Sentinel Report - February 2023

This document is the monthly report from the Turris Sentinel team. We are running a network of security probes that are collecting data about attacks ranging from simple port scans to actual attempts to break into systems. We use this data to filter addresses on the Dynamic Firewall and protect our Turris routers. We also display various statistics in real-time on our Sentinel View. Apart from that, we publish this monthly newsletter with statistics that are more complex to compute, and we are taking this opportunity to put the data we have collected into perspective.

Overview

In February, we saw about a 10% decrease in the number of unique attackers, but they were more active. Usually, we see attackers come and go, but in February, although it was fewer attackers in total, we had on average, more attackers blocked every day. This means that those attackers stayed active longer than in January.
Regarding the port attacks, we saw a decrease in attacks on many well-known ports. That is a good sign, but don't let your guard down. An attacker has to succeed just once, while you have to repel his every attempt. The first potentially interesting port that gained some popularity among attackers is 9091. It is the default port for RPC for the Transmission BitTorrent client. That sounds like a potentially juicy target. So keep your RPC endpoints secured, and when exposing them, make sure you have a strong enough password.
In passwords, it looks like bots figured out that many systems requests at least eight characters password, so the most popular password of February is *12345678*. We also have a few well-known candidates on top, but the rest of the chart is occupied by random attacks from Iran that we already spoke about in the report for January. And although there are still a few IPs showing similar behavior, the Iranian network does an order of magnitude more attacks then everybody else combined. We also checked what the used usernames look like. To make sure it wasn't just some random stream of data hitting our mini pots. But even though there are short usernames that look random, like *v5* or *h24*, there is also plenty of valid usernames like *admin*, *postmaster*, or *zztop* and those are much more common.

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.

77 462

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.

11 442

Incident Statistics

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

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 month?

3 071

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 attacker tried to attack on average.

19

Port Trends

This section shows monthly trends in port scans for port-protocol combinations. The description serves as a reminder of the services that the attacker may be interested in. Compared to what we publish in Sentinel View, this list is based on the number of attackers targeting the port, not the number of attacks as in Sentinel View. This can serve as an indication of which services are most interesting to the attackers out there. This information can help security researchers spot new trends and give sysadmins an indication of which services need to be more carefully watched.

Port	Protocol	Previous	Last	Growth	Description
51413	UDP	2 687 416	1 730 542	–36%	N/A
6881	UDP	3 021 725	1 685 486	–44%	BitTorrent beginning of range of ports used most often
6889	UDP	644 162	452 444	–30%	BitTorrent continuation of range of ports used most often
7881	UDP	450 979	304 589	–32%	N/A
445	TCP	378 738	282 660	–25%	Microsoft-DS (Directory Services) Active Directory, | Microsoft-DS (Directory Services) SMB
64541	UDP	260 024	255 801	–2%	N/A
27032	UDP	451 249	253 782	–44%	Steam (In-Home Streaming)
51413	TCP	333 928	237 049	–29%	Certificate Management over CMS
52285	UDP	1 280	177 528	13 769%	N/A
1024	UDP	236 624	161 387	–32%	Reserved
60731	UDP	105 399	141 354	34%	Range from which Mosh – a remote-terminal application similar to SSH – typically assigns ports for ongoing sessions between Mosh servers and Mosh clients.
6881	TCP	186 901	137 788	–26%	BitTorrent beginning of range of ports used most often

Port	Protocol	Previous	Last	Growth	Description
16881	UDP	122 692	118 864	–3%	Used on VoIP networks for receiving and transmitting voice telephony traffic which includes Google Voice via the OBiTalk ATA devices as well as on the MagicJack and Vonage ATA network devices.
16881	TCP	95 859	114 447	19%	N/A
23	TCP	168 141	110 402	–34%	Telnet protocol—unencrypted text communications
59492	UDP	83 590	109 652	31%	N/A
64541	TCP	188 907	100 648	–47%	Certificate Management over CMS
6891	UDP	30 005	89 469	198%	BitTorrent continuation of range of ports used most often | Windows Live Messenger (File transfer)
37215	TCP	28 593	87 486	206%	N/A
1	UDP	161 357	86 616	–46%	TCP Port Service Multiplexer (TCPMUX). Historic. Both TCP and UDP have been assigned to TCPMUX by IANA,
9091	UDP	56 633	84 875	50%	Openfire Administration Console (SSL Secured) | Transmission (BitTorrent client) Web Interface
443	TCP	143 861	80 759	–44%	Hypertext Transfer Protocol Secure (HTTPS)HTTP/3 uses QUIC,
8080	TCP	116 592	79 144	–32%	Alternative port for HTTP. See also ports 80 and 8008. | Apache Tomcat | Atlassian JIRA applications
50011	UDP	352	69 003	19 503%	N/A
47143	UDP	262	68 544	26 062%	N/A
5555	TCP	105 911	67 096	–37%	Oracle WebCenter Content: Inbound Refinery—Intradoc Socket port. (formerly known as Oracle Universal Content Management). Port though often changed during installation | Freeciv versions up to 2.0, Hewlett-Packard Data Protector, McAfee EndPoint Encryption Database Server, SAP, Default for Microsoft Dynamics CRM 4.0, Softether VPN default port
65206	UDP	103	66 417	64 383%	N/A
58818	UDP	155	65 938	42 441%	N/A
27032	TCP	110 160	65 666	–40%	N/A
57957	UDP	3 030	61 409	1 927%	N/A
59997	UDP	238	60 077	25 142%	N/A

Port	Protocol	Previous	Last	Growth	Description
32862	UDP	39 311	54 961	40%	N/A
1433	TCP	66 264	52 568	–21%	Microsoft SQL Server database management system (MSSQL) server
30303	UDP	60 951	51 793	–15%	N/A
38649	UDP	204	50 406	24 609%	N/A
6882	UDP	88 935	49 975	–44%	BitTorrent beginning of range of ports used most often
41870	UDP	8 081	49 293	510%	N/A
38649	TCP	277	46 884	16 826%	N/A
62734	UDP	68 112	45 884	–33%	N/A
59966	UDP	138	45 301	32 727%	N/A
2042	UDP	99	44 848	45 201%	N/A
31402	TCP	43 666	44 725	2%	N/A
6890	UDP	33 293	43 440	30%	BitTorrent continuation of range of ports used most often
45280	UDP	582	43 115	7 308%	N/A
62882	UDP	62 054	43 096	–31%	N/A
55859	UDP	72 973	42 843	–41%	N/A
21336	UDP	42 918	42 175	–2%	N/A
22	TCP	65 942	41 973	–36%	Secure Shell (SSH),file transfers (scp, sftp) and port forwarding
2323	TCP	62 107	41 449	–33%	N/A
4444	UDP	50 534	40 921	–19%	Oracle WebCenter Content: Content Server—Intradoc Socket port. (formerly known as Oracle Universal Content Management). | Metasploit's default listener port | Xvfb X server virtual frame buffer service | OpenOCD (Telnet) | I2P HTTP/S proxy
60023	TCP	57 534	40 783	–29%	Certificate Management over CMS
1	TCP	78 518	40 777	–48%	TCP Port Service Multiplexer (TCPMUX). Historic. Both TCP and UDP have been assigned to TCPMUX by IANA,
62805	UDP	83	40 178	48 307%	N/A
61289	UDP	25 685	40 082	56%	N/A
9006	UDP	44 524	39 666	–11%	Tomcat in standalone mode
6883	UDP	26 288	39 425	50%	BitTorrent beginning of range of ports used most often
80	TCP	54 355	38 745	–29%	Hypertext Transfer Protocol (HTTP)HTTP/3 uses QUIC,

Port	Protocol	Previous	Last	Growth	Description
6884	UDP	26 275	37 643	43%	BitTorrent beginning of range of ports used most often
37388	UDP	46 527	37 533	–19%	N/A
7680	TCP	37 142	37 080	~0%	Delivery Optimization for Windows 10
39841	UDP	37 422	36 959	–1%	N/A
6901	UDP	68 558	36 874	–46%	Windows Live Messenger (Voice) | BitTorrent continuation of range of ports used most often
53	UDP	46 085	36 749	–20%	Domain Name System (DNS)
9000	UDP	32 134	35 964	12%	SonarQube Web Server | ClickHouse default port | DBGp | SqueezeCenter web server & streaming | UDPCast | Play Framework web server | Hadoop NameNode default port | PHP-FPM default port | QBittorrent's embedded torrent tracker default port
6888	UDP	62 113	35 795	–42%	MUSE | BitTorrent continuation of range of ports used most often
49530	UDP	16 902	35 159	108%	N/A
54118	UDP	212	34 665	16 251%	N/A
57017	UDP	38 427	34 409	–10%	N/A
55555	UDP	80 733	34 316	–57%	N/A
6885	UDP	22 966	34 187	49%	BitTorrent beginning of range of ports used most often
81	TCP	39 661	34 004	–14%	TorPark onion routing
6886	UDP	116 528	33 285	–71%	BitTorrent beginning of range of ports used most often
54728	UDP	45 651	32 899	–28%	N/A
50681	UDP	106	32 740	30 787%	N/A
48462	TCP	3 266	32 730	902%	N/A
6887	UDP	23 085	32 468	41%	BitTorrent beginning of range of ports used most often
10322	UDP	60	30 166	50 177%	Used on VoIP networks for receiving and transmitting voice telephony traffic which includes Google Voice via the OBiTalk ATA devices as well as on the MagicJack and Vonage ATA network devices.
47739	UDP	134	29 593	21 984%	N/A
9001	UDP	19 946	28 658	44%	ETL Service Manager | Microsoft SharePoint authoring environment | cisco-xremote router configuration | Tor network default | DBGp Proxy | HSQLDB default port

Port	Protocol	Previous	Last	Growth	Description
53292	UDP	151	28 052	18 477%	N/A
48804	UDP	34 606	27 289	–21%	N/A
9091	TCP	37 435	27 105	–28%	Openfire Administration Console (SSL Secured) | Transmission (BitTorrent client) Web Interface
49001	UDP	105 029	26 223	–75%	N/A
64249	UDP	5 529	25 596	363%	N/A
54728	TCP	33 411	25 552	–24%	Certificate Management over CMS
1037	UDP	7 181	25 498	255%	N/A
55662	UDP	142	25 282	17 704%	N/A
50319	UDP	34 955	25 014	–28%	N/A
2222	TCP	39 033	24 852	–36%	EtherNet/IP implicit messaging for IO data | DirectAdmin Access | ESET Remote administrator
56650	UDP	3 878	24 791	539%	N/A
8444	TCP	30 856	24 003	–22%	Bitmessage
1025	UDP	2 708	23 902	783%	Teradata database management system (Teradata) server
14041	UDP	64	23 509	36 633%	Used on VoIP networks for receiving and transmitting voice telephony traffic which includes Google Voice via the OBiTalk ATA devices as well as on the MagicJack and Vonage ATA network devices.
1539	UDP	55 362	23 465	–58%	N/A
50319	TCP	32 784	23 321	–29%	Certificate Management over CMS
57431	UDP	207	23 086	11 053%	N/A
57957	TCP	927	22 931	2 374%	Certificate Management over CMS
57511	UDP	171	22 852	13 264%	N/A
3306	TCP	26 988	22 392	–17%	MySQL database system
51000	UDP	206 079	22 355	–89%	N/A

Password Deltas

The diagram shows how many times we've seen individual passwords being used in attack attempts last month in comparison to the month before. The data are ordered by count last month, and the last column contains the difference against the previous month in percents for easier comparison. This allows you to spot passwords that just became popular. This information may point out some new vulnerable devices or new malware spreading through the Internet.

Password	Previous Month	Last Month	Growth
12345678	17 643	318 562	1 706%
password	34 630	247 103	614%
12345	182 080	182 838	~0%
123456	189 767	170 978	–10%
1234	115 828	147 769	28%
cfd3HPGn	0	110 377	N/A
life4Ak2g	0	107 886	N/A
ugij2MH	0	97 736	N/A
73ZCD3p4	0	96 981	N/A
OhM62Mz9	0	94 899	N/A
LG454Cr	10 585	91 429	764%
NoL484t	23 995	90 154	276%
2hn69zCgM0	0	90 080	N/A
ogu6MFWo5	0	89 807	N/A
djkdHs2d25c	0	89 412	N/A
KaBMGeJwP2	48 375	89 031	84%
gef2fefluh5	0	87 545	N/A
jf4d3UQN6	0	87 426	N/A
WiPB5JV9DI37	0	86 781	N/A
7dh1x5BnskY	0	86 394	N/A
a092kD	8 362	86 231	931%
QqCkC1T8O9	45 390	86 072	90%
6wCV7j	10 617	86 025	710%
eKT5U62Kr4	0	84 541	N/A
kHIt8	0	84 460	N/A
YKEpyow0Nx8	0	83 413	N/A
0HyHJ	0	83 264	N/A
6UBrkx41B	0	82 658	N/A
ANW5HTaz8	48 566	81 753	68%
GGLKkBtl	0	81 704	N/A
9N3NjA9l	0	81 378	N/A
SM77Eh1Kg	0	80 999	N/A

TURRIS

Password	Previous Month	Last Month	Growth
81uZaUv	46 202	79 400	72%
7Fn95L66	0	79 347	N/A
SggzeW5WK4	0	79 227	N/A
KSqH0dJjg	0	78 844	N/A
QiynS2JL80	0	78 742	N/A
u7fTk6rf	2 236	78 654	3 418%
zPvJT76lR85	0	78 493	N/A
j6ySR6mh1UoX	2 236	78 427	3 407%
6kJ7y5Y9s	0	78 381	N/A
e5UZUEBgv	0	77 670	N/A
024qWbjE	23 785	77 658	226%
8l9JC	0	77 161	N/A
1bbEWWbd	0	77 140	N/A
N2yvwi8JQX3n	0	76 971	N/A
mQ7TN	0	76 641	N/A
md3uV93	24 502	76 245	211%
80iq7tEnf	0	76 227	N/A
JOartYgm24	0	75 910	N/A
3c2HQ2NN5t7R5	0	75 264	N/A
y821Zs5	0	75 020	N/A
Axzl0K2wd	0	74 808	N/A
GH96BLdC8k8X	622	74 730	11 914%
A5zcM	0	74 655	N/A
3N8j0O8iA1fC	0	74 316	N/A
11oy460p	2 236	74 217	3 219%
9L3XIT9	0	73 919	N/A
ccrVu3iS	0	73 775	N/A
DQmD3UVMT5M	0	73 575	N/A
5NcJidS	5 549	73 454	1 224%
RrJ0cqd9g	0	73 265	N/A
3b7eR4ht0g3F	23 695	72 602	206%
xY1678	2 111	72 241	3 322%
7bk841clF	0	72 039	N/A
8Oty3F	0	71 867	N/A
3A0q5yLk	0	71 685	N/A
5P78Ry	0	71 670	N/A
6QJjA2EV	0	71 192	N/A

Password	Previous Month	Last Month	Growth
dPd1x9Tir2DL	0	71 095	N/A
LU9YUNh2bDS	2 236	70 877	3 070%
ZX0kmM	48 311	70 505	46%
97wgej70S4	0	70 400	N/A
tN04MK8	2 236	70 282	3 043%
eLfz4D	23 780	70 204	195%
V1vS8	23 752	70 156	195%
98Okx	25 234	69 970	177%
UxT66gHlomh	0	69 710	N/A
SdeU1H8	14 397	69 695	384%
DA7639	21 556	69 637	223%
u3Gdn6RiA	0	69 632	N/A
l1HBv7t	0	69 520	N/A
aeQEL	0	68 971	N/A
ndmQCRPd	0	68 944	N/A
2p1uilHR1zry	48 231	68 927	43%
Ba478MY9D6c	0	68 882	N/A
VOxaQRgj	0	68 741	N/A
4KLQwr	0	68 558	N/A
rS5vzk7LM	0	68 513	N/A
YEThLny6	0	68 507	N/A
T6p5Qo7j	0	68 359	N/A
0Um72S2J31	0	68 069	N/A
MqE9X9M034Ge	0	67 861	N/A
sK4j75p	0	67 770	N/A
CtL0y	10 615	67 749	538%
mDa0GGf	0	67 475	N/A
43k80k0P75Y	0	67 258	N/A
07VRGW56h6	0	67 122	N/A
H6j7B9B	0	66 610	N/A
35pPHSgYX12U	0	66 522	N/A

Most Used Passwords Wordcloud