Sentinel Report - 2023 July

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

Number of individual attackers had risen and minipot attacks doubled. Last month only three of the top attackers emerged from subnet 46.148.40.0/24, yet this month the majority of all attackers came from this Iraq subnet.
When looking on trending passwords for this month, one of those stands out — P@ssw0rd. It is a nice example of bad practice. It is not a random and seemingly secure password. There were some actual services that used it as a default. That is why we don't have the default and trouble you with choosing your own during initial setup. Using the default password is one of the easiest ways how to invite attackers in.

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.

93 145

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.

11 550

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?

3 899

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.

16

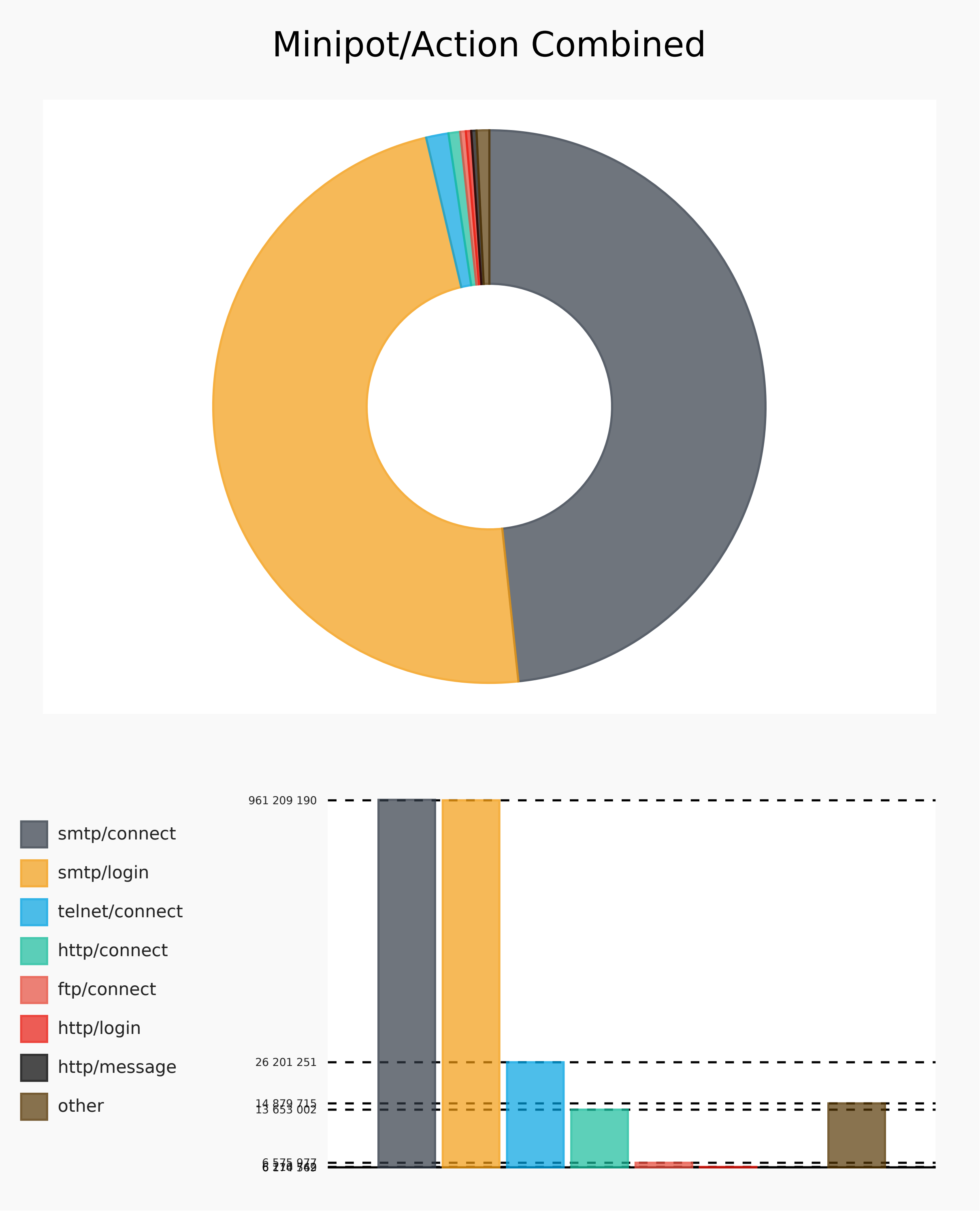
Total Minipot Incidents

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.

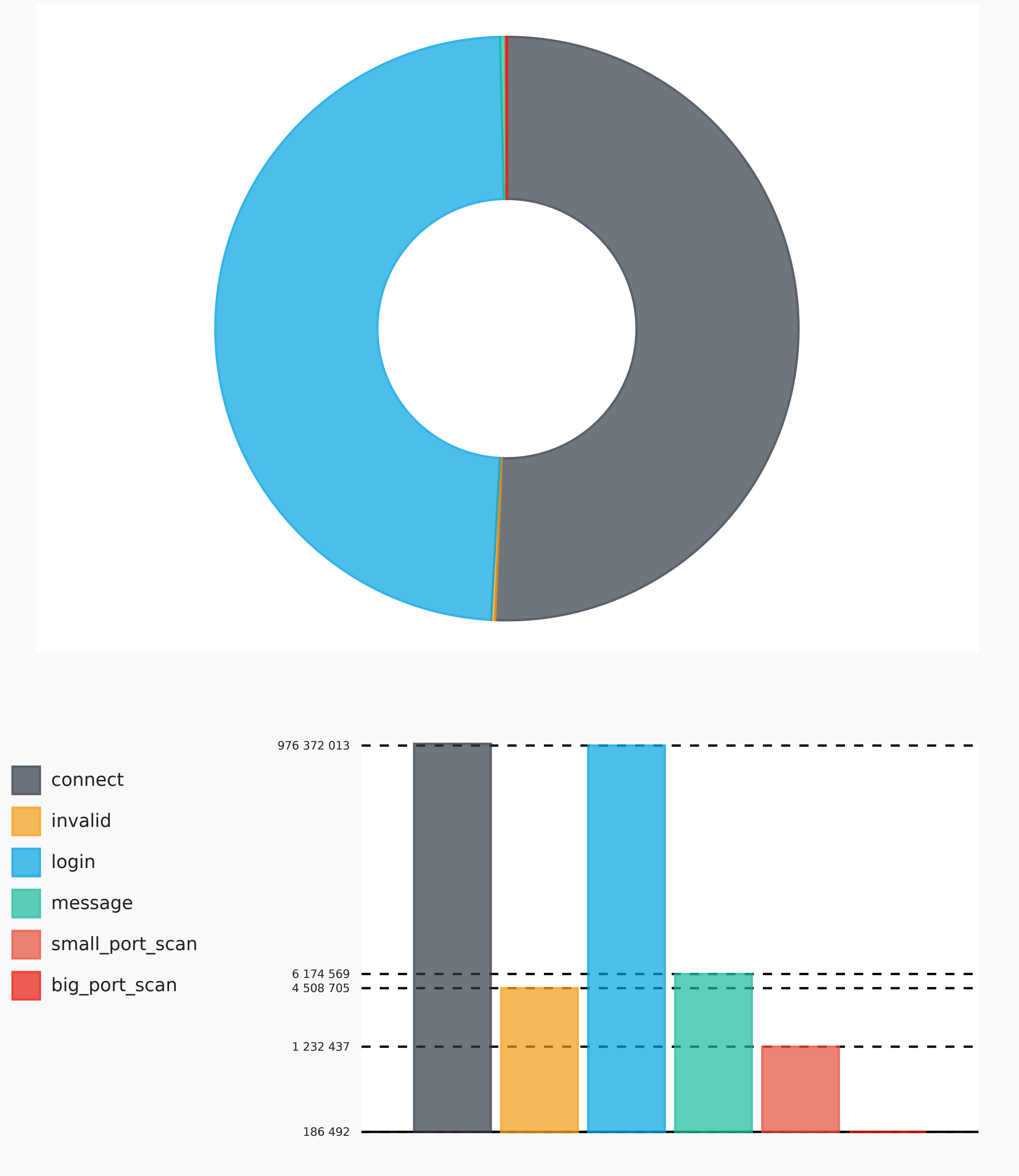
1 938 067 023

Incident Graphs

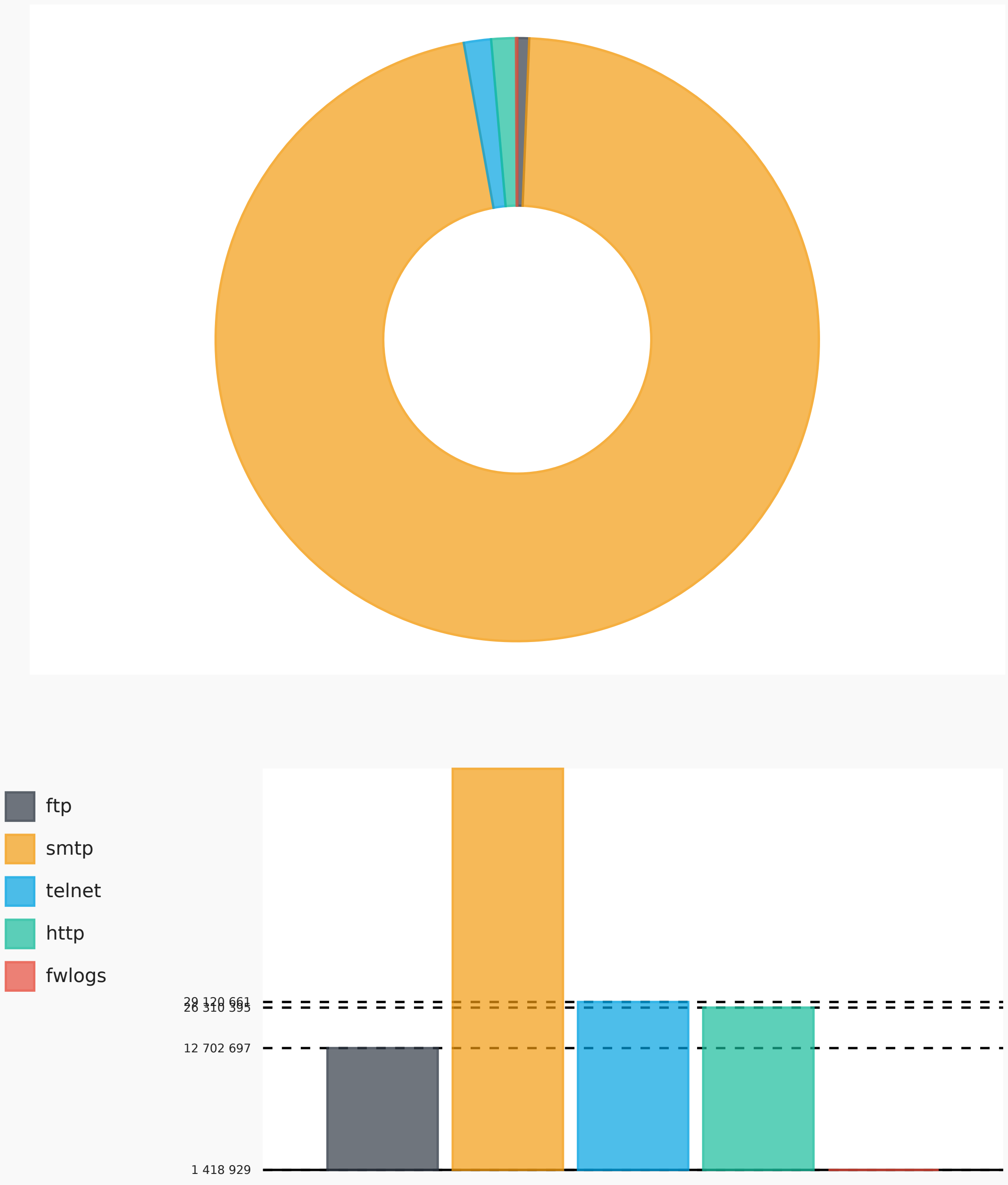
Below pie charts visualize the ratio how actions, minipots or their combinations had been distributed across the pool. While the ratio for pie charts is linear bar chart displays values using logarithmic scale.



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
377 442 330	minipot_smtp	80.94.95.184
2 073 737	minipot_http	200.74.242.40
751 773	minipot_telnet	31.7.60.114
732 735	minipot_ftp	62.217.187.51
10 321	fwlogs	198.12.85.86

Top Attackers

Regardless of the traps, these are the most 15 active attackers.

Count	IP	Country	Flag
377 442 330	80.94.95.184	RO	🇷🇴
340 829 337	45.129.14.31	RO	🇷🇴
165 875 267	46.148.40.44	IR	🇮🇷
154 562 810	46.148.40.40	IR	🇮🇷
141 120 559	77.90.185.18	DE	🇩🇪
136 089 792	46.148.40.45	IR	🇮🇷
86 792 932	46.148.40.41	IR	🇮🇷
80 101 633	46.148.40.43	IR	🇮🇷
76 342 851	46.148.40.42	IR	🇮🇷
36 026 085	46.148.40.61	IR	🇮🇷
33 739 870	46.148.40.63	IR	🇮🇷
32 695 175	46.148.40.156	IR	🇮🇷
31 328 556	46.148.40.154	IR	🇮🇷
31 005 630	46.148.40.155	IR	🇮🇷
30 370 306	46.148.40.64	IR	🇮🇷

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	4 068 048	4 809 613	18%	Transmission bit-torrent client
6881	UDP	3 763 238	2 487 195	–34%	BitTorrent beginning of range of ports used most often
11000	UDP	1 758	1 127 108	64 013%	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.
51413	TCP	575 512	566 754	–2%	Certificate Management over CMS | Transmission bit-torrent client
6889	UDP	544 540	547 261	~0%	BitTorrent continuation of range of ports used most often
27032	UDP	548 245	421 941	–23%	Steam (In-Home Streaming) | Steam Client (Remote Play)
445	TCP	427 852	416 389	–3%	Microsoft-DS (Directory Services) Active Directory, | Microsoft-DS (Directory Services) SMB
7881	UDP	226 656	396 370	75%	Quick Time Streaming Server (formerly)
23	TCP	258 139	319 982	24%	Telnet protocol—unencrypted text communications
16881	UDP	274 039	283 789	4%	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
6881	TCP	305 842	246 898	–19%	BitTorrent beginning of range of ports used most often
65206	UDP	146 504	211 507	44%	Dynamic and/or private ports
54586	UDP	21 787	197 796	808%	Unassigned (IANA)
44519	UDP	97	196 487	202 464%	Unassigned (IANA)
443	TCP	128 939	185 977	44%	Hypertext Transfer Protocol Secure (HTTPS)HTTP/3 uses QUIC,
1024	UDP	179 036	176 595	–1%	Reserved

Port	Protocol	Previous	Last	Growth	Description
16881	TCP	160 054	174 558	9%	Synology NAS DSM download service
54728	UDP	148 503	164 263	11%	Unassigned (IANA)
24902	UDP	155 746	162 100	4%	Unassigned (IANA)
8080	TCP	141 432	155 089	10%	Alternative port for HTTP. See also ports 80 and 8008. | Apache Tomcat | Atlassian JIRA applications
54728	TCP	137 994	152 757	11%	Certificate Management over CMS
47143	UDP	111 891	152 360	36%	Unassigned (IANA)
49001	UDP	70 963	151 953	114%	Far Cry | Nuance Unity Service Discovery Protocol
1	UDP	175 746	145 491	–17%	TCP Port Service Multiplexer (TCPMUX). Historic. Both TCP and UDP have been assigned to TCPMUX by IANA,
59492	UDP	136 005	145 437	7%	Unassigned (IANA)
51416	UDP	2 208	143 917	6 418%	Unassigned (IANA)
51000	UDP	194 892	141 589	–27%	Unassigned (IANA)
50160	UDP	184	136 817	74 257%	Unassigned (IANA)
44519	TCP	655	135 361	20 566%	Unassigned (IANA)
51834	UDP	18 778	133 676	612%	Unassigned (IANA)
21742	UDP	236 013	131 153	–44%	Unassigned (IANA)
8621	UDP	55 290	125 495	127%	Unassigned (IANA)
55859	UDP	93 175	124 233	33%	Unassigned (IANA)
42508	UDP	94	118 821	126 305%	Unassigned (IANA)
30303	UDP	100 242	106 513	6%	Ethereum Client
18979	UDP	77 156	104 376	35%	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	72 496	103 503	43%	Hypertext Transfer Protocol (HTTP)HTTP/3 uses QUIC,
50188	UDP	53 325	101 974	91%	Unassigned (IANA)
27032	TCP	124 641	94 329	–24%	Unassigned (IANA)
31849	UDP	192	93 882	48 797%	Unassigned (IANA)
2310	UDP	42	93 697	222 988%	Unassigned (IANA)
58736	UDP	4 658	93 487	1 907%	Unassigned (IANA)
54170	UDP	269	92 184	34 169%	Unassigned (IANA)
47943	UDP	79	89 201	112 813%	Unassigned (IANA)

Port	Protocol	Previous	Last	Growth	Description
1028	UDP	5 739	84 968	1 381%	IANA Reserved port
1433	TCP	85 379	84 553	–1%	Microsoft SQL Server database management system (MSSQL) server
6901	UDP	64 304	82 597	28%	Windows Live Messenger (Voice) | BitTorrent continuation of range of ports used most often
12000	UDP	73 953	81 776	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. | CubeForm, Multiplayer SandBox Game
56881	UDP	76 878	81 236	6%	Unassigned (IANA)
56575	UDP	64 543	80 859	25%	Unassigned (IANA)
23667	UDP	25 827	80 813	213%	Unassigned (IANA)
51412	UDP	62 678	78 450	25%	Unassigned (IANA)
60023	TCP	67 450	77 317	15%	Certificate Management over CMS
4000	UDP	85 170	77 268	–9%	Diablo II game
3074	TCP	908	76 449	8 319%	Xbox LIVE and Games for Windows – Live
2323	TCP	90 115	76 047	–16%	Unassigned (IANA)
1026	UDP	22 861	73 850	223%	Microsoft DCOM services | CAP - Calendar Access Protocol (IANA official)
53	UDP	66 536	73 026	10%	Domain Name System (DNS)
58187	UDP	697	72 987	10 372%	Unassigned (IANA)
15000	UDP	92 403	72 979	–21%	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)
34188	UDP	79 554	71 482	–10%	Unassigned (IANA)
0	other	86 269	70 669	–18%	Unassigned (IANA)
1027	UDP	21 170	66 899	216%	Native IPv6 behind IPv4-to-IPv4 NAT Customer Premises Equipment (6a44)
48804	UDP	199 040	65 069	–67%	Unassigned (IANA)

Port	Protocol	Previous	Last	Growth	Description
17713	UDP	120	65 009	54 074%	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.
9000	UDP	62 181	64 649	4%	UDPCast
64541	UDP	115 947	64 562	–44%	Unassigned (IANA)
25413	UDP	18 615	64 050	244%	Unassigned (IANA)
17238	UDP	71	60 918	85 700%	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.
62783	TCP	52 817	60 306	14%	Certificate Management over CMS
1	TCP	73 679	60 190	–18%	TCP Port Service Multiplexer (TCPMUX). Historic. Both TCP and UDP have been assigned to TCPMUX by IANA,
42000	UDP	45 424	59 749	32%	Unassigned (IANA)
36080	UDP	37 850	57 928	53%	Unassigned (IANA)
39841	UDP	38 501	57 573	50%	Unassigned (IANA)
53985	UDP	10 299	57 538	459%	Unassigned (IANA)
9002	UDP	32	57 247	178 797%	Newforma Server comms
8444	TCP	47 790	56 865	19%	Bitmessage | Chia
7680	TCP	63 701	56 847	–11%	Delivery Optimization for Windows 10
52869	TCP	126 243	56 751	–55%	Certificate Management over CMS
11516	UDP	33 818	56 042	66%	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.
65458	UDP	7 442	56 009	653%	Unassigned (IANA)
80	UDP	45 200	55 663	23%	Hypertext Transfer Protocol (HTTP)HTTP/3 uses QUIC,
22	TCP	48 457	55 578	15%	Secure Shell (SSH),file transfers (scp, sftp) and port forwarding
61678	UDP	43 857	55 190	26%	Unassigned (IANA)
6885	UDP	59 654	54 270	–9%	BitTorrent beginning of range of ports used most often
50376	UDP	146	53 723	36 697%	Unassigned (IANA)

Port	Protocol	Previous	Last	Growth	Description
5555	TCP	44 016	53 104	21%	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 | Wireless adb (Android Debug Bridge) control of an Android device over the network.
17713	TCP	846	52 891	6 152%	Unassigned (IANA)
9006	UDP	50 203	52 749	5%	IANA Reserved port
31402	TCP	60 998	52 572	–14%	Unassigned (IANA)
51834	TCP	4 582	52 517	1 046%	Certificate Management over CMS
15817	UDP	94	50 302	53 413%	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.
6886	UDP	56 549	50 158	–11%	BitTorrent beginning of range of ports used most often
37991	UDP	91	50 008	54 854%	Unassigned (IANA)
6882	UDP	50 690	49 839	–2%	BitTorrent beginning of range of ports used most often
42000	TCP	32 807	49 810	52%	Brothers in Arms Online
15882	UDP	82	48 664	59 246%	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.
6890	UDP	40 049	47 529	19%	BitTorrent continuation of range of ports used most often
62754	UDP	214	46 973	21 850%	Unassigned (IANA)
37388	UDP	28 182	46 686	66%	Unassigned (IANA)

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

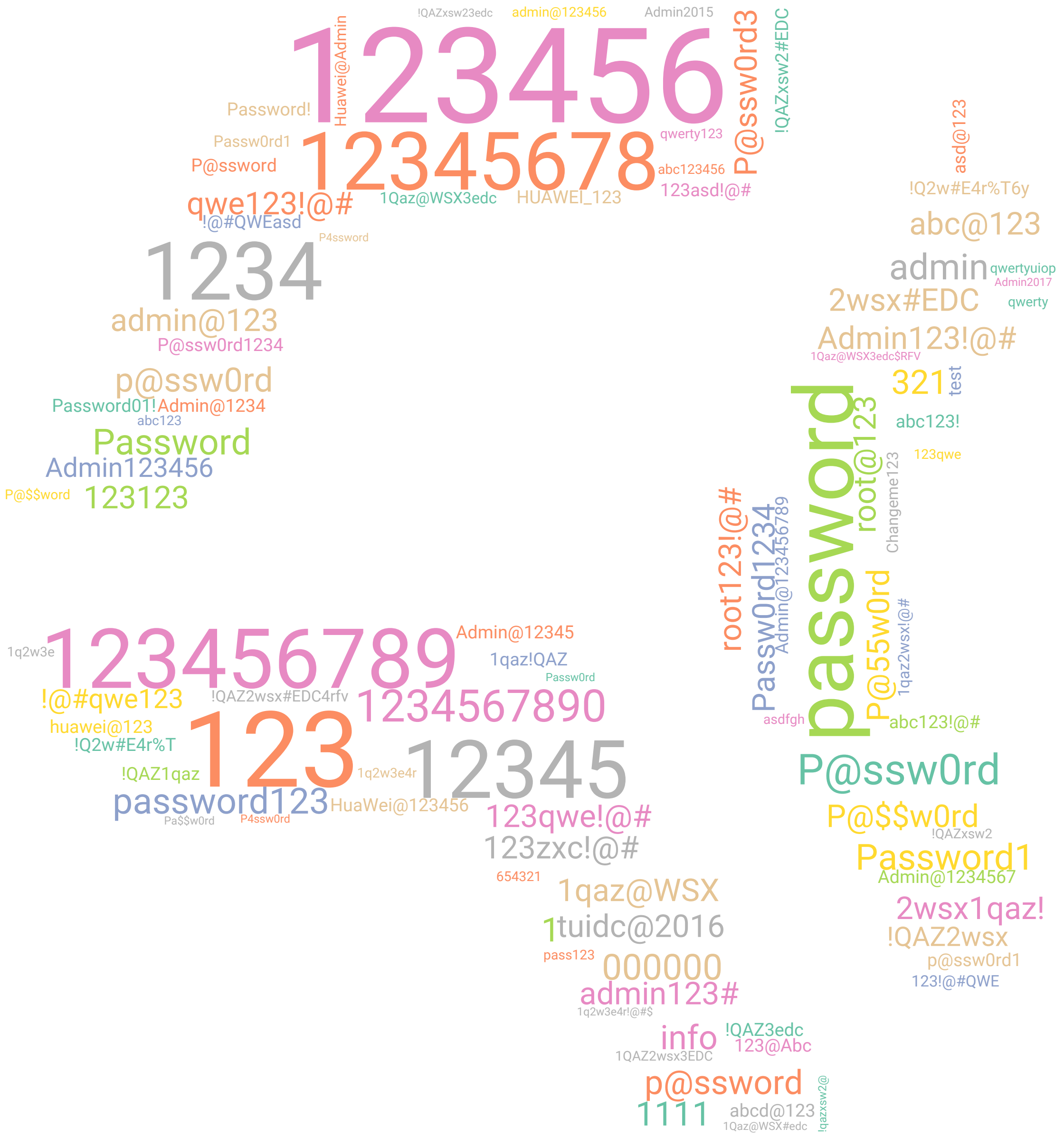
The diagram shows how many times we've seen individual passwords being used in attack attempts last period in comparison to the period before. The data are ordered by count last period, and the last column contains the difference against the previous period in percents for easier comparison. This allows 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	34 862 687	60 116 631	72%
123	16 310 242	35 572 980	118%
password	1 937 012	19 927 767	929%
123456789	695 520	19 811 669	2 748%
12345	747 189	18 914 669	2 431%
12345678	1 162 845	18 845 648	1 521%
1234	1 104 375	18 697 731	1 593%
1234567890	287 316	14 921 478	5 093%
P@ssw0rd	1 679 543	13 846 227	724%
admin	1 084 328	9 368 593	764%
password123	54 842	8 906 535	16 140%
Password1	334 797	8 291 669	2 377%
Password	6 975	8 032 987	115 068%
000000	111 886	7 984 874	7 037%
p@ssw0rd	317 958	6 238 807	1 862%
info	80 478	6 124 268	7 510%
1	442 902	5 668 569	1 180%
p@ssword	116 866	5 641 228	4 727%
321	16 577	5 226 170	31 427%
1111	168 651	5 170 621	2 966%
123123	447 390	4 695 870	950%
1qaz@WSX	1 223 627	4 637 920	279%
admin@123	868 317	4 624 765	433%
123qwe!@#	881 284	4 617 715	424%
Admin123!@#	803 802	4 568 132	468%
root@123	809 609	4 553 576	462%
2wsx#EDC	100 971	4 531 502	4 388%
qwe123!@#	802 519	4 525 570	464%
root123!@#	800 824	4 516 897	464%
P@$$w0rd	821 966	4 478 056	445%
tuidc@2016	100 984	4 472 500	4 329%
2wsx1qaz!	100 947	4 469 248	4 327%

Password	Previous	Last	Growth
123zxc!@#	100 989	4 336 406	4 194%
admin123#	800 039	4 178 243	422%
abc@123	807 888	4 147 712	413%
P@55w0rd	101 297	4 135 752	3 983%
Passw0rd1234	101 058	4 124 318	3 981%
P@ssw0rd3	100 876	4 124 288	3 988%
!@#qwe123	100 903	4 112 603	3 976%
!QAZ2wsx	101 248	4 090 214	3 940%
Admin123456	801 504	4 058 395	406%
P@ssw0rd1234	245 812	3 919 190	1 494%
p@ssw0rd1	823 159	3 841 586	367%
huawei@123	797 881	3 525 097	342%
P@ssword	846 519	3 402 964	302%
!QAZ1qaz	799 986	3 348 448	319%
abc123!	799 670	3 319 432	315%
asd@123	103 290	3 309 608	3 104%
abcd@123	802 975	3 253 957	305%
test	202 422	2 934 406	1 350%
Password01!	100 921	2 504 034	2 381%
1qaz!QAZ	428 768	2 372 677	453%
HuaWei@123456	100 743	2 334 038	2 217%
abc123!@#	100 687	2 330 002	2 214%
Admin@1234567	100 796	2 327 457	2 209%
Admin@1234	101 228	2 327 241	2 199%
Admin@123456789	100 552	2 316 383	2 204%
!QAZ3edc	100 750	2 314 067	2 197%
!QAZxsw2#EDC	100 829	2 302 493	2 184%
!Q2w#E4r%T	100 763	2 273 222	2 156%
!Q2w#E4r%T6y	100 750	2 265 050	2 148%
HUAWEI_123	100 732	2 152 183	2 037%
123asd!@#	101 065	2 118 535	1 996%
Password!	101 037	2 105 619	1 984%
123@Abc	100 660	2 105 298	1 991%
Admin@12345	101 120	2 101 110	1 978%
!@#QWEasd	100 692	2 100 408	1 986%
1Qaz@WSX3edc	100 832	2 099 290	1 982%
123!@#QWE	100 674	2 097 636	1 984%

Password	Previous	Last	Growth
Huawei@Admin	100 681	2 096 690	1 983%
Changeme123	100 908	2 095 422	1 977%
!QAZ2wsx#EDC4rfv	100 777	2 093 588	1 977%
1qaz2wsx!@#	100 920	2 092 846	1 974%
Passw0rd1	123 713	2 092 535	1 591%
admin@123456	100 719	2 068 314	1 954%
1QAZ2wsx3EDC	100 873	2 056 919	1 939%
P@$$word	120 872	2 001 842	1 556%
abc123	492 304	1 640 785	233%
qwerty	586 570	1 569 231	168%
654321	415 454	1 531 646	269%
1q2w3e4r	442 050	1 530 587	246%
123qwe	434 285	1 514 488	249%
abc123456	402 983	1 478 888	267%
qwerty123	363 560	1 457 823	301%
1q2w3e	352 802	1 452 438	312%
qwertyuiop	347 931	1 432 467	312%
pass123	333 576	1 424 679	327%
asdfgh	326 950	1 406 027	330%
Admin2015	225 093	912 613	305%
!QAZxsw2	100 736	912 026	805%
1Qaz@WSX3edc$RFV	100 474	911 942	808%
1q2w3e4r!@#$	100 637	911 841	806%
P4ssword	100 983	911 041	802%
Admin2017	224 700	910 239	305%
P4ssw0rd	100 923	909 237	801%
Pa$$w0rd	220 503	908 997	312%
!QAZxsw23edc	219 565	908 434	314%
1Qaz@WSX#edc	219 700	908 271	313%
!qazxsw2@	219 839	907 842	313%
Passw0rd	246 652	907 820	268%

Most Used Passwords Wordcloud


!QAZxsw23edc
admin@123456
Admin2015
123456
Huawei@Admin
P@ssw0rd3
!QAZxsw2#EDC
Password!
Passw0rd1
12345678
qwerty123
P@ssword
abc123456
asd@123
qwe123!@#
1Qaz@WSX3edc
HUAWEI_123
123asd!@#
!Q2w#E4r%T6y
!@#QWEasd
P4ssword
abc@123
1234
admin
qwertyuiop
Admin2017
2wsx#EDC
qwerty
admin@123
Admin123!@#
P@ssw0rd1234
1Qaz@WSX3edc$RFV
p@ssw0rd
321
test
Password01!
Admin@1234
abc123
abc123!
Password
123qwe
Admin123456
P@$$word
123123
password
root@123
Changeme123
root123!@#
Passw0rd1234
Admin@123456789
P@55w0rd
1qaz2wsx!@#
1q2w3e
123456789
Admin@12345
1qaz!QAZ
Passw0rd
!@#qwe123
!QAZ2wsx#EDC4rfv
1234567890
asdfgh
abc123!@#
huawei@123
!Q2w#E4r%T
123
1q2w3e4r
12345
P@ssw0rd
!QAZ1qaz
password123
HuaWei@123456
Pa$$w0rd
P4ssw0rd
123qwe!@#
P@$$w0rd
!QAZxsw2
123zxc!@#
Password1
Admin@1234567
654321
1qaz@WSX
2wsx1qaz!
1tuidc@2016
!QAZ2wsx
pass123
000000
p@ssw0rd1
123!@#QWE
admin123#
1q2w3e4r!@#$
info
!QAZ3edc
123@Abc
1QAZ2wsx3EDC
p@ssword
!qazxsw2@
1111
abcd@123
1Qaz@WSX#edc