TURRIS

Sentinel Report - 2023 October

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

An interesting dynamic is happening at the top of the attackers' chart. First of all, Iranian attacks were overshadowed by other countries to the degree that we no longer see them in higher positions. To mention the current top four most significant, we would highlight Romania, Germany, Bulgaria, and the Netherlands. There had been consistent attacks from Germany that came into prominence about the 4th of October and then slowly started to disappear on the 16th until the final dissolution on the 18th of October. The graph line for German attacks looks very stable and consistent. On the other hand, Romania's malicious activity, which took the top of the charts, looked erratic and unorganized in the graph. To the degree that Sentinel View graphs in the *Incidents* section, except for *Top countries by recorded incidents*, are rendered almost useless. The count of incidents for the most-used password from the previous month, 1234562, had been 47 031 867. If we compare it to this month's winner password, we see that the number is smaller by half, having 21 329 701 records. The most active attacker that used any password last month used a German IP address and rotated passwords on a daily basis. And we mean that literally. Picked one password, used it the whole day everywhere possible, and only then moved to the following one the next day. So does the attacker from Romania, yet we see no connection between the two. Another interesting point is that there are a lot of SMTP minipot attacks with empty passwords.

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.

82 627

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.

11 337

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?

3 236

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

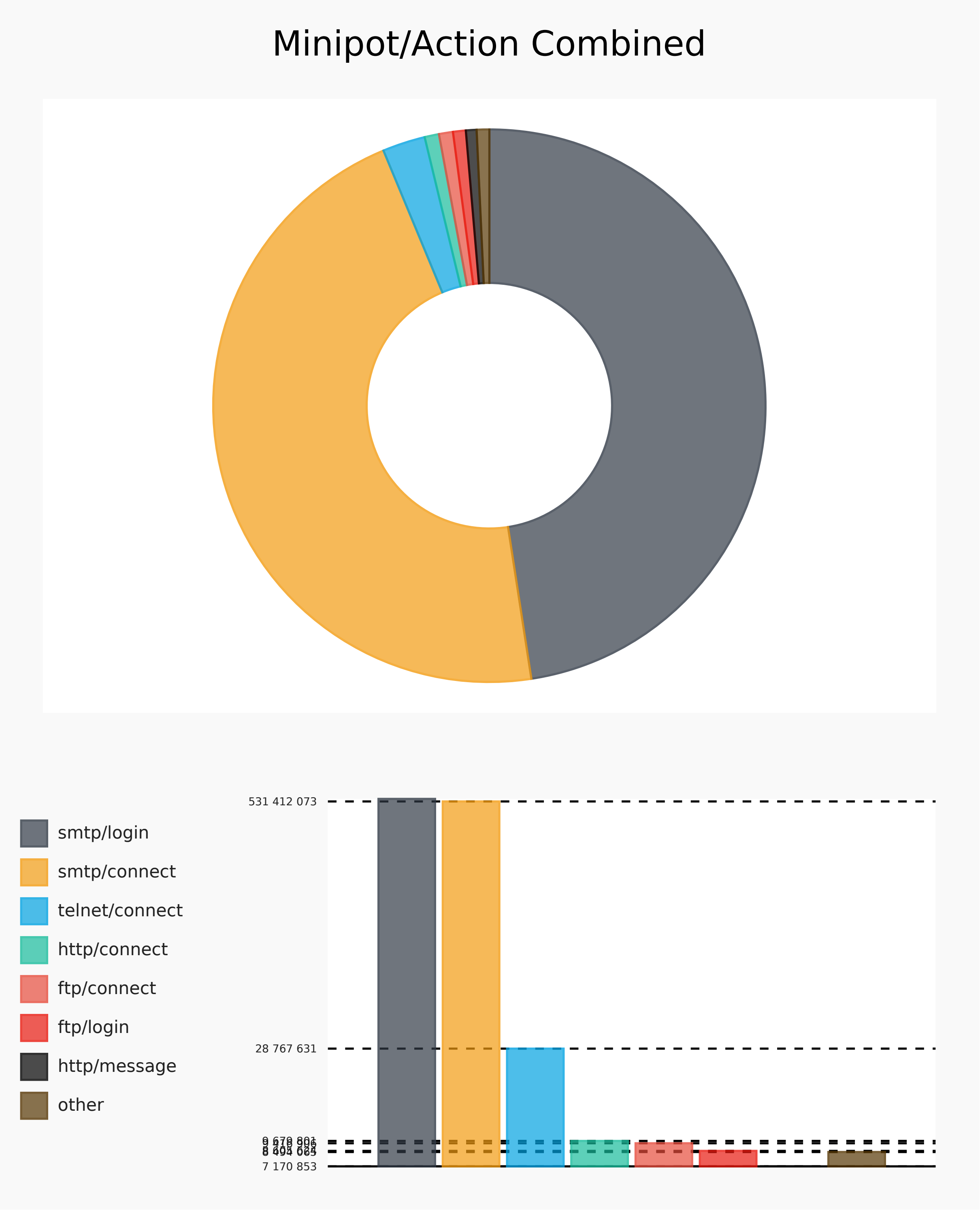
Total Minipot Incidents

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.

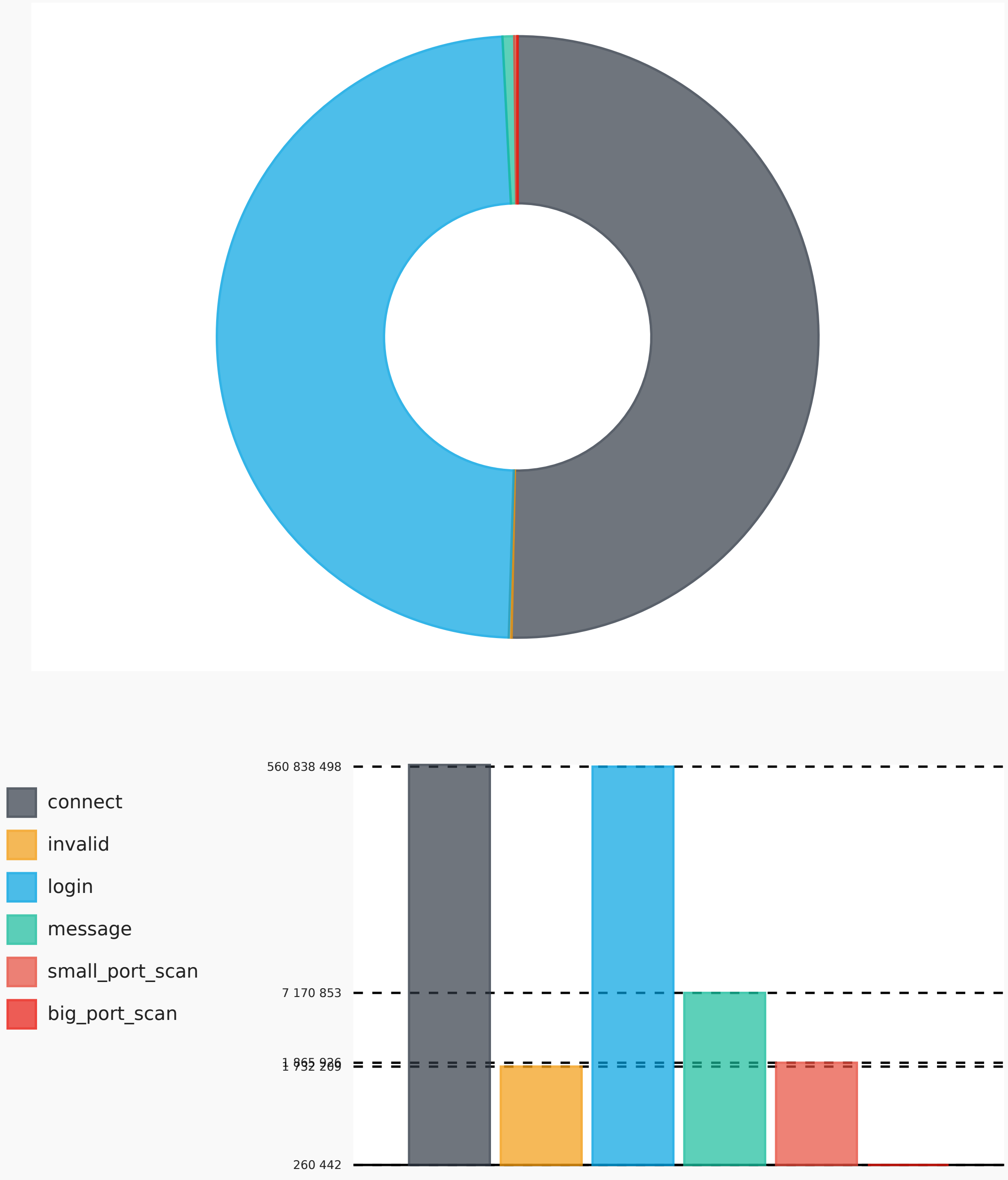
1 114 010 650

Incident Graphs

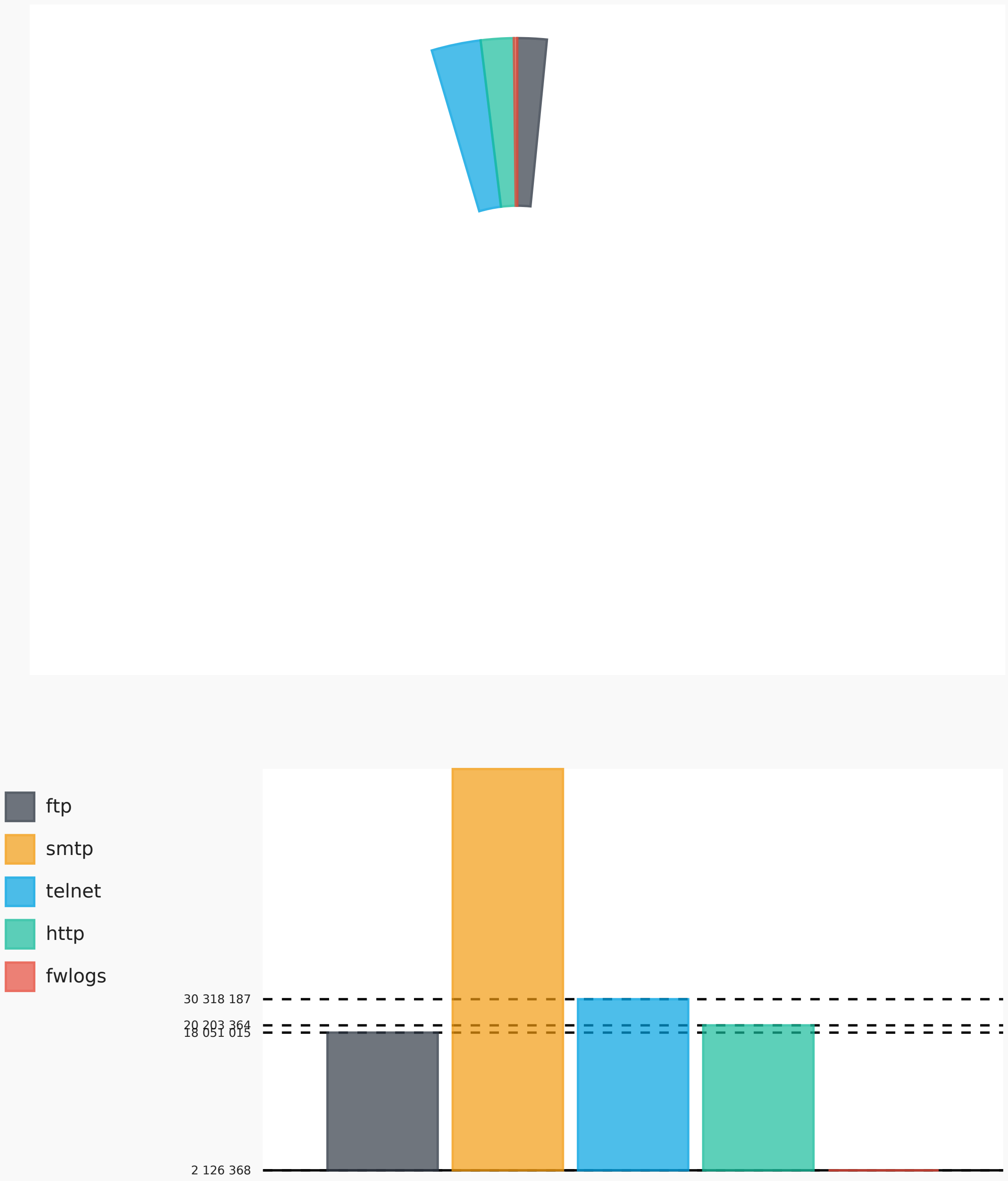
Below pie charts visualize the ratio how actions, minipots or their combinations had been distributed across the pool. While the ratio for pie charts is linear bar chart displays values using logarithmic scale.



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
490 982 025	minipot_smtp	80.94.95.181
1 403 512	minipot_telnet	46.19.139.138
840 059	minipot_ftp	185.225.28.5
485 645	minipot_http	37.57.192.98
11 309	fwlogs	80.94.95.249

Top Attackers

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

Count	IP	Country	Flag
490 982 025	80.94.95.181	RO	🇷🇴
295 883 703	77.90.185.59	DE	🇩🇪
176 937 379	45.129.14.106	RO	🇷🇴
49 880 106	212.70.149.70	BG	🇧🇬
14 277 472	103.151.122.52	VN	🇻🇳
12 402 549	20.212.9.216	SG	🇸🇬
1 786 106	87.120.84.110	NL	🇳🇱
1 604 657	87.120.84.139	NL	🇳🇱
1 448 137	182.44.53.61	CN	🇨🇳
1 055 069	103.144.152.10	VN	🇻🇳
1 052 077	110.188.23.166	CN	🇨🇳
979 106	87.120.84.61	NL	🇳🇱
949 007	141.98.10.220	LT	🇱🇹
876 467	93.95.27.7	IR	🇮🇷
857 786	193.42.33.232	NL	🇳🇱

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	4 943 130	5 495 657	11%	Transmission bit-torrent client
6881	UDP	2 824 791	2 971 595	5%	BitTorrent beginning of range of ports used most often
53	UDP	74 023	1 613 185	2 079%	Domain Name System (DNS)
11000	UDP	709 445	1 101 380	55%	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	773 590	1 033 289	34%	Certificate Management over CMS | Transmission bit-torrent client
7881	UDP	980 353	846 534	–14%	Quick Time Streaming Server (formerly)
6889	UDP	612 960	600 242	–2%	BitTorrent continuation of range of ports used most often
27032	UDP	528 435	592 894	12%	Steam (In-Home Streaming) | Steam Client (Remote Play)
445	TCP	396 436	421 902	6%	Microsoft-DS (Directory Services) Active Directory, | Microsoft-DS (Directory Services) SMB
6881	TCP	355 504	308 334	–13%	BitTorrent beginning of range of ports used most often
16881	UDP	321 786	275 795	–14%	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
22	TCP	67 530	273 855	306%	Secure Shell (SSH),file transfers (scp, sftp) and port forwarding
23	TCP	248 367	273 016	10%	Telnet protocol—unencrypted text communications
16881	TCP	273 881	254 143	–7%	Synology NAS DSM download service
64541	UDP	324 234	246 527	–24%	Unassigned (IANA)
33113	UDP	290 265	224 360	–23%	Unassigned (IANA)

Port	Protocol	Previous	Last	Growth	Description
1024	UDP	184 776	200 375	8%	Reserved
48804	UDP	106 676	190 896	79%	Unassigned (IANA)
65206	UDP	112 658	185 199	64%	Dynamic and/or private ports
40227	UDP	85 180	184 925	117%	Unassigned (IANA)
17801	UDP	35 202	171 721	388%	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.
27032	TCP	132 070	155 191	18%	Unassigned (IANA)
1	UDP	162 077	150 691	–7%	TCP Port Service Multiplexer (TCPMUX). Historic. Both TCP and UDP have been assigned to TCPMUX by IANA,
443	TCP	160 711	148 834	–7%	Hypertext Transfer Protocol Secure (HTTPS)HTTP/3 uses QUIC,
8080	TCP	108 815	147 803	36%	Alternative port for HTTP. See also ports 80 and 8008. | Apache Tomcat | Atlassian JIRA applications
61564	UDP	104	146 847	141 099%	Unassigned (IANA)
30295	UDP	127 241	145 010	14%	Unassigned (IANA)
54385	UDP	193	140 495	72 695%	Unassigned (IANA)
51412	UDP	137 780	137 644	~0%	Unassigned (IANA)
51000	UDP	178 279	130 471	–27%	Unassigned (IANA)
8202	UDP	57	117 023	205 204%	Unassigned (IANA)
51416	UDP	113 769	116 507	2%	Unassigned (IANA)
49001	UDP	257 899	114 461	–56%	Far Cry | Nuance Unity Service Discovery Protocol
10889	UDP	134 460	114 293	–15%	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.
64541	TCP	157 416	113 045	–28%	Certificate Management over CMS
18979	UDP	117 234	107 693	–8%	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	100 399	106 622	6%	Certificate Management over CMS
42001	UDP	235	106 341	45 151%	Unassigned (IANA)

Port	Protocol	Previous	Last	Growth	Description
60636	UDP	184	105 154	57 049%	Range from which Mosh – a remote-terminal application similar to SSH – typically assigns ports for ongoing sessions between Mosh servers and Mosh clients.
24902	UDP	93	103 463	111 151%	Unassigned (IANA)
8621	UDP	31 192	103 256	231%	Unassigned (IANA)
62534	UDP	139 679	91 298	–35%	Unassigned (IANA)
6901	UDP	72 271	90 887	26%	Windows Live Messenger (Voice) | BitTorrent continuation of range of ports used most often
49648	UDP	85 941	89 864	5%	Unassigned (IANA)
7653	UDP	212	89 712	42 217%	Unassigned (IANA)
36080	UDP	67 191	84 489	26%	Unassigned (IANA)
64545	UDP	28 954	81 312	181%	Unassigned (IANA)
1433	TCP	76 795	81 269	6%	Microsoft SQL Server database management system (MSSQL) server
0	other	68 512	77 589	13%	Unassigned (IANA)
54140	UDP	807	71 840	8 802%	Unassigned (IANA)
80	TCP	69 367	68 325	–2%	Hypertext Transfer Protocol (HTTP)HTTP/3 uses QUIC,
32000	UDP	88 216	65 967	–25%	Unassigned (IANA)
62636	UDP	187	65 871	35 125%	Unassigned (IANA)
56575	UDP	41 802	64 501	54%	Unassigned (IANA)
16527	UDP	1 975	63 694	3 125%	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.
1	TCP	69 953	62 696	–10%	TCP Port Service Multiplexer (TCPMUX). Historic. Both TCP and UDP have been assigned to TCPMUX by IANA,
39841	UDP	39 692	61 579	55%	Unassigned (IANA)
64962	UDP	98	61 420	62 573%	Unassigned (IANA)
31410	UDP	64	61 267	95 630%	Unassigned (IANA)
21742	UDP	75 330	60 391	–20%	Unassigned (IANA)
7680	TCP	59 304	59 949	1%	Delivery Optimization for Windows 10
27839	UDP	78	59 364	76 008%	id Software's QuakeWorld
8444	TCP	56 028	58 554	5%	Bitmessage | Chia

Port	Protocol	Previous	Last	Growth	Description
12080	UDP	20 881	57 693	176%	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.
64644	UDP	86 847	57 691	–34%	Unassigned (IANA)
50513	UDP	480	57 109	11 798%	Unassigned (IANA)
1043	UDP	519	56 169	10 723%	Unassigned (IANA)
51765	UDP	57 811	53 790	–7%	Unassigned (IANA)
45282	UDP	157	53 614	34 049%	Unassigned (IANA)
14463	UDP	58	52 426	90 290%	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	69 904	52 398	–25%	Unassigned (IANA)
123	UDP	17 366	51 187	195%	Network Time Protocol (NTP), used for time synchronization
20030	UDP	10 906	50 788	366%	Unassigned (IANA)
24588	UDP	51 321	50 593	–1%	Unassigned (IANA)
55555	UDP	55 115	49 300	–11%	Unassigned (IANA)
62882	UDP	39 160	49 168	26%	Unassigned (IANA)
37215	TCP	25 475	47 583	87%	Huawei HG532 routers
4444	UDP	46 498	47 454	2%	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
61678	UDP	52 323	47 307	–10%	Unassigned (IANA)
61289	UDP	58 814	46 916	–20%	Unassigned (IANA)
59492	UDP	74 400	46 690	–37%	Unassigned (IANA)
16774	UDP	101	46 618	46 056%	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.
48804	TCP	28 806	46 554	62%	Unassigned (IANA)
28123	UDP	219	46 235	21 012%	Unassigned (IANA)

Port	Protocol	Previous	Last	Growth	Description
10570	UDP	563	46 056	8 080%	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.
40318	UDP	29 682	45 484	53%	Unassigned (IANA)
14028	TCP	32 629	44 487	36%	Unassigned (IANA)
60205	UDP	140	44 438	31 641%	Range from which Mosh – a remote-terminal application similar to SSH – typically assigns ports for ongoing sessions between Mosh servers and Mosh clients.
23380	UDP	33 315	43 801	31%	Unassigned (IANA)
16438	UDP	3 901	43 704	1 020%	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. | Real-time Transport Protocol (RTP), RTP Control Protocol (RTCP), used by Apple's Game Center
45282	TCP	959	43 034	4 387%	Unassigned (IANA)
14463	TCP	370	42 651	11 427%	Unassigned (IANA)
11645	UDP	82	41 586	50 615%	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.
52680	UDP	23 270	40 748	75%	Unassigned (IANA)
62938	UDP	43 774	40 168	–8%	Unassigned (IANA)
38706	UDP	94	40 003	42 456%	Unassigned (IANA)
64485	UDP	514	39 991	7 680%	Unassigned (IANA)
9000	UDP	60 273	39 856	–34%	UDPCast
47594	UDP	481	39 575	8 128%	Unassigned (IANA)
1843	UDP	11 308	39 463	249%	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

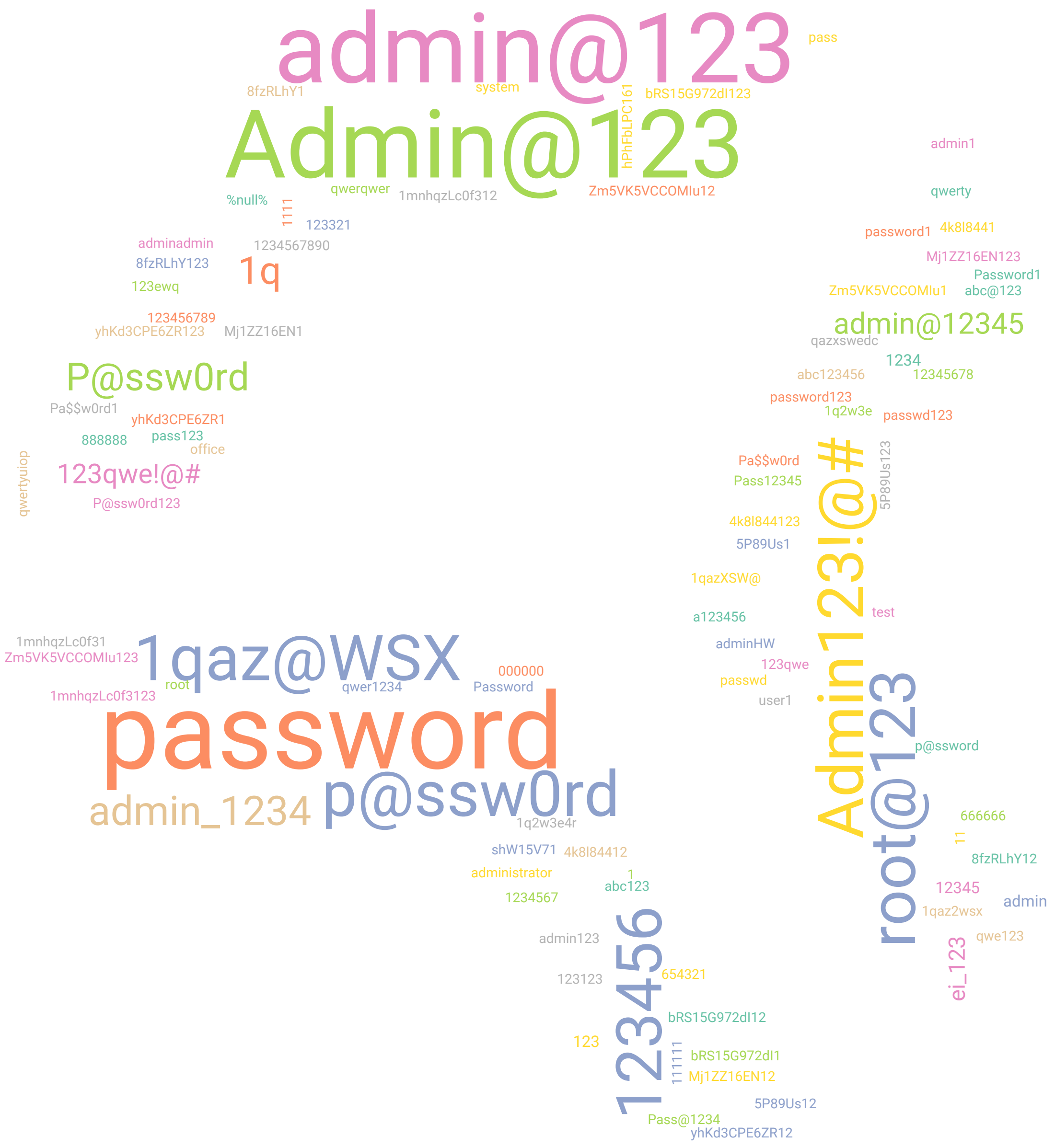
The diagram shows how many times we've seen individual passwords being used in attack attempts last period in comparison to the period before. The data are ordered by count last period, and the last column contains the difference against the previous period in percents for easier comparison. This allows 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
password	14 762 725	21 329 701	44%
admin@123	2 411 818	20 883 234	766%
Admin@123	253 161	20 759 416	8 100%
1qaz@WSX	2 347 938	20 555 410	775%
p@ssw0rd	14 121 698	20 378 215	44%
Admin123!@#	1 967 335	20 154 342	924%
root@123	1 962 572	19 854 630	912%
123456	47 031 867	19 617 738	–58%
admin_1234	0	19 347 366	N/A
P@ssw0rd	20 685 884	16 877 591	–18%
1q	0	16 650 146	N/A
admin@12345	91	8 278 931	9 097 626%
123qwe!@#	2 021 245	6 307 162	212%
ei_123	3 192 018	4 292 647	34%
123	1 203 066	1 450 916	21%
admin	1 479 587	1 345 613	–9%
12345	15 586 716	1 142 249	–93%
1234	1 256 151	1 098 357	–13%
1234567890	379 221	756 444	99%
1234567	692 974	739 146	7%
12345678	654 370	720 371	10%
123123	1 030 507	702 797	–32%
123456789	765 175	690 343	–10%
000000	404 974	642 719	59%
1qaz2wsx	410 895	621 573	51%
111111	13 949 357	559 321	–96%
1	419 813	557 968	33%
admin123	603 611	488 187	–19%
abc123	413 046	443 303	7%
1mnhqzLc0f31	0	439 078	N/A
1mnhqzLc0f312	0	413 757	N/A
adminHW	294 512	408 227	39%

Password	Previous	Last	Growth
1q2w3e4r	151 177	402 839	166%
1mnhqzLc0f3123	0	391 551	N/A
666666	370 782	383 723	3%
123321	140 360	362 903	159%
test	274 754	360 091	31%
1qazXSW@	1 852 382	357 126	–81%
Pass@1234	370 289	356 467	–4%
Pass12345	97	355 900	366 807%
888888	301 317	343 148	14%
qwerty	227 661	319 894	41%
abc123456	619 243	312 373	–50%
adminadmin	23 141	308 738	1 234%
654321	413 195	306 309	–26%
5P89Us1	0	304 923	N/A
4k8l844123	0	299 027	N/A
4k8l8441	0	297 271	N/A
p@ssword	49 437	296 383	500%
4k8l84412	0	293 417	N/A
	309 048	286 870	–7%
5P89Us12	0	286 245	N/A
yhKd3CPE6ZR12	0	285 342	N/A
Mj1ZZ16EN1	0	284 563	N/A
yhKd3CPE6ZR1	0	283 869	N/A
Mj1ZZ16EN12	0	281 715	N/A
5P89Us123	0	270 502	N/A
yhKd3CPE6ZR123	0	264 379	N/A
11	26 460	262 490	892%
123ewq	413	262 346	63 422%
a123456	1 311	262 284	19 906%
passwd123	567 072	257 215	–55%
1111	13 773 328	255 615	–98%
123qwe	151 428	252 923	67%
P@ssw0rd123	617 310	252 596	–59%
qwe123	2 951	251 389	8 419%
qwer1234	2 265	250 525	10 961%
root	206 487	248 885	21%
qwerqwer	159	248 519	156 201%

Password	Previous	Last	Growth
Password	7 308	241 264	3 201%
Mj1ZZ16EN123	0	238 152	N/A
Pa$$w0rd1	110 144	232 158	111%
bRS15G972dI1	0	231 837	N/A
bRS15G972dI12	0	227 271	N/A
Zm5VK5VCCOMIu1	0	223 794	N/A
Pa$$w0rd	614 991	220 600	–64%
system	106 227	219 354	106%
%null%	561 128	218 647	–61%
bRS15G972dI123	0	217 281	N/A
administrator	203 600	208 117	2%
qwertyuiop	306 834	205 670	–33%
8fzRLhY1	0	205 396	N/A
password123	39 941	204 866	413%
Zm5VK5VCCOMIu12	0	204 317	N/A
qazxswedc	79 145	201 397	154%
1q2w3e	104 880	199 446	90%
pass	138 591	194 147	40%
passwd	50 805	191 959	278%
Password1	402 341	190 769	–53%
admin1	176 153	189 507	8%
pass123	301 835	181 731	–40%
hPhFbLPC161	0	181 425	N/A
8fzRLhY12	0	181 210	N/A
password1	456 147	180 257	–60%
shW15V71	0	179 792	N/A
abc@123	1 859 386	177 829	–90%
8fzRLhY123	0	171 762	N/A
Zm5VK5VCCOMIu123	0	170 076	N/A
user1	39 681	169 967	328%
office	75 293	169 255	125%

Most Used Passwords Wordcloud


admin@123
pass
8fzRLhY1
system
hPhFbLPC161
bRS15G972dl123
Admin@123
admin1
%null%
qwerqwer
1mnhqzLc0f312
Zm5VK5VCCOMlu12
qwerty
1111
123321
password1
4k8l8441
adminadmin
1234567890
Mj1ZZ16EN123
8fzRLhY123
1q
Password1
123ewq
Zm5VK5VCCOMlu1
abc@123
123456789
admin@12345
yhKd3CPE6ZR123
Mj1ZZ16EN1
qazxswedc
1234
P@ssw0rd
abc123456
12345678
Pa$$w0rd1
password123
yhKd3CPE6ZR1
1q2w3e
passwd123
888888
pass123
office
Admin123!@#
5P89Us123
qwertyuiop
Pa$$w0rd
123qwe!@#
Pass12345
P@ssw0rd123
4k8l844123
5P89Us1
1qazXSW@
a123456
test
1mnhqzLc0f31
adminHW
Zm5VK5VCCOMlu123
1qaz@WSX
000000
123qwe
root
qwer1234
Password
passwd
1mnhqzLc0f3123
user1
password
root@123
p@ssword
admin_1234
p@ssw0rd
666666
1q2w3e4r
11
shW15V71
4k8l84412
8fzRLhY12
administrator
1
abc123
12345
1234567
admin
1qaz2wsx
admin123
123456
qwe123
ei_123
123123
654321
bRS15G972dl12
123
11111
bRS15G972dl1
Mj1ZZ16EN12
5P89Us12
Pass@1234
yhKd3CPE6ZR12