Sentinel Report - 2023 December

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 Romanian attack peak was recorded on December 6th, with 52,576,312. Overall, attacks from Romania are dominant, as we can see in the *Attackers* section. Is the Steam port 27032 on the rise because of Christmas, and more people with misconfigured firewalls were playing in December? We can only guess. The lower-case password was overshadowed by other variants, of which the most interesting are conspiratory dates added to Pa55word. Like Pa55word2011, Pa55word2015, and Pa55word2016. We wish we could correlate them with something, but we could not figure out anything useful apart from trying to use Tyler Vigen's observations.

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.

100 032

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.

12 608

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?

4 671

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.

18

Total Minipot Incidents

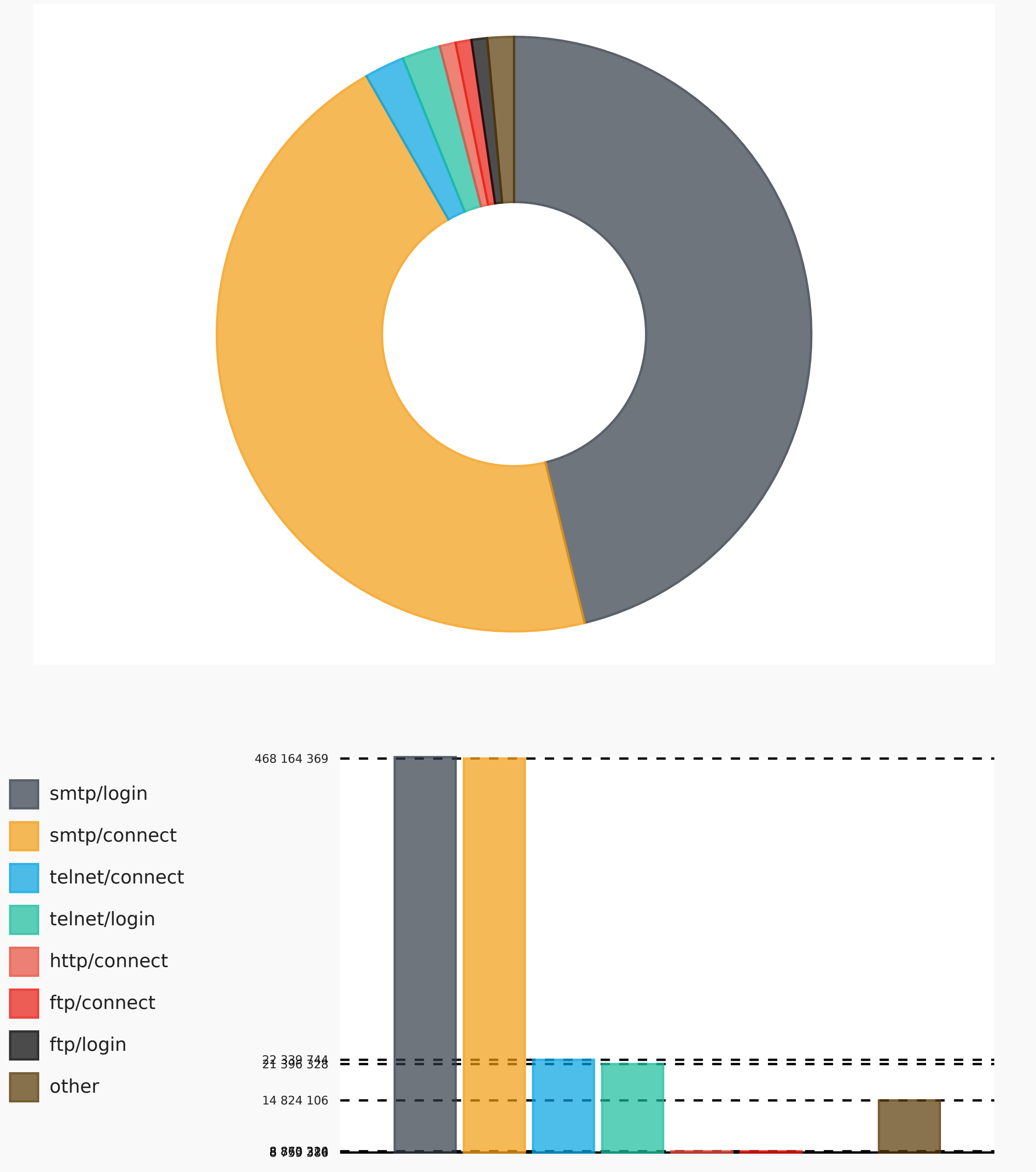
This figure shows how many total incidents were recorded with minipots. Please keep in mind that not each individual port scan is recorded. Given that port scan is really fast action, we consider two incidents, small port scan and big port scan.

994 838 074

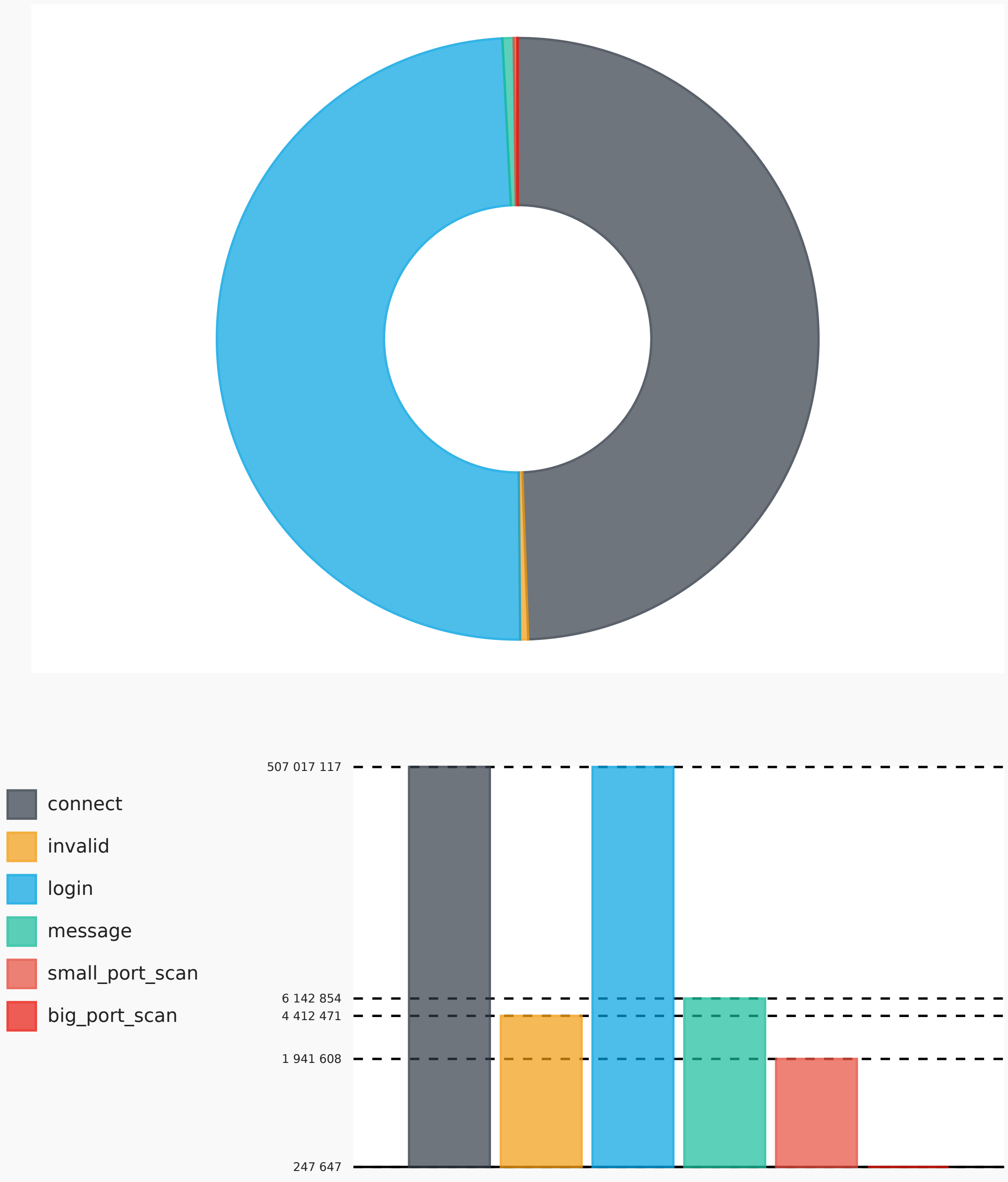
Incident Graphs

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.

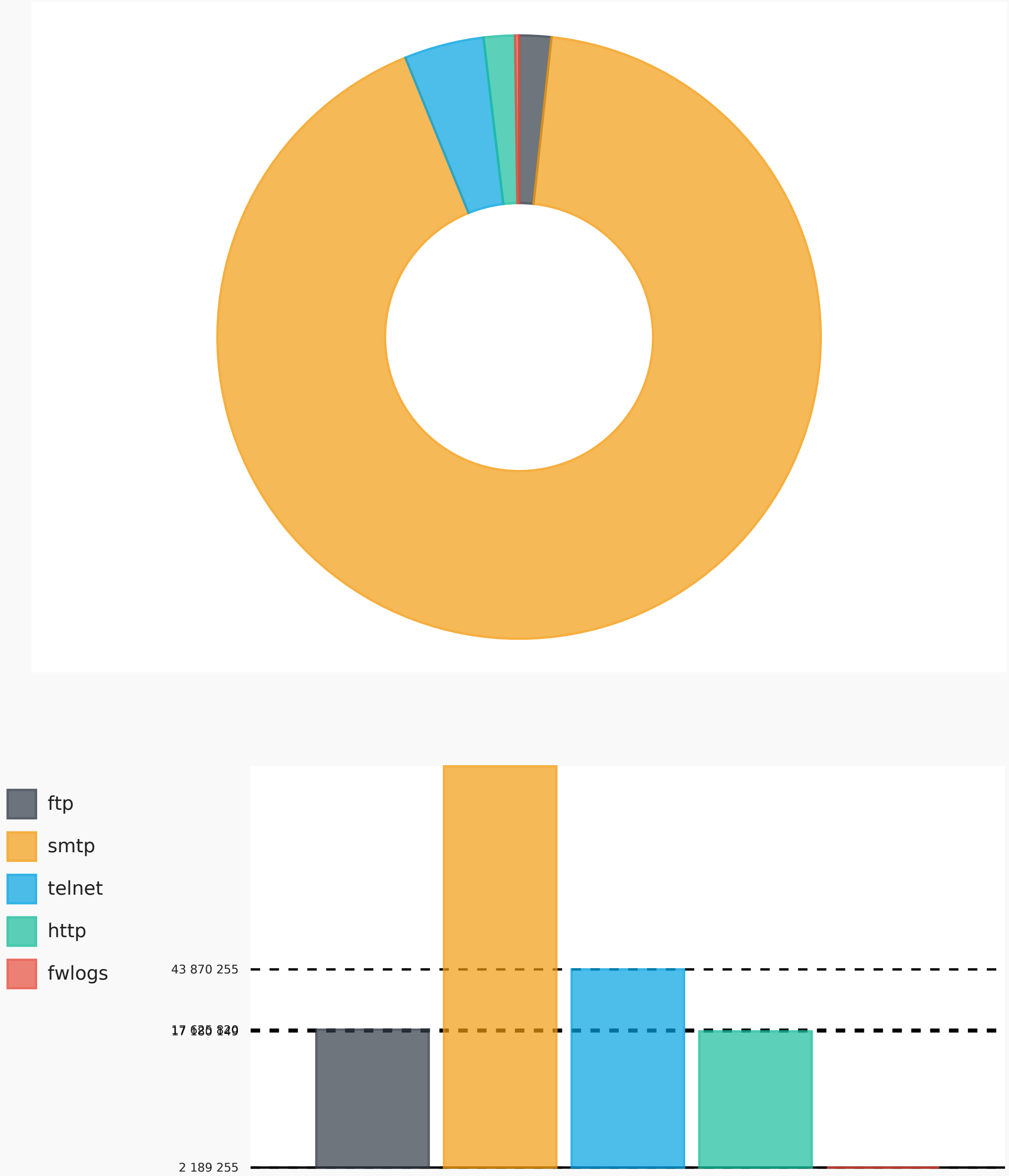
Minipot/Action Combined



Attacker Action Pie Chart



Trap Pie Chart



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
405 666 022	minipot_smtp	80.94.95.181
1 838 357	minipot_ftp	89.238.176.6
1 645 390	minipot_telnet	46.19.139.138
520 929	minipot_http	45.142.182.76
11 594	fwlogs	92.63.197.210

Top Attackers

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

Count	IP	Country	Flag
405 666 022	80.94.95.181	RO	🇷🇴
345 308 462	45.129.14.120	RO	🇷🇴
147 707 281	141.98.11.68	LT	🇱🇹
3 232 467	91.92.252.239	BG	🇧🇬
2 406 499	91.92.250.93	BG	🇧🇬
2 277 091	45.129.14.166	RO	🇷🇴
1 901 685	69.70.146.98	CA	🇨🇦
1 838 369	89.238.176.6	GB	🇬🇧
1 704 894	89.255.71.12	RU	🇷🇺
1 654 332	46.19.139.138	PA	🇵🇦
1 349 373	212.37.146.207	DK	🇩🇰
1 142 952	43.139.223.75	CN	🇨🇳
968 376	128.65.164.7	IR	🇮🇷
952 137	91.92.248.132	BG	🇧🇬
949 494	91.92.252.79	BG	🇧🇬

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	5 110 493	4 925 403	–4%	Transmission bit-torrent client
6881	UDP	2 803 686	2 859 764	2%	BitTorrent beginning of range of ports used most often
63649	UDP	97	736 880	759 570%	Unassigned (IANA)
6889	UDP	635 997	727 301	14%	BitTorrent continuation of range of ports used most often
51413	TCP	754 519	713 977	–5%	Certificate Management over CMS | Transmission bit-torrent client
27032	UDP	502 361	619 628	23%	Steam (In-Home Streaming) | Steam Client (Remote Play)
445	TCP	405 966	375 057	–8%	Microsoft-DS (Directory Services) Active Directory, | Microsoft-DS (Directory Services) SMB
1024	UDP	281 324	325 509	16%	Reserved
23	TCP	305 183	315 473	3%	Telnet protocol—unencrypted text communications
6881	TCP	347 621	294 349	–15%	BitTorrent beginning of range of ports used most often
60621	UDP	49 630	276 225	457%	Range from which Mosh – a remote-terminal application similar to SSH – typically assigns ports for ongoing sessions between Mosh servers and Mosh clients.
51936	UDP	269 079	266 315	–1%	Unassigned (IANA)
56883	UDP	424 263	252 984	–40%	Unassigned (IANA)
16881	UDP	212 301	161 783	–24%	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
48804	UDP	179 386	151 094	–16%	Unassigned (IANA)
1	UDP	142 646	150 839	6%	TCP Port Service Multiplexer (TCPMUX). Historic. Both TCP and UDP have been assigned to TCPMUX by IANA,

Port	Protocol	Previous	Last	Growth	Description
16881	TCP	208 135	150 788	–28%	Synology NAS DSM download service
30295	UDP	139 618	136 248	–2%	Unassigned (IANA)
6885	UDP	35 717	133 556	274%	BitTorrent beginning of range of ports used most often
27032	TCP	142 663	133 379	–7%	Unassigned (IANA)
51416	UDP	135 012	131 452	–3%	Unassigned (IANA)
24902	UDP	202 395	126 948	–37%	Unassigned (IANA)
49001	UDP	146 457	126 310	–14%	Far Cry | Nuance Unity Service Discovery Protocol
62783	TCP	102 649	124 275	21%	Certificate Management over CMS
443	TCP	144 913	117 818	–19%	Hypertext Transfer Protocol Secure (HTTPS)HTTP/3 uses QUIC,
51000	UDP	69 317	116 767	68%	Unassigned (IANA)
39057	UDP	784	111 629	14 138%	Unassigned (IANA)
6887	UDP	39 379	109 519	178%	BitTorrent beginning of range of ports used most often
8202	UDP	387 630	107 196	–72%	Unassigned (IANA)
55665	UDP	379	106 485	27 996%	Unassigned (IANA)
18979	UDP	105 932	102 803	–3%	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	103 437	100 957	–2%	Alternative port for HTTP. See also ports 80 and 8008. | Apache Tomcat | Atlassian JIRA applications
1029	UDP	3 646	98 373	2 598%	Microsoft DCOM services
59705	UDP	13 317	95 311	616%	Unassigned (IANA)
8621	UDP	89 082	94 856	6%	Unassigned (IANA)
60205	UDP	118 249	88 879	–25%	Range from which Mosh – a remote-terminal application similar to SSH – typically assigns ports for ongoing sessions between Mosh servers and Mosh clients.
2457	UDP	42	84 026	199 962%	Unassigned (IANA)
0	other	73 730	79 257	7%	Unassigned (IANA)
1027	UDP	40 985	79 091	93%	Native IPv6 behind IPv4-to-IPv4 NAT Customer Premises Equipment (6a44)
6890	UDP	30 131	78 296	160%	BitTorrent continuation of range of ports used most often

Port	Protocol	Previous	Last	Growth	Description
10889	UDP	69 029	77 930	13%	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.
59705	TCP	9 463	77 480	719%	Certificate Management over CMS
1433	TCP	80 328	77 304	–4%	Microsoft SQL Server database management system (MSSQL) server
27839	UDP	82 631	72 037	–13%	id Software's QuakeWorld
37215	TCP	61 295	71 163	16%	Huawei HG532 routers
39841	UDP	133 451	70 309	–47%	Unassigned (IANA)
51412	UDP	134 815	68 480	–49%	Unassigned (IANA)
59492	UDP	87 333	68 391	–22%	Unassigned (IANA)
65206	UDP	110 341	68 193	–38%	Dynamic and/or private ports
12275	UDP	100 212	67 743	–32%	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.
49189	UDP	95 233	67 699	–29%	Unassigned (IANA)
62938	UDP	60 915	64 021	5%	Unassigned (IANA)
6901	UDP	98 446	62 403	–37%	Windows Live Messenger (Voice) | BitTorrent continuation of range of ports used most often
6891	UDP	51 514	62 222	21%	BitTorrent continuation of range of ports used most often | Windows Live Messenger (File transfer)
64545	UDP	55 315	60 976	10%	Unassigned (IANA)
123	UDP	38 263	60 731	59%	Network Time Protocol (NTP), used for time synchronization
32000	UDP	29 945	60 604	102%	Unassigned (IANA)
8444	TCP	56 731	57 531	1%	Bitmessage | Chia
61289	UDP	70 594	56 554	–20%	Unassigned (IANA)
63996	UDP	146 099	56 158	–62%	Unassigned (IANA)
22	TCP	54 511	53 138	–3%	Secure Shell (SSH),file transfers (scp, sftp) and port forwarding
38477	UDP	563	52 687	9 258%	Unassigned (IANA)
56881	UDP	39 492	52 632	33%	Unassigned (IANA)

Port	Protocol	Previous	Last	Growth	Description
1	TCP	70 457	52 270	–26%	TCP Port Service Multiplexer (TCPMUX). Historic. Both TCP and UDP have been assigned to TCPMUX by IANA,
6886	UDP	38 474	51 633	34%	BitTorrent beginning of range of ports used most often
6882	UDP	72 089	50 920	–29%	BitTorrent beginning of range of ports used most often
54476	UDP	555	50 057	8 919%	Unassigned (IANA)
6884	UDP	66 440	50 038	–25%	BitTorrent beginning of range of ports used most often
7881	UDP	360 721	49 845	–86%	Quick Time Streaming Server (formerly)
25413	UDP	35 603	49 728	40%	Unassigned (IANA)
80	TCP	57 514	49 573	–14%	Hypertext Transfer Protocol (HTTP)HTTP/3 uses QUIC,
50513	UDP	173 193	49 479	–71%	Unassigned (IANA)
9771	UDP	57	49 428	86 616%	Unassigned (IANA)
8333	TCP	47 767	48 650	2%	Bitcoin | VMware VI Web Access via HTTPS
51765	UDP	17 130	48 033	180%	Unassigned (IANA)
1026	UDP	29 030	47 805	65%	Microsoft DCOM services | CAP - Calendar Access Protocol (IANA official)
55323	UDP	286	47 268	16 427%	Unassigned (IANA)
4787	UDP	1 052	47 045	4 372%	Unassigned (IANA)
15000	UDP	1 589	46 279	2 812%	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)
39841	TCP	65 697	46 229	–30%	Unassigned (IANA)
61678	UDP	73 199	45 755	–37%	Unassigned (IANA)
7680	TCP	59 388	44 639	–25%	Delivery Optimization for Windows 10
12701	UDP	26 123	43 664	67%	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	40 820	43 436	6%	Unassigned (IANA)

Port	Protocol	Previous	Last	Growth	Description
44005	TCP	7 033	43 367	517%	Unassigned (IANA)
1024	TCP	15 002	43 071	187%	Reserved
60023	TCP	13 246	42 320	219%	Certificate Management over CMS
8360	UDP	7 228	42 159	483%	Unassigned (IANA)
12080	UDP	58 595	41 699	−29%	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.
44005	UDP	4 939	41 420	739%	Unassigned (IANA)
29252	TCP	544	41 350	7 501%	Unassigned (IANA)
19467	UDP	51 158	41 098	−20%	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.
52943	UDP	38 375	40 474	5%	Unassigned (IANA)
42399	UDP	496	40 037	7 972%	Unassigned (IANA)
6888	UDP	47 543	39 115	−18%	MUSE | BitTorrent continuation of range of ports used most often
10617	UDP	91	38 910	42 658%	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.
61706	UDP	599	38 801	6 378%	Unassigned (IANA)
42926	TCP	1 314	38 722	2 847%	Brothers in Arms Online
53049	UDP	183	38 465	20 919%	Unassigned (IANA)
64671	UDP	197	37 763	19 069%	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

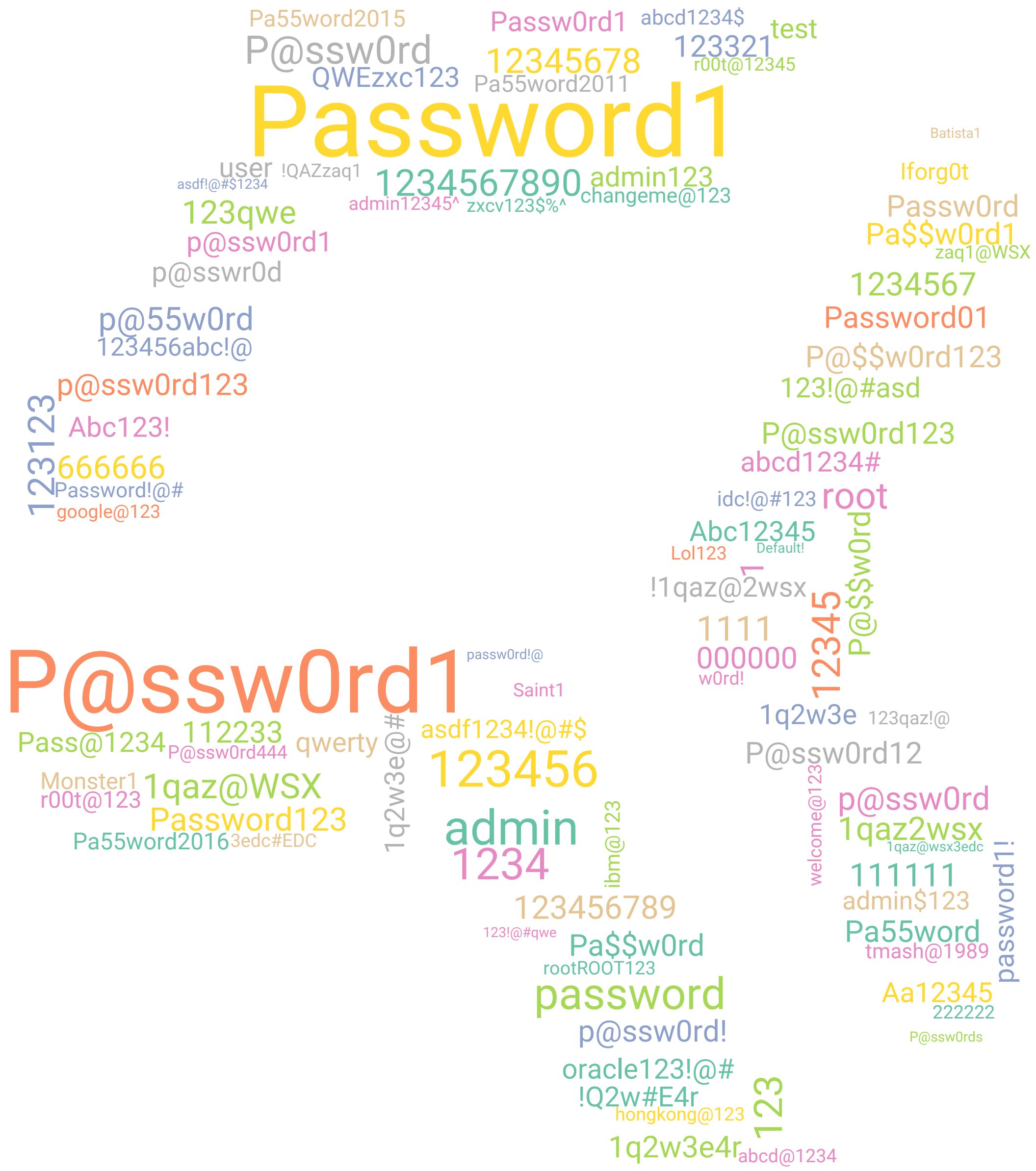
The diagram shows how many times we've seen individual passwords being used in attack attempts last period in comparison to the period before. The data are ordered by count last period, and the last column contains the difference against the previous period in percents for easier comparison. This allows 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
Password1	240 711	25 808 986	10 622%
P@ssw0rd1	883 634	19 185 351	2 071%
123456	1 554 176	2 501 564	61%
admin	1 049 935	2 177 053	107%
1234	913 049	1 727 572	89%
password	35 175 575	1 684 323	–95%
123	842 137	1 307 378	55%
12345	927 409	1 243 475	34%
P@ssw0rd	58 122 867	1 209 093	–98%
1234567890	418 131	1 053 298	152%
root	208 150	1 018 850	389%
123123	618 227	1 001 075	62%
12345678	694 083	802 369	16%
1111	162 851	760 786	367%
1qaz@WSX	808 761	734 562	–9%
p@ssw0rd	20 150 578	694 944	–97%
111111	17 610 912	679 271	–96%
123456789	610 163	677 862	11%
1qaz2wsx	20 761 855	676 088	–97%
1	344 158	674 307	96%
666666	17 129 743	671 562	–96%
p@55w0rd	284 338	654 039	130%
1234567	609 748	651 960	7%
Password123	207 246	648 887	213%
	292 565	647 082	121%
123qwe	253 676	636 230	151%
Passw0rd	19 754 547	622 488	–97%
112233	126 668	619 406	389%
123321	233 915	602 774	158%
1q2w3e4r	270 292	582 328	115%
P@ssw0rd123	219 782	580 405	164%
Pa$$w0rd	211 248	576 779	173%

Password	Previous	Last	Growth
Pa55word	204 987	575 977	181%
Password01	205 179	574 895	180%
P@$$w0rd123	102 739	573 863	459%
Pa$$w0rd1	204 881	573 169	180%
P@ssw0rd12	102 597	573 040	459%
p@ssw0rd123	107 861	572 451	431%
p@ssw0rd!	79 434	547 260	589%
P@$$w0rd	777 946	532 122	–32%
000000	319 304	526 426	65%
admin123	396 412	508 762	28%
Passw0rd1	555 850	473 946	–15%
user	202 836	472 047	133%
1q2w3e	227 132	471 689	108%
qwerty	405 658	471 293	16%
p@ssw0rd1	676 197	470 302	–30%
test	346 209	468 634	35%
Abc12345	103 328	467 968	353%
oracle123!@#	1	467 900	46 789 900%
p@sswr0d	0	467 488	N/A
Abc123!	9	467 390	5 193 122%
!Q2w#E4r	1	467 287	46 728 600%
password1!	31	467 284	1 507 268%
123!@#asd	0	467 151	N/A
Aa12345	108 202	467 147	332%
Pass@1234	28	467 111	1 668 154%
QWEzxc123	1	466 982	46 698 100%
1q2w3e@#	0	466 981	N/A
abcd1234#	51	466 947	915 482%
!1qaz@2wsx	0	466 839	N/A
123456abc!@	0	466 811	N/A
asdf1234!@#$	6	466 799	7 779 883%
admin$123	102 062	466 660	357%
Pa55word2016	0	466 563	N/A
Pa55word2015	0	466 533	N/A
Pa55word2011	7	466 509	6 664 314%
Monster1	6	466 485	7 774 650%
r00t@123	0	466 448	N/A

Password	Previous	Last	Growth
Iforg0t	0	466 429	N/A
changeme@123	0	466 397	N/A
Password!@#	18	466 336	2 590 656%
idc!@#123	0	466 300	N/A
tmash@1989	1	466 283	46 628 200%
ibm@123	0	466 215	N/A
abcd1234$	0	466 191	N/A
hongkong@123	0	466 157	N/A
admin12345^	1	466 109	46 610 800%
google@123	9	466 005	5 177 733%
222222	17 440 130	465 895	–97%
3edc#EDC	1	465 891	46 589 000%
w0rd!	1	465 784	46 578 300%
!QAZzaq1	9	465 767	5 175 089%
rootROOT123	0	465 659	N/A
123qaz!@	0	465 631	N/A
Saint1	0	465 598	N/A
r00t@12345	1	465 423	46 542 200%
P@ssw0rd444	1	465 393	46 539 200%
zaq1@WSX	78	465 296	596 433%
abcd@1234	55	465 203	845 724%
Lol123	5	465 014	9 300 180%
welcome@123	62	464 904	749 745%
zxcv123$%^	0	464 815	N/A
1qaz@wsx3edc	0	464 769	N/A
Default!	0	464 719	N/A
123!@#qwe	12	464 709	3 872 475%
Batista1	0	464 687	N/A
passw0rd!@	0	464 673	N/A
P@ssw0rds	6	464 619	7 743 550%
asdf!@#$1234	0	464 542	N/A

Most Used Passwords Wordcloud


Pa55word2015
Passw0rd1
abcd1234$
test
P@ssw0rd
123321
12345678
r00t@12345
QWEzxc123
Pa55word2011
Password1
Batista1
user
!QAZzaq1
asdf!@#$1234
1234567890
admin123
Iforg0t
admin12345^
zxcv123$%^
changeme@123
Passw0rd
123qwe
Pa$$w0rd1
zaq1@WSX
p@ssw0rd1
p@sswr0d
1234567
p@55w0rd
Password01
123456abc!@
P@$$w0rd123
p@ssw0rd123
123!@#asd
123123
Abc123!
P@ssw0rd123
666666
abcd1234#
Password!@#
idc!@#123
root
google@123
Abc12345
Lol123
Default!
P@$$w0rd
1
!1qaz@2wsx
12345
1111
000000
passw0rd!@
w0rd!
P@ssw0rd1
Saint1
1q2w3e
123qaz!@
asdf1234!@#$
Pass@1234
112233
qwerty
P@ssw0rd444
P@ssw0rd12
1q2w3e@#
123456
Monster1
1qaz@WSX
r00t@123
welcome@123
p@ssw0rd
Password123
1qaz2wsx
1qaz@wsx3edc
Pa55word2016
3edc#EDC
admin
ibm@123
password1!
1234
111111
admin$123
123456789
123!@#qwe
Pa55word
Pa$$w0rd
tmash@1989
rootROOT123
password
Aa12345
222222
p@ssw0rd!
P@ssw0rds
oracle123!@#
!Q2w#E4r
123
hongkong@123
1q2w3e4r
abcd@1234