Paravirtualized Honeypot Deployment for the Analysis of Malicious Activity

Andronikos Kyriakou – @andronkyr
Member of SCYTALE Research Group

Presentation Outline

1. Introduction to Honeypots
2. System Implementation
3. Data Analysis
4. Results
5. Future Work

whoami

Undergraduate Student @ Computer Engineering & Informatics Department (CEID)

Member of SCYTALE Research Group:
http://www.scytale.ceid.upatras.gr/

Interests: Honeypots, Penetration Testing, Forensics

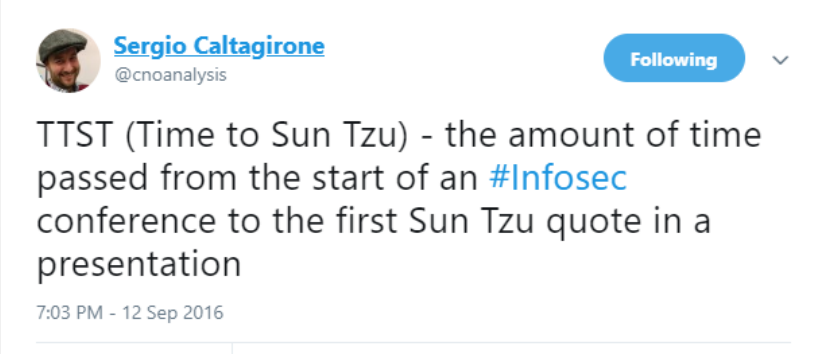
Twitter: @andronkyr
Email: andronkyr@outlook.com
Website: http://www.andronkyr.com

1.Introduction to Honeypots

SCYTALE group

“If you know the enemy and know yourself, you need not fear the result of a hundred battles.”

Sun Tzu, The Art of War



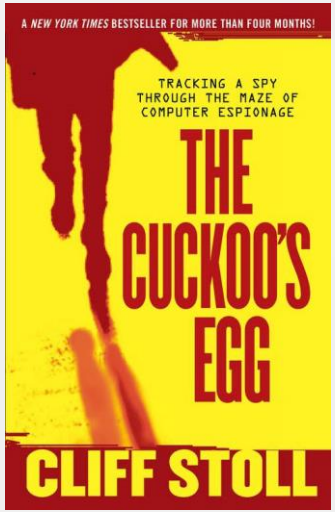
Honeypot Fundamentals

"A security resource whose value lies in being probed, attacked or compromised" - Lance Spitzner

Detect & Learn from Attacks

History of Honeypots

- 1990-91: Clifford Stoll's “The Cuckoo's Egg”
- 1997: Fred Cohen’s Deception Toolkit
- 1999: Formation of the Honeynet Project



Why use a Honeypot?

- Mean Time to Detect ~ 206 days
- Mean Time to Respond ~ 55 days

- Production vs Research Honeypots
- Complementary to Intrusion Detection Systems & Firewalls

Categorization based on level of interaction

Low Interaction

Easy to install & configure

Emulation of services

Response in predetermined manner

Limited amount of information

Medium Interaction

Emulation of applications

Abillity to capture malware and attack techniques

High Interaction

Real OS, nothing restricted

No production value

Cowrie

- Medium Interaction SSH & Telnet Honeypot
- Developed by Michel Oosterhof, successor of Kippo Honeypot
- Written in Python

- Fake filesystem and shell
- SFTP support – Downloads files using wget for later examination
- Logging to JSON

- https://github.com/micheloosterhof/cowrie

Replay of Attack – gweerwe323f

```
andronikos:~/Desktop/Backup Server$ python playlog.py 20180420-025136-44f2fdc095f2-0i.log
```

Dionaea – *catches bugs*

- Low interaction honeypot
- Protocols: SMB, ftp, http, https, mssql, mysql, sip, upnp, tftp and others
- Nepenthes successor, initially developed @ GSoC 2009 by The Honeynet Project
- Python as scripting language

- Uses Libemu to detect shellcode
- Logs to JSON & SQLite db

- https://github.com/DinoTools/dionaea

Glastopf

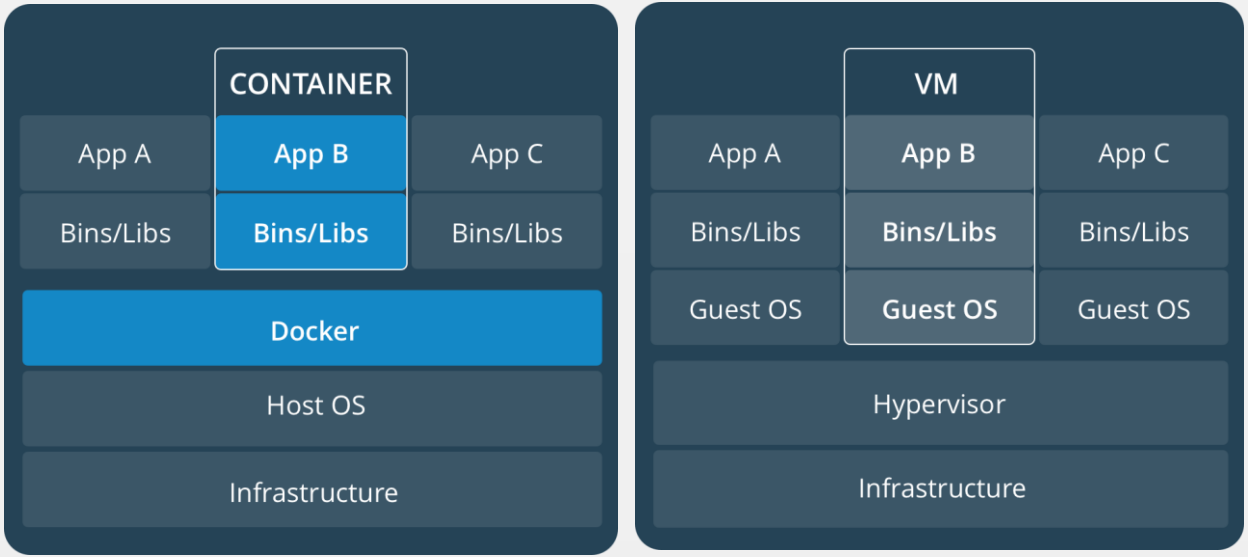
- Low Interaction Web Application Honeypot by Lukas Rist
- Written in Python

- Vulnerability type emulation
- Attack type emulation included: Remote file inclusion. Local file inclusion, HTML injection via POST
- Logging to SQLite db

- https://github.com/mushorg/glastopf

2. System Implementation

Docker



Source: https://www.docker.com/what-container#/package_software

Docker-compose

```yaml
glastopf:
  container_name: glastopf
  restart: always
  image: glastopf:latest
  networks:
    - glastopf_net
  ports:
    - "80:80"
  volumes:
    - /data/glastopf:/opt/myhoneypot
```

Docker-compose

```
user@snf-813372: ~
File  Edit  View  Search  Terminal  Help
user@snf-813372:~$ sudo docker-compose -f honeypot.yaml ps
  Name                 Command               State                Ports
-------------------------------------------------------------------------------
cowrie      /cowrie/cowrie-git/bin/cow      Up      0.0.0.0:22->2222/tcp,
            ...                                     0.0.0.0:2223->2223/tcp
dionaea     /opt/dionaea/bin/dionaea        Up      0.0.0.0:11211->11211/tcp,
                                                    0.0.0.0:135->135/tcp,
                                                    0.0.0.0:1433->1433/tcp,
                                                    0.0.0.0:1723->1723/tcp,
                                                    0.0.0.0:1883->1883/tcp,
                                                    0.0.0.0:1900->1900/udp,
                                                    0.0.0.0:21->21/tcp,
                                                    0.0.0.0:3306->3306/tcp,
                                                    0.0.0.0:42->42/tcp,
                                                    0.0.0.0:443->443/tcp,
                                                    0.0.0.0:445->445/tcp,
                                                    0.0.0.0:5060->5060/tcp,
                                                    0.0.0.0:5060->5060/udp,
                                                    0.0.0.0:5061->5061/tcp,
                                                    0.0.0.0:69->69/udp,
                                                    0.0.0.0:8081->80/tcp
glastopf    glastopf-runner                 Up      0.0.0.0:80->80/tcp
user@snf-813372:~$
```

Load Balance

```
 1  [||||||||||||                                                    18.0%]   Tasks: 72, 161 thr; 3 running
 2  [||||||||||||||||||||||||||||||||||||||||||||||||||||||||||||||||99.3%]   Load average: 1.12 1.20 1.22
 Mem[||||||||||||||||||||||||||||||||                            1.16G/3.86G]   Uptime: 33 days, 07:25:33
 Swp[                                                                0K/0K]

  PID USER      PRI  NI  VIRT   RES   SHR S CPU% MEM%   TIME+  Command
 7046 root       20   0 1054M  687M 19488 R 113. 17.4 10:17.07 /opt/dionaea/bin/dionaea
 7140 root       20   0 1054M  687M 19488 S 12.5 17.4  0:20.17 /opt/dionaea/bin/dionaea
 7267 user       20   0 26296  4036  3140 R  1.3  0.1  0:00.34 htop
 1103 root       20   0  539M 65916 13540 S  1.3  1.6 15h57:43 /usr/bin/dockerd -H fd://
 7141 root       20   0 1054M  687M 19488 S  1.3 17.4  0:22.45 /opt/dionaea/bin/dionaea
 1115 root       20   0  539M 65916 13540 S  0.7  1.6  3h40:46 /usr/bin/dockerd -H fd://
 7038 root       20   0  7520  4556  3220 S  0.7  0.1  0:00.95 docker-containerd-shim -namespace moby -workdir /var/lib/docker/containerd/daemon/io.co
 2781 root       20   0  539M 65916 13540 S  0.0  1.6 53:05.75 /usr/bin/dockerd -H fd://
 1945 root       20   0  398M 22884  4188 S  0.0  0.6  2h52:44 docker-containerd --config /var/run/docker/containerd/containerd.toml
 1954 root       20   0  398M 22884  4188 S  0.0  0.6 15:19.18 docker-containerd --config /var/run/docker/containerd/containerd.toml
 7031 root       20   0  7520  4556  3220 S  0.0  0.1  0:01.34 docker-containerd-shim -namespace moby -workdir /var/lib/docker/containerd/daemon/io.co
 1118 root       20   0  539M 65916 13540 S  0.0  1.6 57:39.78 /usr/bin/dockerd -H fd://
 3125 root       20   0  539M 65916 13540 S  0.0  1.6 49:01.44 /usr/bin/dockerd -H fd://
 1946 root       20   0  539M 65916 13540 S  0.0  1.6  1h05:20 /usr/bin/dockerd -H fd://
 1950 root       20   0  398M 22884  4188 S  0.0  0.6 15:18.97 docker-containerd --config /var/run/docker/containerd/containerd.toml
 7268 postfix    20   0 85404  8652  7720 S  0.0  0.2  0:00.03 smtpd -n smtp -t inet -u -c -o stress= -s 2
 7269 postfix    20   0 67476  4428  3964 S  0.0  0.1  0:00.01 proxymap -t unix -u
 1948 root       20   0  398M 22884  4188 S  0.0  0.6 24:48.80 docker-containerd --config /var/run/docker/containerd/containerd.toml
 7254 user       20   0 92828  3528  2600 S  0.0  0.1  0:00.01 sshd: user@pts/0
 7032 root       20   0  7520  4556  3220 S  0.0  0.1  0:00.36 docker-containerd-shim -namespace moby -workdir /var/lib/docker/containerd/daemon/io.co
 6797 user       20   0  109M 61048  9372 S  0.0  1.5  0:04.46 /cowrie/cowrie-git/cowrie-env/bin/python2 /cowrie/cowrie-git/cowrie-env/bin/twistd --um
    1 root       20   0  117M  5524  3196 S  0.0  0.1  5:02.19 /sbin/init
  350 root       20   0 40876  7980  3208 S  0.0  0.2  2:53.36 /lib/systemd/systemd-journald
  375 root       20   0  100M   960   776 S  0.0  0.0  0:00.00 /sbin/lvmetad -f
  391 root       20   0 44780  4000  2728 S  0.0  0.1  2:28.07 /lib/systemd/systemd-udevd
  653 root       20   0  4396  1308  1220 S  0.0  0.0  0:00.00 /usr/sbin/acpid
  713 root       20   0  280M  5076  3996 S  0.0  0.1  2:06.72 /usr/lib/accountsservice/accounts-daemon
F1Help  F2Setup F3SearchF4FilterF5Tree  F6SortByF7Nice -F8Nice +F9Kill  F10Quit
```

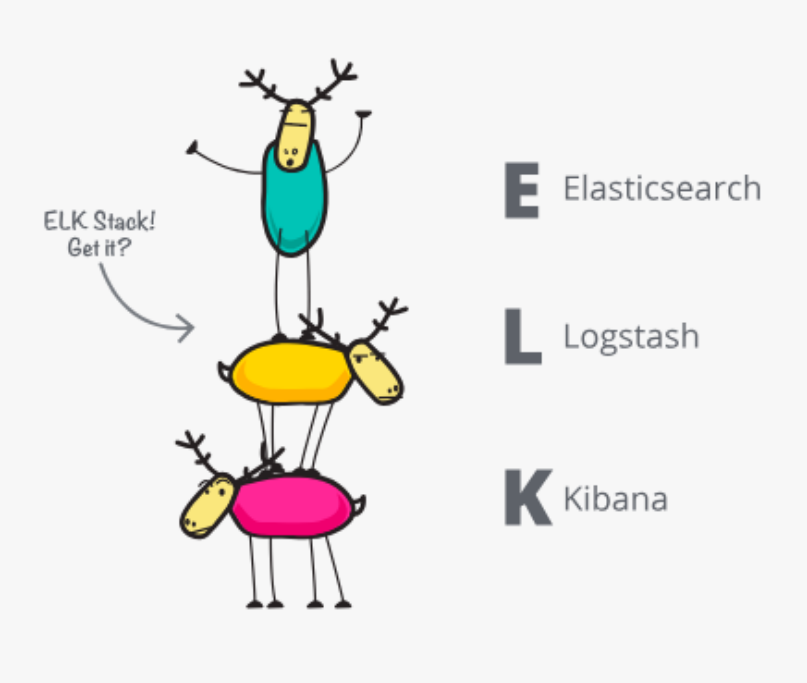
Looks Like a Real System!

```
andronikos:~$ nmap [redacted]

Starting Nmap 7.60 ( https://nmap.org ) at 2018-06-12 19:39 EEST
Nmap scan report for [redacted]
Host is up (0.040s latency).
Not shown: 985 closed ports
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
25/tcp   open  smtp
42/tcp   open  nameserver
80/tcp   open  http
135/tcp  open  msrpc
443/tcp  open  https
445/tcp  open  microsoft-ds
1433/tcp open  ms-sql-s
1723/tcp open  pptp
3306/tcp open  mysql
5060/tcp open  sip
5061/tcp open  sip-tls
8081/tcp open  blackice-icecap
8090/tcp open  opsmessaging
```

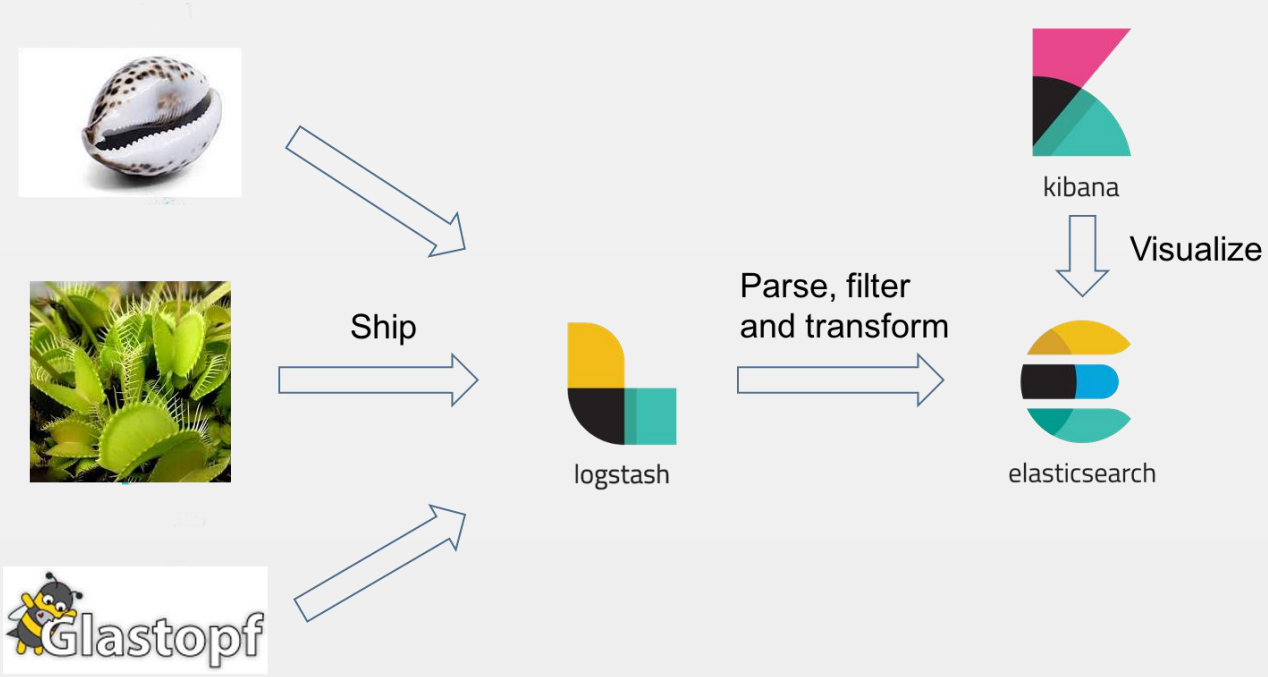
```
root:~# nmap -sS -sV [redacted]

Starting Nmap 7.60 ( https://nmap.org ) at 2018-06-12 19:39 EEST
Nmap scan report for [redacted]
Host is up (0.038s latency).
Not shown: 985 closed ports
PORT     STATE SERVICE      VERSION
21/tcp   open  ftp          Synology DiskStation NAS ftpd
22/tcp   open  ssh          OpenSSH 6.0p1 Debian 4+deb7u2 (protocol 2.0)
25/tcp   open  smtp         Postfix smtpd
42/tcp   open  nameserver?
80/tcp   open  http         Apache httpd 2.0.48
135/tcp  open  msrpc?
443/tcp  open  ssl/https?
445/tcp  open  microsoft-ds Dionaea honeypot smbd
1433/tcp open  ms-sql-s     Dionaea honeypot MS-SQL server
1723/tcp open  pptp          (Firmware: 1)
3306/tcp open  mysql        MySQL 5.7.16
5060/tcp open  sip          (SIP end point; Status: 200 OK)
5061/tcp open  ssl/sip-tls?
8081/tcp open  http         nginx
8090/tcp open  http         nginx 1.10.3 (Ubuntu)
```

3. Data Analysis

Elastic Stack



System Overview



Malware Analysis

- Access to Academic API
- 20k API requests per day at 1k requests per minute

4. Results

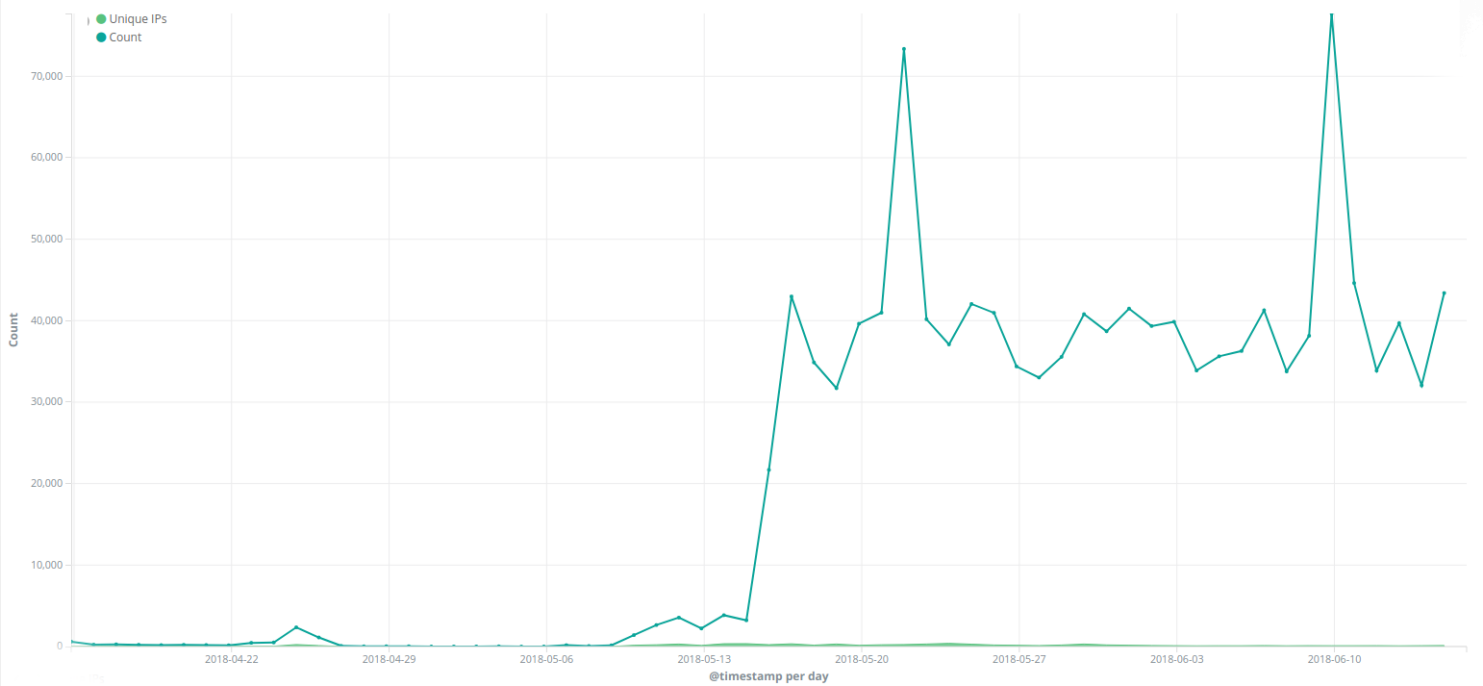
Event Captured

1,537,588 - Dionaea

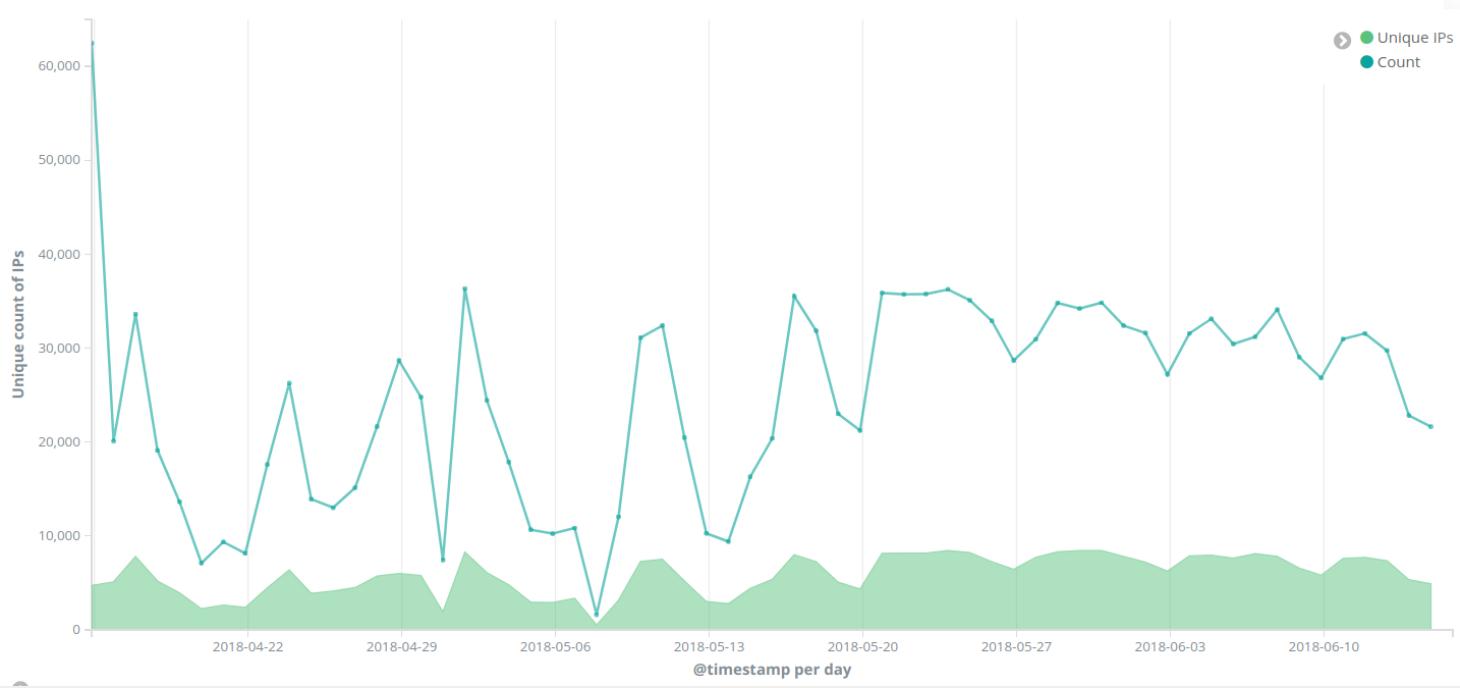
1,255,283 - Cowrie

7,944 - Glastopf

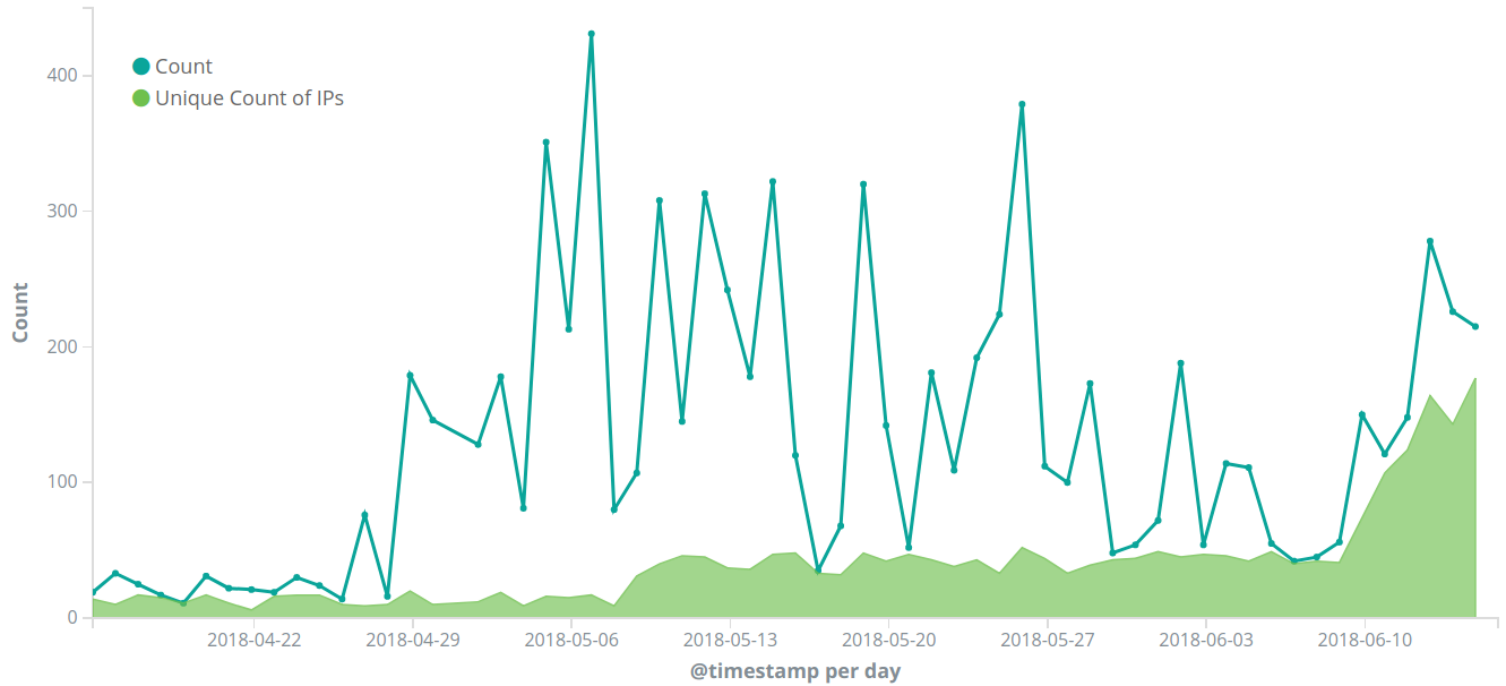
Cowrie – Events By Day



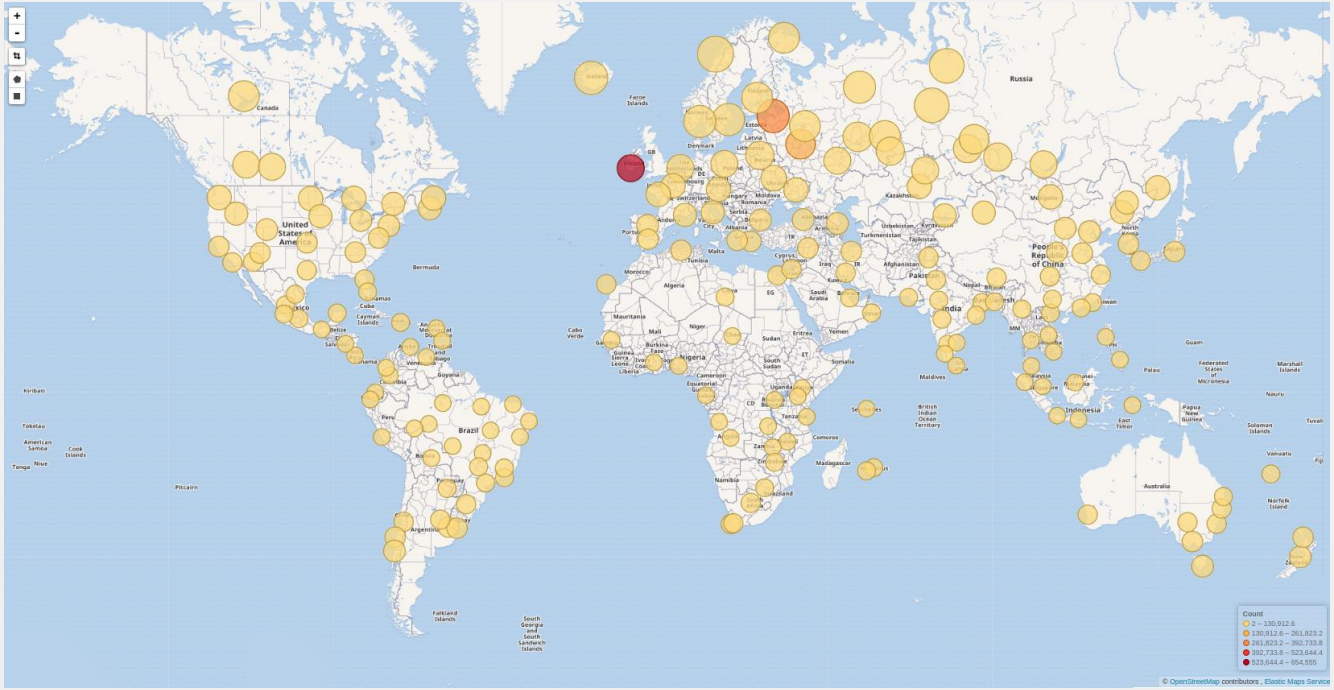
Dionaea – Events By Day



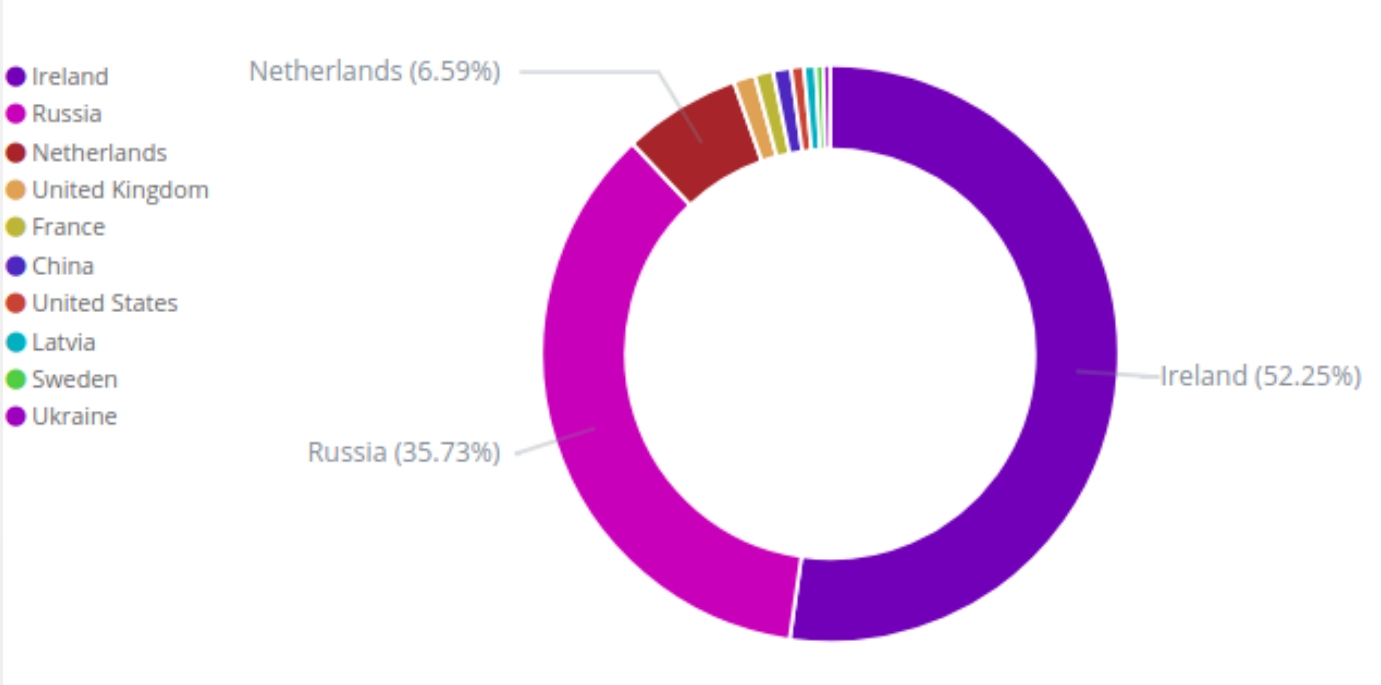
Glastopf – Events By Day



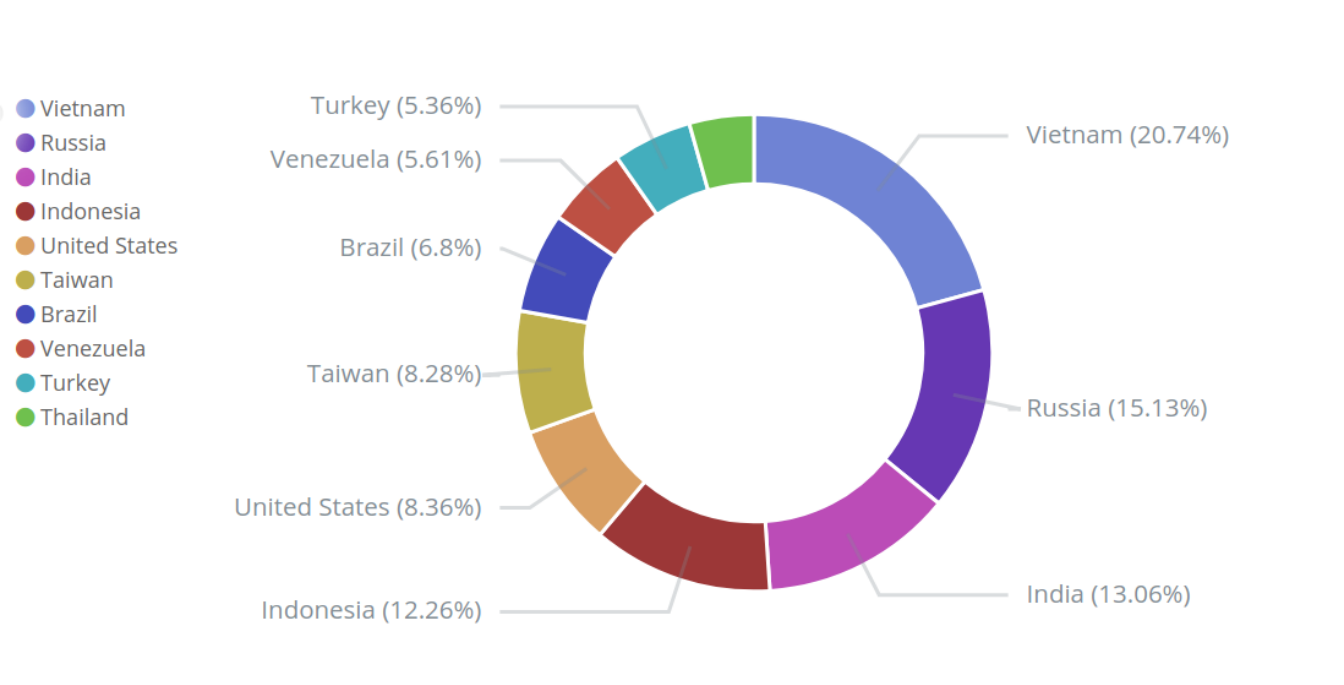
Cowrie – Attack Sources



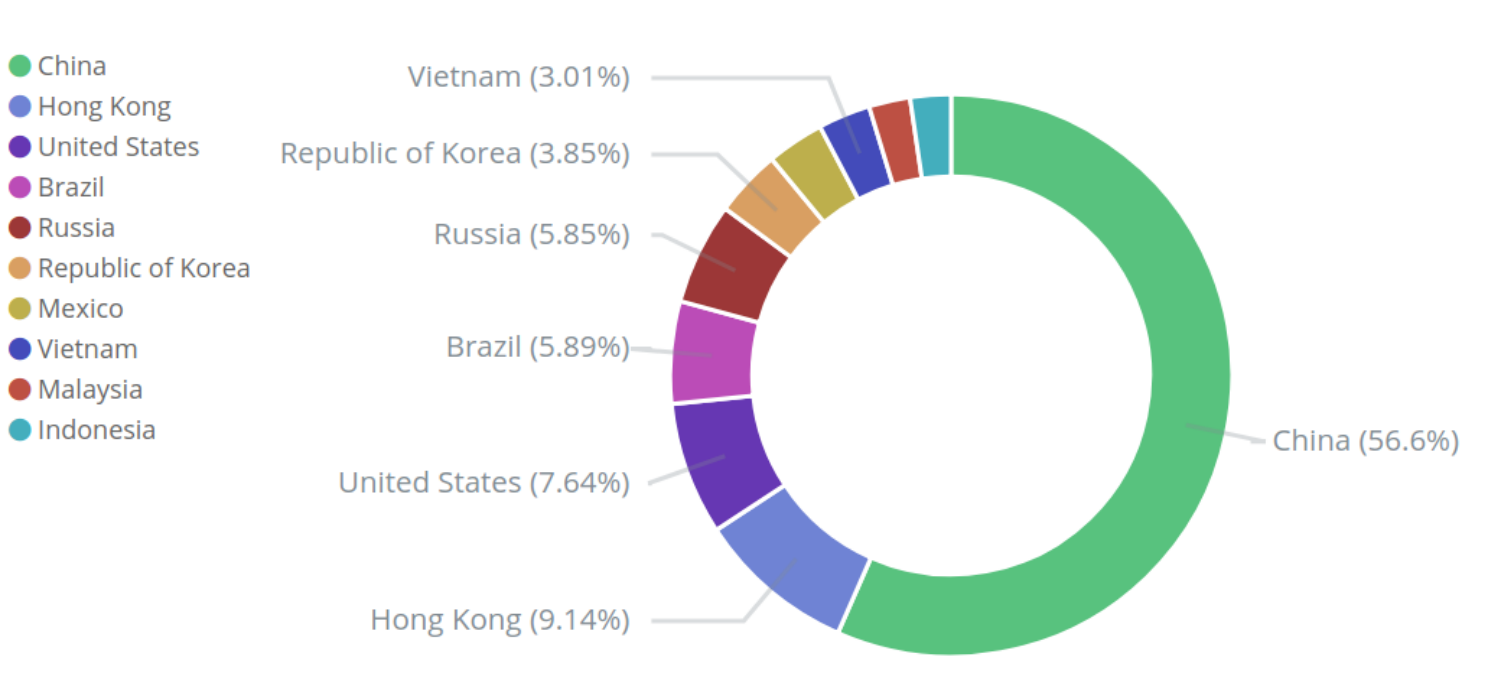
Cowrie – Events By Country



Dionaea – Events By Country



Glastopf – Events By Country



Cowrie – Usernames

Cowrie – Passwords

Cowrie – Common Commands

Common Commands	Count
cat /proc/cpuinfo	696
free -m	693
uname	693
ps -x	692
uname -a	534
help	131
uname -a & lscpu	69
unset HISTORY HISTFILE HISTSAVE HISTZONE HISTORY HISTLOG WATCH ; history -n ; export HISTFILE=/dev/null ; export HISTSIZE=0; export HISTFILESIZE=0;	61
uname -n -s -r -v	32
	20

Glastopf – Requested URL

URL	Count
/	2,305
/admin/index.php	149
/mysql-admin/index.php	149
/pmd/index.php	149
/claroline/phpMyAdmin/index.php	148
/typo3/phpmyadmin/index.php	147
/phpadmin/index.php	146
/xampp/phpmyadmin/index.php	146
/admin/mysql/index.php	145
/myadmin2/index.php	145

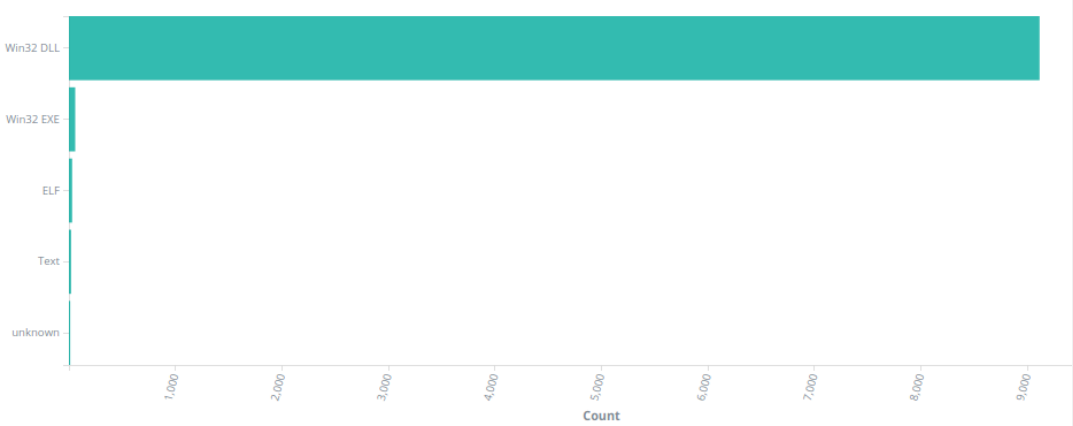
Dionaea – Connection Protocol

Connection Protocol	Count
smbd	1,461,560
upnpd	50,923
SipSession	7,943
mssqld	5,112
SipCall	5,088

Malware Analysis

9,248

Unique Samples



Magic Info

Type	Count
PE32 executable for MS Windows (DLL) (GUI) Intel 80386 32-bit	9,100
PE32 executable for MS Windows (GUI) Intel 80386 32-bit	56
ASCII text	18
ELF 32-bit LSB executable, Intel 80386, version 1 (SYSV), statically linked, for GNU/Linux 2.6.9, not stripped	13
HTML document text	9

Malware – Tags

Tag	Count
pedll	9,113
exploit	9,084
cve-2017-0147	9,082
overlay	9,069
honeypot	3,225
peexe	59
elf	30
text	20
corrupt	13
upx	11

CVE-2017-0147

CVE-ID	
CVE-2017-0147	Learn more at National Vulnerability Database (NVD) • CVSS Severity Rating • Fix Information • Vulnerable Software Versions • SCAP Mappings • CPE Information

Description

The SMBv1 server in Microsoft Windows Vista SP2; Windows Server 2008 SP2 and R2 SP1; Windows 7 SP1; Windows 8.1; Windows Server 2012 Gold and R2; Windows RT 8.1; and Windows 10 Gold, 1511, and 1607; and Windows Server 2016 allows remote attackers to obtain sensitive information from process memory via a crafted packets, aka "Windows SMB Information Disclosure Vulnerability."

References

Note: References are provided for the convenience of the reader to help distinguish between vulnerabilities. The list is not intended to be complete.

- EXPLOIT-DB:41891
- URL:https://www.exploit-db.com/exploits/41891/
- EXPLOIT-DB:41987
- URL:https://www.exploit-db.com/exploits/41987/
- EXPLOIT-DB:43970
- URL:https://www.exploit-db.com/exploits/43970/
- MISC:https://ics-cert.us-cert.gov/advisories/ICSMA-18-058-02
- CONFIRM:https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-0147
- CONFIRM:https://cert-portal.siemens.com/productcert/pdf/ssa-701903.pdf
- CONFIRM:https://cert-portal.siemens.com/productcert/pdf/ssa-966341.pdf
- BID:96709
- URL:http://www.securityfocus.com/bid/96709
- SECTRACK:1037991
- URL:http://www.securitytracker.com/id/1037991

Assigning CNA

Microsoft Corporation

Date Entry Created

20160909	Disclaimer: The entry creation date may reflect when the CVE ID was allocated or reserved, and does not necessarily indicate when this vulnerability was discovered, shared with the affected vendor, publicly disclosed, or updated in CVE.

Scans

virustotal

SHA256: 2988273e3c7b09a8ec04c0a4d18891a5165ec35bd8ef2bb6647742861bbb2afb

File name: 2871db9f799e63904a37425ade6438d6

Detection ratio: 55 / 65

Analysis date: 2018-05-31 23:54:14 UTC (3 εβδομάδες ago)

1 0

Analysis | File detail | Additional information | Comments 1 | Votes

Antivirus	Result	Update
Ad-Aware	Trojan.GenericKD.40267082	20180601
AegisLab	Troj.Ransom.W32.Wanna.toP0	20180531
AhnLab-V3	Trojan/Win32.WannaCryptor.R200894	20180531
ALYac	Trojan.GenericKD.40267082	20180531
Antiy-AVL	Trojan[Ransom]/Win32.Wanna	20180601
Arcabit	Trojan.Generic.D2666D4A	20180601
Avast	Win32:WannaCry-C [Trj]	20180601
AVG	Win32:WannaCry-C [Trj]	20180601
Avira (no cloud)	TR/Wanna.jrevh	20180531
AVware	Trojan.Win32.Generic!BT	20180601

5. Future Work

Future Work

- Deployment of a sensor to different country
- Malware Analysis

Closing Remarks

- Honeypots
- Our approach
- Generated Insights

References

[1] L. Spitnzer, Honeypots: Tracking Hackers, Addison-Wesley Professional, 2002

[2] DTAG Community Honeypot Project, Deutsche Telekom, http://dtag-dev-sec.github.io/

Special Thanks

- Dr. Nicolas Sklavos
- Michel Oosterhof
- Lukas Rist
- The Honeynet Project
- VirusTotal

Thank you!

Any questions?

Please send me your feedback and suggestions:

- @andronkyr
- andronkyr@outlook.com