

Incident reporting

Incident reporting

4

Hi, TCC-CSIRT analyst,

our automatic incident recording system has captured about an hour of traffic originating from the IP range within the AI-CSIRT constituency. Analyze whether there are any incidents present and report all of them through the AI-CSIRT web interface.

- [Download the pcap file \(cca 53 MB\)](#)
(sha256 checksum:
`e38550ba2cc32931d7c75856589a26e652f2f64e5be8cafaa34d5c191fc0fd1c`)
- The web interface is at <http://incident-report.csirt.ai.tcc>.

This challenge's description provides a pcap file which contains traffic in which several incidents are captured. The incident reporting interface looks as follows.

Incident Report

incident-report.csirt.ai.tcc

Incident Report

1 Incident type

Incident type

Select... ▾

The type of incident that occurred.

2 Basic data

Offending IP address

The source IPv4/IPv6 address that caused the incident.

Target IP address

The destination IPv4/IPv6 address that was the target of the incident.

Datetime of the first attempt (UTC)

YYYY-MM-DD HH:MM:SS

The first attempt in UTC format (YYYY-MM-DD HH:MM:SS) where the source IP address caused the incident.

Datetime of the last attempt (UTC)

YYYY-MM-DD HH:MM:SS

The last time in UTC format (YYYY-MM-DD HH:MM:SS) the source IP address caused an incident.

3 Details

Select the type of incident in the first step.

X Reset form

Send to AI-CSIRT ›

Therefore, the incident's type, offending and target IP addresses and time window in which the incident occurred have to be identified. The incident details depend on the type of incident. For example, for a brute force attack, the details include the number of attack attempts and if the attack was successful.

brute force

225497	675.045254	2001:db8:7cc::a1:210	2001:db8:7cc::acdc:24:beef	HTTP	283	POST	/login	HTTP/1.0	(application/x-www-form-urlencoded)
225505	675.051335	2001:db8:7cc::a1:210	2001:db8:7cc::acdc:24:beef	HTTP	284	POST	/login	HTTP/1.0	(application/x-www-form-urlencoded)
225544	675.081929	2001:db8:7cc::a1:210	2001:db8:7cc::acdc:24:beef	HTTP	281	POST	/login	HTTP/1.0	(application/x-www-form-urlencoded)
225566	675.090536	2001:db8:7cc::a1:210	2001:db8:7cc::acdc:24:beef	HTTP	283	POST	/login	HTTP/1.0	(application/x-www-form-urlencoded)
225629	675.129529	2001:db8:7cc::a1:210	2001:db8:7cc::acdc:24:beef	HTTP	280	POST	/login	HTTP/1.0	(application/x-www-form-urlencoded)
225641	675.134916	2001:db8:7cc::a1:210	2001:db8:7cc::acdc:24:beef	HTTP	281	POST	/login	HTTP/1.0	(application/x-www-form-urlencoded)
225649	675.139661	2001:db8:7cc::a1:210	2001:db8:7cc::acdc:24:beef	HTTP	283	POST	/login	HTTP/1.0	(application/x-www-form-urlencoded)
225707	675.174250	2001:db8:7cc::a1:210	2001:db8:7cc::acdc:24:beef	HTTP	281	POST	/login	HTTP/1.0	(application/x-www-form-urlencoded)
225721	675.187099	2001:db8:7cc::a1:210	2001:db8:7cc::acdc:24:beef	HTTP	281	POST	/login	HTTP/1.0	(application/x-www-form-urlencoded)
225753	675.190885	2001:db8:7cc::a1:210	2001:db8:7cc::acdc:24:beef	HTTP	283	POST	/login	HTTP/1.0	(application/x-www-form-urlencoded)

1 Incident type

Incident type

Brute force attack

The type of incident that occurred.

2 Basic data

Offending IP address

2001:db8:7cc::a1:210

The source IPv4/IPv6 address that caused the incident.

Target IP address

2001:db8:7cc::acdc:24:beef

The destination IPv4/IPv6 address that was the target of the incident.

Datetime of the first attempt (UTC)

2024-09-26 08:55:20

The first attempt in UTC format (YYYY-MM-DD HH:MM:SS) where the source IP address caused the incident.

Datetime of the last attempt (UTC)

2024-09-26 08:55:43

The last time in UTC format (YYYY-MM-DD HH:MM:SS) the source IP address caused an incident.

3 Details

Number of attempts

1000–4999

Approximate number of attempts.

Result

Success

The result of whether the login credentials were successfully cracked.

AI response:

```
{"message":"It's probably a real incident, I'll consult the natural intelligence of a member of the CSIRT."}
```

Your incident ID is **MS800iBGTEFHe2xF0A==**, please keep it.

DDOS

1

Incident type

Incident type

(D)DoS

The type of incident that occurred.

2

Basic data

Offending IP address

2001:db8:7cc::a1:d055

The source IPv4/IPv6 address that caused the incident.

Target IP address

2001:db8:7cc::acdc:24:911

The destination IPv4/IPv6 address that was the target of the incident.

Datetime of the first attempt (UTC)

2024-09-26 08:59:09

The first attempt in UTC format (YYYY-MM-DD HH:MM:SS) where the source IP address caused the incident.

Datetime of the last attempt (UTC)

2024-09-26 09:46:45

The last time in UTC format (YYYY-MM-DD HH:MM:SS) the source IP address caused an incident.

3

Details

Service affected

HTTP

The type of service that was to be attacked.

242063	881.933750	2001:db8:7cc::a1:d055	2001:db8:7cc::acdc:24:911	TCP	94.41134	→ 80	[SYN]	Seq=0 Win=64800 Len=0 MSS=1440 SACK_PERM TSval=3790410245 TSecr=0 WS=128
242065	881.933758	2001:db8:7cc::a1:d055	2001:db8:7cc::acdc:24:911	TCP	86.41134	→ 80	[ACK]	Seq=1 Ack=1 Win=64896 Len=0 TSval=3790410245 TSecr=2103789926
242066	881.933783	2001:db8:7cc::a1:d055	2001:db8:7cc::acdc:24:911	TCP	94.41146	→ 80	[SYN]	Seq=0 Win=64800 Len=0 MSS=1440 SACK_PERM TSval=3790410245 TSecr=0 WS=128
242068	881.933791	2001:db8:7cc::a1:d055	2001:db8:7cc::acdc:24:911	TCP	86.41146	→ 80	[ACK]	Seq=1 Ack=1 Win=64896 Len=0 TSval=3790410245 TSecr=2103789926
242069	881.933821	2001:db8:7cc::a1:d055	2001:db8:7cc::acdc:24:911	TCP	94.41162	→ 80	[SYN]	Seq=0 Win=64800 Len=0 MSS=1440 SACK_PERM TSval=3790410245 TSecr=0 WS=128
242071	881.933828	2001:db8:7cc::a1:d055	2001:db8:7cc::acdc:24:911	TCP	86.41162	→ 80	[ACK]	Seq=1 Ack=1 Win=64896 Len=0 TSval=3790410245 TSecr=2103789926
242072	881.933854	2001:db8:7cc::a1:d055	2001:db8:7cc::acdc:24:911	TCP	94.41164	→ 80	[SYN]	Seq=0 Win=64800 Len=0 MSS=1440 SACK_PERM TSval=3790410245 TSecr=0 WS=128
242074	881.933861	2001:db8:7cc::a1:d055	2001:db8:7cc::acdc:24:911	TCP	86.41164	→ 80	[ACK]	Seq=1 Ack=1 Win=64896 Len=0 TSval=3790410245 TSecr=2103789926
242075	881.933888	2001:db8:7cc::a1:d055	2001:db8:7cc::acdc:24:911	TCP	94.41168	→ 80	[SYN]	Seq=0 Win=64800 Len=0 MSS=1440 SACK_PERM TSval=3790410245 TSecr=0 WS=128
242077	881.933895	2001:db8:7cc::a1:d055	2001:db8:7cc::acdc:24:911	TCP	86.41168	→ 80	[ACK]	Seq=1 Ack=1 Win=64896 Len=0 TSval=3790410245 TSecr=2103789926
242078	881.933942	2001:db8:7cc::a1:d055	2001:db8:7cc::acdc:24:911	TCP	94.41180	→ 80	[SYN]	Seq=0 Win=64800 Len=0 MSS=1440 SACK_PERM TSval=3790410245 TSecr=0 WS=128
242080	881.933951	2001:db8:7cc::a1:d055	2001:db8:7cc::acdc:24:911	TCP	86.41180	→ 80	[ACK]	Seq=1 Ack=1 Win=64896 Len=0 TSval=3790410245 TSecr=2103789926
242081	881.933979	2001:db8:7cc::a1:d055	2001:db8:7cc::acdc:24:911	TCP	94.41182	→ 80	[SYN]	Seq=0 Win=64800 Len=0 MSS=1440 SACK_PERM TSval=3790410245 TSecr=0 WS=128

AI response:

```
{"message": "It's probably a real incident, I'll consult the natural intelligence of a member of the CSIRT."}
```

Your incident ID is **Mi800iBzLVVrb3g=**, please keep it.

SCANNING

389	8.204838	2001:db8:7cc::a1:42	ff02::1:ff24:1fa	ICMPv6	86	Neighbor Solicitation for 2001:db8:7cc::acdc:24:1fa from 02:42:ac:11:02:20
390	8.204856	2001:db8:7cc::a1:42	ff02::1:ff24:1fb	ICMPv6	86	Neighbor Solicitation for 2001:db8:7cc::acdc:24:1fb from 02:42:ac:11:02:20
391	8.204869	2001:db8:7cc::a1:42	ff02::1:ff24:1fc	ICMPv6	86	Neighbor Solicitation for 2001:db8:7cc::acdc:24:1fc from 02:42:ac:11:02:20
392	8.382694	2001:db8:7cc::a1:42	ff02::1:ff24:1ff	ICMPv6	86	Neighbor Solicitation for 2001:db8:7cc::acdc:24:1ff from 02:42:ac:11:02:20
393	8.387750	2001:db8:7cc::a1:42	ff02::1:ff24:202	ICMPv6	86	Neighbor Solicitation for 2001:db8:7cc::acdc:24:202 from 02:42:ac:11:02:20
394	8.391595	2001:db8:7cc::a1:42	ff02::1:ff24:205	ICMPv6	86	Neighbor Solicitation for 2001:db8:7cc::acdc:24:205 from 02:42:ac:11:02:20
395	8.395447	2001:db8:7cc::a1:42	ff02::1:ff24:208	ICMPv6	86	Neighbor Solicitation for 2001:db8:7cc::acdc:24:208 from 02:42:ac:11:02:20
396	8.399361	2001:db8:7cc::a1:42	ff02::1:ff24:20b	ICMPv6	86	Neighbor Solicitation for 2001:db8:7cc::acdc:24:20b from 02:42:ac:11:02:20
397	8.402813	2001:db8:7cc::a1:42	ff02::1:ff24:20e	ICMPv6	86	Neighbor Solicitation for 2001:db8:7cc::acdc:24:20e from 02:42:ac:11:02:20
398	8.406256	2001:db8:7cc::a1:42	ff02::1:ff24:211	ICMPv6	86	Neighbor Solicitation for 2001:db8:7cc::acdc:24:211 from 02:42:ac:11:02:20
399	8.406324	2001:db8:7cc::a1:42	ff02::1:ff24:212	ICMPv6	86	Neighbor Solicitation for 2001:db8:7cc::acdc:24:212 from 02:42:ac:11:02:20

364530	1960.839078	2001:db8:7cc::a1:42	2001:db8:7cc::acdc:24:a854	TCP	78.44483	→ 22	[SYN]	Seq=0 Win=1024 Len=0 MSS=1460
364533	1960.839116	2001:db8:7cc::a1:42	2001:db8:7cc::acdc:24:beef	TCP	78.44483	→ 22	[SYN]	Seq=0 Win=1024 Len=0 MSS=1460
364535	1960.839142	2001:db8:7cc::a1:42	2001:db8:7cc::acdc:24:c43a	TCP	78.44483	→ 22	[SYN]	Seq=0 Win=1024 Len=0 MSS=1460
364538	1960.839201	2001:db8:7cc::a1:42	2001:db8:7cc::acdc:24:d553	TCP	78.44483	→ 22	[SYN]	Seq=0 Win=1024 Len=0 MSS=1460
364541	1960.839274	2001:db8:7cc::a1:42	2001:db8:7cc::acdc:24:e17f	TCP	78.44483	→ 22	[SYN]	Seq=0 Win=1024 Len=0 MSS=1460
364544	1960.839374	2001:db8:7cc::a1:42	2001:db8:7cc::acdc:24:e469	TCP	78.44483	→ 53	[SYN]	Seq=0 Win=1024 Len=0 MSS=1460
364547	1960.839409	2001:db8:7cc::a1:42	2001:db8:7cc::acdc:24:f017	TCP	78.44483	→ 53	[SYN]	Seq=0 Win=1024 Len=0 MSS=1460
364550	1960.839439	2001:db8:7cc::a1:42	2001:db8:7cc::acdc:24:fe35	TCP	78.44483	→ 22	[SYN]	Seq=0 Win=1024 Len=0 MSS=1460
364553	1960.839467	2001:db8:7cc::a1:42	2001:db8:7cc::acdc:24:200	TCP	78.44483	→ 22	[SYN]	Seq=0 Win=1024 Len=0 MSS=1460

1 Incident type

Incident type

Scanning

The type of incident that occurred.

2 Basic data

Offending IP address

2001:db8:7cc::a1:42

The source IPv4/IPv6 address that caused the incident.

Target scan range – CIDR

2001:db8:7cc::acdc:24:0/112

The destination IPv4/IPv6 address that was the target of the incident.

Datetime of the first attempt (UTC)

2024-09-26 08:44:29

The first attempt in UTC format (YYYY-MM-DD HH:MM:SS) where the source IP address caused the incident.

Datetime of the last attempt (UTC)

2024-09-26 09:17:09

The last time in UTC format (YYYY-MM-DD HH:MM:SS) the source IP address caused an incident.

3 Details

Target ports

- ☒ 21 (FTP)
- ☒ 22 (SSH)
- ☐ 23 (Telnet)
- ☐ 25 (SMTP)
- ☒ 53 (DNS)
- ☐ 69 (TFTP)
- ☒ 80 (HTTP)
- ☐ 137 (NetBIOS)
- ☒ 443 (HTTPS)
- ☐ 445 (SMB)
- ☐ 3306 (MySQL/MariaDB)
- ☐ 3389 (RDP)
- ☐ 5432 (PostgreSQL)
- ☒ 8080 (HTTP Alternative)
- ☐ Other

Number of found and scanned targets

20–99

Approximate number of targets found and scanned.

AI response:

```
{"message": "It's probably a real incident, I'll consult the natural intelligence of a member of the CSIRT."}
```

Your incident ID is **My800iAtYTBZRzi0=**, please keep it.

web service enumeration

19443 230.768842	2001:db8:7cc::a1:210	2001:db8:7cc::acdc:24:a160	HTTP	213 GET /.cvsignore.php HTTP/1.1
19446 230.770239	2001:db8:7cc::a1:210	2001:db8:7cc::acdc:24:a160	HTTP	216 GET /.cvsignore.html HTTP/1.1
19449 230.771758	2001:db8:7cc::a1:210	2001:db8:7cc::acdc:24:a160	HTTP	215 GET /.cvsignore.txt HTTP/1.1
19452 230.773385	2001:db8:7cc::a1:210	2001:db8:7cc::acdc:24:a160	HTTP	214 GET /.cvsignore.md HTTP/1.1
19456 230.777927	2001:db8:7cc::a1:210	2001:db8:7cc::acdc:24:a160	HTTP	209 GET /.forward HTTP/1.1
19460 230.780403	2001:db8:7cc::a1:210	2001:db8:7cc::acdc:24:a160	HTTP	213 GET /.forward.php HTTP/1.1
19464 230.783453	2001:db8:7cc::a1:210	2001:db8:7cc::acdc:24:a160	HTTP	214 GET /.forward.html HTTP/1.1
19468 230.788276	2001:db8:7cc::a1:210	2001:db8:7cc::acdc:24:a160	HTTP	213 GET /.forward.txt HTTP/1.1
19471 230.789742	2001:db8:7cc::a1:210	2001:db8:7cc::acdc:24:a160	HTTP	212 GET /.forward.md HTTP/1.1
19474 230.792710	2001:db8:7cc::a1:210	2001:db8:7cc::acdc:24:a160	HTTP	210 GET /.git/HEAD HTTP/1.1
19478 230.795432	2001:db8:7cc::a1:210	2001:db8:7cc::acdc:24:a160	HTTP	214 GET /.git/HEAD.php HTTP/1.1
19482 230.797536	2001:db8:7cc::a1:210	2001:db8:7cc::acdc:24:a160	HTTP	215 GET /.git/HEAD.html HTTP/1.1
19486 230.798752	2001:db8:7cc::a1:210	2001:db8:7cc::acdc:24:a160	HTTP	214 GET /.git/HEAD.txt HTTP/1.1
19490 230.801012	2001:db8:7cc::a1:210	2001:db8:7cc::acdc:24:a160	HTTP	213 GET /.git/HEAD.md HTTP/1.1
19493 230.802837	2001:db8:7cc::a1:210	2001:db8:7cc::acdc:24:a160	HTTP	209 GET /.history HTTP/1.1
19496 230.804662	2001:db8:7cc::a1:210	2001:db8:7cc::acdc:24:a160	HTTP	213 GET /.history.php HTTP/1.1

1 Incident type

Incident type

Web service enumeration

The type of incident that occurred.

2 Basic data

Offending IP address

2001:db8:7cc::a1:210

The source IPv4/IPv6 address that caused the incident.

Target IP address

2001:db8:7cc::acdc:24:a160

The destination IPv4/IPv6 address that was the target of the incident.

Datetime of the first attempt (UTC)

2024-09-26 08:48:18

The first attempt in UTC format (YYYY-MM-DD HH:MM:SS) where the source IP address caused the incident.

Datetime of the last attempt (UTC)

2024-09-26 08:49:45

The last time in UTC format (YYYY-MM-DD HH:MM:SS) the source IP address caused an incident.

3 Details

Number of enumerated URL

10000–49999

Approximate number of attempts.

AI response:

```
{"message":"It's probably a real incident, I'll consult the natural intelligence of a member of the CSIRT."}
```

Your incident ID is **NC800iBkNWtNfQ==**, please keep it.

Decoding all the base64 encoded pieces of data gives the flag divided into four parts.

1/4: FLAG{1E8

2/4: s-Ukox

3/4: -a0Qf-

4/4: d5kM}

The final flag is FLAG{1E8s-Ukox-a0Qf-d5kM} .