Sentinel Report - 2023 March

This document is the Sentinel report from the Turris 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 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

Looking at Greylist and Incidents Statistics, March data seem to be quite stable in comparison with the previous month. The total count of incidents did not drop significantly from February as the difference is about 100k incidents. The total number of incidents in February, divided by the number of days in the month and then multiplied by 30.36 (average number of days in a month) is 20,543,356.40. For March, using the same rules, we get 20,461,799.03.
We can see that there are many port hits probably caused by Transmission BitTorrent client again. But this time it is not the API, but the default port used for data transfers. Other commonly used ports for connecting BitTorrent clients (6881, 6889) are also on top. That makes sense. Misconfigured clients can attract a lot of different IPs that will eventually get stopped on firewall. But apart from that, we see once again a rising popularity of searching for open ports belonging to Windows shares. The previous analysis prompted us to take the opportunity to rework the list of port descriptions. We decided to add entries that are not listed on Wikipedia. From now on, we will fill in additional details in the table whenever we find a probable cause that made the port appear in our statistics.
The number of tries for popular passwords dropped significantly. No idea why. Even the Iranian network that is trying random passwords is slowed down. But they are still there, although due to being less active, we got some expected passwords back in the top of the chart.

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.

74 119

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.

10 789

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?

3 317

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.

18

Port Trends

This section shows trends in port scans for port-protocol combinations relevant. For current period. 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	1 730 542	3 698 196	114%	Transmission bit-torrent client
6881	UDP	1 685 486	3 017 196	79%	BitTorrent beginning of range of ports used most often
27032	UDP	253 782	909 647	258%	Steam (In-Home Streaming) | Steam Client (Remote Play)
6889	UDP	452 444	884 792	96%	BitTorrent continuation of range of ports used most often
51413	TCP	237 049	479 358	102%	Certificate Management over CMS | Transmission bit-torrent client
45280	UDP	43 115	470 064	990%	N/A
445	TCP	282 660	463 654	64%	Microsoft-DS (Directory Services) Active Directory, | Microsoft-DS (Directory Services) SMB
27032	TCP	65 666	296 829	352%	N/A
6881	TCP	137 788	291 653	112%	BitTorrent beginning of range of ports used most often
48804	UDP	27 289	275 863	911%	N/A

Port	Protocol	Previous	Last	Growth	Description
60731	UDP	141 354	250 556	77%	Range from which Mosh – a remote-terminal application similar to SSH – typically assigns ports for ongoing sessions between Mosh servers and Mosh clients.
1	UDP	86 616	242 577	180%	TCP Port Service Multiplexer (TCPMUX). Historic. Both TCP and UDP have been assigned to TCPMUX by IANA,
23	TCP	110 402	210 994	91%	Telnet protocol—unencrypted text communications
7881	UDP	304 589	199 297	–35%	Quick Time Streaming Server (formerly)
6891	UDP	89 469	178 485	99%	BitTorrent continuation of range of ports used most often | Windows Live Messenger (File transfer)
59492	UDP	109 652	176 487	61%	N/A
51000	UDP	22 355	154 435	591%	N/A
49001	UDP	26 223	151 842	479%	Far Cry | Nuance Unity Service Discovery Protocol
1024	UDP	161 387	151 726	–6%	Reserved
8080	TCP	79 144	146 223	85%	Alternative port for HTTP. See also ports 80 and 8008. | Apache Tomcat | Atlassian JIRA applications
16881	UDP	118 864	144 625	22%	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. | Synology NAS DSM download service
1026	UDP	867	140 702	16 129%	Microsoft DCOM services | CAP - Calendar Access Protocol (IANA official)
36901	UDP	51	139 223	272 886%	N/A
65206	UDP	66 417	138 277	108%	Dynamic and/or private ports
21742	UDP	8 422	129 477	1 437%	N/A
1065	UDP	214	129 058	60 207%	SYSCOMLAN
16881	TCP	114 447	119 269	4%	Synology NAS DSM download service
6882	UDP	49 975	118 796	138%	BitTorrent beginning of range of ports used most often
32862	UDP	54 961	116 347	112%	World of Tanks
443	TCP	80 759	115 513	43%	Hypertext Transfer Protocol Secure (HTTPS)HTTP/3 uses QUIC,

Port	Protocol	Previous	Last	Growth	Description
55555	UDP	34 316	115 141	236%	N/A
32793	UDP	61	113 270	185 589%	N/A
39373	UDP	39	107 956	276 710%	N/A
1	TCP	40 777	104 059	155%	TCP Port Service Multiplexer (TCPMUX). Historic. Both TCP and UDP have been assigned to TCPMUX by IANA,
6901	UDP	36 874	99 688	170%	Windows Live Messenger (Voice) | BitTorrent continuation of range of ports used most often
1433	TCP	52 568	89 716	71%	Microsoft SQL Server database management system (MSSQL) server
37215	TCP	87 486	89 504	2%	Huawei HG532 routers
63048	UDP	62	89 246	143 845%	N/A
51412	UDP	12 181	88 635	628%	N/A
50921	UDP	10 619	87 628	725%	N/A
43995	UDP	255	86 089	33 660%	N/A
4444	UDP	40 921	83 258	103%	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
40973	UDP	71	83 075	116 907%	N/A
60023	TCP	40 783	82 401	102%	Certificate Management over CMS
54741	UDP	15 331	81 705	433%	N/A
54728	UDP	32 899	81 267	147%	N/A
6888	UDP	35 795	80 746	126%	MUSE | BitTorrent continuation of range of ports used most often
5555	TCP	67 096	80 016	19%	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
43995	TCP	186	79 415	42 596%	N/A
30303	UDP	51 793	76 884	48%	Ethereum Client

Port	Protocol	Previous	Last	Growth	Description
16376	UDP	9 113	76 239	737%	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.
12701	UDP	17 112	75 735	343%	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.
39373	TCP	177	75 102	42 331%	N/A
55859	UDP	42 843	74 945	75%	N/A
39841	UDP	36 959	74 307	101%	N/A
48804	TCP	955	70 693	7 302%	N/A
62882	UDP	43 096	68 789	60%	N/A
64541	UDP	255 801	66 149	–74%	N/A
58996	UDP	180	65 698	36 399%	N/A
55802	UDP	72	65 679	91 121%	N/A
1025	UDP	23 902	65 468	174%	Teradata database management system (Teradata) server
9006	UDP	39 666	65 368	65%	IANA Reserved port
54728	TCP	25 552	65 139	155%	Certificate Management over CMS
11516	UDP	22 079	64 463	192%	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.
80	TCP	38 745	64 294	66%	Hypertext Transfer Protocol (HTTP)HTTP/3 uses QUIC,
22	TCP	41 973	64 179	53%	Secure Shell (SSH),file transfers (scp, sftp) and port forwarding
1900	UDP	4 949	63 596	1 185%	Simple Service Discovery Protocol (SSDP),UPnP devices
31402	TCP	44 725	63 579	42%	N/A
61289	UDP	40 082	62 663	56%	N/A
37388	UDP	37 533	61 899	65%	N/A
52413	UDP	144	61 703	42 749%	N/A
64249	UDP	25 596	61 076	139%	N/A
9000	UDP	35 964	60 827	69%	UDPCast
7680	TCP	37 080	60 065	62%	Delivery Optimization for Windows 10

Port	Protocol	Previous	Last	Growth	Description
6887	UDP	32 468	59 964	85%	BitTorrent beginning of range of ports used most often
40973	TCP	172	59 958	34 759%	Brothers in Arms Online
2323	TCP	41 449	59 414	43%	N/A
32793	TCP	519	58 583	11 188%	N/A
57017	UDP	34 409	58 489	70%	N/A
16542	UDP	16 473	58 022	252%	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.
81	TCP	34 004	57 976	70%	TorPark onion routing
53	UDP	36 749	56 457	54%	Domain Name System (DNS)
10322	UDP	30 166	55 317	83%	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.
43469	UDP	52	54 418	104 550%	N/A
56882	TCP	530	53 928	10 075%	Certificate Management over CMS
33051	UDP	75	53 729	71 539%	N/A
6885	UDP	34 187	52 553	54%	BitTorrent beginning of range of ports used most often
55662	UDP	25 282	52 171	106%	N/A
36080	UDP	78	50 652	64 838%	N/A
43237	UDP	21 464	50 568	136%	N/A
8444	TCP	24 003	48 882	104%	Bitmessage
13833	UDP	117	48 130	41 037%	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.
58818	UDP	65 938	48 065	–27%	N/A
34876	UDP	86	46 882	54 414%	N/A
6883	UDP	39 425	45 740	16%	BitTorrent beginning of range of ports used most often
57619	UDP	115	45 342	39 328%	N/A
6886	UDP	33 285	44 221	33%	BitTorrent beginning of range of ports used most often

Port	Protocol	Previous	Last	Growth	Description
6890	UDP	43 440	43 626	~0%	BitTorrent continuation of range of ports used most often
65472	UDP	84	42 126	50 050%	N/A
10889	UDP	9 941	41 755	320%	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.

Port descriptions are taken from Wikipedia under the CC-Share-Alike license. https://en.wikipedia.org/wiki/List_of_TCP_and_UDP_port_numbers

Password Deltas

The diagram shows how many times we've seen individual passwords being used in attack attempts last period in comparison to the period before. The data are ordered by count last period, and the last column contains the difference against the previous period 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	Last	Growth
password	247 103	149 732	–39%
123456	170 978	108 000	–37%
1234	147 769	89 012	–40%
12345678	318 562	88 254	–72%
12345	182 838	77 581	–58%
123456789	63 273	60 010	–5%
123	59 970	37 479	–38%
1234567	23 089	28 588	24%
AB■	40 504	24 542	–39%
1qaz2wsx	5 415	21 975	306%
eKT5U62Kr4	84 541	18 072	–79%
123123	12 624	17 212	36%
kHIt8	84 460	17 188	–80%
7Fn95L66	79 347	17 177	–78%
ogu6MFWo5	89 807	17 172	–81%
0HyHJ	83 264	17 168	–79%
life4Ak2g	107 886	17 161	–84%
KSqH0dJjg	78 844	17 159	–78%
dPd1x9Tir2DL	71 095	17 150	–76%
9N3NjA9l	81 378	17 146	–79%
YKEpyow0Nx8	83 413	17 138	–79%
SM77Eh1Kg	80 999	17 130	–79%
3P01p68L	66 217	17 127	–74%
73ZCD3p4	96 981	17 114	–82%
6UBrkx41B	82 658	17 108	–79%
e5UZUEBgv	77 670	17 094	–78%
rS5vzk7LM	68 513	17 093	–75%
WQoRDw68	57 441	17 052	–70%
DEclxRzMNSzH	52 496	17 046	–68%
OhM62Mz9	94 899	17 035	–82%
zPvJT76lR85	78 493	17 031	–78%
N2yvwi8JQX3n	76 971	17 022	–78%

TURRIS

Password	Previous	Last	Growth
u3Gdn6RiA	69 632	17 017	–76%
50wFTA8	59 416	17 016	–71%
P7yH7gacqi27	32 387	16 989	–48%
z82xl3VJBQr	55 453	16 987	–69%
T6p5Qo7j	68 359	16 976	–75%
L60hi41	51 535	16 971	–67%
o2PP5lI60	60 676	16 966	–72%
0qWlGi	44 199	16 966	–62%
00ZCNV	59 871	16 951	–72%
N443b	42 702	16 949	–60%
545GK	36 712	16 947	–54%
q90ge5mM1W8	52 318	16 940	–68%
vloD7AD8	54 694	16 927	–69%
8sE0sm	50 044	16 921	–66%
5nE2jKtFK	53 370	16 916	–68%
gWT5074l	35 899	16 880	–53%
zAHt9f5	64 493	16 822	–74%
m37b512JM2	58 758	16 687	–72%
9L3XIT9	73 919	16 580	–78%
3N8j0O8iA1fC	74 316	16 569	–78%
F141F20	53 435	16 533	–69%
0Um72S2J31	68 069	16 500	–76%
gef2fefluh5	87 545	16 495	–81%
7bk841clF	72 039	16 452	–77%
ugij2MH	97 736	16 450	–83%
71j7aD6k	63 754	16 372	–74%
D82jYrD26	47 687	16 260	–66%
80XbJp4igP	56 211	16 254	–71%
3ibwE7	28 686	16 194	–44%
1Gqy29YrQ	49 264	16 124	–67%
53lnx47TG56	48 091	16 030	–67%
6wCV7j	86 025	15 925	–81%
7zge22	34 589	14 730	–57%
bbimguDG4u	17 266	14 680	–15%
3jHy4bc1tM46	15 066	14 666	–3%
qcd0e	31 239	14 654	–53%
JE3RB8y	53 878	14 640	–73%

Password	Previous	Last	Growth
e7e2wM	40 970	14 616	–64%
PE5365JXPoU	60 404	14 613	–76%
ar9s2P	18 447	14 603	–21%
59619xcN2U	31 082	14 592	–53%
mnwYx01s4H	31 389	14 547	–54%
xVND7hD0	15 096	14 529	–4%
1cQ21276K4S0	31 273	14 511	–54%
4vD0Gb1gV5ab8S	16 480	14 485	–12%
7D81a	15 139	14 477	–4%
FSW1F1T1	30 976	14 474	–53%
2pG477	25 647	14 474	–44%
12v1G	23 991	14 471	–40%
u7IsDm5	5 808	14 464	149%
eCk5l08	6 069	14 453	138%
SFvIN0Ey	14 973	14 448	–4%
1fckl65	11 640	14 439	24%
1u0Yo20RVP	31 381	14 435	–54%
5J2HKQz9A	10 077	14 433	43%
ebeU41nR	42 690	14 432	–66%
dC82T7oU5	15 051	14 431	–4%
WA64ee4UOj01	15 085	14 427	–4%
J1febuhH	27 528	14 427	–48%
UK5AjD36l	4 965	14 427	191%
aPryL9	32 220	14 425	–55%
tqZBam77XT	14 818	14 423	–3%
3ZOx0fFmt3	16 188	14 423	–11%
8WDkX03	11 120	14 423	30%
H6j7B9B	66 610	14 422	–78%
6Uv99r	43 731	14 418	–67%
8i04t11i	31 143	14 417	–54%
3qK6207	32 498	14 417	–56%

Most Used Passwords Wordcloud