

Sentinel Report - 2023 August

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

Minipot attacks decreased by nearly a half from the preceding month in August. The subnet 46.148.40.0/24 members were not so active last month, and we can see addresses from other countries emerging at the top of the table. Notable mentions go to some European countries, namely Germany and Romania, who got back into the spotlight.

Thanks to the fact that there is consistently a lack of a bigger margin between telnet and HTTP attack counts, we can say that there were slightly more attacks regarding the HTTP protocol than telnet this month. When we compare all previous reports (and include this one, of course), we can state that big port scans are not that frequent. It looks like attackers are more often going after specific ports to exploit than doing a full-range sweep.

UDP port numbers 52666 and 24293 jumped to the top of the table out of nowhere. We were unable to find any information about what might be running on those ports; if you have any theories about what it is and why it might be interesting, let us know.

The *P@ssw0rd* mentioned in the previous report dropped significantly, but it does not make it any safer. Sequential passwords like last month's winner *1qazXSW@* can look safe but could be an open invitation for hackers. Do not use them; although they look random, sequences seem to be, according to our gathered data, much more popular than dictionary terms these days.

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.

80 934

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.

11 376

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?

3 657

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

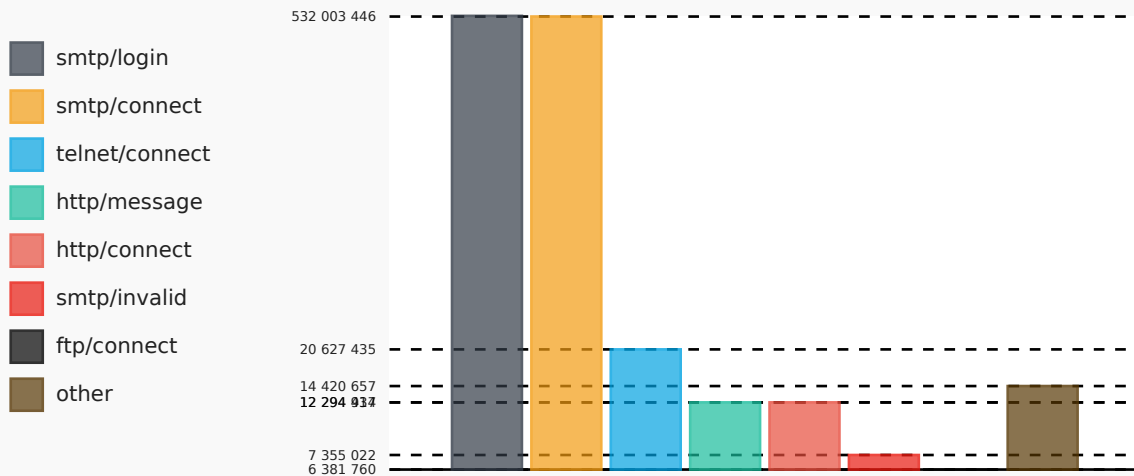
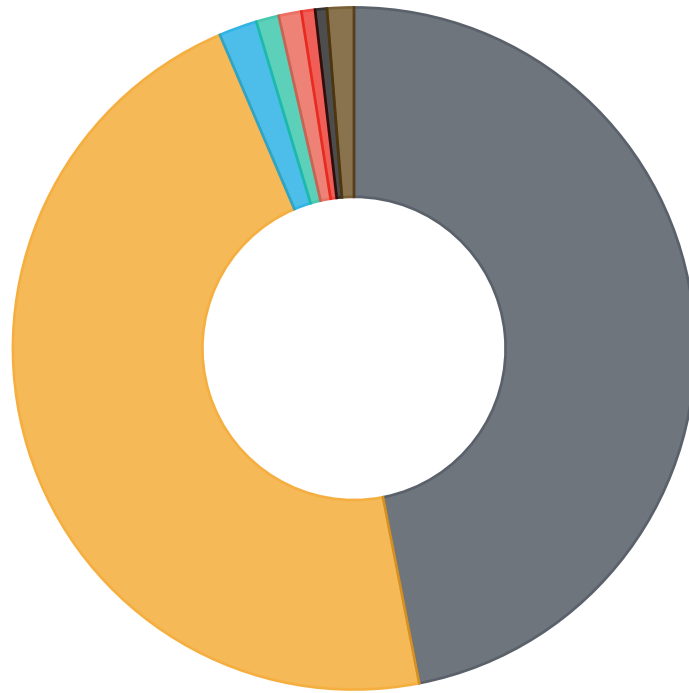
This figure shows how many total incidents were recorded with minipots. Please keep in mind that not each individual port scan is recorded. Given that port scan is really fast action, we consider two incidents, small port scan and big port scan.

1 104 016 882

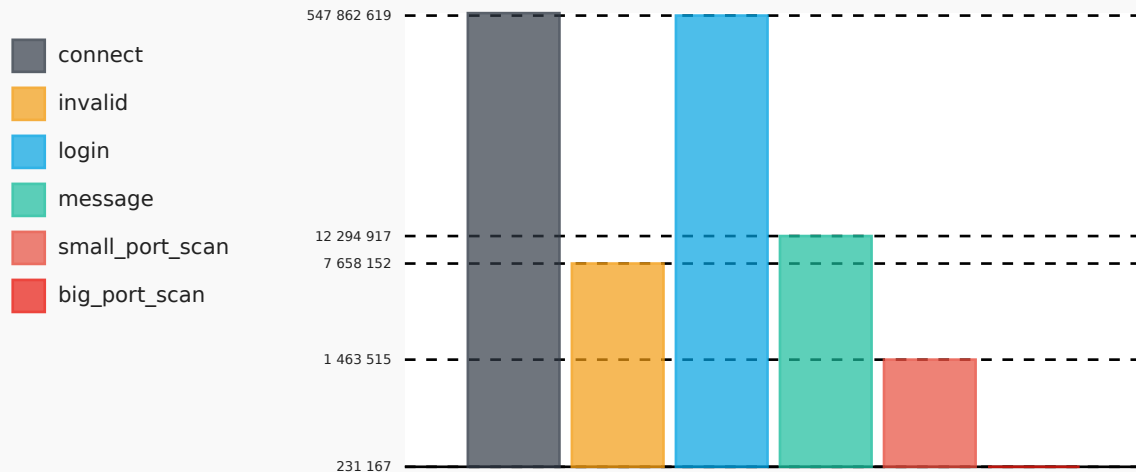
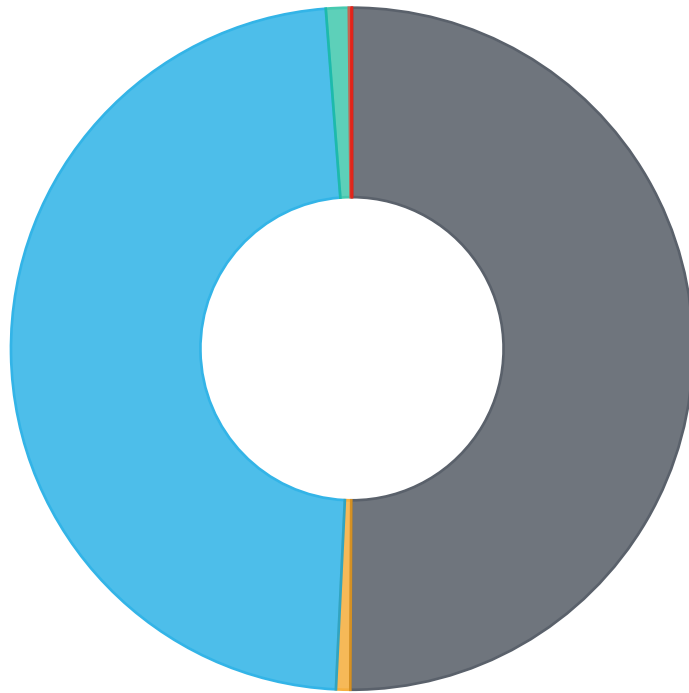
Incident Graphs

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.

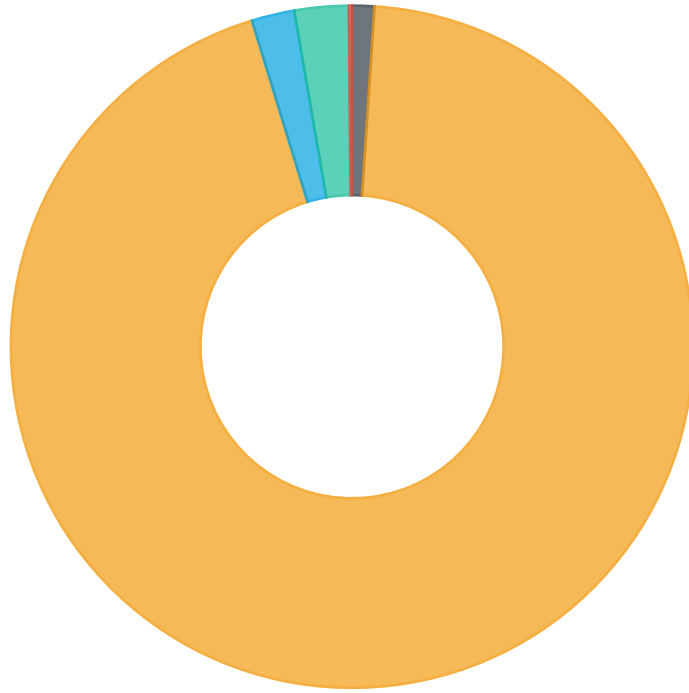
Minipot/Action Combined



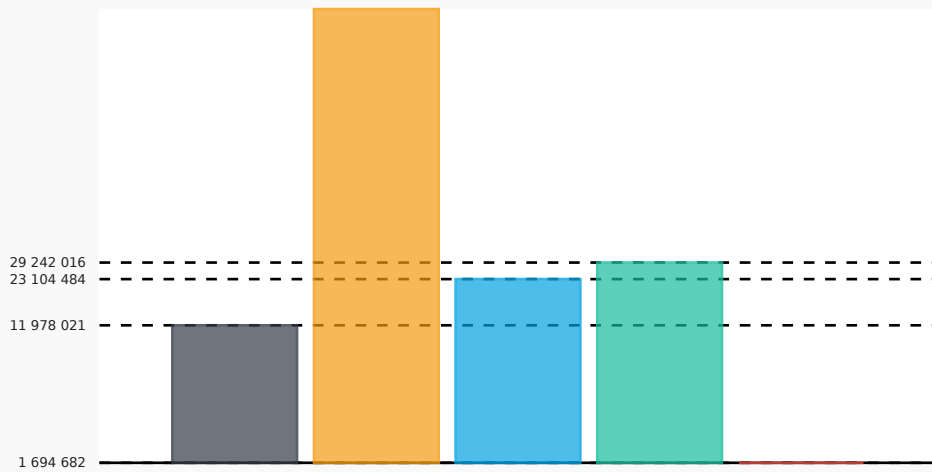
Attacker Action Pie Chart



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
372 018 459	minipot_smtp	80.94.95.184
959 128	minipot_http	31.7.60.114
709 964	minipot_telnet	31.7.60.114
350 682	minipot_ftp	62.217.187.51
10 123	fwlogs	80.66.83.165

Top Attackers

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

Count	IP	Country	Flag
372 018 459	80.94.95.184	RO	
242 548 958	77.90.185.18	DE	
150 971 364	45.129.14.31	RO	
113 369 828	77.90.185.60	DE	
103 537 747	45.129.14.99	RO	
8 486 571	103.149.12.207	VN	
3 416 797	194.59.204.33	DE	
2 020 581	46.148.40.61	IR	
1 991 772	46.148.40.63	IR	
1 892 004	46.148.40.64	IR	
1 806 643	46.148.40.62	IR	
1 669 092	31.7.60.114	CH	
1 455 909	58.208.84.245	CN	
1 382 369	82.223.114.243	ES	
1 310 344	181.40.91.90	PY	

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	4 809 613	4 779 185	-1%	Transmission bit-torrent client
6881	UDP	2 487 195	2 509 462	1%	BitTorrent beginning of range of ports used most often
11000	UDP	1 127 108	1 100 849	-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.
6889	UDP	547 261	936 603	71%	BitTorrent continuation of range of ports used most often
7881	UDP	396 370	806 852	104%	Quick Time Streaming Server (formerly)
51413	TCP	566 754	665 247	17%	Certificate Management over CMS Transmission bit-torrent client
445	TCP	416 389	424 711	2%	Microsoft-DS (Directory Services) Active Directory, Microsoft-DS (Directory Services) SMB
27032	UDP	421 941	399 306	-5%	Steam (In-Home Streaming) Steam Client (Remote Play)
64541	UDP	64 562	386 881	499%	Unassigned (IANA)
6881	TCP	246 898	276 482	12%	BitTorrent beginning of range of ports used most often
23	TCP	319 982	271 999	-15%	Telnet protocol—unencrypted text communications
52666	UDP	146	214 828	147 042%	Unassigned (IANA)
8621	UDP	125 495	200 473	60%	Unassigned (IANA)
64541	TCP	45 090	198 719	341%	Certificate Management over CMS
1024	UDP	176 595	195 376	11%	Reserved
24293	UDP	274	193 970	70 692%	Unassigned (IANA)
58187	UDP	72 987	193 166	165%	Unassigned (IANA)
55859	UDP	124 233	180 617	45%	Unassigned (IANA)

Port	Protocol	Previous	Last	Growth	Description
16881	UDP	283 789	171 903	-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. Synology NAS DSM download service
443	TCP	185 977	170 961	-8%	Hypertext Transfer Protocol Secure (HTTPS)HTTP/3 uses QUIC,
65458	UDP	56 009	170 704	205%	Unassigned (IANA)
1	UDP	145 491	160 895	11%	TCP Port Service Multiplexer (TCPMUX). Historic. Both TCP and UDP have been assigned to TCPMUX by IANA,
51000	UDP	141 589	149 572	6%	Unassigned (IANA)
65206	UDP	211 507	146 301	-31%	Dynamic and/or private ports
28116	UDP	307	145 470	47 284%	Unassigned (IANA)
46151	UDP	16 156	137 436	751%	Unassigned (IANA)
62747	UDP	7 529	137 108	1 721%	Unassigned (IANA)
59492	UDP	145 437	133 335	-8%	Unassigned (IANA)
8080	TCP	155 089	133 091	-14%	Alternative port for HTTP. See also ports 80 and 8008. Apache Tomcat Atlassian JIRA applications
49877	UDP	18 943	128 267	577%	Unassigned (IANA)
51416	UDP	143 917	127 235	-12%	Unassigned (IANA)
4010	UDP	108	126 608	117 130%	Unassigned (IANA)
16881	TCP	174 558	118 946	-32%	Synology NAS DSM download service
30303	UDP	106 513	111 836	5%	Ethereum Client
62783	TCP	60 306	111 652	85%	Certificate Management over CMS
24902	UDP	162 100	110 737	-32%	Unassigned (IANA)
1025	UDP	43 759	107 650	146%	Teradata database management system (Teradata) server
80	TCP	103 503	100 578	-3%	Hypertext Transfer Protocol (HTTP)HTTP/3 uses QUIC,
26845	UDP	80	98 359	122 849%	Unassigned (IANA)
10889	UDP	23 314	95 268	309%	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	94 329	94 515	~0%	Unassigned (IANA)

Port	Protocol	Previous	Last	Growth	Description
46151	TCP	9 578	92 168	862%	Unassigned (IANA)
56575	UDP	80 859	88 906	10%	Unassigned (IANA)
9000	UDP	64 649	87 279	35%	UDPCast
36178	UDP	411	86 417	20 926%	Unassigned (IANA)
32000	UDP	21 883	84 909	288%	Unassigned (IANA)
1433	TCP	84 553	84 497	~0%	Microsoft SQL Server database management system (MSSQL) server
18979	UDP	104 376	84 496	-19%	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	UDP	65 069	82 142	26%	Unassigned (IANA)
12000	UDP	81 776	82 119	~0%	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
37388	UDP	46 686	81 526	75%	Unassigned (IANA)
1028	UDP	84 968	81 271	-4%	IANA Reserved port
34343	UDP	117	81 166	69 273%	Unassigned (IANA)
51412	UDP	78 450	80 363	2%	Unassigned (IANA)
50188	UDP	101 974	78 838	-23%	Unassigned (IANA)
52869	TCP	56 751	78 828	39%	Certificate Management over CMS
6901	UDP	82 597	77 518	-6%	Windows Live Messenger (Voice) BitTorrent continuation of range of ports used most often
9006	UDP	52 749	76 950	46%	IANA Reserved port
6882	UDP	49 839	74 447	49%	BitTorrent beginning of range of ports used most often
2323	TCP	76 047	72 313	-5%	Unassigned (IANA)
12807	UDP	67	70 689	105 406%	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.
24588	UDP	13 738	70 474	413%	Unassigned (IANA)

Port	Protocol	Previous	Last	Growth	Description
1	TCP	60 190	70 220	17%	TCP Port Service Multiplexer (TCPMUX). Historic. Both TCP and UDP have been assigned to TCPMUX by IANA,
53882	UDP	286	69 139	24 074%	Unassigned (IANA)
0	other	70 669	67 027	-5%	Unassigned (IANA)
33867	UDP	90	66 756	74 073%	Unassigned (IANA)
47143	UDP	152 360	66 412	-56%	Unassigned (IANA)
53	UDP	73 026	65 936	-10%	Domain Name System (DNS)
40816	UDP	2 654	62 374	2 250%	Unassigned (IANA)
64644	UDP	5 133	61 670	1 101%	Unassigned (IANA)
8444	TCP	56 865	61 217	8%	Bitmessage Chia
4444	UDP	36 127	60 719	68%	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
30990	UDP	1 353	60 468	4 369%	Unassigned (IANA)
31849	UDP	93 882	59 811	-36%	Unassigned (IANA)
60731	UDP	744	58 813	7 805%	Range from which Mosh – a remote-terminal application similar to SSH – typically assigns ports for ongoing sessions between Mosh servers and Mosh clients.
22	TCP	55 578	58 811	6%	Secure Shell (SSH),file transfers (scp, sftp) and port forwarding
16574	UDP	254	58 561	22 956%	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.
36080	UDP	57 928	55 424	-4%	Unassigned (IANA)
61678	UDP	55 190	55 143	~0%	Unassigned (IANA)
49648	UDP	40 433	54 825	36%	Unassigned (IANA)
7680	TCP	56 847	54 618	-4%	Delivery Optimization for Windows 10
15875	UDP	123	51 909	42 102%	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.
61289	UDP	35 202	51 680	47%	Unassigned (IANA)

Port	Protocol	Previous	Last	Growth	Description
33346	UDP	154	51 160	33 121%	Unassigned (IANA)
1029	UDP	1 284	51 083	3 878%	Microsoft DCOM services
34360	UDP	3 697	49 370	1 235%	Unassigned (IANA)
33867	TCP	400	48 581	12 045%	Unassigned (IANA)
49168	UDP	42 621	48 367	13%	Unassigned (IANA)
57017	UDP	388	46 286	11 829%	Unassigned (IANA)
49168	TCP	38 755	46 052	19%	Certificate Management over CMS
81	TCP	45 678	45 937	1%	TorPark onion routing
6885	UDP	54 270	45 636	-16%	BitTorrent beginning of range of ports used most often
1027	UDP	66 899	44 747	-33%	Native IPv6 behind IPv4-to-IPv4 NAT Customer Premises Equipment (6a44)
6886	UDP	50 158	44 529	-11%	BitTorrent beginning of range of ports used most often
31402	TCP	52 572	44 113	-16%	Unassigned (IANA)
8333	TCP	40 966	43 404	6%	Bitcoin VMware VI Web Access via HTTPS
25268	UDP	85	42 486	49 884%	Unassigned (IANA)
6888	UDP	42 893	42 371	-1%	MUSE BitTorrent continuation of range of ports used most often
56197	UDP	147	41 032	27 813%	Unassigned (IANA)
25681	UDP	81	40 020	49 307%	SamsidParty Operational Ports

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
1qazXSW@	907 111	4 163 359	359%
P4ssword	911 041	4 094 325	349%
P4ssw0rd	909 237	4 068 186	347%
Admin2013	907 485	4 034 644	345%
1q2w3e4r!@#\$	911 841	4 016 983	341%
!QAZxsw2	912 026	4 015 088	340%
1Qaz@WSX3edc\$RFV	911 942	4 013 208	340%
P@ssw0rd	13 846 227	3 429 609	-75%
123456aA	192 836	3 101 805	1 509%
admin@2012	192 989	3 016 965	1 463%
admin_2012	192 747	2 981 714	1 447%
admin_2008	194 218	2 980 325	1 435%
admin_2015	195 133	2 979 944	1 427%
Test123	231 369	2 966 294	1 182%
admin_2016	196 350	2 951 648	1 403%
123abc!	197 525	2 947 280	1 392%
admin@2008	192 862	2 944 851	1 427%
C0mput3r	196 026	2 939 608	1 400%
1q2w3e4r!@	197 953	2 928 427	1 379%
P@\$sword	2 001 842	2 917 295	46%
www@123	197 465	2 899 753	1 368%
Aa123456	355 725	2 891 723	713%
1qaz2wsx!@	197 497	2 861 471	1 349%
Passw0rd1	2 092 535	2 834 842	35%
123asd!@#	2 118 535	2 832 917	34%
Password!	2 105 619	2 829 437	34%
123@Abc	2 105 298	2 823 657	34%
1Qaz@WSX3edc	2 099 290	2 816 986	34%
1qaz2wsx!@#	2 092 846	2 815 502	35%
Changeme123	2 095 422	2 809 147	34%
1QAZ2wsx3EDC	2 056 919	2 808 618	37%
!QAZ2wsx#EDC4rfv	2 093 588	2 806 176	34%

Password	Previous	Last	Growth
Admin@12345	2 101 110	2 774 581	32%
!@#QWEasd	2 100 408	2 734 621	30%
admin@123456	2 068 314	2 701 270	31%
Huawei@Admin	2 096 690	2 696 946	29%
123!@#QWE	2 097 636	2 690 284	28%
HUAWEI_123	2 152 183	2 680 368	25%
Admin@1234567	2 327 457	2 678 868	15%
HuaWei@123456	2 334 038	2 677 147	15%
Admin@1234	2 327 241	2 671 224	15%
!Q2w#E4r%T6y	2 265 050	2 635 497	16%
Admin@123456789	2 316 383	2 609 900	13%
1qaz!QAZ	2 372 677	2 375 876	-0%
admin@123	4 624 765	2 103 807	-55%
123456	60 116 631	2 005 357	-97%
Admin2015	912 613	1 953 603	114%
Password01!	2 504 034	1 866 333	-25%
P@ssw0rd123	890 605	1 767 750	98%
1qaz2wsx3edc4RFV	903 829	1 764 320	95%
Pa55word	892 429	1 762 879	98%
!@#QWEASDzxc	875 270	1 761 276	101%
P@ssw0rd!	873 713	1 758 217	101%
P4ssw0rd123	904 996	1 756 926	94%
Passw0rd@123	872 192	1 755 020	101%
Passw0rd123	875 531	1 754 475	100%
123QWEASDzxc	866 924	1 753 474	102%
1q@w#e\$r	864 852	1 751 695	103%
admin!@#123	864 003	1 749 722	103%
!Q2w#E4r%T	2 273 222	1 748 209	-23%
1qaz2wsx!QAZ@WSX	865 387	1 747 472	102%
N0th1n9	863 844	1 747 315	102%
Hua@wei123!@#	847 678	1 746 090	106%
HWServer2015	861 380	1 743 852	102%
HWServer2016	836 294	1 742 890	108%
HWServer201	864 245	1 739 140	101%
1qa@WS3ed	863 020	1 721 236	99%
Admin2016	897 462	1 709 943	91%
Admin2017	910 239	1 700 308	87%

Password	Previous	Last	Growth
!qazxsw2@	907 842	1 689 261	86%
1qaz#EDC5tgb	907 175	1 687 715	86%
qwer1234!@#\$	906 130	1 687 091	86%
!QAZxsw23edc	908 434	1 686 152	86%
!Q@W3e4r	906 565	1 683 423	86%
1Qaz@WSX#edc	908 271	1 683 047	85%
!@#\$qwerASDF	906 941	1 682 999	86%
!Q@W#E4r5t6y	906 096	1 679 353	85%
Pa\$\$w0rd	908 997	1 678 320	85%
!QAZ2was	901 463	1 677 319	86%
Admin!@#456	905 974	1 676 193	85%
4rfv\$RFV	904 613	1 672 395	85%
HWServer2011	860 123	1 672 050	94%
1Qazxsw23edc	904 837	1 670 085	85%
1q2w3e!Q@W#E	905 577	1 669 151	84%
Stinger0	193 043	1 624 359	741%
asd@123	3 309 608	1 576 471	-52%
!QAZ3edc	2 314 067	1 270 175	-45%
password	19 927 767	1 255 699	-94%
123	35 572 980	1 220 811	-97%
1234	18 697 731	1 205 954	-94%
12345678	18 845 648	1 201 581	-94%
Admin2012	861 476	1 198 524	39%
!QAZxsw2#EDC	2 302 493	1 192 230	-48%
123456789	19 811 669	1 059 046	-95%
abc123!@#	2 330 002	1 058 167	-55%
admin	9 368 593	998 545	-89%
12345	18 914 669	974 990	-95%
123123	4 695 870	944 015	-80%
123qwe	1 514 488	919 748	-39%
654321	1 531 646	909 873	-41%

