FastResponder: New Open Source weapon to detect and understand a large scale compromise
“About us”

French Company in Cyber Security
Cert Sekoia
Detection Intrusion experts
Digital Forensics and Incidence Response
Co-Organizer of #BotConf
Members of Honeynet Project
“Symantec Executive Says Antivirus is Dead”

1/3 of malware is customized (no signature available at time of exploit)

85% of breaches took weeks or more to discover (+6%)

91% of organizations believe exploits bypassing their IDS and AV systems

(VzB, 2012)  
(VzB, 2012)  
(Ponemon)

Wall Street Journal 2014, May 4th - Brian Dye, senior vice-president Symantec
Our 3 objectives

**Fast Data Acquisition** for Detection of compromises

**Fast Analysis** of an attack

**Fast Incident Response** to mitigate the impact
Common denominator after an attack?

Traditional Forensic investigation
Common denominator of traditional forensic?

Slow
Painful
Expensive
Business independent
Old fashioned holistic approach tools

Hardware for data acquisition

Software for data acquisition

Spreadshit macroro for data analysis
What is #FastForensic?

Easy to use
Focused
Fast
Context aware
#FastForensic: a all new approach

- Specialized hardware for data acquisition
- 1 click software for data acquisition
- « Big data » technologies for data analysis
Process

Detection

Assessment

Intelligence

Datas → Alerts → Interested parties
Process | A Lean Cybersecurity approach

Detection

Datas

Assessment

Intelligence

Alerts

Interested partie
Large company integrated model

Information sources
- AV
- IDS
- AD
- ...

Logs collection / correlation
- Collection → Correlation

SOC L1
- Referentiels,
- HR
- CMDB
- Interested parties

1. Event recording
2. Event assessment
3. Threat intelligence
4. Remediation
5. Feedback
6. Workshop, reporting

SOC L2 CERT

Sec community

Business Lines
Large company integrated model

Information sources

- AV
- IDS
- AD
- ...

Logs collections / correlation

- collection
- correlation

SOC L1
- Referentiels,
- HR
- CMDB
- Interested Parties

Malware Intl

SOC L2
- CERT

Security community

Business Lines

1. Event recording
2. Event assessment
3. Threat intelligence
4. Remediation
5. Feedback
6. Workshop, reporting

1 Click Forensic
So we have develop FastResponder
Focus on FastResponder

Need for a fast artefact acquisition tool, easy to use and robust

Source: SANS Windows Forensic FOR 408
Focus on FastResponder

- Decoding MBR and BootSector
- Dump MFT
- MD5 files of drive system
- Detect malicious files with yara signatures
FastResponder: Enter the code

*Python 2.7 + ctypes*
*PyWin32*
*WMI requests*
*Psutils*
*Events logs new channels*
*Export CSV*
*CLI or Config File*
*Detect encoding of Operating System*
FastResponder: On IR

- Very simple to distribute and collect the results
- Very simple to use
- The program doesn’t crash of an decoding artefact
- Easy to add a artefact source
- Fast Collector
FastResponder: On IR

- *Profile collector like volatility*
- *Choose an artefact to collect to minimize and concentrate searching*
- *One module, one source of artefacts*
- *With CSV, you can index in ELK or Splunk results*
- *You can deploy by script or GPO the .exe*
- *MD5 of all files to compare with your threat intel data base*
- *You can use your threat intel signatures with yara integration*
FastResponder: Demo time
FastResponder: Future Features

Ram Dump and analyses
DNS Cache
Embedded Certificates in PE
Multi Browser history
Windows 8.1/10
Console collect like Viper or Meterpreter
For the community

https://github.com/SekoiaLab/FastResponder
Thanks to CERT team
Sébastien Larinier
Sebastien.larinier@sekoia.fr
@sebdraven

SEKOIA
16, Place de la Madeleine
75008 Paris

www.sekoia.fr