Sentinel Report - 2023 April

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

Moving to April, we gained almost ten thousand more unique attackers on average, according to the Greylist. To provide even more context to the events, we added yet another interesting figure — the number of total incidents recorded.
But we haven't stopped at that yet. As you can see, we added pie charts for minipot sources, actions, and their combinations. The majority of attackers target SMTP servers. Both connect and login actions for SMTP are so frequent that they almost overshadow other data. We might try to address that somehow in future reports. Similarly it is hard to see the bottom of the chart in Sentinel View, so it is good to be able to get some idea about them here. While Telnet is far behind SMTP, it is still the second-most targeted service. As we said before, the protocol is either used by some old devices or devices that don't prioritize security — those are definitely the most desirable target. With the move from the FTP protocol to various more secure options and CMSes, we can say that *HTTP* seems more interesting for attackers these days. The conclusion would be that you should never ever use *Telnet* and secure your *HTTP* with most attention to security.
In regards to port descriptions, we started enriching the information from Wikipedia with other sources. However, with the port number *37183* that had jumped up by more than 300 000%, we still have no idea what service is using this port. The port is from class of *dynamic/private range*, which means that it can be used with virtually any application.
On the top, we see a drop by 28% for port *27032* from last month. This one is used with Steam applications. Apart from that we see a decrease in BitTorrent related ports (maybe people were torrenting less last month) and slight decrease in attacks on Windows Shares. But don't get sloppy and keep your shares out of the Internet.
In passwords, the usual Iranian network is gone at last. We had high hopes for this month's password list. But we run into someone trying random passwords. You can see it in the password lists. This time, it is just one very active attacker trying passwords starting at April 1st through April 3rd and every one of them approximately 14 thousand times. This IP belonged to a hosting provider. That might explain why the attack stopped quite shortly after it started. Someone on the provider side responded to the abuse report. Nevertheless we get a different noise this time. We might also rethink in the future how do we chart the top passwords to get more relevant data.

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.

86 125

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.

11 220

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?

3 230

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.

17

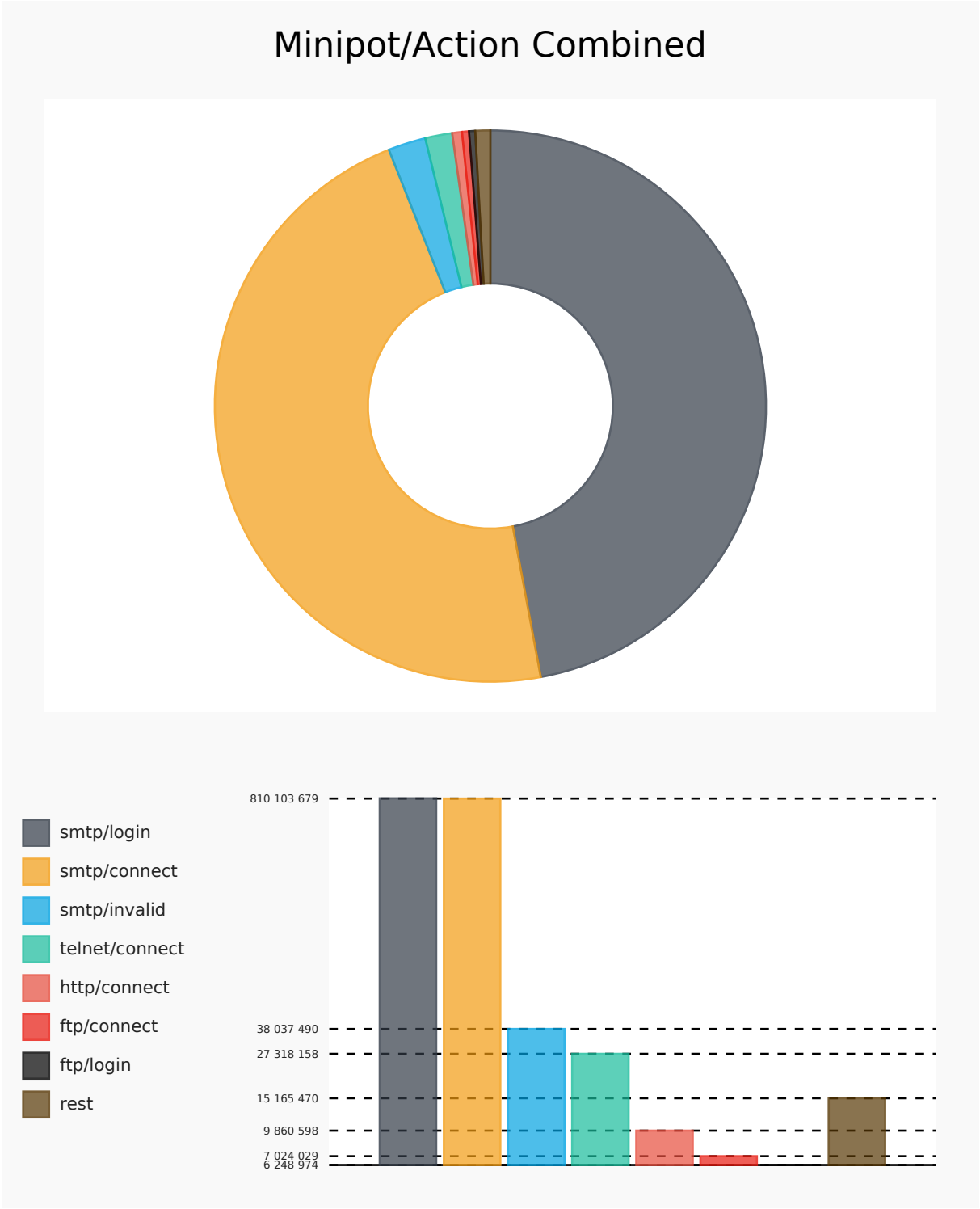
Total Minipot Incidents

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.

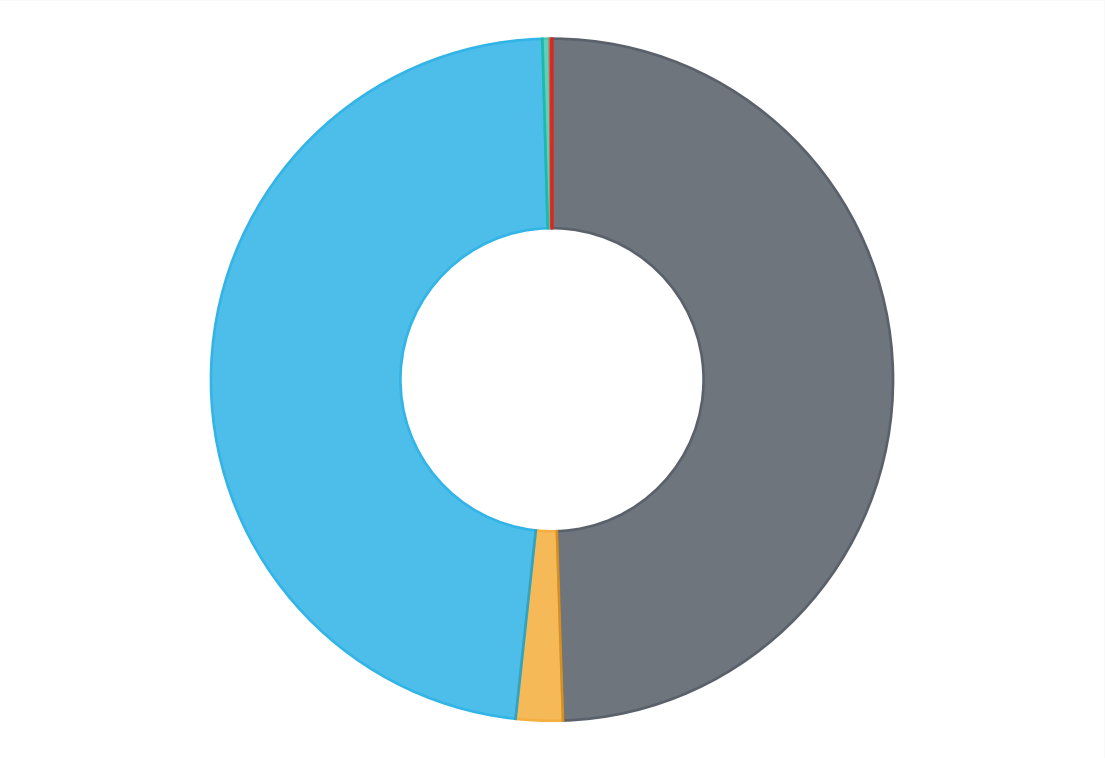
1 726 393 551

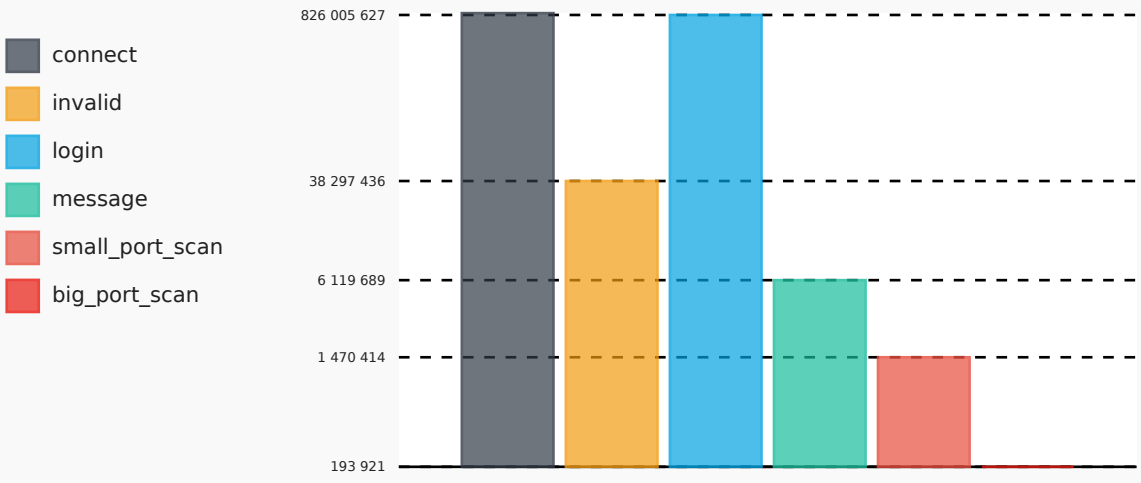
Incident Graphs

Below pie charts visualize the ratio how actions, minipots or their combinations had been distributed across the pool. While the ratio for pie charts is linear bar chart displays values using logarithmic scale.

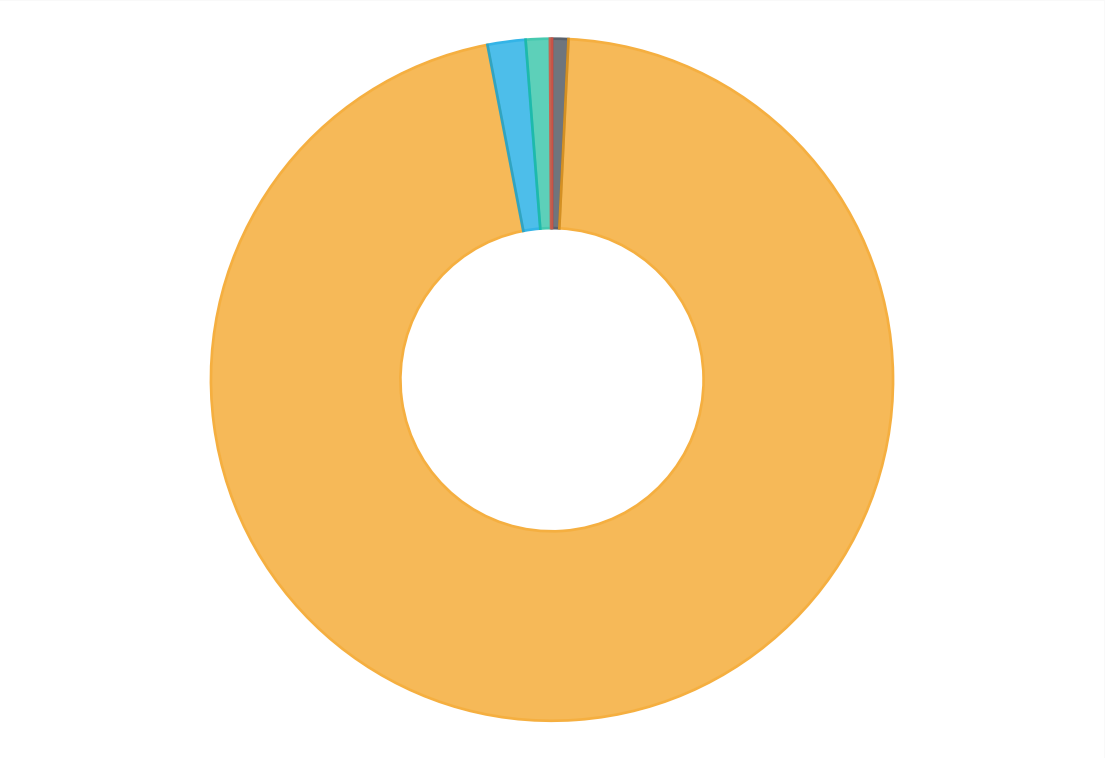


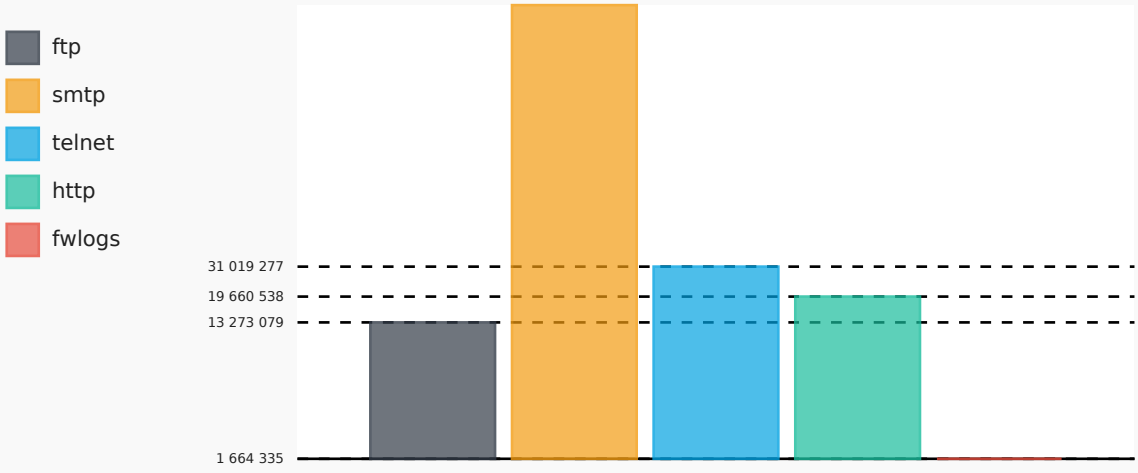
Attacker Action Pie Chart





Minipot Target Pie Chart





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	3 698 196	4 054 248	10%	Transmission bit-torrent client
6881	UDP	3 017 196	2 701 332	–10%	BitTorrent beginning of range of ports used most often
6889	UDP	884 792	669 660	–24%	BitTorrent continuation of range of ports used most often
27032	UDP	909 647	655 507	–28%	Steam (In-Home Streaming) | Steam Client (Remote Play)
445	TCP	463 654	438 903	–5%	Microsoft-DS (Directory Services) Active Directory, | Microsoft-DS (Directory Services) SMB
51413	TCP	479 358	437 293	–9%	Certificate Management over CMS | Transmission bit-torrent client
64541	UDP	66 149	435 281	558%	N/A
1024	UDP	151 726	400 903	164%	Reserved
37183	UDP	112	340 067	303 531%	N/A
6881	TCP	291 653	309 451	6%	BitTorrent beginning of range of ports used most often
1	UDP	242 577	253 284	4%	TCP Port Service Multiplexer (TCPMUX). Historic. Both TCP and UDP have been assigned to TCPMUX by IANA,
55859	UDP	74 945	252 596	237%	N/A
21130	UDP	94	231 452	246 126%	N/A
51000	UDP	154 435	225 802	46%	N/A
23	TCP	210 994	222 885	6%	Telnet protocol—unencrypted text communications
48804	UDP	275 863	211 348	–23%	N/A
27032	TCP	296 829	204 410	–31%	N/A
443	TCP	115 513	187 154	62%	Hypertext Transfer Protocol Secure (HTTPS)HTTP/3 uses QUIC,
35789	UDP	123	175 644	142 700%	N/A
44353	UDP	111	172 345	155 166%	N/A

Port	Protocol	Previous	Last	Growth	Description
16881	UDP	144 625	160 724	11%	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
59492	UDP	176 487	159 190	–10%	N/A
64592	UDP	5 374	156 471	2 812%	N/A
65206	UDP	138 277	152 664	10%	Dynamic and/or private ports
8080	TCP	146 223	148 387	1%	Alternative port for HTTP. See also ports 80 and 8008. | Apache Tomcat | Atlassian JIRA applications
55555	UDP	115 141	140 310	22%	N/A
64541	TCP	27 427	126 665	362%	Certificate Management over CMS
35789	TCP	319	124 020	38 778%	N/A
44353	TCP	339	122 768	36 115%	N/A
49001	UDP	151 842	118 961	–22%	Far Cry | Nuance Unity Service Discovery Protocol
27250	UDP	52	116 096	223 162%	N/A
24902	UDP	61	109 579	179 538%	N/A
1	TCP	104 059	104 843	1%	TCP Port Service Multiplexer (TCPMUX). Historic. Both TCP and UDP have been assigned to TCPMUX by IANA,
45280	UDP	470 064	103 526	–78%	N/A
39841	UDP	74 307	98 354	32%	N/A
7881	UDP	199 297	98 261	–51%	Quick Time Streaming Server (formerly)
34291	UDP	17 395	97 618	461%	N/A
30303	UDP	76 884	96 808	26%	Ethereum Client
43451	UDP	19 796	95 459	382%	N/A
6882	UDP	118 796	95 440	–20%	BitTorrent beginning of range of ports used most often
39199	UDP	106	94 694	89 234%	N/A
2457	UDP	41	93 567	228 112%	N/A
16881	TCP	119 269	92 913	–22%	Synology NAS DSM download service
1433	TCP	89 716	91 875	2%	Microsoft SQL Server database management system (MSSQL) server
9006	UDP	65 368	89 082	36%	IANA Reserved port
56331	TCP	672	88 341	13 046%	Certificate Management over CMS

Port	Protocol	Previous	Last	Growth	Description
2323	TCP	59 414	86 585	46%	N/A
60466	UDP	257	85 491	33 165%	Range from which Mosh – a remote-terminal application similar to SSH – typically assigns ports for ongoing sessions between Mosh servers and Mosh clients.
54728	UDP	81 267	80 235	–1%	N/A
37215	TCP	89 504	78 936	–12%	Huawei HG532 routers
42000	UDP	40 238	76 549	90%	N/A
9000	UDP	60 827	76 473	26%	UDPCast
9173	UDP	70	74 158	105 840%	N/A
5740	UDP	23	73 904	321 222%	N/A
4444	UDP	83 258	73 363	–12%	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
5555	TCP	80 016	73 243	–8%	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
52806	UDP	182	72 885	39 947%	N/A
62427	UDP	2 452	71 990	2 836%	N/A
43451	TCP	12 921	70 687	447%	N/A
60023	TCP	82 401	68 310	–17%	Certificate Management over CMS
24832	UDP	64	67 943	106 061%	N/A
54728	TCP	65 139	67 761	4%	Certificate Management over CMS
49530	UDP	933	66 025	6 977%	N/A
32862	UDP	116 347	65 811	–43%	World of Tanks
39199	TCP	367	64 610	17 505%	N/A
31402	TCP	63 579	63 732	~0%	N/A
42000	TCP	29 068	63 247	118%	Brothers in Arms Online
22	TCP	64 179	62 737	–2%	Secure Shell (SSH),file transfers (scp, sftp) and port forwarding
56881	UDP	30 530	61 693	102%	N/A

Port	Protocol	Previous	Last	Growth	Description
37388	UDP	61 899	60 189	–3%	N/A
62882	UDP	68 789	59 676	–13%	N/A
80	TCP	64 294	57 953	–10%	Hypertext Transfer Protocol (HTTP)HTTP/3 uses QUIC,
9001	UDP	553	57 471	10 293%	ETL Service Manager | Microsoft SharePoint authoring environment | cisco-xremote router configuration | Tor network default
53	UDP	56 457	57 309	2%	Domain Name System (DNS)
49952	UDP	166	56 378	33 863%	N/A
7680	TCP	60 065	55 225	–8%	Delivery Optimization for Windows 10
62864	UDP	263	55 200	20 889%	N/A
1025	UDP	65 468	54 763	–16%	Teradata database management system (Teradata) server
51412	UDP	88 635	53 948	–39%	N/A
11516	UDP	64 463	53 051	–18%	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.
36080	UDP	50 652	52 580	4%	N/A
81	TCP	57 976	52 103	–10%	TorPark onion routing
30620	UDP	207	51 712	24 882%	N/A
52755	UDP	1 752	51 213	2 823%	N/A
61289	UDP	62 663	50 400	–20%	N/A
10889	UDP	41 755	49 322	18%	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.
6884	UDP	41 712	48 713	17%	BitTorrent beginning of range of ports used most often
6886	UDP	44 221	48 280	9%	BitTorrent beginning of range of ports used most often
6891	UDP	178 485	48 196	–73%	BitTorrent continuation of range of ports used most often | Windows Live Messenger (File transfer)
8444	TCP	48 882	46 771	–4%	Bitmessage
54368	UDP	385	44 874	11 556%	N/A
32729	UDP	72	43 958	60 953%	N/A

Port	Protocol	Previous	Last	Growth	Description
6885	UDP	52 553	42 515	–19%	BitTorrent beginning of range of ports used most often
12701	UDP	75 735	41 912	–45%	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.
50646	UDP	245	41 732	16 933%	N/A
16197	UDP	28 898	41 325	43%	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.
44064	UDP	111	40 747	36 609%	N/A
59598	UDP	1 058	40 610	3 738%	N/A
6883	UDP	45 740	40 531	–11%	BitTorrent beginning of range of ports used most often
8333	TCP	36 436	40 345	11%	Bitcoin | VMware VI Web Access via HTTPS

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
123456	108 000	155 712	44%
123	37 479	67 835	81%
12345	77 581	64 913	–16%
1234	89 012	62 688	–30%
12345678	88 254	62 255	–29%
password	149 732	60 842	–59%
123456789	60 010	43 603	–27%
1qaz@WSX	2 687	26 825	898%
AB■	24 542	25 283	3%
1qaz2wsx	21 975	18 454	–16%
P@ssword	2 460	16 259	561%
1234567	28 588	15 341	–46%
123123	17 212	14 870	–14%
abcd	304	14 446	4 652%
1qazXSW@	2 722	14 280	425%
c5z06m	0	14 111	N/A
14MY3bw	2 334	14 110	505%
PE19Ochw3R	2 363	14 082	496%
80ABu0CcYLW9	0	14 039	N/A
26Jn4qr7	0	14 039	N/A
LXDqrv1bpsfS	0	14 039	N/A
mCu0MW7Z	0	14 039	N/A
rUt2422BW9U	0	14 038	N/A
O42xc19	0	14 038	N/A
15L6ha35a	0	14 038	N/A
WVBzO63084	0	14 038	N/A
EX867p15L	0	14 038	N/A
F7YbAzJX	0	14 038	N/A
jSFddZ48fq9	0	14 038	N/A
r2efpK8	0	14 038	N/A
x5dfj	0	14 037	N/A
Vz304q66	0	14 037	N/A

Password	Previous	Last	Growth
T9csB05z052	0	14 037	N/A
Z2qG476ZKoX32BO	0	14 037	N/A
0XWVYa	0	14 037	N/A
8ZZMB	0	14 037	N/A
471hf	0	14 037	N/A
3Ulug1gbA	0	14 037	N/A
53WQNv4a1	0	14 037	N/A
2A3y0	0	14 037	N/A
X8l7t8V	0	14 036	N/A
y6s77P95a	0	14 036	N/A
7k5ek7n	0	14 036	N/A
cx6uhxu	0	14 036	N/A
QV63uh2y	0	14 036	N/A
8uWKT1aC	0	14 036	N/A
4aj0u52xKj8H4E	0	14 035	N/A
m5L95Oi03	0	14 035	N/A
89Rj1e	0	14 035	N/A
9SxIAN5B	0	14 035	N/A
A23hB12XKoFg	0	14 035	N/A
33J34sZ7	0	14 035	N/A
0sTU49	0	14 035	N/A
4NzTMr8	0	14 034	N/A
L0n99d	0	14 034	N/A
b2s54W8Wo	0	14 034	N/A
U1m1f2W	0	14 034	N/A
Q1p71	0	14 034	N/A
y4V1Elfdpt	0	14 034	N/A
7Pkf7LByqJa	0	14 034	N/A
JR48uS7bl	0	14 034	N/A
56x93K6	0	14 033	N/A
AjDnwpv	0	14 033	N/A
d0ApM5EW	0	14 033	N/A
F50hVTZ1Z	0	14 033	N/A
g65V781Xp1	0	14 033	N/A
s18Lke	0	14 033	N/A
1o29Rse3dL48EY	0	14 033	N/A
i85rtPH	8 571	14 032	64%

Password	Previous	Last	Growth
P9FBDrR7	0	14 032	N/A
u879271aK	0	14 032	N/A
8t7197WW	0	14 032	N/A
W4WhGT9A	0	14 032	N/A
ce02N4703	0	14 031	N/A
2ulwx2	0	14 031	N/A
8r59qsW	0	14 031	N/A
fTpziEe	0	14 031	N/A
K4pD4H	0	14 031	N/A
Kh3wTI	0	14 031	N/A
L9R37Xkde	0	14 031	N/A
m88jRH	0	14 031	N/A
pQtRXE	0	14 031	N/A
SR1b6pbL907S	0	14 031	N/A
71VZKLOXA	0	14 030	N/A
6QA2tt13g	0	14 030	N/A
x319AS6yPq	2 553	14 030	450%
f45Wq67zp4Md	0	14 030	N/A
545GK	16 947	14 030	–17%
50xFF5c3	0	14 030	N/A
4j8SE4zzt	0	14 030	N/A
nXA8608I	0	14 030	N/A
5SOw5Mg13684	0	14 029	N/A
nXP8y7c	0	14 029	N/A
nV5eH	0	14 029	N/A
1a805bzB	0	14 029	N/A
tVpKO9	0	14 029	N/A
tXiE8BkMEh	0	14 029	N/A
Er1QzK1nq	1 080	14 029	1 199%
alq7XJ3QK630	0	14 029	N/A
7u79XEF7ML6R	14 371	14 029	–2%

TURRIS

Most Used Passwords Wordcloud