

Sentinel Report - 2023 September

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

On the first pages of the Report, we can see that September numbers are very comparable to August data.

Iran-based attackers moved away from top charts, and we see that addresses from the United States now take the lead in the HTTP minipot incidents records.

There is again a rise in popularity of some ports used for unknown services, particularly ports 33113 and 62534. We still don't know what could be behind those.

After a couple of months, the 123456 password regains its first position on the top of the passwords table. There are three passwords that are in the top table, which were not present, at least in the previous month. %users% is most likely somehow related to MS Windows. It might be caused by some broken script used by some attacker. Looks like some inexperienced attackers are still trying to use the proprietary closed source OS to conduct their evil deeds and are luckily failing. ei_123 does not look like anything in particular, but we have seen a tendency between attackers trying some simple password in combination with the 123 suffix. It seems like attackers think that people tend to often pass security policies by adding those numbers to their simple passwords. Zz3AEcMM looks quite random. It might be a default password somewhere or part of some leak.

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.

69 213

Daily Average

On some days, attackers are more active than on others. But how many attackers did we have on our greylist on average each day.

10 099

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 greylist 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?

3 413

Attackers Promiscuity

Are the attackers targeting one specific individual or are they attacking the whole Internet hoping to get lucky? We have seen both. But to sum it up somehow, we calculated how many victims every attacker tried to attack on average.

18

Total Minipot Incidents

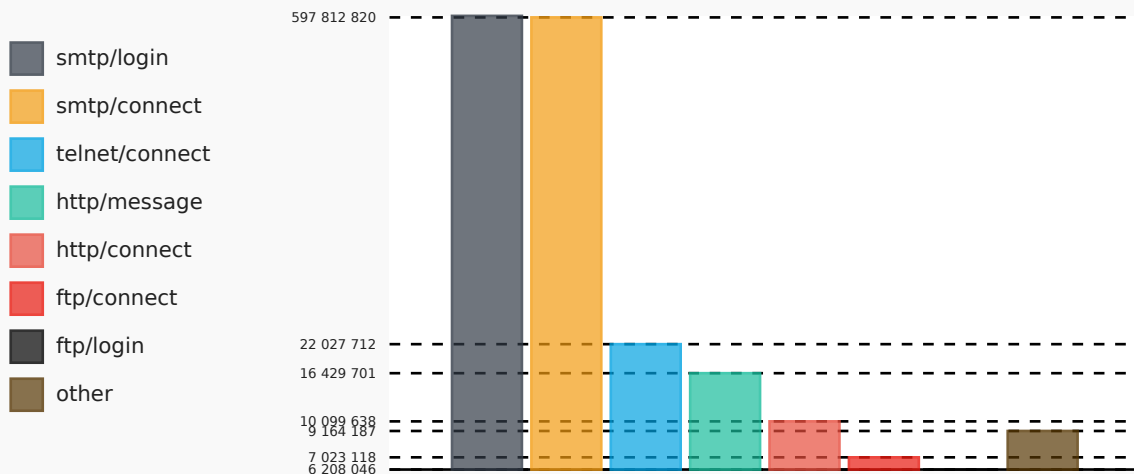
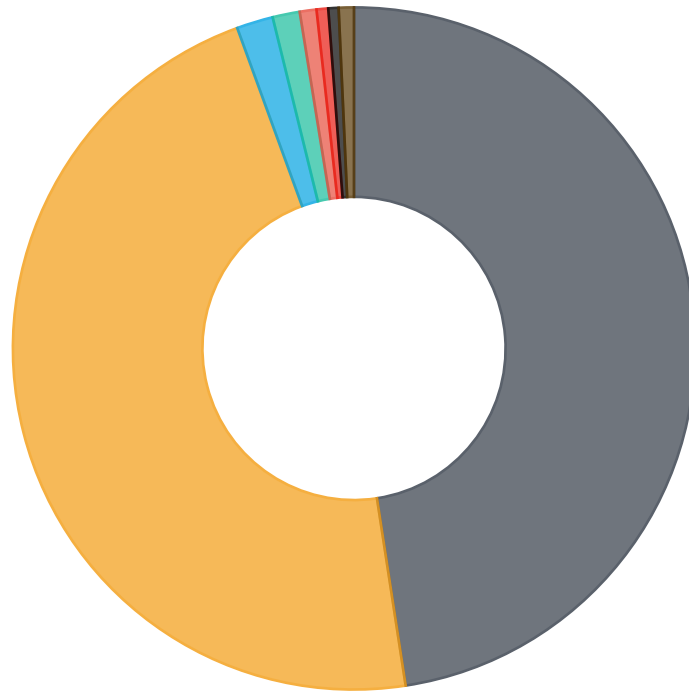
This figure shows how many total incidents were recorded with minipots. Please keep in mind that not each individual port scan is recorded. Given that a port scan is really fast action, we consider two incidents, small port scan and big port scan.

1 275 766 403

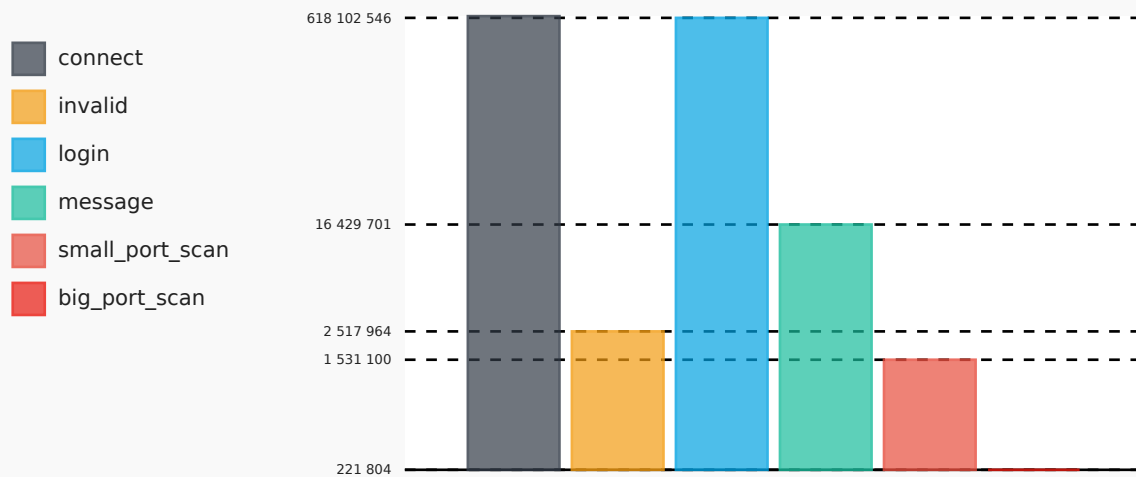
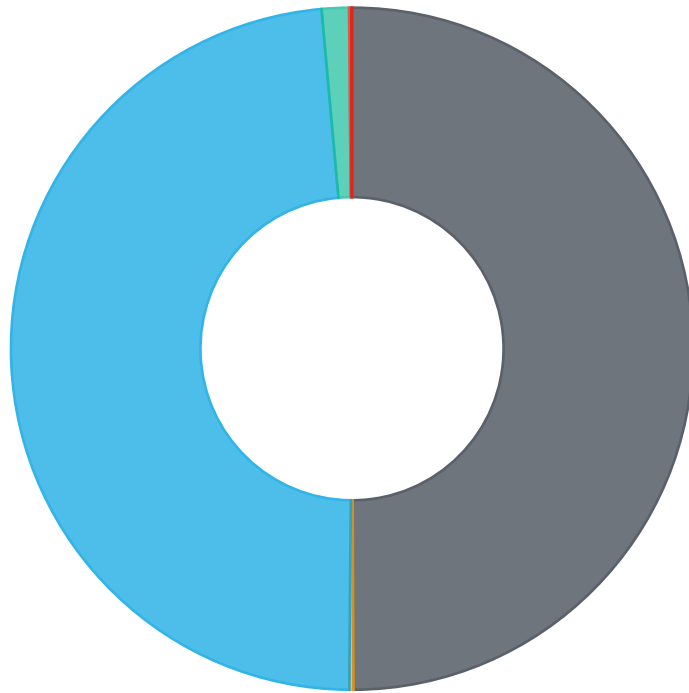
Incident Graphs

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.

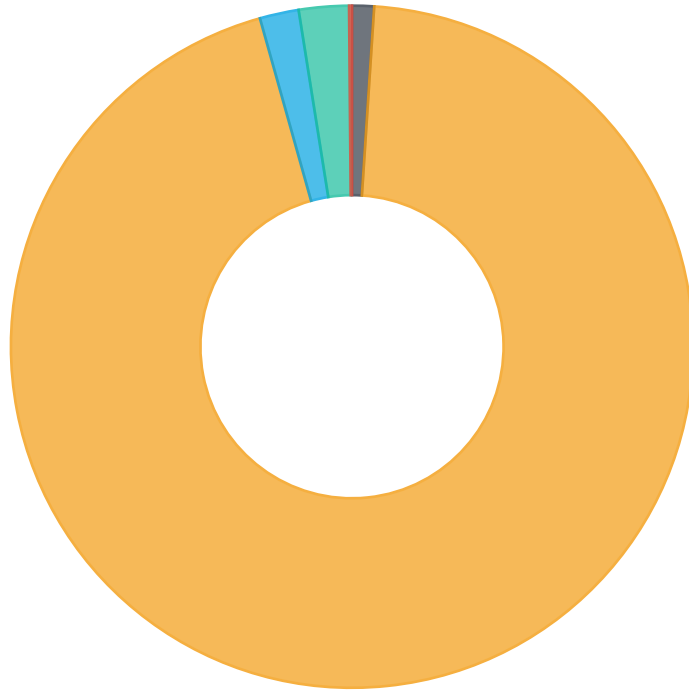
Minipot/Action Combined



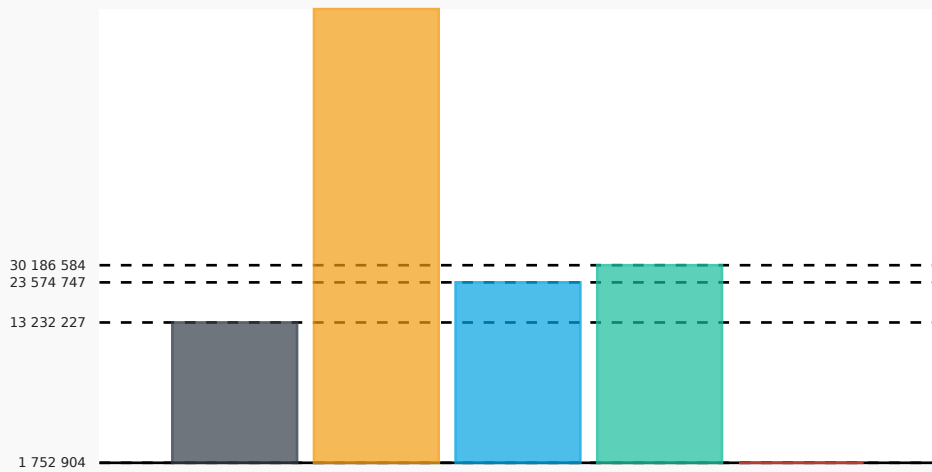
Attacker Action Pie Chart



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
333 561 779	minipot_smtp	80.94.95.181
9 315 555	minipot_http	92.118.236.114
960 165	minipot_telnet	81.17.18.98
380 482	minipot_ftp	62.217.187.51
9 645	fwlogs	94.102.61.39

Top Attackers

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

Count	IP	Country	Flag
333 561 779	80.94.95.181	RO	
319 946 886	45.129.14.99	RO	
298 918 851	77.90.185.59	DE	
192 013 679	212.70.149.70	BG	
9 315 555	92.118.236.114	US	
5 246 521	77.90.185.60	DE	
3 349 215	45.129.14.80	RO	
3 003 221	117.66.241.77	CN	
1 801 206	45.129.14.95	RO	
1 649 657	79.110.48.16	NL	
1 601 998	94.156.6.215	NL	
1 393 576	79.110.62.39	NL	
1 304 357	110.188.23.166	CN	
1 205 808	92.118.39.83	US	
1 083 718	85.31.45.41	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	4 779 185	4 943 130	3%	Transmission bit-torrent client
6881	UDP	2 509 462	2 824 791	13%	BitTorrent beginning of range of ports used most often
7881	UDP	806 852	980 353	22%	Quick Time Streaming Server (formerly)
51413	TCP	665 247	773 590	16%	Certificate Management over CMS Transmission bit-torrent client
11000	UDP	1 100 849	709 445	-36%	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.
6889	UDP	936 603	612 960	-35%	BitTorrent continuation of range of ports used most often
27032	UDP	399 306	528 435	32%	Steam (In-Home Streaming) Steam Client (Remote Play)
445	TCP	424 711	396 436	-7%	Microsoft-DS (Directory Services) Active Directory, Microsoft-DS (Directory Services) SMB
6881	TCP	276 482	355 504	29%	BitTorrent beginning of range of ports used most often
64541	UDP	386 881	324 234	-16%	Unassigned (IANA)
16881	UDP	171 903	321 786	87%	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
65458	UDP	170 704	310 389	82%	Unassigned (IANA)
33113	UDP	155	290 265	187 168%	Unassigned (IANA)
16881	TCP	118 946	273 881	130%	Synology NAS DSM download service
49001	UDP	19 997	257 899	1 190%	Far Cry Nuance Unity Service Discovery Protocol
23	TCP	271 999	248 367	-9%	Telnet protocol—unencrypted text communications

Port	Protocol	Previous	Last	Growth	Description
1024	UDP	195 376	184 776	-5%	Reserved
51000	UDP	149 572	178 279	19%	Unassigned (IANA)
1	UDP	160 895	162 077	1%	TCP Port Service Multiplexer (TCPMUX). Historic. Both TCP and UDP have been assigned to TCPMUX by IANA,
443	TCP	170 961	160 711	-6%	Hypertext Transfer Protocol Secure (HTTPS)HTTP/3 uses QUIC,
64541	TCP	198 719	157 416	-21%	Certificate Management over CMS
57017	UDP	46 286	143 026	209%	Unassigned (IANA)
62534	UDP	95	139 679	146 931%	Unassigned (IANA)
58187	UDP	193 166	137 948	-29%	Unassigned (IANA)
51412	UDP	80 363	137 780	71%	Unassigned (IANA)
10889	UDP	95 268	134 460	41%	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	94 515	132 070	40%	Unassigned (IANA)
30295	UDP	3 953	127 241	3 119%	Unassigned (IANA)
18979	UDP	84 496	117 234	39%	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.
51416	UDP	127 235	113 769	-11%	Unassigned (IANA)
65206	UDP	146 301	112 658	-23%	Dynamic and/or private ports
8080	TCP	133 091	108 815	-18%	Alternative port for HTTP. See also ports 80 and 8008. Apache Tomcat Atlassian JIRA applications
48804	UDP	82 142	106 676	30%	Unassigned (IANA)
62783	TCP	111 652	100 399	-10%	Certificate Management over CMS
32000	UDP	84 909	88 216	4%	Unassigned (IANA)
64644	UDP	61 670	86 847	41%	Unassigned (IANA)
49648	UDP	54 825	85 941	57%	Unassigned (IANA)
40227	UDP	247	85 180	34 386%	Unassigned (IANA)
6886	UDP	44 529	80 769	81%	BitTorrent beginning of range of ports used most often
64271	UDP	39 838	79 469	99%	Unassigned (IANA)
1433	TCP	84 497	76 795	-9%	Microsoft SQL Server database management system (MSSQL) server

Port	Protocol	Previous	Last	Growth	Description
21742	UDP	29 968	75 330	151%	Unassigned (IANA)
59492	UDP	133 335	74 400	-44%	Unassigned (IANA)
53	UDP	65 936	74 023	12%	Domain Name System (DNS)
6901	UDP	77 518	72 271	-7%	Windows Live Messenger (Voice) BitTorrent continuation of range of ports used most often
1	TCP	70 220	69 953	~0%	TCP Port Service Multiplexer (TCPMUX). Historic. Both TCP and UDP have been assigned to TCPMUX by IANA,
55859	UDP	180 617	69 904	-61%	Unassigned (IANA)
80	TCP	100 578	69 367	-31%	Hypertext Transfer Protocol (HTTP)HTTP/3 uses QUIC,
0	other	67 027	68 512	2%	Unassigned (IANA)
51056	UDP	118	68 115	57 625%	Unassigned (IANA)
22	TCP	58 811	67 530	15%	Secure Shell (SSH),file transfers (scp, sftp) and port forwarding
28116	UDP	145 470	67 292	-54%	Unassigned (IANA)
36080	UDP	55 424	67 191	21%	Unassigned (IANA)
60685	UDP	36 053	64 594	79%	Range from which Mosh – a remote-terminal application similar to SSH – typically assigns ports for ongoing sessions between Mosh servers and Mosh clients.
30303	UDP	111 836	62 659	-44%	Ethereum Client
9000	UDP	87 279	60 273	-31%	UDPCast
12000	UDP	82 119	60 218	-27%	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
7680	TCP	54 618	59 304	9%	Delivery Optimization for Windows 10
61289	UDP	51 680	58 814	14%	Unassigned (IANA)
39662	UDP	89	57 872	64 925%	Unassigned (IANA)
51765	UDP	35 775	57 811	62%	Unassigned (IANA)
56327	UDP	241	57 071	23 581%	Unassigned (IANA)
1030	UDP	5 562	56 406	914%	Unassigned (IANA)
8444	TCP	61 217	56 028	-8%	Bitmessage Chia
55555	UDP	28 896	55 115	91%	Unassigned (IANA)
57017	TCP	18 235	53 883	195%	Certificate Management over CMS

Port	Protocol	Previous	Last	Growth	Description
59127	UDP	321	52 874	16 372%	Unassigned (IANA)
6883	UDP	38 095	52 542	38%	BitTorrent beginning of range of ports used most often
61678	UDP	55 143	52 323	-5%	Unassigned (IANA)
2323	TCP	72 313	51 842	-28%	Unassigned (IANA)
24588	UDP	70 474	51 321	-27%	Unassigned (IANA)
57606	UDP	154	51 223	33 162%	Unassigned (IANA)
28757	UDP	444	50 473	11 268%	Unassigned (IANA)
63303	UDP	89	48 261	54 126%	Unassigned (IANA)
4444	UDP	60 719	46 498	-23%	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
9002	UDP	36 457	44 923	23%	Newforma Server comms
1900	UDP	8 246	44 732	442%	Simple Service Discovery Protocol (SSDP),UPnP devices
6890	UDP	39 232	44 008	12%	BitTorrent continuation of range of ports used most often
62938	UDP	111	43 774	39 336%	Unassigned (IANA)
31402	TCP	44 113	43 639	-1%	Unassigned (IANA)
21610	UDP	75	42 420	56 460%	Unassigned (IANA)
27033	UDP	7 645	42 096	451%	Steam (In-Home Streaming) Steam Client (Remote Play)
56575	UDP	88 906	41 802	-53%	Unassigned (IANA)
6882	UDP	74 447	41 659	-44%	BitTorrent beginning of range of ports used most often
51414	UDP	5 014	40 621	710%	Unassigned (IANA)
56650	UDP	4 657	40 563	771%	Unassigned (IANA)
46379	UDP	7 912	39 757	402%	Unassigned (IANA)
39841	UDP	751	39 692	5 185%	Unassigned (IANA)
65212	TCP	37 330	39 452	6%	Certificate Management over CMS
62882	UDP	22 170	39 160	77%	Unassigned (IANA)
39223	UDP	101	39 027	38 541%	Unassigned (IANA)
1032	UDP	894	38 046	4 156%	Unassigned (IANA)

Port	Protocol	Previous	Last	Growth	Description
5555	TCP	40 001	37 624	-6%	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.
8333	TCP	43 404	37 039	-15%	Bitcoin VMware VI Web Access via HTTPS
17801	UDP	173	35 202	20 248%	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.
81	TCP	45 937	34 163	-26%	TorPark onion routing
15915	UDP	81	34 045	41 931%	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.
28791	UDP	1 046	33 988	3 149%	Unassigned (IANA)
54636	UDP	24 543	33 571	37%	Unassigned (IANA)
23380	UDP	70	33 315	47 493%	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	2 005 357	47 031 867	2 245%
P@ssw0rd	3 429 609	20 685 884	503%
12345	974 990	15 586 716	1 499%
%users%	0	15 266 652	N/A
password	1 255 699	14 762 725	1 076%
p@ssw0rd	481 616	14 121 698	2 832%
111111	545 022	13 949 357	2 459%
1111	554 427	13 773 328	2 384%
11111	153 537	13 670 269	8 804%
1111111	136 278	13 347 924	9 695%
ei_123	0	3 192 018	N/A
admin_123	245 871	2 886 265	1 074%
t3mpp@ss	246 125	2 882 572	1 071%
root_123	246 218	2 874 140	1 067%
1qaz@wsx	245 844	2 738 649	1 014%
1234qwer!	245 920	2 735 649	1 012%
Qwer1234	246 143	2 675 151	987%
Server2000	246 278	2 426 828	885%
admin@123	2 103 807	2 411 818	15%
1qaz@WSX	599 852	2 347 938	291%
!QAZ1qaz	396 269	2 174 778	449%
1qaz!QAZ	2 375 876	2 168 295	-9%
!QAZ2wsx	415 425	2 157 857	419%
Passw0rd1	2 834 842	2 150 022	-24%
Admin2016	1 709 943	2 098 358	23%
P4ssw0rd	4 068 186	2 073 163	-49%
123qwe!@#	499 371	2 021 245	305%
P@\$w0rd	384 079	1 974 914	414%
Admin123!@#	316 077	1 967 335	522%
root@123	296 679	1 962 572	562%
p@ssw0rd1	402 894	1 961 386	387%
qwe123!@#	367 019	1 957 226	433%

Password	Previous	Last	Growth
admin123#	397 714	1 955 876	392%
root123!@#	295 798	1 955 466	561%
P@ssword	402 550	1 938 856	382%
huawei@123	396 443	1 931 589	387%
abcd@123	396 425	1 928 206	386%
abc123!	396 151	1 923 933	386%
P@ssw0rd1234	396 153	1 922 665	385%
Admin123456	397 623	1 921 847	383%
P@ssw0rd3	395 789	1 918 662	385%
Passw0rd1234	396 159	1 907 686	382%
P@55w0rd	395 956	1 904 891	381%
!@#qwe123	395 787	1 903 083	381%
123zxc!@#	395 636	1 902 723	381%
2wsx1qaz!	395 555	1 900 483	380%
2wsx#EDC	395 778	1 899 518	380%
tuidc@2016	395 755	1 898 234	380%
Password!	2 829 437	1 897 107	-33%
Changeme123	2 809 147	1 894 789	-33%
1QAZ2wsx3EDC	2 808 618	1 891 821	-33%
1Qaz@WSX3edc	2 816 986	1 888 535	-33%
!QAZ2wsx#EDC4rfv	2 806 176	1 887 493	-33%
Admin@12345	2 774 581	1 886 919	-32%
!@#QWEasd	2 734 621	1 884 502	-31%
123@Abc	2 823 657	1 882 731	-33%
admin@123456	2 701 270	1 880 031	-30%
asd@123	1 576 471	1 878 931	19%
Huawei@Admin	2 696 946	1 878 065	-30%
123asd!@#	2 832 917	1 875 492	-34%
123!@#QWE	2 690 284	1 875 330	-30%
Admin@1234567	2 678 868	1 874 205	-30%
HUAWEI_123	2 680 368	1 872 335	-30%
Admin@1234	2 671 224	1 872 245	-30%
P@\$word	2 917 295	1 870 510	-36%
1qaz2wsx!@#	2 815 502	1 864 856	-34%
Admin@123456789	2 609 900	1 864 693	-29%
!QAZxsw2#EDC	1 192 230	1 863 987	56%
!QAZ3edc	1 270 175	1 862 578	47%

Password	Previous	Last	Growth
abc123!@#	1 058 167	1 861 615	76%
abc@123	427 089	1 859 386	335%
!Q2w#E4r%T	1 748 209	1 858 802	6%
HuaWei@123456	2 677 147	1 858 245	-31%
!Q2w#E4r%T6y	2 635 497	1 854 274	-30%
!QAZxsw2	4 015 088	1 853 925	-54%
qwer1234!@#\$	1 687 091	1 852 501	10%
1qazXSW@	4 163 359	1 852 382	-56%
P4ssword	4 094 325	1 851 799	-55%
Admin2017	1 700 308	1 851 545	9%
Admin2015	1 953 603	1 850 239	-5%
!@#\$qwerASDF	1 682 999	1 849 689	10%
1Qaz@WSX3edc\$RFV	4 013 208	1 848 707	-54%
1Qaz@WSX#edc	1 683 047	1 845 341	10%
Admin2013	4 034 644	1 845 033	-54%
1q2w3e4r!@#\$	4 016 983	1 844 455	-54%
1qaz#EDC5tgb	1 687 715	1 844 403	9%
!qazxsw2@	1 689 261	1 844 279	9%
Password01!	1 866 333	1 840 861	-1%
!Q@W3e4r	1 683 423	1 832 639	9%
!QAZxsw23edc	1 686 152	1 825 856	8%
admin	998 545	1 479 587	48%
Stinger0	1 624 359	1 359 719	-16%
1234	1 205 954	1 256 151	4%
123	1 220 811	1 203 066	-1%
123123	944 015	1 030 507	9%
123456789	1 059 046	765 175	-28%
1234567	516 442	692 974	34%
Zz3AEcMM	0	654 435	N/A
12345678	1 201 581	654 370	-46%
Welcome1	256 919	620 929	142%



Most Used Passwords Wordcloud

