cesnet

CESNET-CERTS
Introduction and current challenges

Digital Partnership for Cybersecurity and Resilience in Regions
Telč
October 6th 2022

Radko Krkoš

Who are we?

- NREN of the Czech Republic:
  - Communication infrastructure,
  - Computation and data storage,
  - Research and applications.
- Customers:
  - Universities,
  - Academy of Sciences,
  - Hospitals, Schools, Public libraries, …

CESNET-CERTS

- Computer Security Incident Response Team,
- certs@cesnet.cz, abuse@cesnet.cz, https://csirt.cesnet.cz,
- Constituency:
  - AS 2852 – CESNET communication infrastructure,
  - AS 48091 – Vysočina Region,
- 13 team members,
- TF-CSIRT Trusted Introducer:
  - Listed since 2004 (First in Czech Republic),
  - Accredited since 2008 (First in Czech Republic),
  - https://tiw.trusted-introducer.org/directory/teams/cesnet-certs.html

What does CESNET-CERTS do?

- Incident handling and IH coordination,
- ISMS, legislative conformance,
- Automation of Security Event collection and processing,
- Tool development,
- Running support services (DNS, e-mail, web, wiki, …),
- Training, publication and knowledge transfer.

Incident handling

- Tier 1: 24/7 Service Desk:
  - Point of first contact – direct reports from institutions,
  - Low severity incidents,
  - Spam, Copyright infringement, low profile scanning, Backscatter, …
  - Well-defined process, mechanic work with need for operator interaction,
  - Escalation: Affected organization or Tier 2,
- Tier 2: CESNET-CERTS:
  - Incident analysis,
  - Coordination, response planning & execution,
  - Advisory & knowledge transfer.

Security events & incidents

- Security events:
  - ~2M per day,
  - Detections from probes, honeypots, services (logs), …
- Security incidents:
  - 20 – 30 being handled at any given time (Tier 2),
- Automation is a must:
  - Event collection and processing,
  - Also for incident handling – for large scale ongoing attacks,
  - Need for human review,
  - Constant tuning.

Mentat – Event collection and processing

M20220603SL-XQJOA

Target abuse group: eduroam-abuse@cesnet.cz

Unprotected access link: M20220603SL-XQJOA

Report created: Jun 3, 2022, 9:20:31 PM (4 days ago) | **Report window:** Jun 2, 2022, 9:20:00 PM - Jun 3, 2022, 9:20:00 PM (1 day) |
Report mailed: Jun 3, 2022, 9:20:31 PM (4 days ago)

Search | Delete

Message | Metadata | Statistics | Data

Dear colleagues.

Our detection systems registered following possible problem(s) related to Your IP address range or domain (timestamps are in timezone Europe/Prague):

[1] The machine is compromised and serve as bot drone.

Source	First event	Last event	Detectors	Messages	Feedback
195.113.[redacted]	Jun 2, 2022, 2:40:59 AM	Jun 2, 2022, 2:40:59 AM	1	1	Feedback

More information: https://csirt.cesnet.cz/cs/services/eventclass/intrusion-botnet-bot

This report contains events with LOW severity. Please consider reviewing the host systems mentioned in this report and fix any possible issues.

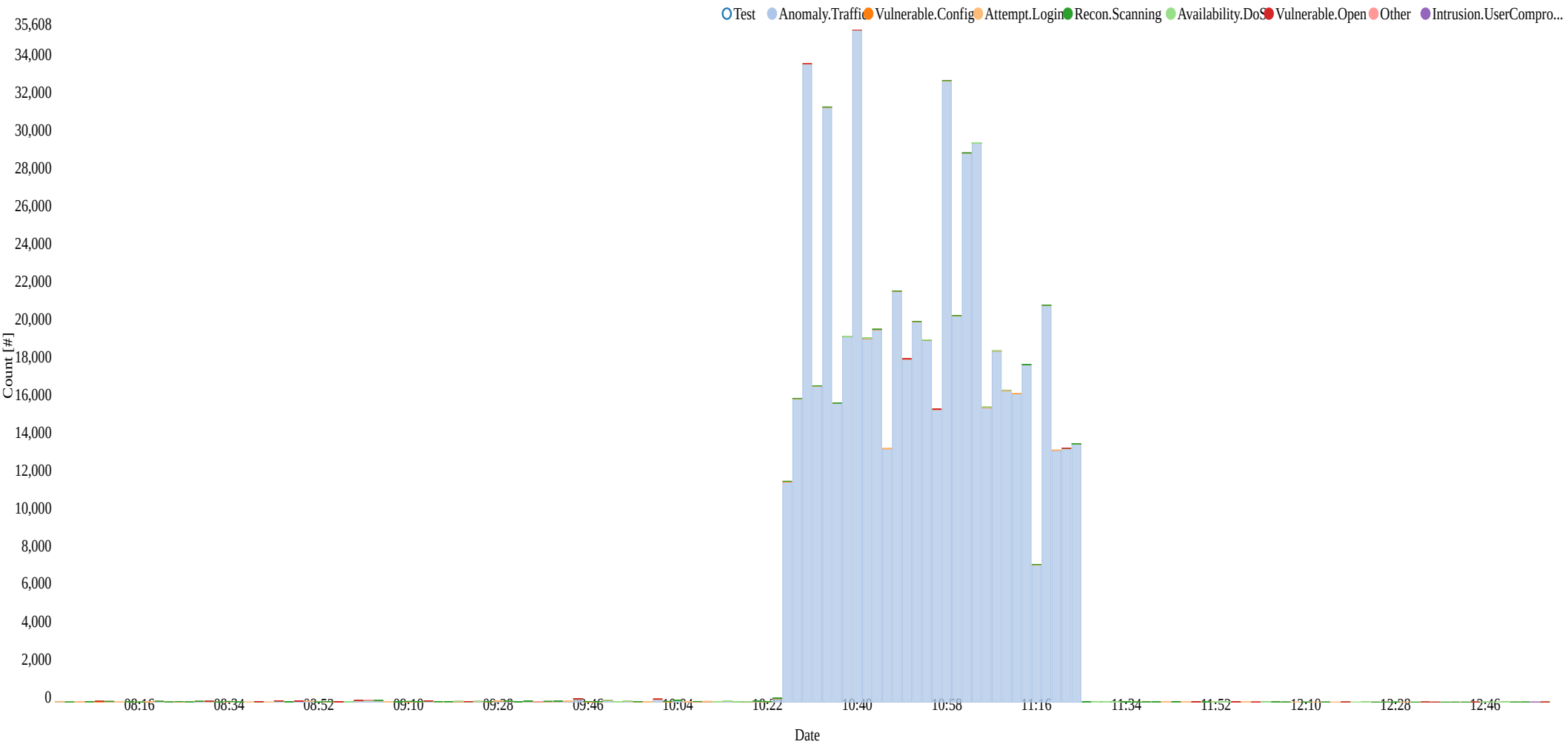
Attachment files containing complete information available for each event can be downloaded above message in JSON format.

This message was generated by an automated system. For further communication please use the contact email address <abuse@cesnet.cz> and for easier orientation please keep the identifier [M20220603SL-XQJOA] in email subject.

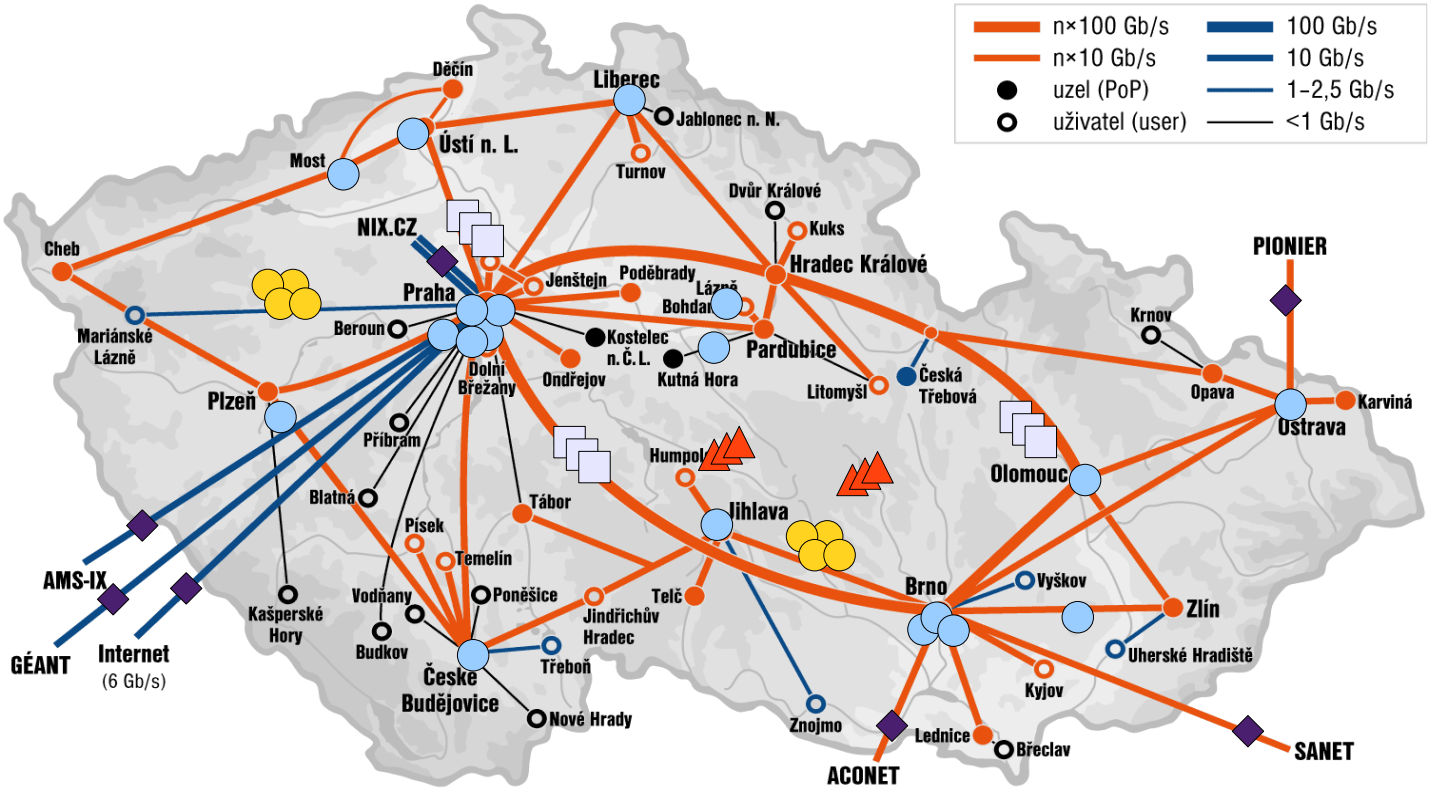
Thank you in advance for your cooperation

Mentat System (https://csirt.cesnet.cz/en/services/mentat)
CESNET-CERTS Computer Security Team <certs@cesnet.cz> (https://csirt.cesnet.cz/en/index)
CESNET, a.l.e. (http://www.ces.net/)

How to spot an attack?



CESNET Network Monitoring



- HW accelerated probes
- large scale (backbone-wide) flow based monitoring (NetFlow data sources)
- Honey Pots
- IDS, IPS, tar pit based systems, etc..
- SNMP based monitoring

cesnet Flow Traffic Analysis System

Selected Objects Information

Object	Active Data
Praha 1: R118 - backbone, border router (NIX Ce Colo) *id=13* *type=Flow Data Source*	**PRIMARY** - *table size=5 minutes, history=200 days, aggregation=none* ***Oldest data table: 2021/12/26 13:05:00*** *...real history ~ 163 days*
Praha 1: R148 - backbone, border router (AMS-IX, GEANT, LHCONE) *id=1251* *type=Flow Data Source*	**PRIMARY** - *table size=2 minutes, history=183 days, aggregation=none* ***Oldest data table: 2021/12/06 20:18:00*** *...real history ~ 183 days*

Query Parameters *..?*

Fields to store in results *..?*

Flow Src/Dst Fields

- Src-IP / Dst-IP
- Src-Port / Dst-Port
- Src-ifIndex / Dst-ifIndex
- Ingress-VRFID / Egress-VRFID
- Src/Prev-AS / Dst/Next-AS
- Src-Bitmask / Dst-Bitmask

Flow Common Fields

- Flow-Direction / TCP-flags
- FWD-Status / Nexthop
- Protocol / Flow-Data-Source
- TOS-flags

Time, Value and Count Fields

- Flow-Start / Pkts-measured
- Flow-End / Pkts-estimated
- Bytes-measured / Flow-Cnt
- Bytes-estimated

Fields Query Condition - Simple Form *..?*

...you can switch to 'generic' condition form

Query traffic (in form below) ● *from Source to Destination* ○ *bidirectional* ○ *from Destination to Source*

	Source	relation	Destination
IP address	aaa.bbb.ccc.ddd	and	
Service Port		and	
AS Number		and	
Interface Index		and	
VRFID		and	

Protocol	TCP-flags	TOS-flags	Flow-Direction	FWD-Status
255 ax.25 dccp	ack fin push	critic_ecp flash high_relibility	egress ingress	

○ Query Condition Management

Time Parameters *..?* ...advanced ○

-10 minutes - now ○ GMT time

Aggregation → no - 'group by' clause applied on each source data table (depends on 'selected fields' and 'table size' values)... *..?*

Results *(time values in **CEST**)*

	Src-IP	Dst-IP	Src-Port	Dst-Port	Flow-Start [CEST]	Flow-End [CEST]	Bytes-measured	Bytes-estimated	Pkts-measured	Pkts-estimated	Flow-Cnt
1.	164.92.196.140 (USA)	aaa.bbb.ccc.ddd (CZE) vulnerable.host.cz	34844	socks (1080)	22/05/19 19:54:17.697	22/05/19 19:54:17.697	52.000 B	1.040 KB	1.000 p	20.000 p	1
2.	aaa.bbb.ccc.ddd (CZE) vulnerable.host.cz	45.61.185.190 (USA) tor-node1.rage.one	socks (1080)	43020	22/05/19 22:48:31.555	22/05/19 22:48:31.555	44.000 B	880.000 B	1.000 p	20.000 p	1
3.	aaa.bbb.ccc.ddd (CZE) vulnerable.host.cz	198.12.121.211 (USA) 198-12-121-211-host.colocrossing.com	socks (1080)	52118	22/05/20 12:32:15.311	22/05/20 12:32:15.311	44.000 B	880.000 B	1.000 p	20.000 p	1
4.	aaa.bbb.ccc.ddd (CZE) vulnerable.host.cz	78.85.171.13 (RUS) a13.sub171.net78.udm.net	socks (1080)	61713	22/05/20 14:06:36.615	22/05/20 14:06:36.615	40.000 B	800.000 B	1.000 p	20.000 p	1
5.	aaa.bbb.ccc.ddd (CZE) vulnerable.host.cz	45.61.185.190 (USA) tor-node1.rage.one	socks (1080)	59190	22/05/20 14:06:36.615	22/05/20 14:06:36.615	52.000 B	1.040 KB	1.000 p	20.000 p	1
6.	aaa.bbb.ccc.ddd (CZE) vulnerable.host.cz	78.85.171.13 (RUS) a13.sub171.net78.udm.net	socks (1080)	55638	22/05/20 14:06:41.324	22/05/20 14:06:41.324	40.000 B	800.000 B	1.000 p	20.000 p	1
7.	aaa.bbb.ccc.ddd (CZE) vulnerable.host.cz	106.75.229.12 (CHN) sellerbulknewscom.top	socks (1080)	15754	22/05/20 14:06:42.340	22/05/20 14:06:42.340	52.000 B	1.040 KB	1.000 p	20.000 p	1

PassiveDNS Search

Query: 78.128.211.46

Query type: (•) IP ( ) domain ( ) domain & subdomains

Date limit: Since: mm / dd / yyyy Until: mm / dd / yyyy

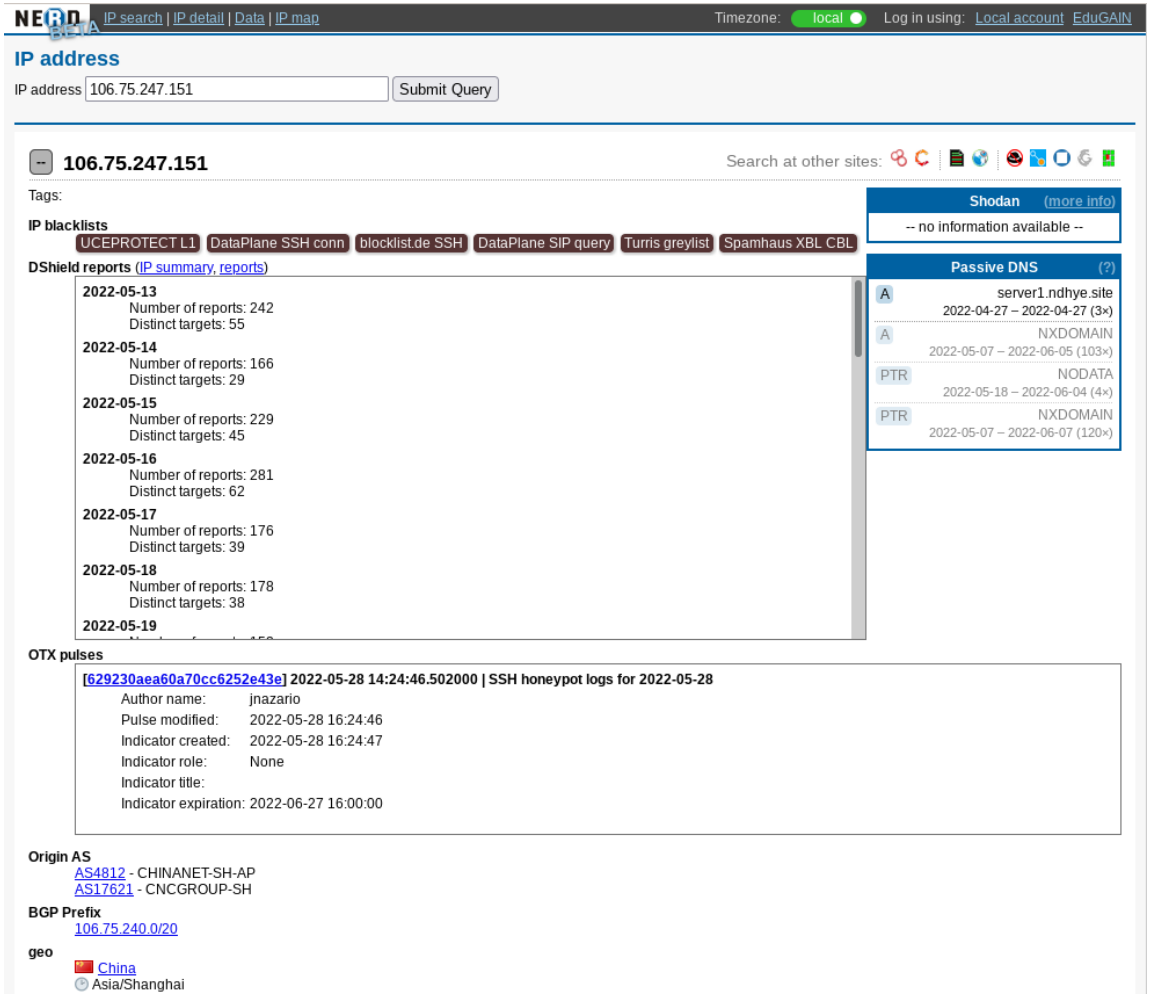
Search

Elapsed time: 0.036255s

Page 1

IP	Domain	RTYPE	First seen	Last seen	Count	Details
78.128.211.46	vyzkumne-infrastruktury.cz	A	2021-06-07 13:21:33.157842	2022-05-03 09:22:11.964581	112	i
78.128.211.46	nren.cz	A	2022-02-14 10:59:54.483857	2022-04-08 09:05:02.337680	10	i
78.128.211.46	research-infrastructures.cz	A	2021-06-07 13:21:33.163023	2022-04-27 08:02:41.262069	29	i
78.128.211.46	30letinternetu.cz	A	2022-01-20 10:05:37.853247	2022-06-06 09:19:51.230190	203	i
78.128.211.46	www.cesnet.cz	A	2021-06-01 07:45:05.316191	2022-06-07 19:10:24.609391	186446	i
78.128.211.46	cesnet.cz	A	2021-06-01 07:45:04.144546	2022-06-07 19:10:03.445035	56692	i
46.211.128.78.in-addr.arpa	www.cesnet.cz	PTR	2021-06-01 08:41:10.032874	2022-06-07 18:39:10.188938	12603	i
NODATA	46.211.128.78.in-addr.arpa	A	2022-03-07 19:37:28.790013	2022-06-07 18:52:13.007149	2561	i
NODATA	46.211.128.78.in-addr.arpa	PTR	2022-04-22 13:03:36.015960	2022-05-14 19:15:02.278222	2	i

cesnet Network Entity Reputation Database



NERD BETA | IP search | IP detail | Data | IP map | Timezone: local | Log in using: Local account EduGAIN

IP address

IP address 106.75.247.151 Submit Query

106.75.247.151

Search at other sites:

Tags:

IP blacklists

UCEPROTECT L1 | DataPlane SSH conn | blocklist.de SSH | DataPlane SIP query | Turris greylist | Spamhaus XBL CBL

DShield reports (IP summary, reports)

2022-05-13
Number of reports: 242
Distinct targets: 55

2022-05-14
Number of reports: 166
Distinct targets: 29

2022-05-15
Number of reports: 229
Distinct targets: 45

2022-05-16
Number of reports: 281
Distinct targets: 62

2022-05-17
Number of reports: 176
Distinct targets: 39

2022-05-18
Number of reports: 178
Distinct targets: 38

2022-05-19

Shodan (more info)

-- no information available --

Passive DNS (?)

A	server1.ndhye.site	2022-04-27 – 2022-04-27 (3×)
A	NXDOMAIN	2022-05-07 – 2022-06-05 (103×)
PTR	NODATA	2022-05-18 – 2022-06-04 (4×)
PTR	NXDOMAIN	2022-05-07 – 2022-06-07 (120×)

OTX pulses

[629230aea60a70cc6252e43e] 2022-05-28 14:24:46.502000 | SSH honeypot logs for 2022-05-28

Author name: jnazario
Pulse modified: 2022-05-28 16:24:46
Indicator created: 2022-05-28 16:24:47
Indicator role: None
Indicator title:
Indicator expiration: 2022-06-27 16:00:00

Origin AS

AS4812 - CHINANET-SH-AP
AS17621 - CNCGROUP-SH

BGP Prefix

106.75.240.0/20

geo

China
Asia/Shanghai

IP address	Hostname	ASN	Country	Events	Rep.(?)	Other properties
172.105.89.161	.threatsinkhole.com	AS63949	DE	45769 | 7 | 2 + 16 OTX pulses	0.969	12 blacklists Scanner
123.160.221.24	--	AS4134	CN	15504 | 5 | 1	0.968	5 blacklists Scanner
111.7.96.135	--	AS9808	CN	58912 | 6 | 2	0.967	6 blacklists Scanner
123.160.221.57	--	AS4134	CN	13635 | 5 | 1	0.967	5 blacklists Scanner
123.160.221.63	--	AS4134	CN	13618 | 5 | 1	0.966	5 blacklists Scanner
123.160.221.49	--	AS4134	CN	12030 | 5 | 1	0.965	5 blacklists Scanner
111.7.96.134	--	AS9808	CN	71579 | 6 | 2	0.965	5 blacklists Scanner
111.7.96.133	--	AS9808	CN	44113 | 6 | 2	0.963	6 blacklists Scanner
111.7.96.132	--	AS9808	CN	45734 | 6 | 2	0.963	6 blacklists Scanner
123.160.221.32	--	AS4134	CN	30594 | 5 | 1	0.963	5 blacklists Scanner
123.160.221.53	--	AS4134	CN	14178 | 5 | 1	0.963	5 blacklists Scanner
123.160.221.56	--	AS4134	CN	13760 | 5 | 1	0.963	4 blacklists Scanner
123.160.221.51	--	AS4134	CN	12017 | 5 | 1	0.963	5 blacklists Scanner
123.160.221.37	--	AS4134	CN	15328 | 5 | 1	0.962	4 blacklists Scanner
123.160.221.61	--	AS4134	CN	13587 | 5 | 1	0.961	5 blacklists Scanner
123.160.221.41	--	AS4134	CN	13264 | 5 | 1	0.961	5 blacklists Scanner
123.160.221.62	--	AS4134	CN	14699 | 5 | 1	0.961	4 blacklists Scanner
123.160.221.52	--	AS4134	CN	15467 | 5 | 1	0.961	5 blacklists Scanner
123.160.221.43	--	AS4134	CN	12764 | 5 | 1	0.961	5 blacklists Scanner
123.160.221.55	--	AS4134	CN	14589 | 5 | 1	0.960	5 blacklists Scanner

DDoS resiliency exercise

Od: Jan Hoffmann
Komu: abuse@cesnet.cz, [redacted]

FORWARD THIS MAIL TO WHOEVER IS IMPORTANT IN YOUR COMPANY AND CAN MAKE DECISION!

We are Armada Collective and we have chosen CESNET as target for our next DDoS attack

Your whole network will be DDoS-ed starting next Thursday if you don't pay 1 Bitcoin @ [redacted]

When we say your network, we have your IP ranges, so we will be targeting you directly and no protection will help. And our attacks are very powerful (peak at 2 Gpbs).

As proof right now we will start 10-15 minutes amplification attack on 195.113.[redacted] with 5 of our 117 servers, so do the math. We are just making a short time small demonstration, because we don't want cause you any damage at this moment. Check your logs!

But if you don't pay by Thursday, long-term attack will start, price to stop will increase to 2 BTC and will go up 1 BTC for every day of attack.

If you report this to media and try to get some free publicity by using our name, instead of paying, attack will start permanently and will last for a long time.

This is not a joke.

Our attacks are extremely powerful - peak over 2 Tbps per second. So, no cheap protection will help.
We are not sure if it is enough to completely shut down your network, but we will surely cause you large damage, both to you and your users. You do the calculation.

Prevent it all with just one Bitcoin!

Do not reply, we will probably not read. Pay and we will know its you. AND YOU WILL NEVER AGAIN HEAR FROM US!

Nobody will ever know you cooperated.

Handling the threat

- We have:
  - Plans: incident handling, disaster recovery,
  - Experience: under constant attack, table-tops & CTFs,
  - Reaction teams: Service Desk, CERTS, Network Operators, Forensic Laboratory,
  - Communication schemes: between reaction teams, towards individual users, management, employees, customers, administrators,
- Time to put it under test:
  - We MUST be able to withstand an attack like this,
  - The “demo” was handled by automated protection mechanisms,

Rate of exploitation

Source: https://trunc.org/learning/brute-force-attacks-against-windows-remote-desktop

4 pillars of SOC

- Incident response & handling – CSIRT,
- Security event collection and processing,
- Situational awareness / CTI:
  - Vulnerability monitoring,
  - Threat monitoring (to know the enemy),
- Security Asset Management (to know yourself):
  - Threat modeling,
  - Patch management,
  - Attack surface minimization.

Thank you for your attention.

Any questions or suggestions?

Radko Krkoš
krkos@cesnet.cz

certs@cesnet.cz