Praktické výstupy z projektu PROKI

Pavel Bašta • pavel.basta@nic.cz • 1.06.2016

Motivace PROKI

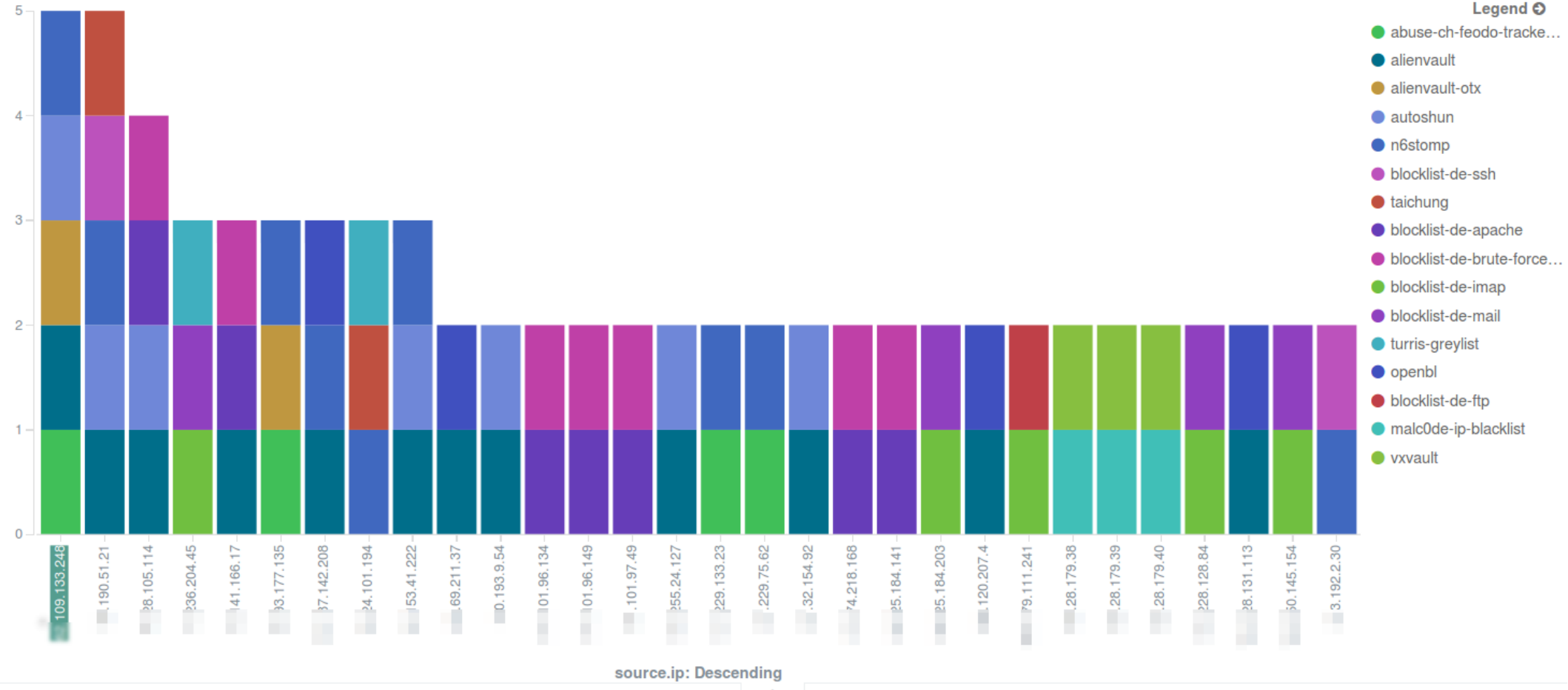
- Potřeba automatizovaně rozesílat informace o bezpečnostních incidentech týkajících se sítí v ČR
  - Veřejné i neveřejné zdroje
  - Služba pro správce z koncových sítí
- Potřeba hlubšího pochopení významu incidentů
  - Turris router
  - Pochopení již známých incidentů → Identifikace dosud nezjištěných problémů
  - Identifikace problematických IP

Části systému

- Sběr bezpečnostních incidentů
  - IntelMQ
    - Open source
    - Snadná tvorba vlastních modulů
    - Důraz na modularitu
    - Možnost obohacování dat
- Upozorňování subjektů
  - Pouze informace relevantní pro ČR
  - Agregace informací do jedné zprávy

Části systému

- Trvalé úložiště a analýza událostí
  - Elasticsearch + Kibana
    - Dlouhodobé uložení dat
    - Jednoduché analytické funkce
    - Další obohacení dat (PassiveDNS, proces IH, Virustotal.com, IP reputační systémy) → vyhledávání vztahů mezi incidenty, dohledávání dalších souvislostí, historie incidentů na IP adrese



virustotal

.109.133.248 IP address information

Geolocation

Country	CZ
Autonomous System	

Passive DNS replication

VirusTotal's passive DNS only stores address records. **The following domains resolved to the given IP address.**

2016-01-16	myqbee
2016-01-10	mojeglo
2016-01-06	hv2248.

Latest detected URLs

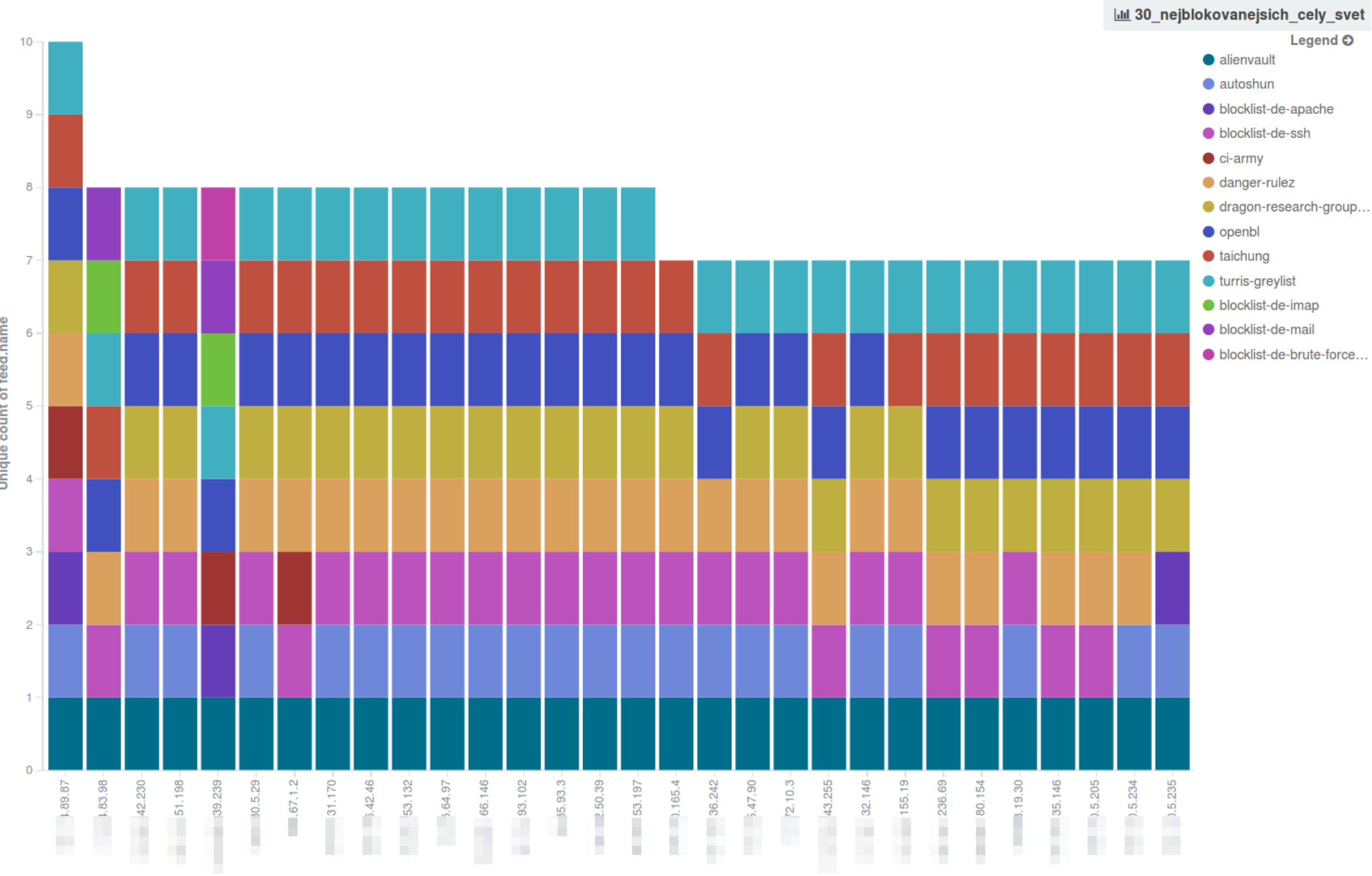
Latest URLs hosted in this IP address **detected by at least one URL scanner or malicious URL dataset**.

4/66	2016-02-07 17:51:47	http:/ 09.133.248/
2/66	2016-02-05 13:16:57	https .109.133.248:444/
2/66	2016-02-04 11:48:31	https .109.133.248:444/dridex/220/c2-node/
2/66	2016-02-01 13:16:30	https .109.133.248:444/dridex/220/c2-node
2/66	2016-01-22 04:54:16	https .109.133.248/
2/66	2016-01-15 12:32:03	http:/ 09.133.248:444/

Latest undetected files that were downloaded from this IP address

Latest files that are **not detected by any antivirus solution and were downloaded by VirusTotal from the IP address provided**.

0/55	2015-12-21 14:21:35	4bfe514f9c9090f613ca7da05c40f4a747e1bcc8a22482f680ec3a097fb21cc3



LEFT	RTYPE	RIGHT
aaw5zjuu.info	A	56.64.97
acl4tsgf.info	A	56.64.97
aebmayn.info	A	56.64.97
ahwqxmm.info	A	56.64.97
ajdxzru.info	A	56.64.97
akfbjke.info	A	56.64.97
anpvqug.info	A	56.64.97
antxxit.info	A	56.64.97
aplrcbp.info	A	56.64.97
apm3qjyp.info	A	56.64.97
asbojayg.info	A	56.64.97
ato2voqt.info	A	56.64.97
ayfdzrc.info	A	56.64.97
azo1pinz.info	A	56.64.97
badnnri.info	A	56.64.97
bavwehfm.info	A	56.64.97
bicembyn.info	A	56.64.97
bjewzvj.us	A	56.64.97
bjiwchl.us	A	56.64.97
bndosgs.us	A	56.64.97
bnizxyi.us	A	56.64.97
bnxextd.info	A	56.64.97
boaerbp.info	A	56.64.97
braftam.us	A	56.64.97

to the given IP address.

2015-09-02 ccubfyo.info

2015-08-27 bicembyn.info

2015-08-26 cmzmkwz.info

2015-08-09 dbrimdg.info

More

⚠ Latest detected URLs

Latest URLs hosted in this IP address **detected by at least one URL scanner or malicious URL dataset**.

1/63	2015-09-14 23:51:06	http://aplrcbp.info/
1/63	2015-09-11 00:15:07	http://ddpstbq.us/
1/63	2015-08-27 04:48:53	http://bicembyn.info/
1/63	2015-08-26 23:46:40	http://cmzmkwz.info/
1/63	2015-08-08 23:51:06	http://ayfdzrc.info/
1/63	2015-06-20 00:07:33	http://braftam.us/
1/63	2015-05-24 23:25:12	http://bujeerbs.info/

May 3rd 2016, 02:38:12.000

source.ip: [redacted]200 **feed.url:** https://www.tc.edu.tw/net/netflow/lkout/recent/30 **feed.name:** taichung **feed.accuracy:** 50 **event_description.text:** C&C Server **classification.taxonomy:** Malicious Code **classification.type:** c&c **raw:** PHRkPjEwOTA8L3RkPjx0ZD48aW1nIHNyYz0iL2ltYWdlcy9mbGFncy9jei5naWYiIGFsdD0iIj48c3BhbiBzdHlsZT0iY29sb3I6IGJsYWNrOyI+MTQ3LjMyLjEyNy4yMDA8L3NwYW4+PC90ZD48dGQ+QyZDIFNlcnZlcjwvdGQ+CiAgICAgICAgPHRkPuaJi+WLeioreWumjwvdGQ+PHRkPjIwMTQtMDEtMDcgMTU6NDY6MjQ8L3RkPjx0ZD44NDYuNzwvdGQ+CiAgICAgICAgPHRkIHN0eWxlPSJjb2xvcjpyZWQ7Ij7lsIHpjpY8L3RkPjwvdHI+ICAgICA= **source.geolocation.latitude:** 50.083 **source.geolocation.city:** Prague **source.geolocation.cc:** CZ **source.geolocation.longitude:** 14.467 **source.asn:** 2,852 **source.network:** 147.32.0.0/15 **time.source:** January 7th 2014, 08:46:24.000 **time.observation:** May 3rd 2016, 02:38:12.000 **id:** AVR0DaXbedUOq2C_Tqq **type:** event **index:** intelmq-test **score:**

April 27th 2016, 06:00:54.000

source.ip: [redacted]200 **feed.url:** stomp://n6stream.cert.pl:61614//exchange/nic.cz/*.*.*.* **feed.name:** n6stomp **destination.port:** 6,667 **classification.taxonomy:** Malicious Code **classification.identifier:** c&c server **classification.type:** c&c **raw:** eyJjYXRlZ29yeSI6ICJjbmMiLCAiY29uZmlkZW5jZSI6ICJtZWRpdW0iLCAiZXhwaXJlcyI6ICIyMDE2LTA0LTMwVDAwOjM2OjA0WiIsICJzb3VyY2UiOiAiaGlkZGVuLjM5IiwgInRpbWUiOiAiMjAxNi0wNC0xOVQwMDozNjowM1oiLCAiZHBvcnQiOiA2NjY3LCAidHlwZSI6ICJibC11cGRhdGUiLCAiaWQiOiAiYjg0MTY5NDNiOWIwMzhiZGY3YjFmMDU2ZDA0YzY2ODAiLCAiYWRkcmVzcyI6IFt7ImNjIjogIkNaIiwgImlwIjogIjE0Ny4zMi4xMjcuMjAwIiwgImFzbiI6IDI4NTJ9XX0= **extra:** {"feed_id": "b8416943b9b038bdf7b1f056d04c6680"} **source.geolocation.latitude:** 50.083 **source.geolocation.city:** Prague **observation:** April 27t

virustotal

[redacted] IP address information

Geolocation

Country	CZ
Autonomous System	[redacted]

Passive DNS replication

VirusTotal's passive DNS only stores address records. **The following domains resolved to the given IP address.**

No domains! VirusTotal has never resolved any domain name to the IP address under consideration.

Latest detected files that communicate with this IP address

Latest files submitted to VirusTotal that are **detected by one or more antivirus solutions and communicate with the IP address provided** when executed in a sandboxed environment.

44/52	2014-06-03 23:20:16	29192c865b623585b24a068513c40871e4cca[redacted]
40/51	2014-04-22 21:28:13	43b7f0581b813ac12a25f973052396d8d0b8f4[redacted]
45/51	2014-03-31 02:58:10	7c4d7641acb14f2030f4d4e1d6b25fdb05f3892[redacted]

HTTP requests

URL: http:/[redacted].cz/100minut/file56.gif
TYPE: GET
USER AGENT: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1)

URL: h[redacted]de/phpkit/templates/file56.gif
TYPE: GET
USER AGENT: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1)

URL: h[redacted]de/index/templates/igal/file56.gif
TYPE: GET
USER AGENT: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1)

URL: [redacted].com.ar/file56.gif
TYPE: GET
USER AGENT: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1)

URL: [redacted].com.br/admin/file56.gif
TYPE: GET
USER AGENT: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1)

DNS requests

ww[redacted]c.cz (89.185.231.140)

ww[redacted].jj4u.de (85.13.137.10)

ww[redacted]fkreisel.de (85.13.133.31)

ww[redacted]tavomasieri.com.ar (200.58.112.50)

ww[redacted]naleoa.com.br (69.27.32.114)

TCP connections

[redacted].231.140:80

[redacted]137.10:80

[redacted]133.31:80

[redacted].112.50:80

[redacted]32.114:80

UDP communications

<MACHINE_DNS_SERVER>:53

⚠ Latest detected URLs

Latest URLs hosted in this IP address **detected by at least one URL scanner or malicious URL dataset**.

2/67	2016-05-26 06:30:36	[redacted]asynet.cz/
2/67	2016-05-26 06:29:17	[redacted]z/
2/67	2016-05-26 06:18:39	[redacted].171/
2/67	2016-05-25 15:14:00	[redacted]1.171:40443/dridex/120/c2/loader
2/67	2016-05-25 04:04:23	[redacted].171/\026\003\001
2/67	2016-05-19 16:10:00	[redacted].171:40443/
3/66	2016-02-09 16:20:47	[redacted]net.cz/e11.htm
1/63	2015-06-06 01:43:08	[redacted]net.cz/
1/63	2015-05-09 08:58:28	[redacted]net.cz/c11.htm
2/63	2015-05-09 08:37:16	[redacted]net.cz/c13.htm

More

Latest detected files that were downloaded from this IP address

Latest files that are **detected by at least one antivirus solution and were downloaded by VirusTotal from the IP address provided**.

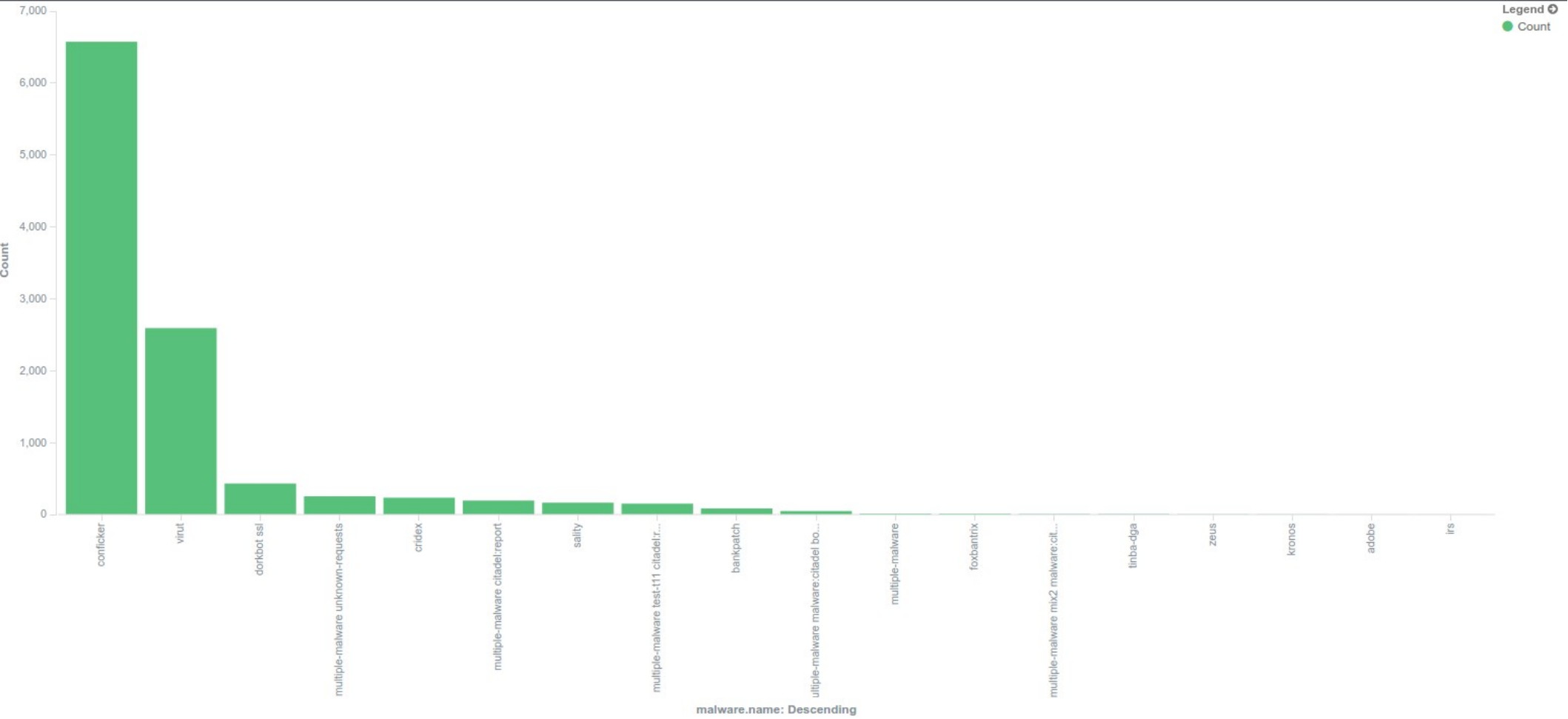
10/53	2016-02-09 16:36:22	1654d58061582b6b62b6a06e0f10419bd222084c35332d3843eb6dad3ff2e282
9/57	2015-05-09 08:58:33	805f1f54d3a6b708465d6d6d36aafeadcc1f1f66f438061cde001757a3f09c2f

⚠ Latest detected URLs

Latest URLs hosted in this IP address **detected by at least one URL scanner or malicious URL dataset**.

2/67	2016-05-18 10:21:19	[redacted]
3/67	2016-05-12 15:22:36	[redacted]
1/67	2016-04-18 04:59:35	[redacted]
1/67	2016-04-07 18:33:32	[redacted]
9/68	2016-03-01 08:48:41	[redacted]
1/67	2016-02-16 16:18:35	[redacted]cz/3181/gate7266-22/.do
1/66	2016-02-14 21:44:44	[redacted]
1/66	2016-02-14 17:17:54	[redacted]cz/3181/gate5367-22/.do
1/66	2016-02-14 16:44:20	[redacted]cz/3181/gate34877-22/.do
1/66	2016-02-13 16:49:13	[redacted]cz/3181/gate9647-22/.do

More



Dobry den,

dekuji za informace, podle vseho to bylo v dobe kdy jsme se potykali s
virem motherfucker.
Nyni veskera zarizeni vykazuji jiz normalni chovani.

Dobrý den,

naše technická podpora kontaktovala zákazníka, aby prověřil své počítače - nalezl spoustu nákaz:
...zakaznik provereoval pocitace, na jednom nasel 65 hrozeb, na dalsim 3 hrozby a na poslednim 1 hrozbu. o vikendu to jeste bude resit, bude na to pravdepodobne potreba specialni nastroj. Po 16.05. by jiz tedy nemelo zadne upozorneni chodit.

Dobrý den,

jednalo se o hacknutý Wordpress, který nikdo neudržoval. Ke zneužití
serveru došlo s největší pravděpodobností skrz něj.
Zákazník vyčistil (i za mě vypadá OK). Stačí takto? Máte hlášeny ještě
nějaké incidenty?

Dobrý den,

skutečně jsem včera na tomto serveru našel napadenou prezentaci WordPress.
Klient prezentaci obnovil ze zálohy, změnil všechna hesla a provedl aktualizaci WP.
Vše vypadá, že je již v pořádku.

Dobry den,

zakaznika jsem dohledal, s tim, ze ma zavirovany pocitac vicemene souhlasil.
Prislibil odvirovani, pripadne reinstalaci windows.

Další plány

- Přidání informací z BotnetFeed GovCERT.CZ
- Integrace dat z externích služeb
  - Virustotal, PassiveDNS, Shodan
- Exit node Tor
- Vyhledávání potenciálně napadených koncových zařízení
  - Routery, ICS (SCADA, PLC), NAS (Synology)
- Přenesení systému na výkonnější hardware

PROKI

PREDIKCE A OCHRANA PŘED KYBERNETICKÝMI INCIDENTY

MINISTERSTVO VNITRA ČESKÉ REPUBLIKY

Projekt **„Predikce a ochrana před kybernetickými incidenty (PROKI)“** *(VI20152020026)* je realizován v rámci Programu bezpečnostního výzkumu ČR na léta 2015 – 2020.

CSIRT.CZ

CZ.NIC | SPRÁVCE DOMÉNY CZ

Děkuji za pozornost

Pavel Bašta • pavel.basta@nic.cz