TURRIS

Sentinel Report - December 2022

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 December, we saw attacks rise globally. It could be related to the holiday season when hobbyists joined the usual group. What seems odd is that attackers are testing more sophisticated passwords lately. We dug into our data deeper regarding passwords like *68ktW79z1U*. We suspected that it might be just one device that acted out or one attacker that got an unusual wordlist. However, the password had been recorded by multiple routers, and attacks came from multiple IP addresses. What is more, the IP addresses even span multiple countries and continents. So, it seems like a regular attack after all.
There is also a spike in the popularity of previously not so abused ports, like 11000, used by old Cisco devices. This might suggest that attackers are trying to find outdated routers again.

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.

80 829

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.

10 049

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?

3 578

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.

21

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	66 736	2 223 610	3 232%	N/A
6881	UDP	4 960	1 792 704	36 043%	BitTorrent beginning of range of ports used most often
6889	UDP	109	563 995	517 327%	BitTorrent continuation of range of ports used most often
27032	UDP	9 407	460 724	4 798%	Steam (In-Home Streaming)
7881	UDP	6 063	375 993	6 101%	N/A
51413	TCP	2 260	341 961	15 031%	Certificate Management over CMS
445	TCP	33 184	299 253	802%	Microsoft-DS (Directory Services) Active Directory, | Microsoft-DS (Directory Services) SMB
11000	UDP	9	274 756	3 052 744%	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.
64541	UDP	9	177 591	1 973 133%	N/A
1024	UDP	60	168 501	280 735%	Reserved
6882	UDP	10	143 609	1 435 990%	BitTorrent beginning of range of ports used most often
1034	UDP	609	121 407	19 835%	N/A
23	TCP	11 379	121 033	964%	Telnet protocol—unencrypted text communications
62882	UDP	32 561	115 781	256%	N/A
60731	UDP	1	114 503	11 450 200%	Range from which Mosh – a remote-terminal application similar to SSH – typically assigns ports for ongoing sessions between Mosh servers and Mosh clients.
47514	UDP	0	111 833	N/A	N/A
6881	TCP	3 559	111 009	3 019%	BitTorrent beginning of range of ports used most often
57017	UDP	0	109 031	N/A	N/A

Port	Protocol	Previous	Last	Growth	Description
43076	UDP	16	100 883	630 419%	N/A
27032	TCP	3 569	98 051	2 647%	N/A
443	TCP	16 194	97 418	502%	Hypertext Transfer Protocol Secure (HTTPS)HTTP/3 uses QUIC,
1	UDP	599	95 321	15 813%	TCP Port Service Multiplexer (TCPMUX). Historic. Both TCP and UDP have been assigned to TCPMUX by IANA,
8080	TCP	10 653	91 226	756%	Alternative port for HTTP. See also ports 80 and 8008. | Apache Tomcat | Atlassian JIRA applications
51000	UDP	116	90 661	78 056%	N/A
2457	UDP	0	82 223	N/A	N/A
5555	TCP	8 278	78 914	853%	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
55555	UDP	25 946	73 616	184%	N/A
46129	UDP	18	72 055	400 206%	N/A
6891	UDP	0	67 982	N/A	BitTorrent continuation of range of ports used most often | Windows Live Messenger (File transfer)
64541	TCP	24	64 002	266 575%	Certificate Management over CMS
53	UDP	1 402	62 783	4 378%	Domain Name System (DNS)
24588	UDP	6	59 759	995 883%	N/A
51718	UDP	2	59 325	2 966 150%	N/A
1026	UDP	93	58 324	62 614%	N/A
1433	TCP	11 034	56 018	408%	Microsoft SQL Server database management system (MSSQL) server
56736	UDP	1	52 416	5 241 500%	N/A
62734	UDP	0	51 862	N/A	N/A
32016	UDP	6	48 855	814 150%	N/A
1892	UDP	0	45 405	N/A	N/A

Port	Protocol	Previous	Last	Growth	Description
12701	UDP	11	45 315	411 855%	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.
51081	UDP	1	42 896	4 289 500%	N/A
6883	UDP	2	42 365	2 118 150%	BitTorrent beginning of range of ports used most often
30303	UDP	85	42 199	49 546%	N/A
49001	UDP	17	40 849	240 188%	N/A
10999	UDP	2	40 087	2 004 250%	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.
4444	UDP	65	37 823	58 089%	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
9006	UDP	0	36 968	N/A	Tomcat in standalone mode
26884	UDP	4	36 887	922 075%	N/A
16881	UDP	143	36 753	25 601%	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.
2323	TCP	10 760	35 575	231%	N/A
80	TCP	2 596	35 392	1 263%	Hypertext Transfer Protocol (HTTP)HTTP/3 uses QUIC,
81	TCP	5 439	35 285	549%	TorPark onion routing
37126	UDP	0	34 453	N/A	N/A
54728	TCP	66	33 449	50 580%	Certificate Management over CMS
9091	UDP	52	33 057	63 471%	Openfire Administration Console (SSL Secured) | Transmission (BitTorrent client) Web Interface
1	TCP	460	32 698	7 008%	TCP Port Service Multiplexer (TCPMUX). Historic. Both TCP and UDP have been assigned to TCPMUX by IANA,

Port	Protocol	Previous	Last	Growth	Description
54728	UDP	52	32 611	62 613%	N/A
6890	UDP	2	32 379	1 618 850%	BitTorrent continuation of range of ports used most often
51064	UDP	2	31 762	1 588 000%	N/A
22	TCP	3 295	31 133	845%	Secure Shell (SSH),file transfers (scp, sftp) and port forwarding
6901	UDP	0	30 953	N/A	Windows Live Messenger (Voice) | BitTorrent continuation of range of ports used most often
21742	UDP	6	30 426	507 000%	N/A
55087	UDP	5	29 111	582 120%	N/A
39841	UDP	3	28 953	965 000%	N/A
7680	TCP	360	28 584	7 840%	Delivery Optimization for Windows 10
13333	UDP	2	28 196	1 409 700%	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.
7254	UDP	0	28 080	N/A	N/A
31402	TCP	8	27 997	349 862%	N/A
21336	UDP	9 877	27 825	182%	N/A
9091	TCP	533	27 408	5 042%	Openfire Administration Console (SSL Secured) | Transmission (BitTorrent client) Web Interface
60023	TCP	623	27 308	4 283%	Certificate Management over CMS
6886	UDP	2	27 117	1 355 750%	BitTorrent beginning of range of ports used most often
33621	UDP	4	26 821	670 425%	N/A
33801	UDP	0	26 577	N/A	N/A
59127	UDP	0	25 951	N/A	N/A
52200	UDP	4	25 740	643 400%	N/A
9000	UDP	15	25 388	169 153%	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

Port	Protocol	Previous	Last	Growth	Description
12814	UDP	4	24 917	622 825%	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.
44618	UDP	4	24 896	622 300%	N/A
20157	UDP	5	24 616	492 220%	N/A
38446	UDP	0	24 528	N/A	N/A
48426	UDP	0	24 514	N/A	N/A
29414	UDP	69	24 397	35 258%	N/A
49124	UDP	4	24 244	606 000%	N/A
8621	UDP	1	23 839	2 383 800%	N/A
10889	UDP	2	23 498	1 174 800%	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.
8668	UDP	2	23 223	1 161 050%	N/A
12570	UDP	1	23 112	2 311 100%	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.
18502	UDP	2	22 656	1 132 700%	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.
61578	UDP	2	22 462	1 123 000%	N/A
37215	TCP	4 034	22 410	456%	N/A
61345	UDP	1	22 235	2 223 400%	N/A
23231	TCP	14	22 235	158 721%	N/A
4001	TCP	355	21 888	6 066%	Microsoft Ants game | CoreOS etcd client communication
16881	TCP	191	21 569	11 193%	N/A
8444	TCP	423	21 392	4 957%	Bitmessage
6885	UDP	3	21 363	712 000%	BitTorrent beginning of range of ports used most often
48804	UDP	2	21 090	1 054 400%	N/A

Port	Protocol	Previous	Last	Growth	Description
14082	UDP	3	21 085	702 733%	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.
40277	UDP	0	21 084	N/A	N/A

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

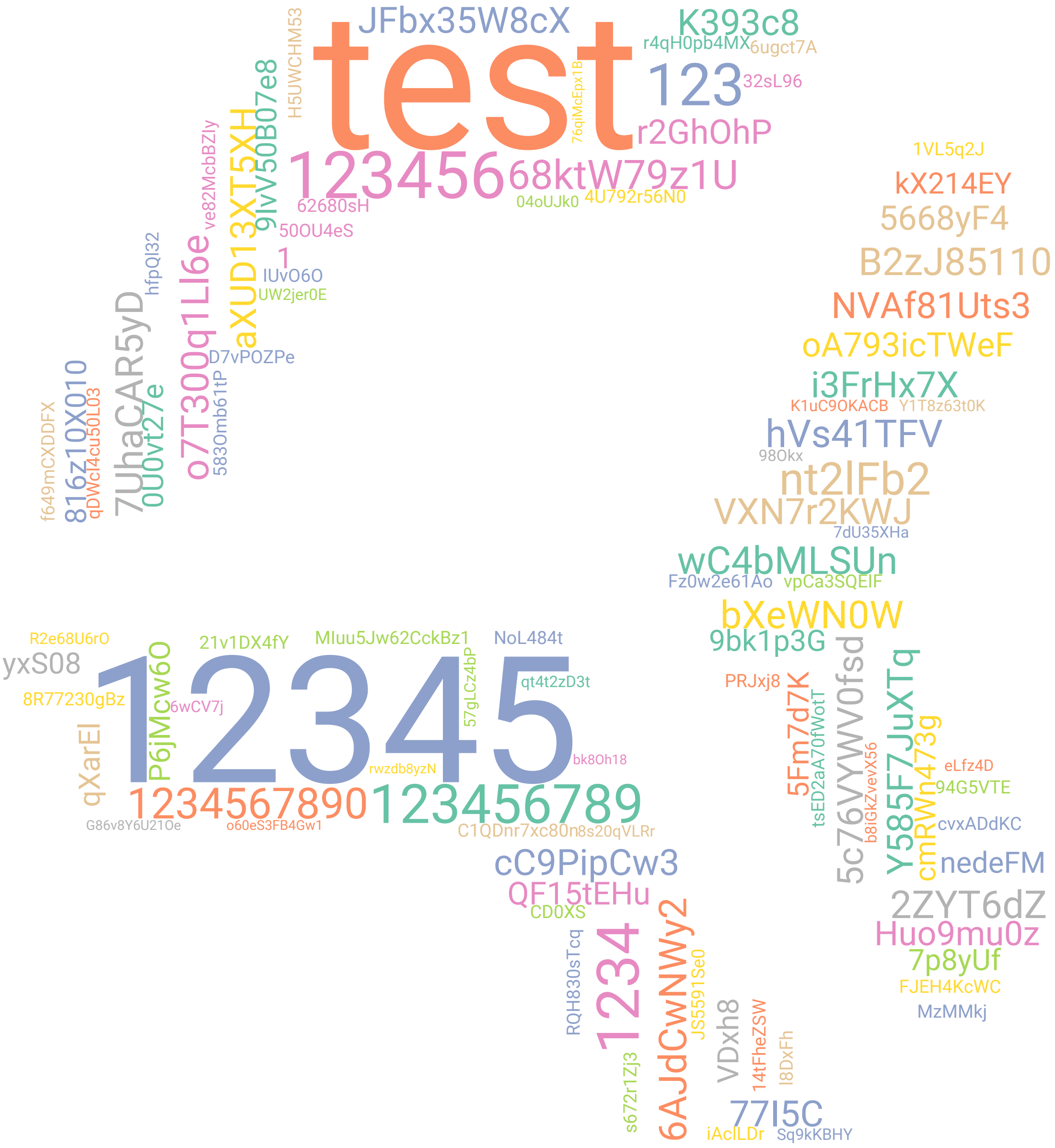
The diagram shows how many times we've seen individual passwords being used in attack attempts last month in comparison to the month before. The data are ordered by count last month, and the last column contains the difference against the previous month in percents for easier comparison. This allows 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
test	49 458	319 359	546%
12345	100 108	297 788	197%
123456	171 403	275 673	61%
1234	99 769	231 878	132%
123	158 211	227 748	44%
123456789	167 797	201 728	20%
nt2lFb2	0	158 106	N/A
1234567890	149 739	151 412	1%
68ktW79z1U	0	143 661	N/A
B2zJ85110	0	130 108	N/A
o7T300q1Ll6e	0	128 769	N/A
hVs41TFV	0	127 272	N/A
bXeWN0W	0	127 213	N/A
6AJdCwNWy2	0	126 727	N/A
2ZYT6dZ	0	126 495	N/A
wC4bMLSUn	0	123 798	N/A
7UhaCAR5yD	0	122 476	N/A
aXUD13XT5XH	0	115 303	N/A
5c76VYWV0fsd	0	112 660	N/A
i3FrHx7X	0	111 565	N/A
NVAf81Uts3	0	111 286	N/A
cC9PipCw3	0	109 293	N/A
JFbx35W8cX	0	106 319	N/A
Y585F7JuXTq	0	105 821	N/A
77I5C	0	104 109	N/A
K393c8	0	103 109	N/A
VXN7r2KWJ	0	102 732	N/A
oA793icTWeF	0	102 702	N/A
5668yF4	0	102 099	N/A
Huo9mu0z	0	100 245	N/A
r2GhOhP	0	100 182	N/A
QF15tEHu	0	93 380	N/A

Password	Previous Month	Last Month	Growth
1	140 965	89 466	–37%
cmRWn473g	0	88 963	N/A
VDxh8	0	88 363	N/A
yxS08	0	88 113	N/A
816z10X010	0	87 583	N/A
9bk1p3G	0	87 062	N/A
7p8yUf	0	85 433	N/A
9IvV50B07e8	0	85 409	N/A
nedeFM	0	84 467	N/A
qXarEl	0	84 197	N/A
kX214EY	0	83 312	N/A
P6jMcw6O	0	82 732	N/A
0U0vt27e	0	82 075	N/A
5Fm7d7K	0	81 928	N/A
vpCa3SQEIF	0	81 828	N/A
MIuu5Jw62CckBz1	563	81 611	14 396%
4U792r56N0	0	81 273	N/A
r4qH0pb4MX	0	81 136	N/A
FJEH4KcWC	0	81 048	N/A
RQH830sTcq	566	81 018	14 214%
JS5591Se0	0	81 012	N/A
94G5VTE	0	80 812	N/A
MzMMkj	0	80 419	N/A
iAclLDr	0	79 461	N/A
D7vPOZPe	0	79 141	N/A
1VL5q2J	0	79 016	N/A
8R77230gBz	0	77 348	N/A
14tFheZSW	0	76 620	N/A
32sL96	0	76 143	N/A
C1QDnr7xc80n	0	76 006	N/A
6ugct7A	0	75 832	N/A
50OU4eS	0	75 271	N/A
IUvO6O	31 308	74 905	139%
21v1DX4fY	558	74 684	13 284%
Fz0w2e61Ao	0	74 251	N/A
hfpQl32	0	74 089	N/A
cvxADdKC	0	74 005	N/A

Password	Previous Month	Last Month	Growth
l8DxFh	0	73 648	N/A
62680sH	0	73 530	N/A
H5UWCHM53	0	73 230	N/A
PRJxj8	0	73 230	N/A
583Omb61tP	0	73 070	N/A
qDWcI4cu50L03	14 821	72 915	392%
tsED2aA70fWotT	79	72 539	91 722%
f649mCXDDFX	0	71 832	N/A
ve82McbBZIy	558	71 719	12 753%
NoL484t	24 742	71 051	187%
s672r1Zj3	560	70 967	12 573%
CD0XS	0	70 852	N/A
K1uC9OKACB	0	70 638	N/A
6wCV7j	515	70 556	13 600%
eLfz4D	570	70 376	12 247%
qt4t2zD3t	0	69 946	N/A
7dU35XHa	7 417	69 943	843%
R2e68U6rO	558	69 900	12 427%
04oUJk0	540	69 558	12 781%
8s20qVLRr	6 035	69 353	1 049%
Sq9kKBHY	0	69 346	N/A
Y1T8z63t0K	20 976	69 337	231%
98Okx	21 446	69 264	223%
57gLCz4bP	568	69 209	12 085%
UW2jer0E	2 725	69 157	2 438%
b8iGkZvevX56	14 523	68 613	372%
o60eS3FB4Gw1	0	68 422	N/A
bk8Oh18	0	67 793	N/A
rwzdb8yzN	0	67 733	N/A
76qiMcEpx1B	9 310	67 679	627%
G86v8Y6U21Oe	8 811	67 636	668%

Most Used Passwords Wordcloud


test
12345
123456
1234567890
123456789
1234
123
JFbx35W8cX
K393c8
r4qH0pb4MX
6ugct7A
32sL96
r2GhOhP
68ktW79z1U
04oUJk0
4U792r56N0
62680sH
50OU4eS
1
IUvO6O
UW2jer0E
D7vPOZPe
H5UWCHM53
9lvV50B07e8
aXUD13XT5XH
ve82McbBZly
o7T300q1Ll6e
5830mb61tP
hfpQl32
7UhaCAR5yD
0U0vt27e
816z10X010
qDWcl4cu50L03
f649mCXDDFX
76qiMcEpx1B
1VL5q2J
kX214EY
5668yF4
B2zJ85110
NVAf81Uts3
oA793icTWeF
i3FrHx7X
K1uC9OKACB
Y1T8z63t0K
hVs41TFV
98Okx
nt2lFb2
VXN7r2KWJ
7dU35XHa
wC4bMLSUn
Fz0w2e61Ao
vpCa3SQElF
bXeWN0W
9bk1p3G
PRJxj8
5Fm7d7K
tsED2aA70fWotT
5c76VYWV0fsd
b8iGkZvevX56
Y585F7JuXTq
cmRWn473g
eLfz4D
94G5VTE
cvxADdKC
nedeFM
2ZYT6dZ
Huo9mu0z
7p8yUf
FJEH4KcWC
MzMMkj
R2e68U6rO
yxS08
8R77230gBz
qXarEl
P6jMcw6O
6wCV7j
21v1DX4fY
Mluu5Jw62CckBz1
NoL484t
57gLCz4bP
qt4t2zD3t
bk8Oh18
rwzdb8yzN
G86v8Y6U21Oe
o60eS3FB4Gw1
C1QDnr7xc80n8s20qVLRr
cC9PipCw3
QF15tEHu
CD0XS
RQH830sTcq
s672r1Zj3
6AJdCwNWy2
JS5591Se0
VDxh8
14tFheZSW
l8DxFh
77I5C
iAclLDr
Sq9kKBHY