

Sentinel Report - 2023 November

This document is the Sentinel report from the Turrus 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 Turrus 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

Iran decreased its efforts, and for a change, most active attackers occupying all top three positions are from Romania. There is a new interesting IP that emerged last month, and that is an attacker from Panama.

Small port scans for port 53 were at their record this month; we could not help but dig deeper. One reason is that the port is dedicated to communication with the DNS server, which is actually essential service that CZ.NIC provides. The other one is that the difference between the previous month is at least suspicious. What might look for the first sight, like a DNS amplification DDoS attack, could also be just a simple configuration error. In case the port scan is recorded on multiple probes, it is obvious that the attackers try random targets. On the other hand, if the "target" is one device, that leans more toward misconfiguration. In our team, we came to the conclusion that this is probably the second case, as, by simple query in our database, the target is one device. It seems like there was a DNS server running, but for now, it is stopped, and everybody who seeks an answer ends up on the firewall. This makes noise that we should ignore similarly to BitTorrent ports.

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.

84 919

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.

11 410

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?

3 933

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

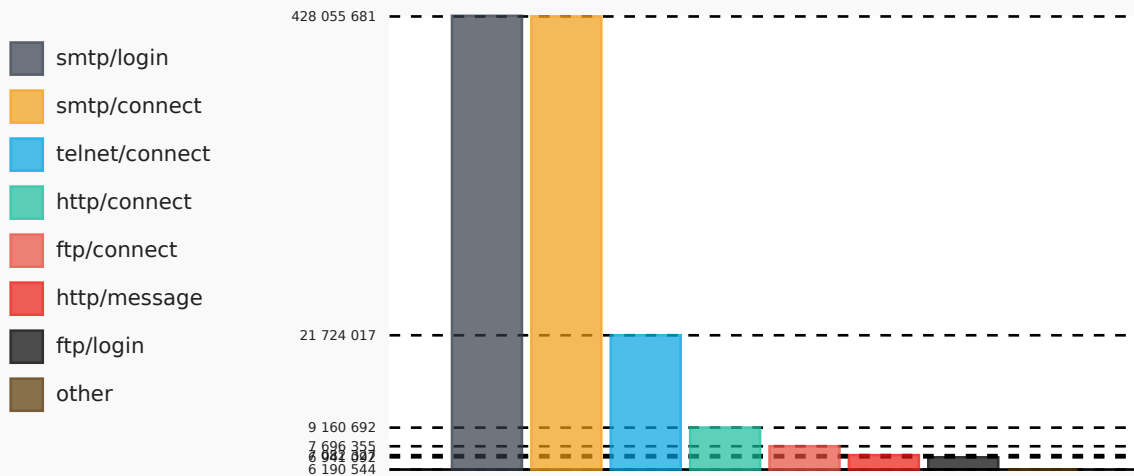
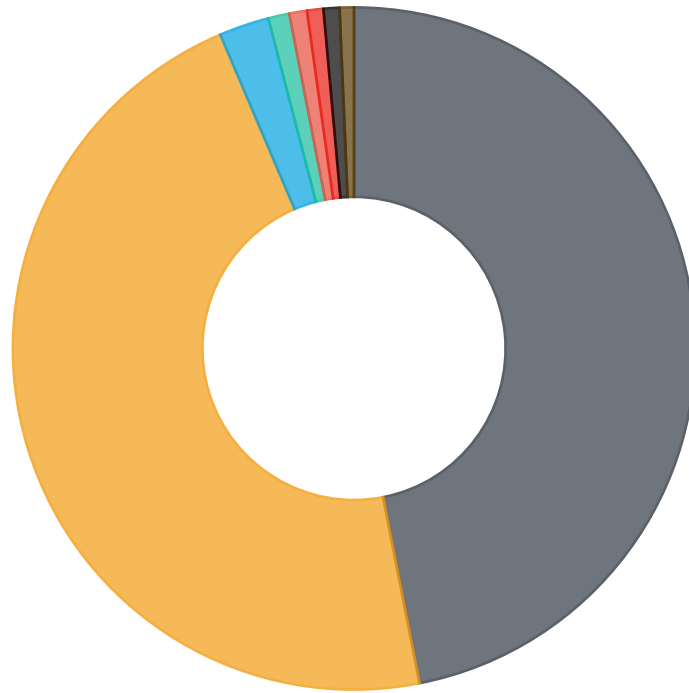
This figure shows how many total incidents were recorded with minipots. Please keep in mind that not each individual port scan is recorded. Given that port scan is really fast action, we consider two incidents, small port scan and big port scan.

917 233 425

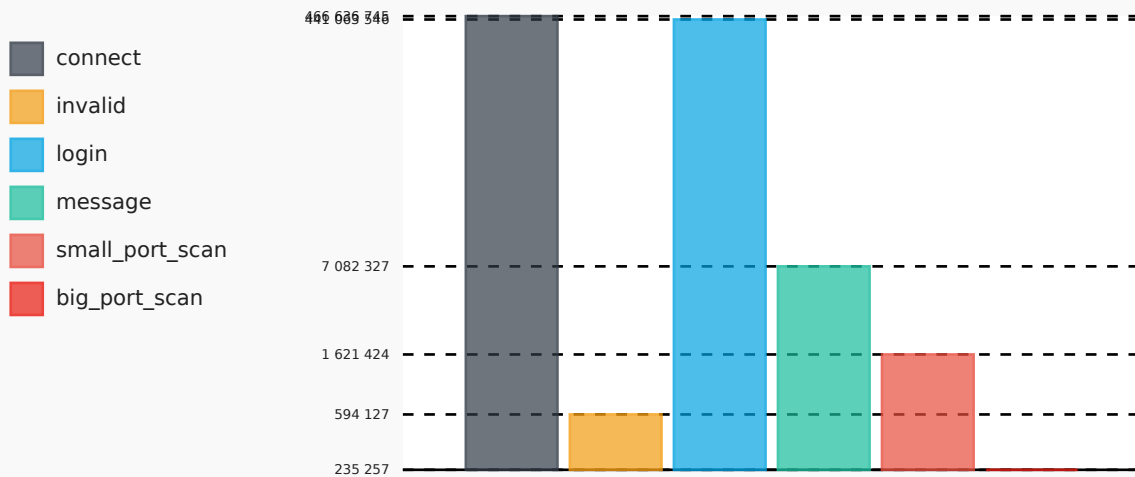
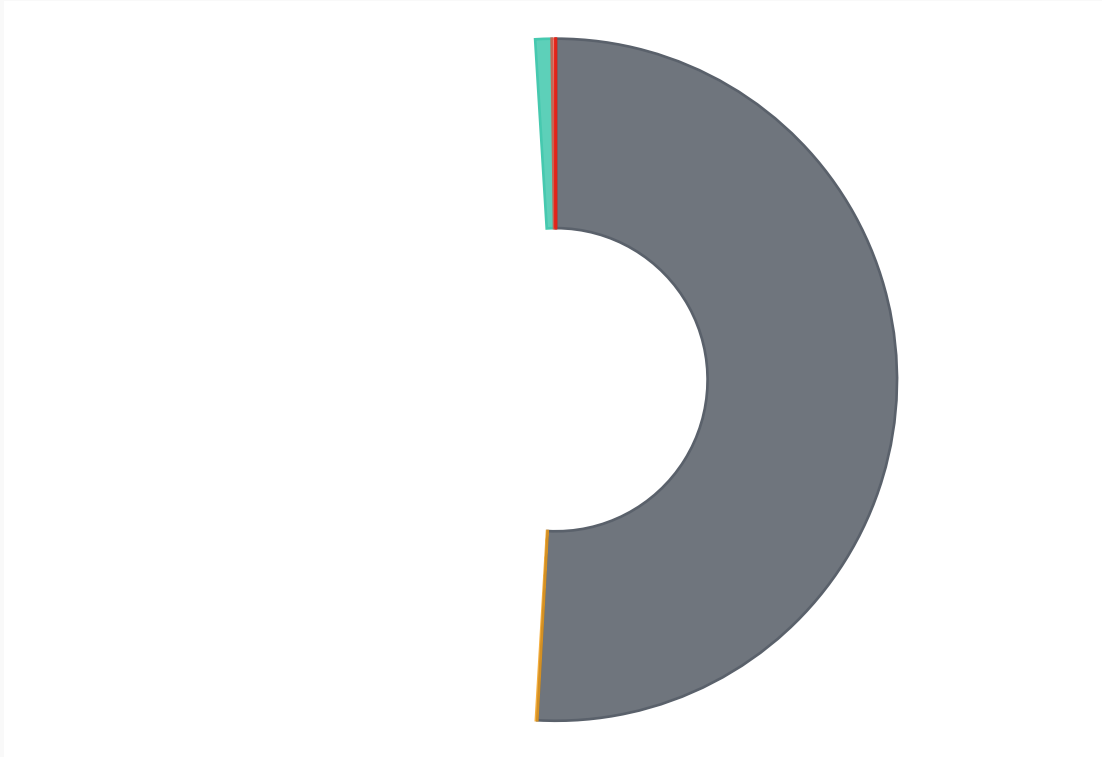
Incident Graphs

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.

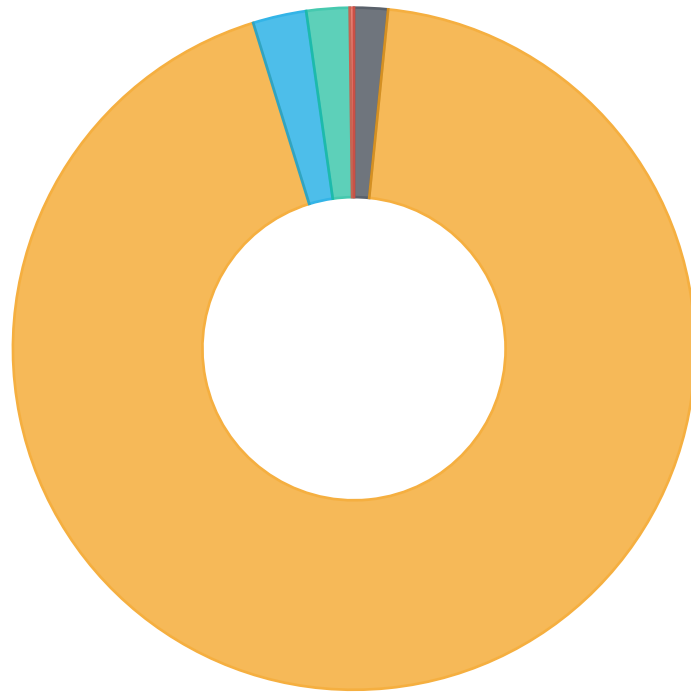
Minipot/Action Combined



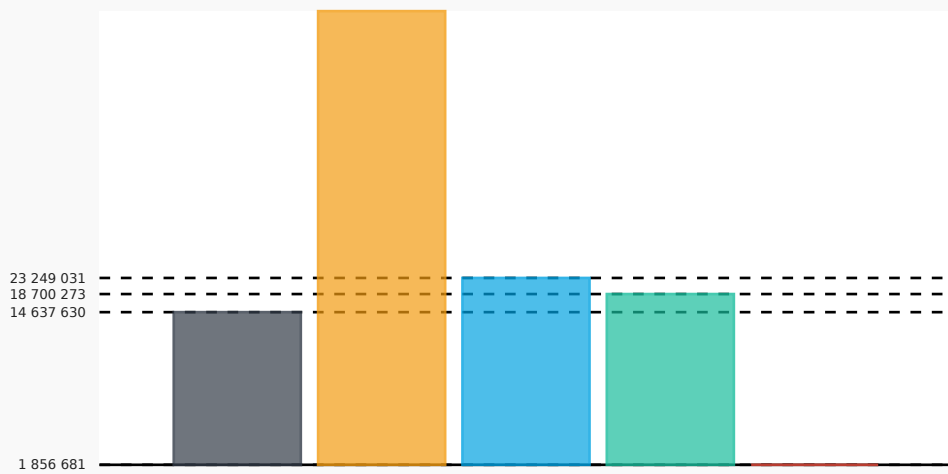
Attacker Action Pie Chart



Trap Pie Chart



- ftp
- smtp
- telnet
- http
- fwlogs



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 Attackers 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
413 645 650	minipot_smtp	80.94.95.181
1 507 430	minipot_telnet	46.19.139.138
753 573	minipot_http	67.217.57.54
724 242	minipot_ftp	152.89.163.246
10 600	fwlogs	94.102.61.39

Top Attackers

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

Count	IP	Country	Flag
413 645 650	80.94.95.181	RO	
199 974 080	45.129.14.120	RO	
162 784 063	45.129.14.106	RO	
46 475 014	185.36.81.40	LT	
2 678 678	20.212.9.216	SG	
1 615 140	103.151.122.52	VN	
1 516 096	46.19.139.138	PA	
1 397 837	124.220.72.164	CN	
1 362 781	147.78.103.182	NL	
1 249 770	91.92.241.95	BG	
1 191 015	91.92.241.214	BG	
1 103 710	163.123.141.194	US	
998 480	163.123.142.228	US	
993 851	67.217.57.54	US	
989 668	128.65.164.7	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
53	UDP	1 613 185	5 512 763	242%	Domain Name System (DNS)
51413	UDP	5 495 657	5 110 493	-7%	Transmission bit-torrent client
6881	UDP	2 971 596	2 803 686	-6%	BitTorrent beginning of range of ports used most often
51413	TCP	1 033 289	754 519	-27%	Certificate Management over CMS Transmission bit-torrent client
6889	UDP	600 242	635 997	6%	BitTorrent continuation of range of ports used most often
27032	UDP	592 894	502 361	-15%	Steam (In-Home Streaming) Steam Client (Remote Play)
56883	UDP	1 412	424 263	29 947%	Unassigned (IANA)
445	TCP	421 904	405 966	-4%	Microsoft-DS (Directory Services) Active Directory, Microsoft-DS (Directory Services) SMB
8202	UDP	117 023	387 630	231%	Unassigned (IANA)
64541	UDP	246 527	364 718	48%	Unassigned (IANA)
7881	UDP	846 534	360 721	-57%	Quick Time Streaming Server (formerly)
6881	TCP	308 336	347 621	13%	BitTorrent beginning of range of ports used most often
23	TCP	273 020	305 183	12%	Telnet protocol—unencrypted text communications
1024	UDP	200 375	281 324	40%	Reserved
51936	UDP	10 599	269 079	2 439%	Unassigned (IANA)
64541	TCP	113 045	250 996	122%	Certificate Management over CMS
7653	UDP	89 712	229 439	156%	Unassigned (IANA)
16881	UDP	275 795	212 301	-23%	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
16881	TCP	254 143	208 135	-18%	Synology NAS DSM download service
24902	UDP	103 463	202 395	96%	Unassigned (IANA)

Port	Protocol	Previous	Last	Growth	Description
48804	UDP	190 896	179 386	-6%	Unassigned (IANA)
50513	UDP	57 109	173 193	203%	Unassigned (IANA)
80	UDP	30 756	169 999	453%	Hypertext Transfer Protocol (HTTP)HTTP/3 uses QUIC,
60261	UDP	8 549	157 133	1 738%	Range from which Mosh – a remote-terminal application similar to SSH – typically assigns ports for ongoing sessions between Mosh servers and Mosh clients.
49001	UDP	114 461	146 457	28%	Far Cry Nuance Unity Service Discovery Protocol
63996	UDP	216	146 099	67 538%	Unassigned (IANA)
443	TCP	148 834	144 913	-3%	Hypertext Transfer Protocol Secure (HTTPS)HTTP/3 uses QUIC,
27032	TCP	155 191	142 663	-8%	Unassigned (IANA)
1	UDP	150 692	142 646	-5%	TCP Port Service Multiplexer (TCPMUX). Historic. Both TCP and UDP have been assigned to TCPMUX by IANA,
30295	UDP	145 010	139 618	-4%	Unassigned (IANA)
51416	UDP	116 507	135 012	16%	Unassigned (IANA)
51412	UDP	137 644	134 815	-2%	Unassigned (IANA)
39841	UDP	61 579	133 451	117%	Unassigned (IANA)
60205	UDP	44 438	118 249	166%	Range from which Mosh – a remote-terminal application similar to SSH – typically assigns ports for ongoing sessions between Mosh servers and Mosh clients.
62636	UDP	65 871	114 794	74%	Unassigned (IANA)
65206	UDP	185 199	110 341	-40%	Dynamic and/or private ports
18979	UDP	107 693	105 932	-2%	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.
8080	TCP	147 805	103 437	-30%	Alternative port for HTTP. See also ports 80 and 8008. Apache Tomcat Atlassian JIRA applications
62783	TCP	106 622	102 649	-4%	Certificate Management over CMS

Port	Protocol	Previous	Last	Growth	Description
12275	UDP	20 085	100 212	399%	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.
6901	UDP	90 887	98 446	8%	Windows Live Messenger (Voice) BitTorrent continuation of range of ports used most often
49189	UDP	38 479	95 233	147%	Unassigned (IANA)
1025	UDP	28 096	93 159	232%	Teradata database management system (Teradata) server
1045	UDP	15 271	89 213	484%	Unassigned (IANA)
8621	UDP	103 256	89 082	-14%	Unassigned (IANA)
59492	UDP	46 690	87 333	87%	Unassigned (IANA)
40227	UDP	184 925	87 165	-53%	Unassigned (IANA)
54385	UDP	140 495	85 234	-39%	Unassigned (IANA)
27839	UDP	59 364	82 631	39%	id Software's QuakeWorld
1433	TCP	81 269	80 328	-1%	Microsoft SQL Server database management system (MSSQL) server
53820	UDP	921	78 375	8 410%	Unassigned (IANA)
17801	UDP	171 721	78 166	-54%	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.
0	other	77 589	73 730	-5%	Unassigned (IANA)
61678	UDP	47 307	73 199	55%	Unassigned (IANA)
58945	UDP	36 605	72 607	98%	Unassigned (IANA)
6882	UDP	7 309	72 089	886%	BitTorrent beginning of range of ports used most often
61289	UDP	46 916	70 594	50%	Unassigned (IANA)
1	TCP	62 698	70 457	12%	TCP Port Service Multiplexer (TCPMUX). Historic. Both TCP and UDP have been assigned to TCPMUX by IANA,
11000	UDP	1 101 381	69 888	-94%	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.
51000	UDP	130 471	69 317	-47%	Unassigned (IANA)

Port	Protocol	Previous	Last	Growth	Description
10889	UDP	114 293	69 029	-40%	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	1 978	66 440	3 259%	BitTorrent beginning of range of ports used most often
39841	TCP	11 312	65 697	481%	Unassigned (IANA)
37215	TCP	47 584	61 295	29%	Huawei HG532 routers
62938	UDP	40 168	60 915	52%	Unassigned (IANA)
12661	UDP	10 668	60 100	463%	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.
7680	TCP	59 950	59 388	-1%	Delivery Optimization for Windows 10
12080	UDP	57 693	58 595	2%	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.
38706	UDP	40 003	58 350	46%	Unassigned (IANA)
4522	UDP	61	57 703	94 495%	Unassigned (IANA)
80	TCP	68 325	57 514	-16%	Hypertext Transfer Protocol (HTTP)HTTP/3 uses QUIC,
40050	UDP	11 424	57 366	402%	Unassigned (IANA)
14082	UDP	27 314	57 034	109%	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.
40498	UDP	23 043	56 818	147%	Unassigned (IANA)
8444	TCP	58 556	56 731	-3%	Bitmessage Chia
64591	UDP	193	55 476	28 644%	Unassigned (IANA)
64545	UDP	81 312	55 315	-32%	Unassigned (IANA)
22	TCP	273 855	54 511	-80%	Secure Shell (SSH),file transfers (scp, sftp) and port forwarding
9892	UDP	17 358	53 611	209%	Unassigned (IANA)
62882	UDP	49 168	53 060	8%	Unassigned (IANA)
25686	UDP	146	52 935	36 157%	SamsidParty Operational Ports

Port	Protocol	Previous	Last	Growth	Description
43208	UDP	252	52 336	20 668%	Unassigned (IANA)
6891	UDP	1 082	51 514	4 661%	BitTorrent continuation of range of ports used most often Windows Live Messenger (File transfer)
19467	UDP	212	51 158	24 031%	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.
13703	UDP	27 865	50 552	81%	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.
58224	UDP	18 523	50 529	173%	Unassigned (IANA)
49629	UDP	169	49 879	29 414%	Unassigned (IANA)
58376	UDP	32 407	49 828	54%	Unassigned (IANA)
60621	UDP	571	49 630	8 592%	Range from which Mosh – a remote-terminal application similar to SSH – typically assigns ports for ongoing sessions between Mosh servers and Mosh clients.
31128	UDP	101	49 117	48 531%	Unassigned (IANA)
55555	UDP	49 300	48 816	-1%	Unassigned (IANA)
64323	UDP	21 445	48 150	125%	Unassigned (IANA)
8333	TCP	39 433	47 767	21%	Bitcoin VMware VI Web Access via HTTPS
6888	UDP	10 240	47 543	364%	MUSE BitTorrent continuation of range of ports used most often
45961	UDP	20 704	46 878	126%	Unassigned (IANA)
11493	UDP	89	45 832	51 397%	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.
19545	UDP	81	45 468	56 033%	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.
55859	UDP	52 398	45 154	-14%	Unassigned (IANA)
54140	UDP	71 840	44 643	-38%	Unassigned (IANA)

Port	Protocol	Previous	Last	Growth	Description
11645	UDP	41 586	44 122	6%	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
P@ssw0rd	16 877 591	58 122 867	244%
password	21 329 701	35 175 575	65%
1qaz2wsx	621 573	20 761 855	3 240%
p@ssw0rd	20 378 215	20 150 578	-1%
Passw0rd	149 121	19 754 547	13 147%
111111	559 321	17 610 912	3 049%
222222	60 323	17 440 130	28 811%
333333	34 704	17 375 078	49 966%
555555	81 847	17 225 484	20 946%
444444	34 692	17 192 820	49 458%
666666	383 723	17 129 743	4 364%
777777	58 725	11 223 206	19 011%
123456	19 617 738	1 554 176	-92%
admin	1 345 613	1 049 935	-22%
12345	1 142 249	927 409	-19%
1234	1 098 357	913 049	-17%
P@ssw0rd1	14 190	883 634	6 127%
123	1 450 916	842 137	-42%
1qaz@WSX	20 555 410	808 761	-96%
P@\$w0rd	5 426	777 946	14 237%
P@55w0rd	15 328	761 617	4 869%
123qwe!@#	6 307 162	748 763	-88%
12345678	720 371	694 083	-4%
abc@123	177 829	681 975	284%
p@ssw0rd1	125 672	676 197	438%
!QAZ2wsx	4 679	674 999	14 326%
admin@123	20 883 234	668 076	-97%
P@ssword	2 756	667 837	24 132%
P@ssw0rd1234	523	660 647	126 219%
!QAZ1qaz	274	660 340	240 900%
Admin123456	541	660 209	121 935%
!@#qwe123	483	659 930	136 531%

Password	Previous	Last	Growth
123123	702 797	618 227	-12%
123456789	690 343	610 163	-12%
1234567	739 146	609 748	-18%
admin123#	279	559 069	200 283%
root123!@#	271	558 109	205 844%
P@ssw0rd3	258	558 102	216 219%
huawei@123	262	557 962	212 863%
Passw0rd1234	103 377	557 808	440%
abc123!	2 771	557 593	20 022%
123zxc!@#	170	557 325	327 738%
qwe123!@#	1 748	557 194	31 776%
Admin123!@#	20 154 342	557 114	-97%
abcd@123	3 210	556 787	17 245%
Passw0rd1	127 447	555 850	336%
root@123	19 854 630	554 911	-97%
2wsx1qaz!	172	553 461	321 680%
2wsx#EDC	189	512 224	270 918%
P@\$word	19 752	447 482	2 166%
abc123	443 303	447 114	1%
password1	180 257	445 173	147%
Password!	108 981	441 686	305%
1qaz!QAZ	113 184	439 861	289%
P4ssw0rd	122 149	439 689	260%
Admin2013	183	437 992	239 240%
asd@123	2 987	437 722	14 554%
1qazXSW@	357 126	437 235	22%
adminHW	408 227	430 340	5%
1234567890	756 444	418 131	-45%
qwerty	319 894	405 658	27%
admin123	488 187	396 412	-19%
test	360 091	346 209	-4%
1	557 968	344 158	-38%
Admin2015	5 495	340 421	6 095%
1Qaz@WSX3edc	85	339 219	398 981%
HUAWEI_123	84	338 033	402 320%
Admin@12345	414	337 985	81 539%
admin@123456	2 726	337 226	12 271%

Password	Previous	Last	Growth
123asd!@#	431	337 153	78 126%
Admin@1234567	139	337 062	242 391%
tuidc@2016	171	336 999	196 975%
123@Abc	87	336 888	387 128%
Admin@1234	445	336 795	75 584%
HuaWei@123456	86	336 567	391 257%
Admin2016	5 483	336 497	6 037%
1QAZ2wsx3EDC	85	336 407	395 673%
!@#QWEasd	91	336 361	369 527%
Changeme123	118	336 190	284 807%
!QAZxsw2#EDC	96	336 180	350 088%
!QAZ2wsx#EDC4rfv	97	336 058	346 352%
!QAZxsw2	137	335 947	245 117%
Password01!	221	335 933	151 906%
!Q2w#E4r%T6y	88	335 889	381 592%
1Qaz@WSX3edc\$RFV	84	335 805	399 668%
Admin@123456789	139	335 803	241 485%
P4ssword	122 081	335 755	175%
1qaz2wsx!@#	118	335 732	284 419%
Huawei@Admin	85	335 600	394 724%
!Q2w#E4r%T	91	335 577	368 666%
1q2w3e4r!@#\$	1 214	335 354	27 524%
123!@#QWE	85	335 255	394 318%
abc123!@#	108 629	334 607	208%
!QAZ3edc	90	329 536	366 051%
000000	642 719	319 304	-50%
	286 870	292 565	2%
qwerty123456	81 071	284 923	251%
p@55w0rd	94 329	284 338	201%
AB■	64 397	282 549	339%
support	95 202	272 147	186%

