TURRIS

Útoky na privátní sítě v roce 2023

z pohledu sítě Turris Sentinel

Filip Hron

DB podpora

Python

V projektu **Turris** od srpna 2020

backend k rozhraní **reForis**

Turris Sentinel

https://blog.nic.cz/author/fhron/

Turris 1.x | Omnia

- Open source
- Aktualizace
- Zálohování
- Server

  (podpora VPN, Nextcloud)

Co je Turris Sentinel?

Sentinel je štít pro router

- síť komponent pro kolekci dat o útocích
- Aplikace vyhodnocených sesbíraných dat
  - Ochrana v reálném čase
  - Aktuální (dynamický) firewall
- Sentinel view a Report

Zdroje dat Pro síť Sentinel

- Minipoty (Mini-honeypoty)
  - FTP minipot
  - SMTP minipot
  - TELNET minipot
  - HTTP minipot
- Firewall logy
  - Agregace port-scanů

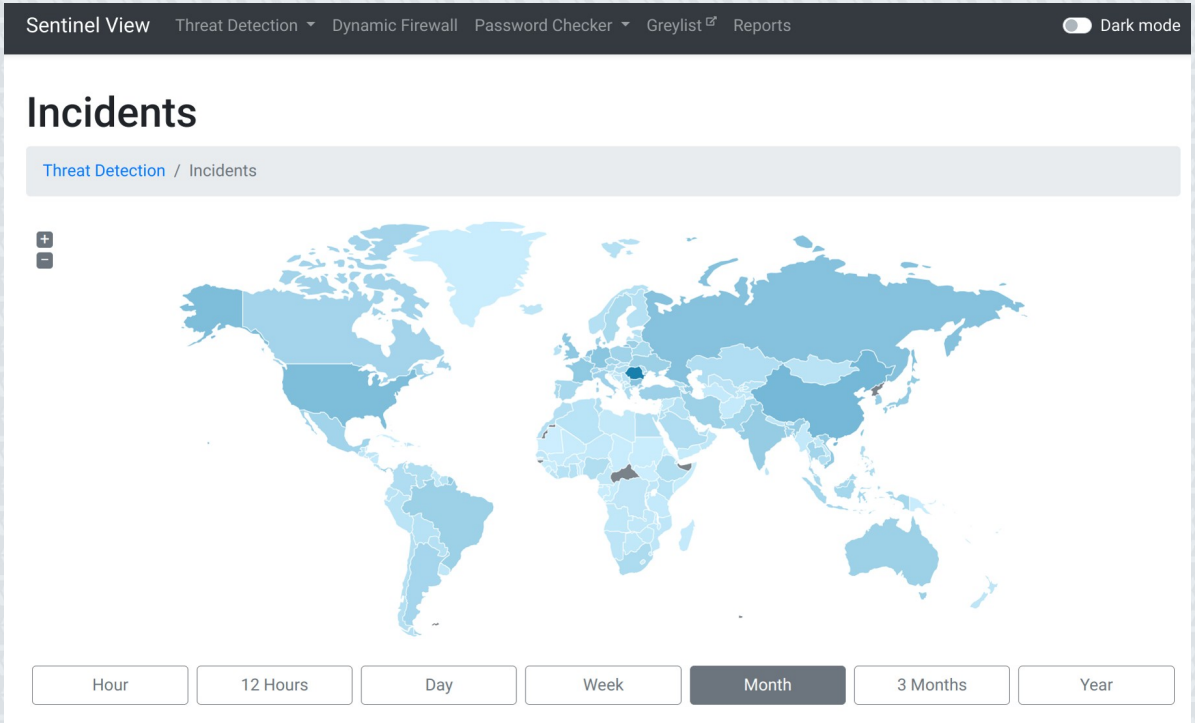
Top incident types by recorded incidents

1.	minipot_smtp	login	8425229610
2.	minipot_smtp	connect	8374963150
3.	minipot_telnet	connect	290059959
4.	minipot_smtp	invalid	136118449
5.	minipot_http	connect	133411195
6.	minipot_ftp	connect	97406717
7.	minipot_http	message	96817598
8.	minipot_ftp	login	90076132
9.	minipot_telnet	login	62598996
10.	minipot_http	login	49478019
11.	fwlogs	small_port_...	18550070
12.	fwlogs	big_port_scan	2680846
13.	minipot_http	invalid	1983454
14.	minipot_telnet	invalid	1334868
15.	minipot_ftp	invalid	36995

Web Sentinel View

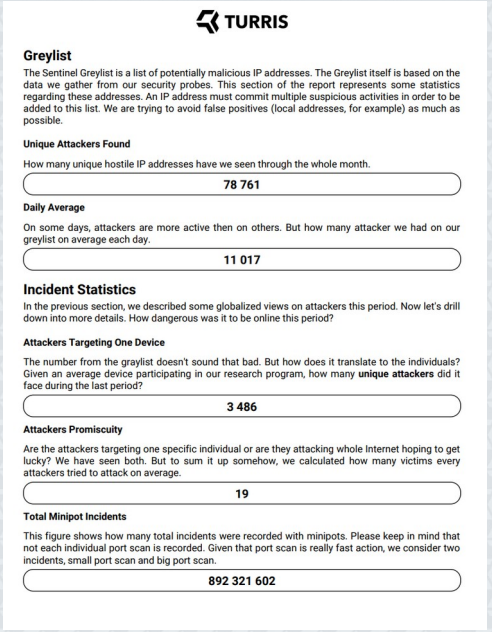
- **Kategorizované** reportování (útoky, útočníci, hesla)
- Aktuální náhled **dynamického firewallu**
- Kontrola **hesel**
  - **Formulář** kontroly hesla
  - **API** pro kontrolu hesel
- Historie **Greylistu**

view.sentinel.turris.cz



Měsíční Sentinel Report

- Kontext v rámci **jednoho** měsíce
- **PDF**
- **Porovnání** mezi jednotlivými měsíci
- Shrnující **komentář**



TURRIS

Greylist

The Sentinel Greylist is a list of potentially malicious IP addresses. The Greylist itself is based on the data we gather from our security probes. This section of the report represents some statistics regarding these addresses. An IP address must commit multiple suspicious activities in order to be added to this list. We are trying to avoid false positives (local addresses, for example) as much as possible.

Unique Attackers Found

How many unique hostile IP addresses have we seen through the whole month.

78 761

Daily Average

On some days, attackers are more active then on others. But how many attacker we had on our greylist on average each day.

11 017

Incident Statistics

In the previous section, we described some globalized views on attackers this period. Now let's drill down into more details. How dangerous was it to be online this period?

Attackers Targeting One Device

The number from the graylist doesn't sound that bad. But how does it translate to the individuals? Given an average device participating in our research program, how many **unique attackers** did it face during the last period?

3 486

Attackers Promiscuity

Are the attackers targeting one specific individual or are they attacking whole Internet hoping to get lucky? We have seen both. But to sum it up somehow, we calculated how many victims every attackers tried to attack on average.

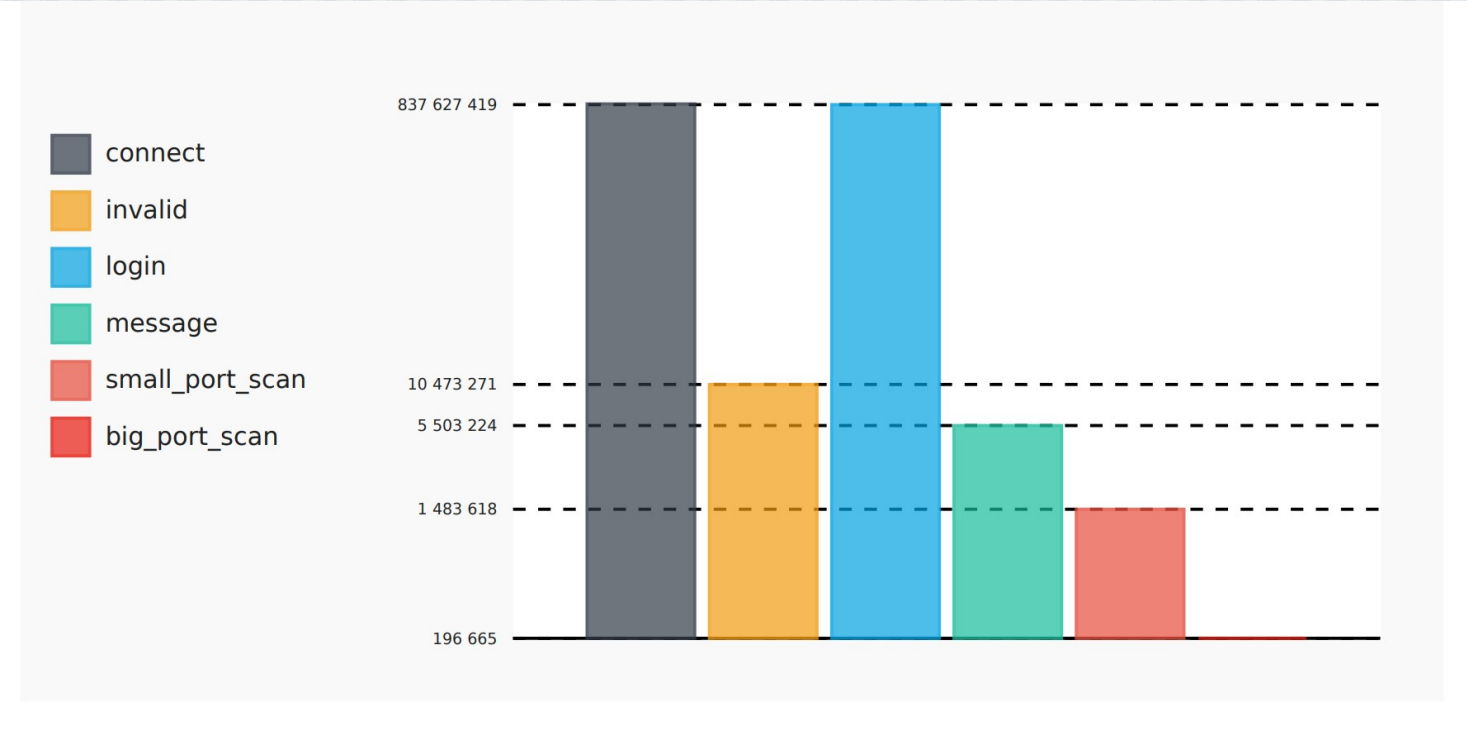
19

Total Minipot Incidents

This figure shows how many total incidents were recorded with minipots. Please keep in mind that not each individual port scan is recorded. Given that port scan is really fast action, we consider two incidents, small port scan and big port scan.

892 321 602

view.sentinel.turris.cz/report



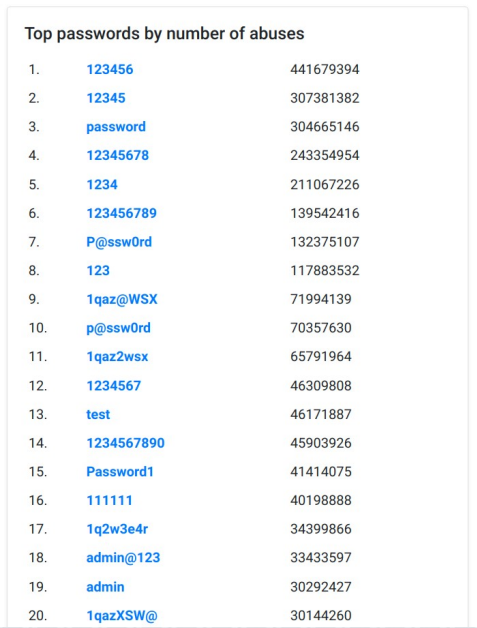
Zhodnocení

Nejčastější hesla

- Číselná řada 1n
- Leetspeak varianta `Password`
- Sekvence stisknutých kláves (QWERTY atp.)

Zajímavě tvořená hesla

- Sekvence stisknutých kláves
- algoritmem tvořená hesla



Top passwords by number of abuses

1.	123456	441679394
2.	12345	307381382
3.	password	304665146
4.	12345678	243354954
5.	1234	211067226
6.	123456789	139542416
7.	P@ssw0rd	132375107
8.	123	117883532
9.	1qaz@WSX	71994139
10.	p@ssw0rd	70357630
11.	1qaz2wsx	65791964
12.	1234567	46309808
13.	test	46171887
14.	1234567890	45903926
15.	Password1	41414075
16.	111111	40198888
17.	1q2w3e4r	34399866
18.	admin@123	33433597
19.	admin	30292427
20.	1qazXSW@	30144260

Metodika zkoušení hesel

- Nejaktivnější útočníci zkouší 1 heslo
- Další den zkouší jiné heslo

Útočníci

Top countries by unique attackers

1.	CN	1056882
2.	IN	791423
3.	US	513190
4.	BR	280365
5.	IR	247813
6.	EG	233587
7.	VE	209943
8.	RU	197604
9.	TW	161271
10.	JP	122552
11.	GB	116189
12.	PK	111457
13.	DE	111080
14.	AR	77980
15.	VN	71670

Top countries by recorded incidents

1.	RO	6531592236
2.	IR	6211682519
3.	LT	1323143783
4.	DE	1140729838
5.	BG	936401180
6.	US	296664762
7.	CN	279498479
8.	MX	184411496
9.	NL	128233620
10.	HK	119326869
11.	PE	62981710
12.	VN	59812448
13.	GB	59363357
14.	RU	57206313
15.	KR	33094720

Malý a velký port scan

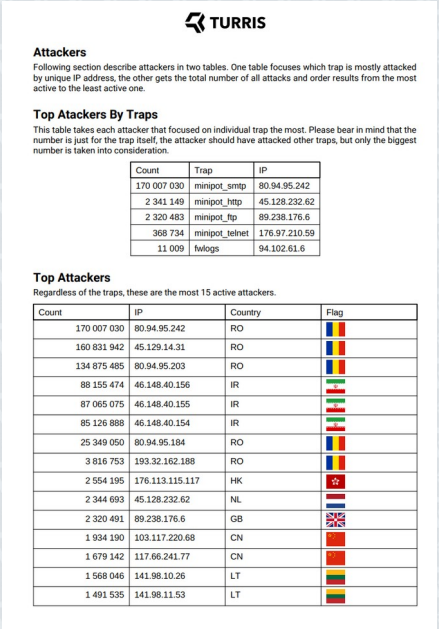
- Záznamy z firewallu
- Agregace scanů z jednoho místa
- Scan malého počtu portů nebo velkého počtu

Top ports by performed scans

1.	**UDP/5353**	198662309
2.	**UDP/5678**	76039134
3.	**UDP/51413**	40601614
4.	**UDP/67**	38410169
5.	**UDP/53**	34122958
6.	**UDP/10002**	33553726
7.	**TCP/51413**	20449865
8.	**UDP/6881**	12024456
9.	**UDP/6667**	10100048
10.	**UDP/10001**	8054733
11.	**UDP/36553**	6357422
12.	**UDP/137**	6357087
13.	**UDP/33204**	4898397
14.	**TCP/16881**	4889688
15.	**UDP/48028**	3183116

Základní společné statistiky

- Minipot SMTP
- Jedna adresa velký počet útoků
- TELNET v porovnání zanedbatelný



TURRIS

Attackers

Following section describe attackers in two tables. One table focuses which trap is mostly attacked by unique IP address, the other gets the total number of all attacks and order results from the most active to the least active one.

Top Atackers By Traps

This table takes each attacker that focused on individual trap the most. Please bear in mind that the number is just for the trap itself, the attacker should have attacked other traps, but only the biggest number is taken into consideration.

Count	Trap	IP
170 007 030	minipot_smtp	80.94.95.242
2 341 149	minipot_http	45.128.232.62
2 320 483	minipot_ftp	89.238.176.6
368 734	minipot_telnet	176.97.210.59
11 009	fwlogs	94.102.61.6

Top Attackers

Regardless of the traps, these are the most 15 active attackers.

Count	IP	Country	Flag
170 007 030	80.94.95.242	RO	
160 831 942	45.129.14.31	RO	
134 875 485	80.94.95.203	RO	
88 155 474	46.148.40.156	IR	
87 065 075	46.148.40.155	IR	
85 126 888	46.148.40.154	IR	
25 349 050	80.94.95.184	RO	
3 816 753	193.32.162.188	RO	
2 554 195	176.113.115.117	HK	
2 344 693	45.128.232.62	NL	
2 320 491	89.238.176.6	GB	
1 934 190	103.117.220.68	CN	
1 679 142	117.66.241.77	CN	
1 568 046	141.98.10.26	LT	
1 491 535	141.98.11.53	LT	

Konec

Díky za pozornost!