Sentinel Report - 2023 June

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

The total number incidents decreased by half. However, there are only slightly fewer than 10,000 distinct attackers on the greylist. The last month's seemingly minor reduction may have been indicative of an ongoing decline.
We updated the report with two new tables that highlight specific violent IP addresses. Since an IP address could also be a proxy server or VPN gateway, NAT or even hacked server, we refrain from using the word "attackers" explicitly.
Although "Changeme123" wasn't a particularly popular password this month, the leetspeak variants of "password" have over dozen variants. Leetspeak used to be a phenomenon to feel exclusive on online forums long time ago. Using it as a cryptography in 2023 will unquestionably not make someone's password much more secure. We have actually seen an online password generator that used leetspeak as a cheap way to add entropy to your passwords. In general, it's not a great idea to use online password generators. The password could be generated by a backend on the server, thus the server will know the password you are about to use and in the past, it could be also sent over the Internet unencrypted. It is much better to use a password generator embedded into your password manager. And if you don't have a password manager, we strongly recommend you to get one.

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

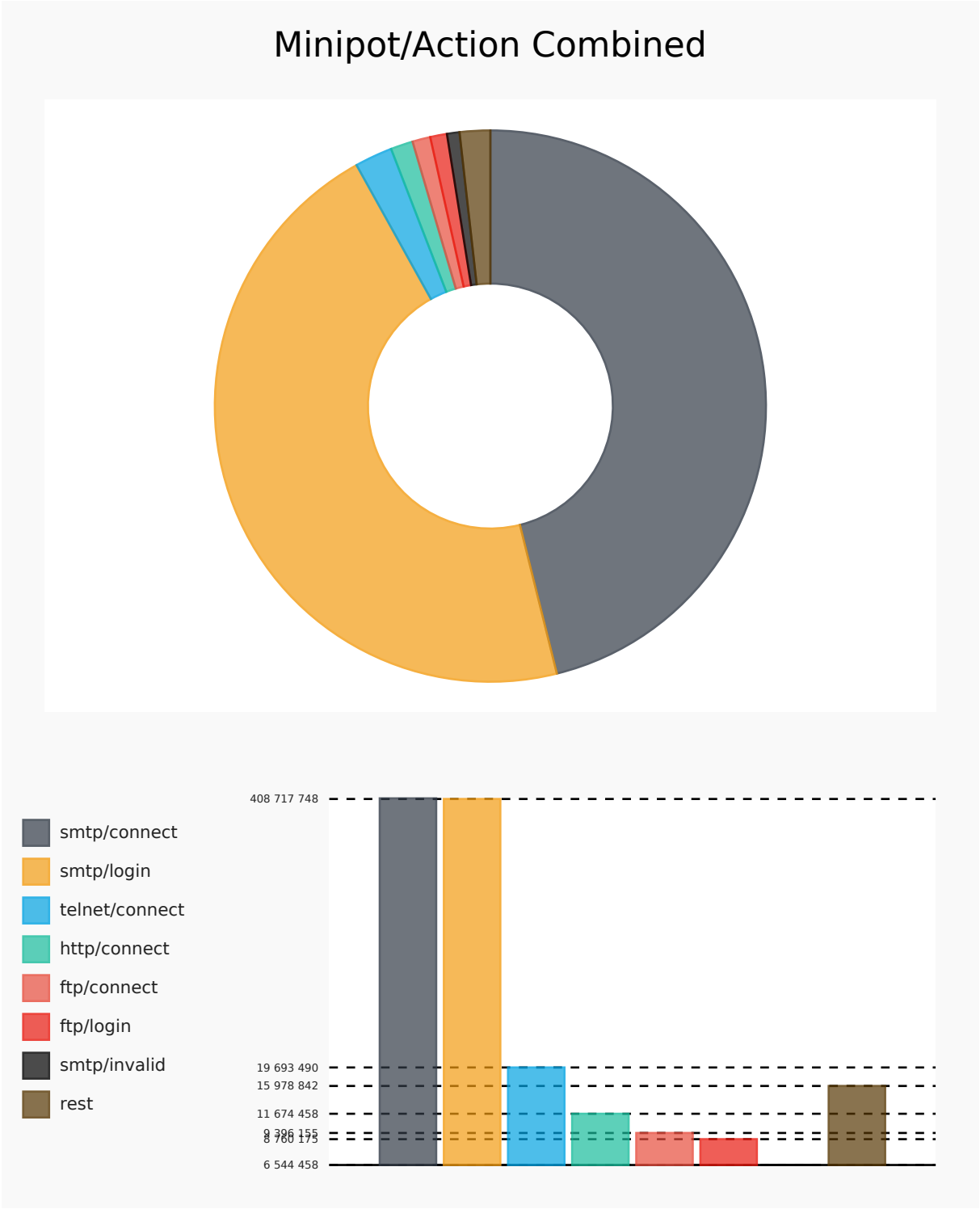
Total Minipot Incidents

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.

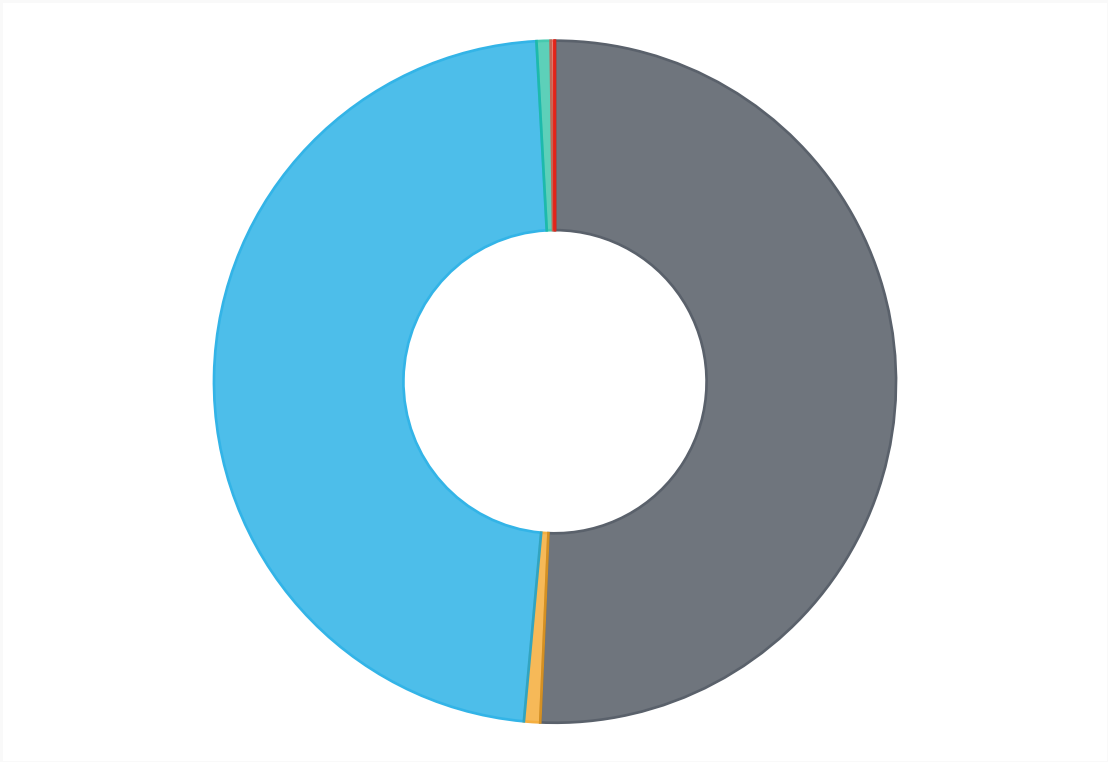
892 321 602

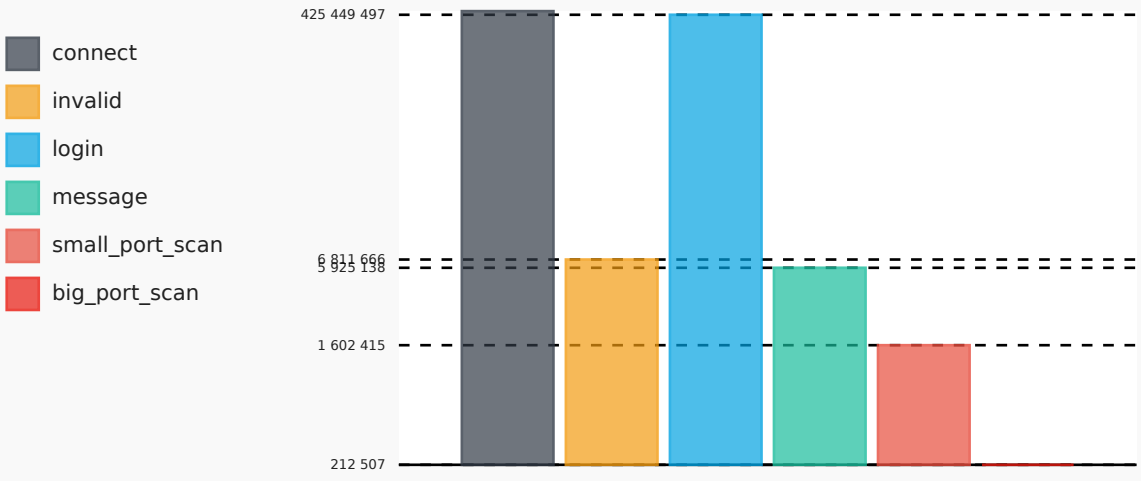
Incident Graphs

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.

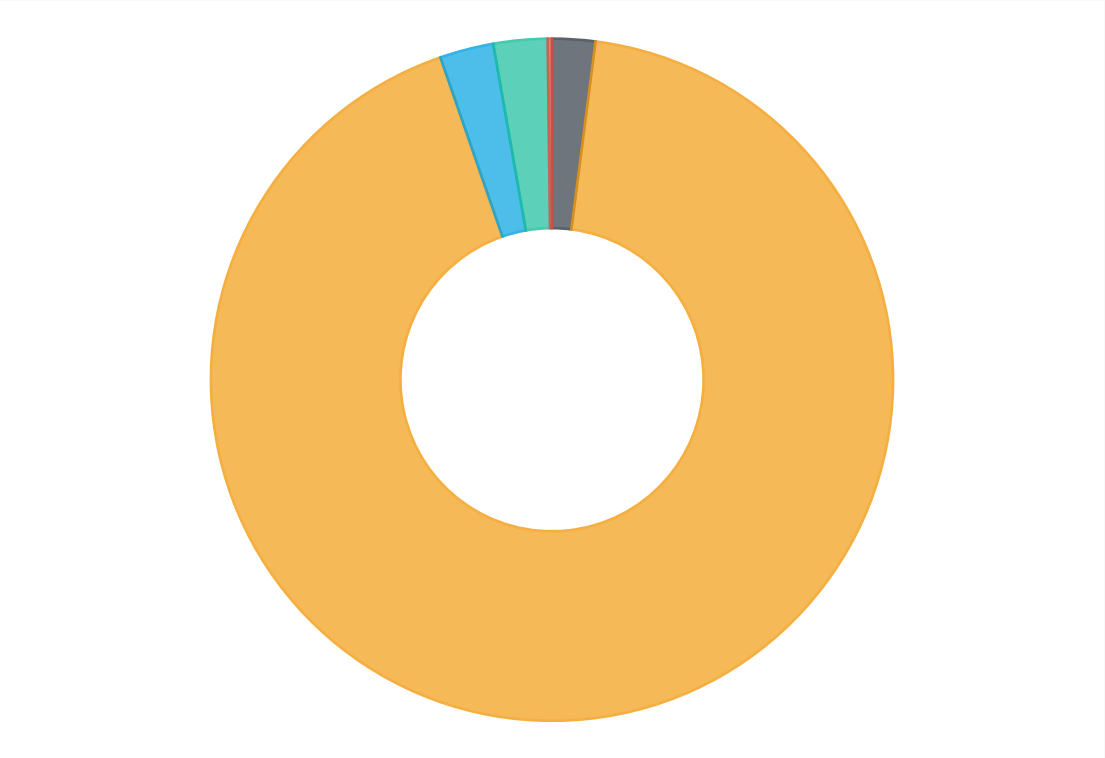


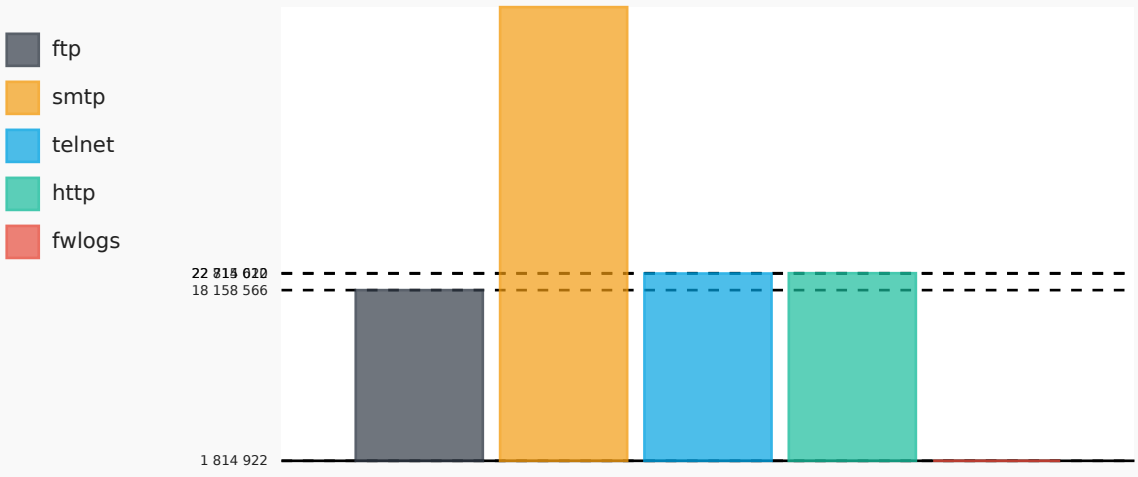
Attacker Action Pie Chart





Trap Pie Chart





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	

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	4 459 096	4 068 048	–9%	Transmission bit-torrent client
6881	UDP	3 908 727	3 763 238	–4%	BitTorrent beginning of range of ports used most often
51413	TCP	589 785	575 512	–2%	Certificate Management over CMS | Transmission bit-torrent client
27032	UDP	398 380	548 245	38%	Steam (In-Home Streaming) | Steam Client (Remote Play)
6889	UDP	606 582	544 540	–10%	BitTorrent continuation of range of ports used most often
445	TCP	455 402	427 852	–6%	Microsoft-DS (Directory Services) Active Directory, | Microsoft-DS (Directory Services) SMB
7929	UDP	986	408 445	41 324%	QuickTime Streaming Server
6881	TCP	435 820	305 842	–30%	BitTorrent beginning of range of ports used most often
39827	UDP	95	279 044	293 631%	Unassigned (IANA)
16881	UDP	190 517	274 039	44%	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
23	TCP	245 253	258 139	5%	Telnet protocol—unencrypted text communications
21742	UDP	99 879	236 013	136%	Unassigned (IANA)
7881	UDP	177 859	226 656	27%	Quick Time Streaming Server (formerly)
39827	TCP	349	221 020	63 230%	Unassigned (IANA)
48804	UDP	234 268	199 040	–15%	Unassigned (IANA)
50456	UDP	149	195 954	131 413%	Unassigned (IANA)
51000	UDP	250 946	194 892	–22%	Unassigned (IANA)
1024	UDP	188 105	179 036	–5%	Reserved
1	UDP	171 638	175 746	2%	TCP Port Service Multiplexer (TCPMUX). Historic. Both TCP and UDP have been assigned to TCPMUX by IANA,

Port	Protocol	Previous	Last	Growth	Description
52998	UDP	3 032	175 687	5 694%	Unassigned (IANA)
16881	TCP	133 465	160 054	20%	Synology NAS DSM download service
24902	UDP	187 454	155 746	–17%	Unassigned (IANA)
55630	UDP	135	151 838	112 373%	Unassigned (IANA)
54728	UDP	117 889	148 503	26%	Unassigned (IANA)
65206	UDP	176 678	146 504	–17%	Dynamic and/or private ports
8080	TCP	137 770	141 432	3%	Alternative port for HTTP. See also ports 80 and 8008. | Apache Tomcat | Atlassian JIRA applications
54728	TCP	110 257	137 994	25%	Certificate Management over CMS
59492	UDP	153 076	136 005	–11%	Unassigned (IANA)
1034	UDP	171	131 255	76 657%	Unassigned (IANA)
443	TCP	120 823	128 939	7%	Hypertext Transfer Protocol Secure (HTTPS)HTTP/3 uses QUIC,
52869	TCP	39 375	126 243	221%	Certificate Management over CMS
27032	TCP	103 443	124 641	20%	Unassigned (IANA)
58679	UDP	164	124 600	75 876%	Unassigned (IANA)
64541	UDP	131	115 947	88 409%	Unassigned (IANA)
47143	UDP	155 053	111 891	–28%	Unassigned (IANA)
21130	UDP	208 146	105 579	–49%	Unassigned (IANA)
1025	UDP	129 886	103 973	–20%	Teradata database management system (Teradata) server
30303	UDP	75 666	100 242	32%	Ethereum Client
41054	TCP	983	97 242	9 792%	Brothers in Arms Online
44170	UDP	132	94 663	71 614%	Unassigned (IANA)
47627	UDP	261 097	93 762	–64%	Unassigned (IANA)
55859	UDP	205 870	93 175	–55%	Unassigned (IANA)
15000	UDP	36 380	92 403	154%	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. | Teltonika networks remote management system (RMS)
2323	TCP	82 928	90 115	9%	Unassigned (IANA)
0	other	7 363	86 269	1 072%	Unassigned (IANA)
1433	TCP	90 662	85 379	–6%	Microsoft SQL Server database management system (MSSQL) server
4000	UDP	51 905	85 170	64%	Diablo II game

Port	Protocol	Previous	Last	Growth	Description
64134	UDP	119 372	83 505	–30%	Unassigned (IANA)
34188	UDP	428	79 554	18 487%	Unassigned (IANA)
23446	UDP	58 563	79 377	36%	Unassigned (IANA)
18979	UDP	83	77 156	92 859%	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.
62319	UDP	462 575	77 149	–83%	Unassigned (IANA)
56881	UDP	21 390	76 878	259%	Unassigned (IANA)
12000	UDP	17 175	73 953	331%	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. | CubeForm, Multiplayer SandBox Game
1	TCP	76 589	73 679	–4%	TCP Port Service Multiplexer (TCPMUX). Historic. Both TCP and UDP have been assigned to TCPMUX by IANA,
31854	UDP	28	73 300	261 686%	Unassigned (IANA)
80	TCP	58 314	72 496	24%	Hypertext Transfer Protocol (HTTP)HTTP/3 uses QUIC,
5740	UDP	71 208	72 076	1%	Unassigned (IANA)
52806	UDP	82 816	70 963	–14%	Unassigned (IANA)
49001	UDP	121 659	70 963	–42%	Far Cry | Nuance Unity Service Discovery Protocol
60023	TCP	69 625	67 450	–3%	Certificate Management over CMS
5345	UDP	71 879	67 106	–7%	League of Legends, a multiplayer online battle arena video game
53	UDP	59 913	66 536	11%	Domain Name System (DNS)
1030	UDP	16 574	65 400	295%	Unassigned (IANA)
2387	UDP	54 794	65 193	19%	Unassigned (IANA)
56575	UDP	5 905	64 543	993%	Unassigned (IANA)
6901	UDP	92 137	64 304	–30%	Windows Live Messenger (Voice) | BitTorrent continuation of range of ports used most often
37787	UDP	154	64 123	41 538%	Unassigned (IANA)
7680	TCP	46 736	63 701	36%	Delivery Optimization for Windows 10
33095	UDP	61 463	62 802	2%	Unassigned (IANA)
51412	UDP	63 058	62 678	–1%	Unassigned (IANA)

Port	Protocol	Previous	Last	Growth	Description
9000	UDP	73 438	62 181	–15%	UDPCast
50482	UDP	110	61 812	56 093%	Unassigned (IANA)
31402	TCP	66 038	60 998	–8%	Unassigned (IANA)
35928	UDP	107	60 866	56 784%	Unassigned (IANA)
6885	UDP	37 138	59 654	61%	BitTorrent beginning of range of ports used most often
42740	UDP	240	59 654	24 756%	Unassigned (IANA)
6886	UDP	41 030	56 549	38%	BitTorrent beginning of range of ports used most often
8621	UDP	32 125	55 290	72%	Unassigned (IANA)
6888	UDP	47 208	54 932	16%	MUSE | BitTorrent continuation of range of ports used most often
50188	UDP	154	53 325	34 527%	Unassigned (IANA)
37787	TCP	341	53 187	15 497%	Unassigned (IANA)
62783	TCP	437	52 817	11 986%	Certificate Management over CMS
34291	UDP	29 647	52 105	76%	Unassigned (IANA)
6882	UDP	68 723	50 690	–26%	BitTorrent beginning of range of ports used most often
1032	UDP	749	50 650	6 662%	Unassigned (IANA)
9006	UDP	93 094	50 203	–46%	IANA Reserved port
64541	TCP	474	49 683	10 382%	Certificate Management over CMS
30620	UDP	92 255	48 711	–47%	Unassigned (IANA)
22	TCP	60 301	48 457	–20%	Secure Shell (SSH),file transfers (scp, sftp) and port forwarding
8444	TCP	41 575	47 790	15%	Bitmessage | Chia
33095	TCP	46 576	47 103	1%	Unassigned (IANA)
6884	UDP	40 400	46 988	16%	BitTorrent beginning of range of ports used most often
4444	UDP	79 778	46 767	–41%	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
10579	UDP	67	45 951	68 484%	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.
62882	UDP	42 270	45 682	8%	Unassigned (IANA)
42000	UDP	30 763	45 424	48%	Unassigned (IANA)

Port	Protocol	Previous	Last	Growth	Description
63460	UDP	86	45 304	52 579%	Unassigned (IANA)
80	UDP	37 983	45 200	19%	Hypertext Transfer Protocol (HTTP)HTTP/3 uses QUIC,
4001	TCP	43 213	44 537	3%	Microsoft Ants game | CoreOS etcd client communication

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

TURRIS

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	39 735 552	34 862 687	–12%
123	10 890 644	16 310 242	50%
password	21 483 481	1 937 012	–91%
P@ssw0rd	4 791 407	1 679 543	–65%
P@$$w0rd123	1 689 455	1 254 242	–26%
1qaz@WSX	1 929 700	1 223 627	–37%
12345678	9 425 958	1 162 845	–88%
1234	49 324 496	1 104 375	–98%
admin	1 681 259	1 084 328	–36%
123qwe!@#	545 329	881 284	62%
admin@123	669 217	868 317	30%
P@ssword	711 824	846 519	19%
p@ssw0rd1	270 596	823 159	204%
P@$$w0rd	270 030	821 966	204%
root@123	267 240	809 609	203%
abc@123	416 402	807 888	94%
Admin123!@#	263 158	803 802	205%
abcd@123	268 083	802 975	200%
qwe123!@#	263 723	802 519	204%
Admin123456	2 715 781	801 504	–70%
root123!@#	261 665	800 824	206%
admin123#	263 166	800 039	204%
!QAZ1qaz	266 091	799 986	201%
abc123!	260 540	799 670	207%
huawei@123	256 549	797 881	211%
12345	29 022 015	747 189	–97%
123456789	48 252 306	695 520	–99%
Aa123456	1 663 091	599 051	–64%
qwerty	1 600 590	586 570	–63%
111111	1 232 327	504 521	–59%
abc123	4 806 072	492 304	–90%
123123	1 565 584	447 390	–71%

Password	Previous	Last	Growth
1qaz2wsx	1 110 332	445 619	–60%
1	1 682 727	442 902	–74%
1q2w3e4r	1 230 197	442 050	–64%
123qwe	1 102 466	434 285	–61%
1qaz!QAZ	15 187 676	428 768	–97%
654321	1 073 172	415 454	–61%
abc123456	1 091 037	402 983	–63%
	430 140	365 327	–15%
qwerty123	1 023 440	363 560	–64%
1q2w3e	1 020 016	352 802	–65%
qwertyuiop	1 016 253	347 931	–66%
Password1	849 649	334 797	–61%
root	716 651	333 583	–53%
pass123	1 019 508	333 576	–67%
asdfgh	1 010 226	326 950	–68%
p@ssw0rd	907 709	317 958	–65%
p@55w0rd	106 337	297 287	180%
user	754 186	287 874	–62%
1234567890	23 337 819	287 316	–99%
1234567	828 192	287 117	–65%
admin123	549 886	281 498	–49%
P@ssword1	467 864	263 955	–44%
Test@123	51 130	261 117	411%
Pa$$word	37 206	254 209	583%
p@ssw0rd!	102 663	252 843	146%
Passw0rd	157 357	246 652	57%
P@ssw0rd1234	255 725	245 812	–4%
P@ssw0rd1	34 878	244 229	600%
p@$$w0rd	36 065	244 033	577%
adminHW	249 472	242 852	–3%
test@123	47 168	239 136	407%
Admin1	52 595	229 907	337%
p@ssword123	28 400	229 725	709%
666666	213 208	226 499	6%
Admin2015	2 485 790	225 093	–91%
Admin2016	2 510 306	225 085	–91%
Admin2017	418 165	224 700	–46%

Password	Previous	Last	Growth
Admin123	373 755	222 664	–40%
Admin@123	162 272	222 289	37%
Admin12345	22 803	222 265	875%
password@123	25 911	222 195	758%
User1	42 497	221 065	420%
Pa$$w0rd	148 313	220 503	49%
4rfv$RFV	21 853	219 871	906%
!QAZ2was	21 864	219 848	906%
!qazxsw2@	22 579	219 839	874%
redhat@123	26 613	219 789	726%
!Q@W3e4r	31 203	219 759	604%
Admin!@#456	21 876	219 744	904%
1qaz#EDC5tgb	21 898	219 725	903%
1Qaz@WSX#edc	21 894	219 700	903%
P@ssw0rd123	31 874	219 646	589%
Test123	49 499	219 627	344%
!QAZxsw23edc	21 891	219 565	903%
P@ssw0rd12	25 450	219 395	762%
Password123	24 424	219 337	798%
qwer1234!@#$	21 991	219 181	897%
!@#$qwerASDF	21 944	219 162	899%
HuaWei@root	21 937	218 902	898%
1qaz2wsx$%^	21 924	218 841	898%
Pa$$s0rd12	22 292	218 807	882%
Pa$$s0rd	22 295	218 759	881%
Pa$$s0rd1234	22 283	218 716	882%
Pass@word	22 008	218 693	894%
pa$$word1	21 985	218 693	895%
P@ssw0rd!@	21 965	218 671	896%
Root@2015	21 893	218 668	899%
P@SSWORD123	22 042	218 663	892%

TURRIS

Most Used Passwords Wordcloud