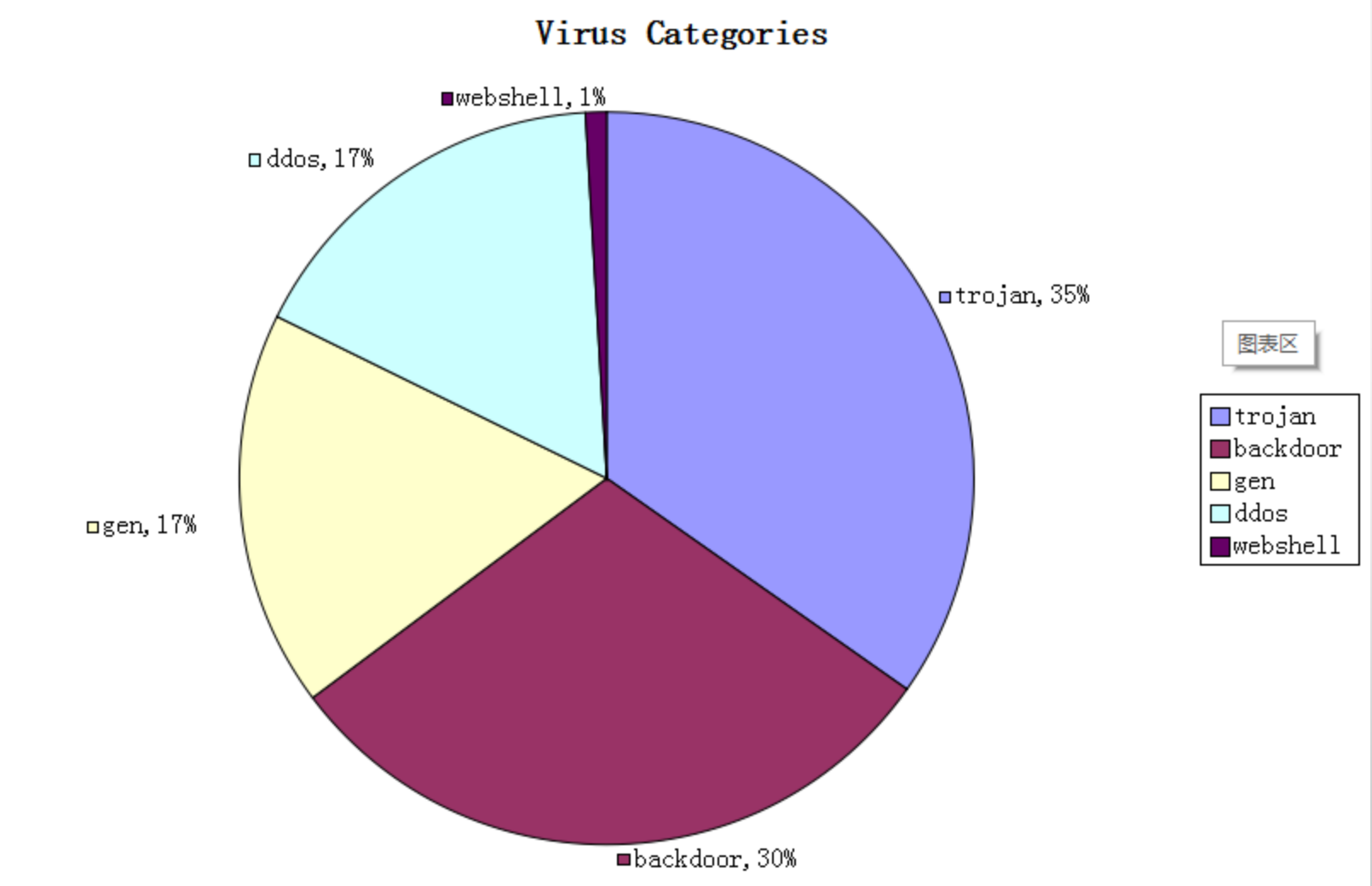
Quantity


File types
1,000,000
100,000
10,000
ELF
Files: 59,479
Win32 EXE
PDF
HTML
Win32 DLL
Java Byt…
Android
Text
ZIP
MS Word…
JPEG
GZIP
RAR
C++
Mach-O
C
PNG
Office Op…
ELF
XML
MS Exce…
Office Op…
OGG
COFF
JAR
GIF
DOS EXE
ZLIB
Windows…
Office Op…
Email

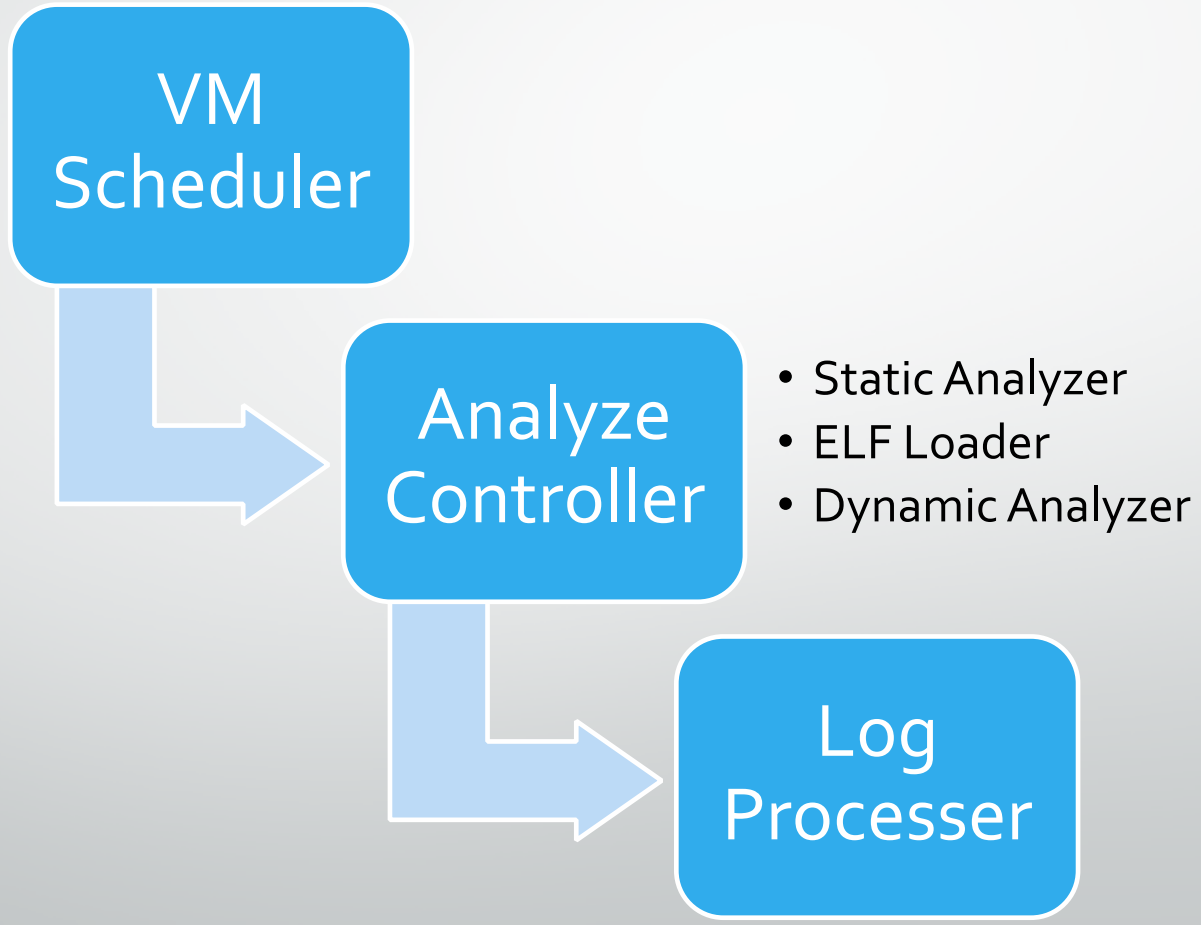
Categories

- Windows
  - Downloader
  - RAT
  - Backdoor
  - Keylogger
  - PUA
  - Ransomware


Virus Families
setag, 3%
flooder, 3%
mrblack, 3%
ganiw, 3%
sm, 3%
xorddos, 3%
dofloo, 5%
lightaidra, 6%
mirai, 8%
rex, 15%
gafgyt, 48%
gafgyt
rex
mirai
lightaidra
dofloo
xorddos
sm
ganiw
mrblack
flooder
setag


Virus Categories
webshell, 1%
ddos, 17%
trojan, 35%
gen, 17%
backdoor, 30%
图表区
trojan
backdoor
gen
ddos
webshell

Architecture



- Static Analyzer
- ELF Loader
- Dynamic Analyzer

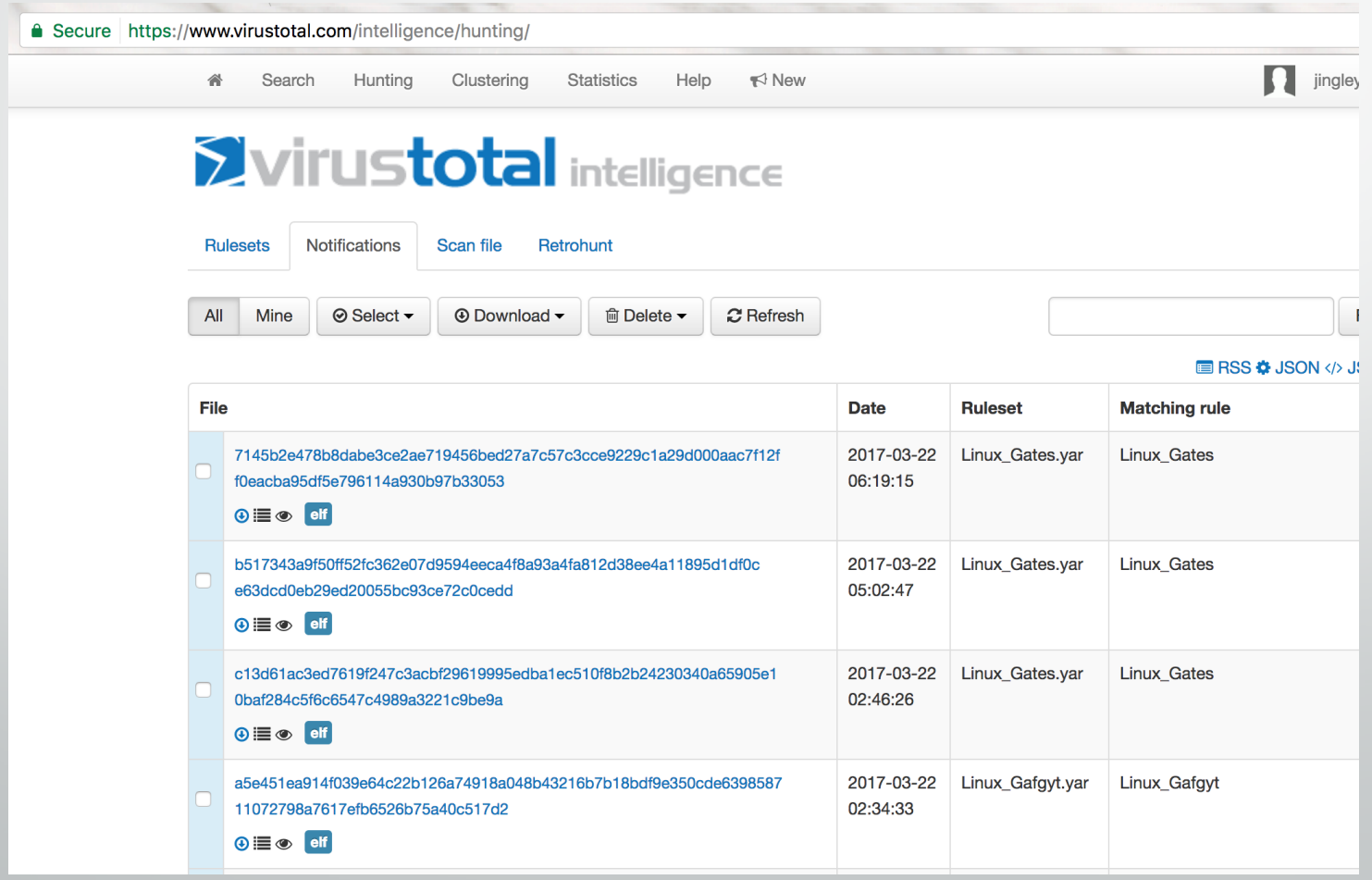
Implementation

- 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


Secure https://www.virustotal.com/intelligence/hunting/
Search
Hunting
Clustering
Statistics
Help
New
virustotal intelligence
Rulesets
Notifications
Scan file
Retrohunt
All
Mine
Select
Download
Delete
Refresh
RSS
JSON
File
Date
Ruleset
Matching rule
7145b2e478b8dabe3ce2ae719456bed27a7c57c3cce9229c1a29d000aac7f12ff0eacba95df5e796114a930b97b33053
elf
2017-03-22 06:19:15
Linux_Gates.yar
Linux_Gates
b517343a9f50ff52fc362e07d9594eeca4f8a93a4fa812d38ee4a11895d1df0ce63dcd0eb29ed20055bc93ce72c0cedd
elf
2017-03-22 05:02:47
Linux_Gates.yar
Linux_Gates
c13d61ac3ed7619f247c3acbf29619995edba1ec510f8b2b24230340a65905e10baf284c5f6c6547c4989a3221c9be9a
elf
2017-03-22 02:46:26
Linux_Gates.yar
Linux_Gates
a5e451ea914f039e64c22b126a74918a048b43216b7b18bdf9e350cde639858711072798a7617efb6526b75a40c517d2
elf
2017-03-22 02:34:33
Linux_Gafgyt.yar
Linux_Gafgyt

Linux.Gafgyt

Linux_Gafgyt.yar

```
rule Linux_Gafgyt
{
    //Unix.Trojan.1;Engine:51-255,target:6;(0&1&2&3&4&5&
    meta:
        Author  = "Jingle"
        Date    = "2016/11/21"
        Description = "Linux/Gafgyt malware"
    strings:
        $s0 = "%d.%d.%d.%d"
        $s1 = "PING"
        $s2 = "PONG"
        $s3 = "PROBING"
        $s4 = "KILLATTK"
        $s5 = "JUNK"
        $s6 = "CNC"
        $elf = {7f 45 4c 46} // ELF header
    condition:
        $elf in (0..4) and all of ($s*)
}
```

Linux. Gates

Linux_Gates.yar

Save

```
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

1. White Paper: https://github.com/Tencent/HaboMalHunter/blob/master/WhitePaper.md
2. YARA: The pattern matching swiss knife for malware researchers, http://virustotal.github.io/yara/
3. Monnappa, Automating Linux Malware Analysis Using Limon Sandbox. Black Hat 2015.
4. Guarnieri, C., Tanasi, A., Bremer, J., & Schloesser, M. (2012). The cuckoo sandbox.