# Sentinel Report - 2023 May

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 overall count for total incidents dropped by 100 million. Sounds like a lot, but given the number of attacks we recorded (1.6 billion), it is just less than 10% decrease. Still significant, but not as shocking as hundred millions sounds. The results for minipot traps have not changed significantly from previous month, it seems the attackers are pretty consistent in regards to what services interest them the most.
With Port Trends we see that the continuation of Torrent domination got the whole top of the table. We did not add any other port specification.
In regards to passwords we observed the biggest jump with password *Changeme123*. The password *1QAZ2wxx* brings another interesting pattern. From Romania and Bulgaria came passwords that start with random alphanumeric characters and end with the pattern *@123*. Again as with interesting passwords from last month, the span was limited to few days, someone started and after two days the passwords had stopped.

## 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.

**82 253**

#### 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.

**10 584**

## 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?

**3 360**

#### 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**

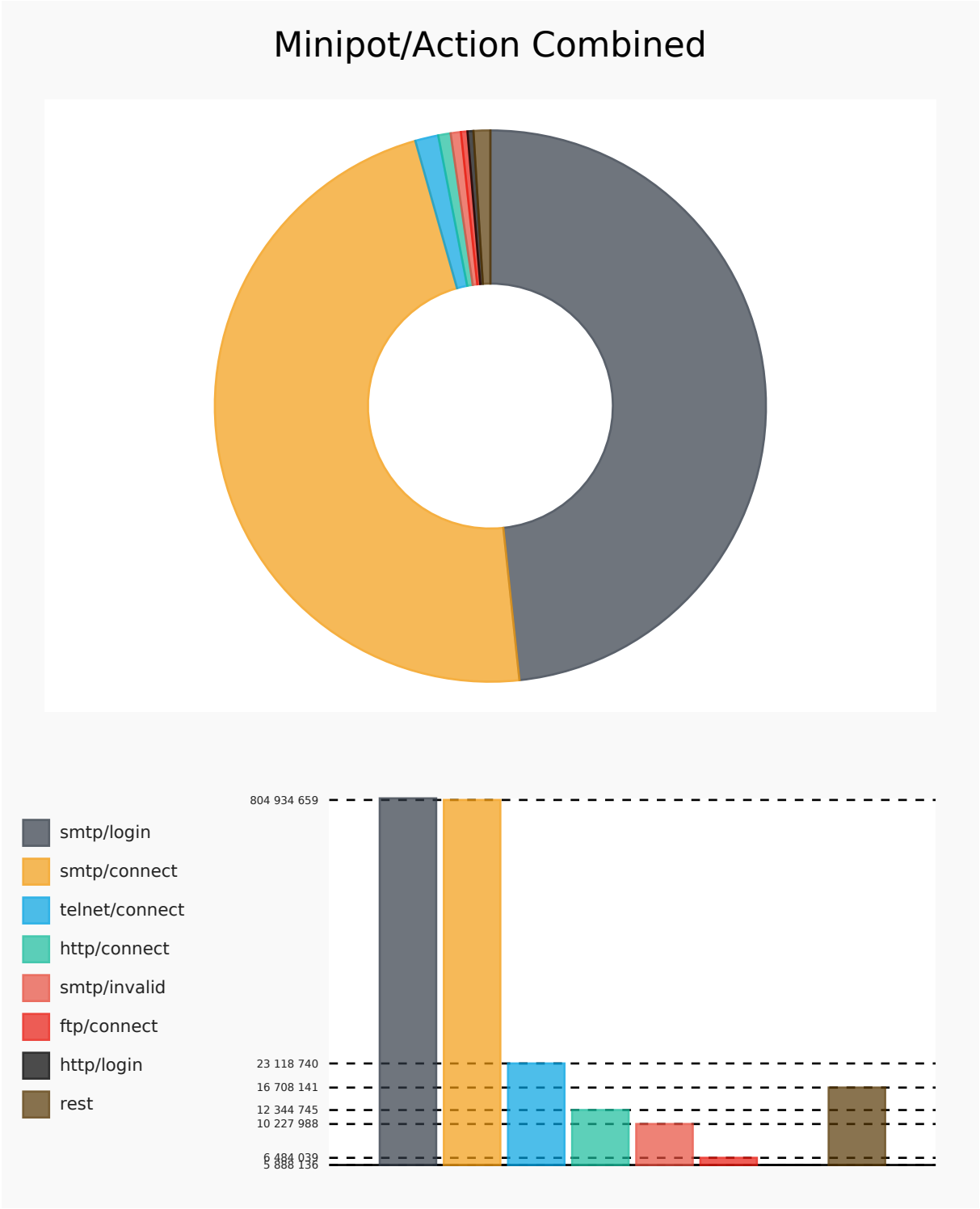
#### Total Minipot Incidents

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.

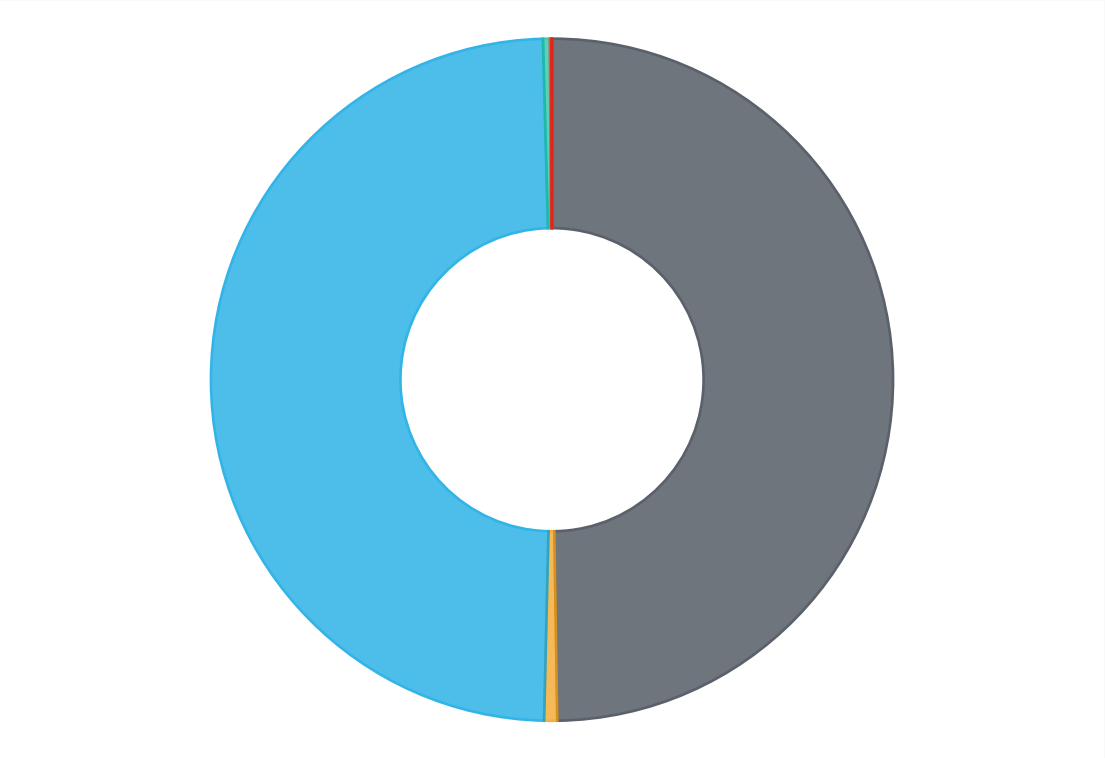
**1 647 257 787**

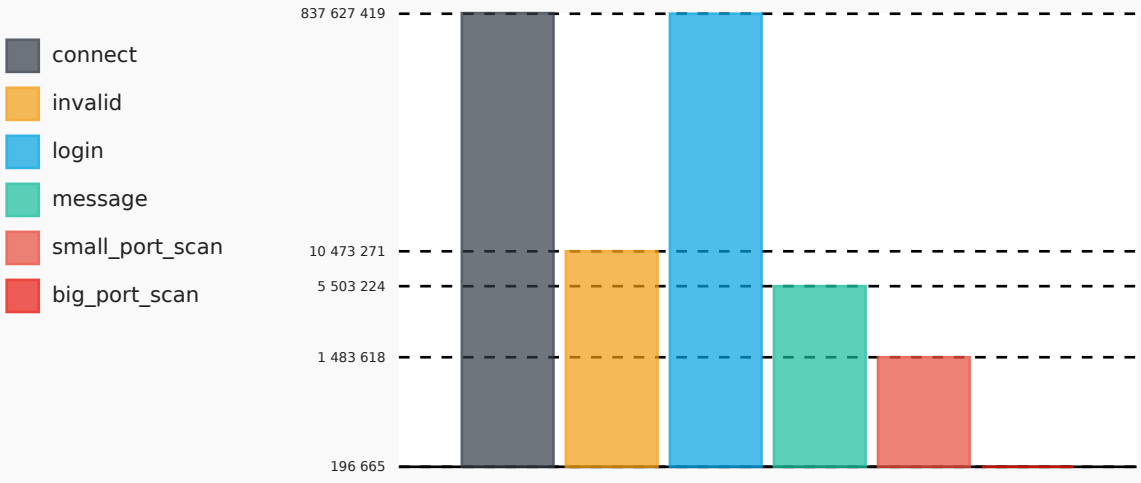
## Incident Graphs

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.

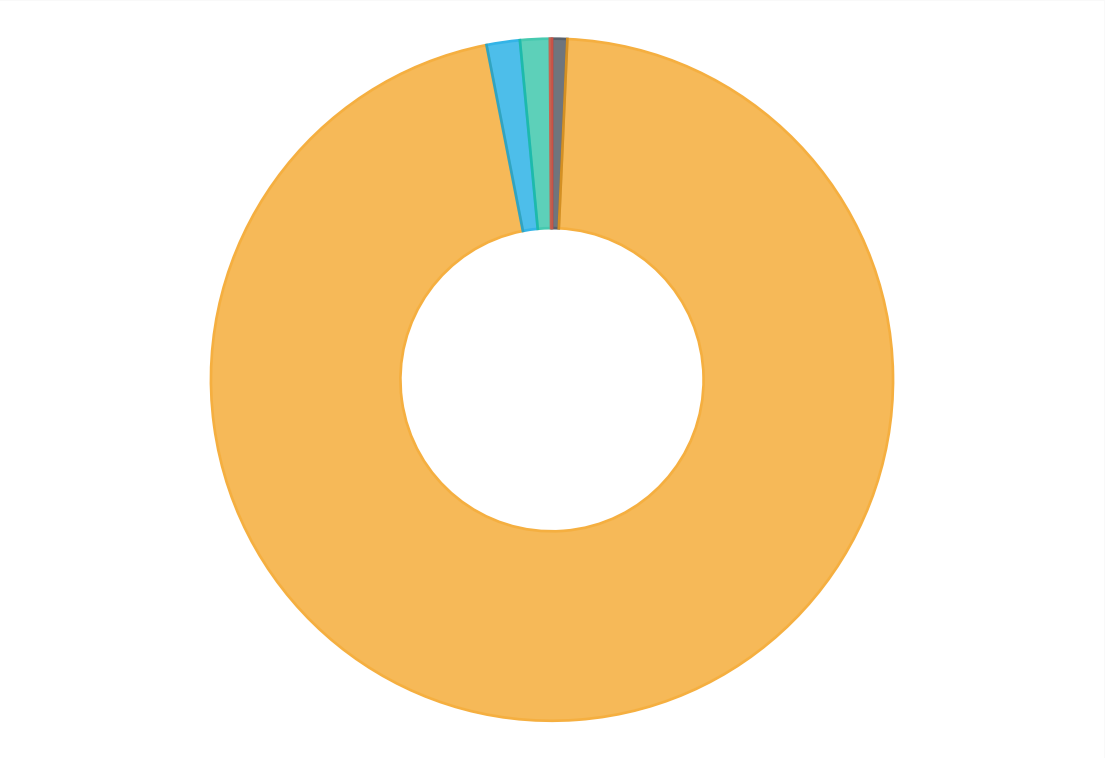


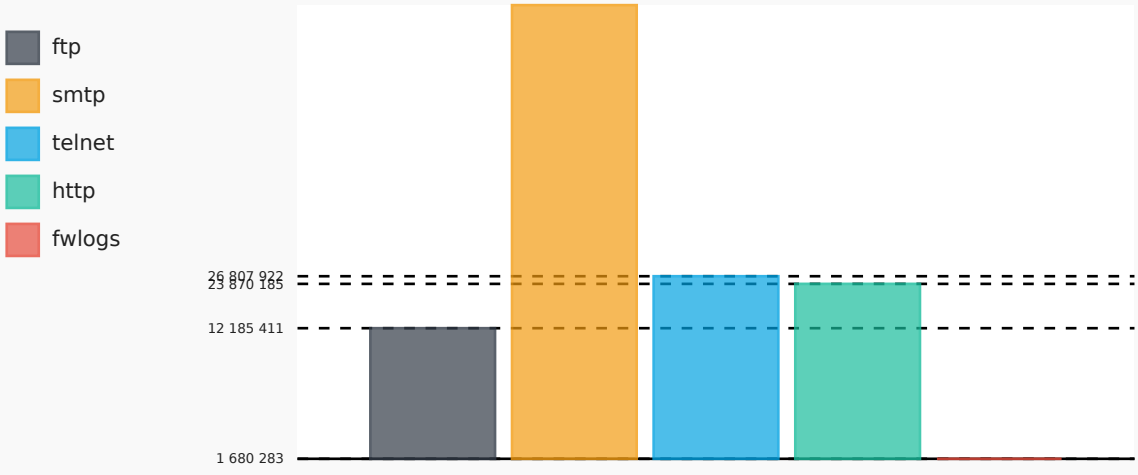
# Attacker Action Pie Chart





# Minipot Target Pie Chart





## 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 | 4 054 248 | 4 459 092 | 10% | Transmission bit-torrent client |
| 6881 | UDP | 2 701 332 | 3 908 727 | 45% | BitTorrent beginning of range of ports used most often |
| 6889 | UDP | 669 660 | 606 582 | –9% | BitTorrent continuation of range of ports used most often |
| 51413 | TCP | 437 293 | 589 783 | 35% | Certificate Management over CMS \| Transmission bit-torrent client |
| 62319 | UDP | 11 538 | 462 575 | 3 909% | N/A |
| 445 | TCP | 438 903 | 455 402 | 4% | Microsoft-DS (Directory Services) Active Directory, \| Microsoft-DS (Directory Services) SMB |
| 6881 | TCP | 309 451 | 435 819 | 41% | BitTorrent beginning of range of ports used most often |
| 27032 | UDP | 655 507 | 398 380 | –39% | Steam (In-Home Streaming) \| Steam Client (Remote Play) |
| 39717 | UDP | 186 | 295 084 | 158 547% | N/A |
| 47627 | UDP | 252 | 261 097 | 103 510% | N/A |
| 51000 | UDP | 225 802 | 250 946 | 11% | N/A |
| 23 | TCP | 222 885 | 245 253 | 10% | Telnet protocol—unencrypted text communications |
| 48804 | UDP | 211 348 | 234 268 | 11% | N/A |
| 39717 | TCP | 344 | 219 782 | 63 790% | N/A |
| 21130 | UDP | 231 452 | 208 146 | –10% | N/A |
| 55859 | UDP | 252 596 | 205 870 | –18% | N/A |
| 40115 | UDP | 210 | 196 050 | 93 257% | N/A |
| 16881 | UDP | 160 724 | 190 517 | 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. \| Synology NAS DSM download service |
| 1024 | UDP | 400 903 | 188 105 | –53% | Reserved |
| 24902 | UDP | 109 579 | 187 453 | 71% | N/A |
| 7881 | UDP | 98 261 | 177 859 | 81% | Quick Time Streaming Server (formerly) |

| Port | Protocol | Previous | Last | Growth | Description |
|---|---|---|---|---|---|
| 65206 | UDP | 152 664 | 176 678 | 16% | Dynamic and/or private ports |
| 1 | UDP | 253 284 | 171 638 | –32% | TCP Port Service Multiplexer (TCPMUX). Historic. Both TCP and UDP have been assigned to TCPMUX by IANA, |
| 47143 | UDP | 1 292 | 155 053 | 11 901% | N/A |
| 59492 | UDP | 159 190 | 153 076 | –4% | N/A |
| 38533 | UDP | 198 | 145 449 | 73 359% | N/A |
| 8080 | TCP | 148 387 | 137 767 | –7% | Alternative port for HTTP. See also ports 80 and 8008. \| Apache Tomcat \| Atlassian JIRA applications |
| 16881 | TCP | 92 913 | 133 465 | 44% | Synology NAS DSM download service |
| 40115 | TCP | 355 | 132 261 | 37 157% | Brothers in Arms Online |
| 1025 | UDP | 54 763 | 129 886 | 137% | Teradata database management system (Teradata) server |
| 17292 | UDP | 12 914 | 126 435 | 879% | 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. |
| 49001 | UDP | 118 961 | 121 659 | 2% | Far Cry \| Nuance Unity Service Discovery Protocol |
| 443 | TCP | 187 154 | 120 822 | –35% | Hypertext Transfer Protocol Secure (HTTPS)HTTP/3 uses QUIC, |
| 64134 | UDP | 73 | 119 372 | 163 423% | N/A |
| 54728 | UDP | 80 235 | 117 889 | 47% | N/A |
| 54728 | TCP | 67 761 | 110 255 | 63% | Certificate Management over CMS |
| 36080 | UDP | 52 580 | 108 485 | 106% | N/A |
| 57017 | UDP | 18 597 | 104 049 | 459% | N/A |
| 27032 | TCP | 204 410 | 103 443 | –49% | N/A |
| 21742 | UDP | 16 677 | 99 879 | 499% | N/A |
| 38533 | TCP | 598 | 98 854 | 16 431% | N/A |
| 1029 | UDP | 1 405 | 97 541 | 6 842% | Microsoft DCOM services |
| 9006 | UDP | 89 082 | 93 094 | 5% | IANA Reserved port |
| 30620 | UDP | 51 712 | 92 255 | 78% | N/A |
| 6901 | UDP | 36 647 | 92 137 | 151% | Windows Live Messenger (Voice) \| BitTorrent continuation of range of ports used most often |
| 1433 | TCP | 91 875 | 90 661 | –1% | Microsoft SQL Server database management system (MSSQL) server |

| Port | Protocol | Previous | Last | Growth | Description |
|---|---|---|---|---|---|
| 2323 | TCP | 86 585 | 82 928 | –4% | N/A |
| 52806 | UDP | 72 885 | 82 816 | 14% | N/A |
| 10047 | UDP | 170 | 81 816 | 48 027% | 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. |
| 4444 | UDP | 73 363 | 79 778 | 9% | 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 |
| 39841 | UDP | 98 354 | 79 250 | –19% | N/A |
| 46579 | UDP | 159 | 79 185 | 49 702% | N/A |
| 60466 | UDP | 85 491 | 76 996 | –10% | Range from which Mosh – a remote-terminal application similar to SSH – typically assigns ports for ongoing sessions between Mosh servers and Mosh clients. |
| 55956 | UDP | 9 311 | 76 810 | 725% | N/A |
| 1 | TCP | 104 843 | 76 589 | –27% | TCP Port Service Multiplexer (TCPMUX). Historic. Both TCP and UDP have been assigned to TCPMUX by IANA, |
| 30303 | UDP | 96 808 | 75 666 | –22% | Ethereum Client |
| 2457 | UDP | 93 567 | 73 795 | –21% | N/A |
| 9000 | UDP | 76 473 | 73 438 | –4% | UDPCast |
| 5345 | UDP | 270 | 71 879 | 26 522% | League of Legends, a multiplayer online battle arena video game |
| 5740 | UDP | 73 904 | 71 208 | –4% | N/A |
| 60023 | TCP | 68 310 | 69 623 | 2% | Certificate Management over CMS |
| 6882 | UDP | 95 440 | 68 723 | –28% | BitTorrent beginning of range of ports used most often |
| 50363 | UDP | 254 | 67 894 | 26 630% | N/A |
| 31402 | TCP | 63 732 | 66 038 | 4% | N/A |
| 9627 | UDP | 220 | 65 511 | 29 678% | N/A |
| 51412 | UDP | 53 948 | 63 058 | 17% | N/A |
| 33095 | UDP | 169 | 61 463 | 36 269% | N/A |
| 49530 | UDP | 66 025 | 61 353 | –7% | N/A |
| 22 | TCP | 62 737 | 60 301 | –4% | Secure Shell (SSH),file transfers (scp, sftp) and port forwarding |

| Port | Protocol | Previous | Last | Growth | Description |
|---|---|---|---|---|---|
| 53 | UDP | 57 309 | 59 913 | 5% | Domain Name System (DNS) |
| 23446 | UDP | 140 | 58 563 | 41 731% | N/A |
| 80 | TCP | 57 953 | 58 313 | 1% | Hypertext Transfer Protocol (HTTP)HTTP/3 uses QUIC, |
| 65230 | UDP | 119 | 57 805 | 48 476% | N/A |
| 34779 | UDP | 4 176 | 55 960 | 1 240% | N/A |
| 49689 | UDP | 186 | 55 889 | 29 948% | N/A |
| 32844 | UDP | 473 | 55 674 | 11 670% | World of Tanks |
| 2387 | UDP | 22 | 54 794 | 248 964% | N/A |
| 50490 | UDP | 9 574 | 54 187 | 466% | N/A |
| 37215 | TCP | 78 936 | 54 044 | –32% | Huawei HG532 routers |
| 18975 | UDP | 112 | 53 852 | 47 982% | 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. |
| 37388 | UDP | 60 189 | 52 688 | –12% | N/A |
| 4000 | UDP | 20 512 | 51 905 | 153% | Diablo II game |
| 6883 | UDP | 40 531 | 51 486 | 27% | BitTorrent beginning of range of ports used most often |
| 63868 | UDP | 12 050 | 51 337 | 326% | N/A |
| 1027 | UDP | 24 159 | 50 685 | 110% | Native IPv6 behind IPv4-to-IPv4 NAT Customer Premises Equipment (6a44) |
| 10889 | UDP | 49 322 | 50 642 | 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. |
| 1028 | UDP | 35 761 | 49 221 | 38% | IANA Reserved port |
| 31781 | UDP | 29 847 | 49 034 | 64% | N/A |
| 81 | TCP | 52 103 | 48 244 | –7% | TorPark onion routing |
| 64398 | UDP | 38 403 | 47 467 | 24% | N/A |
| 6888 | UDP | 31 233 | 47 208 | 51% | MUSE \| BitTorrent continuation of range of ports used most often |
| 8333 | TCP | 40 345 | 47 023 | 17% | Bitcoin \| VMware VI Web Access via HTTPS |
| 7680 | TCP | 55 225 | 46 734 | –15% | Delivery Optimization for Windows 10 |
| 33095 | TCP | 335 | 46 574 | 13 803% | N/A |
| 6367 | UDP | 24 399 | 45 516 | 87% | N/A |

| Port | Protocol | Previous | Last | Growth | Description |
|---|---|---|---|---|---|
| 22266 | UDP | 1 121 | 44 953 | 3 910% | N/A |
| 38057 | UDP | 269 | 44 692 | 16 514% | N/A |
| 12661 | UDP | 656 | 44 445 | 6 675% | 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. |
| 24528 | UDP | 97 | 43 836 | 45 092% | N/A |
| 9627 | TCP | 867 | 43 756 | 4 947% | N/A |

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 |
|---|---|---|---|
| 1234 | 32 703 041 | 49 324 496 | 51% |
| 123456789 | 20 268 515 | 48 252 306 | 138% |
| 123456 | 65 992 722 | 39 735 552 | –40% |
| 12345 | 35 959 111 | 29 022 015 | –19% |
| 1234567890 | 1 116 284 | 23 337 819 | 1 991% |
| password | 28 198 804 | 21 483 481 | –24% |
| 1qaz!QAZ | 1 217 659 | 15 187 676 | 1 147% |
| 123 | 23 696 953 | 10 890 644 | –54% |
| 12345678 | 35 161 121 | 9 425 958 | –73% |
| Changeme123 | 16 | 9 407 393 | 58 796 106% |
| abc123 | 1 866 936 | 4 806 072 | 157% |
| P@ssw0rd | 2 290 241 | 4 791 407 | 109% |
| Admin123456 | 1 259 | 2 715 781 | 215 609% |
| Admin2013 | 1 268 | 2 551 284 | 201 105% |
| 1QAZ2wxx | 0 | 2 532 169 | N/A |
| Admin2016 | 6 627 | 2 510 306 | 37 780% |
| Admin2015 | 6 611 | 2 485 790 | 37 501% |
| 1qaz@WSX | 35 042 869 | 1 929 700 | –94% |
| P@$$w0rd123 | 5 009 520 | 1 689 455 | –66% |
| 1 | 1 335 235 | 1 682 727 | 26% |
| admin | 2 134 964 | 1 681 259 | –21% |
| Aa123456 | 1 246 835 | 1 663 091 | 33% |
| qwerty | 1 544 186 | 1 600 590 | 4% |
| 123123 | 1 042 029 | 1 565 584 | 50% |
| 111111 | 1 330 174 | 1 232 327 | –7% |
| 1q2w3e4r | 1 192 561 | 1 230 197 | 3% |
| 1qaz2wsx | 17 603 993 | 1 110 332 | –94% |
| 123qwe | 1 179 155 | 1 102 466 | –7% |
| abc123456 | 1 170 877 | 1 091 037 | –7% |
| 654321 | 1 155 523 | 1 073 172 | –7% |
| qwerty123 | 1 119 591 | 1 023 440 | –9% |
| 1q2w3e | 2 687 889 | 1 020 016 | –62% |

TURRIS

| Password | Previous | Last | Growth |
|---|---|---|---|
| pass123 | 1 107 996 | 1 019 508 | –8% |
| qwertyuiop | 1 070 842 | 1 016 253 | –5% |
| asdfgh | 1 064 918 | 1 010 226 | –5% |
| p@ssw0rd | 134 646 | 907 709 | 574% |
| Password1 | 1 453 660 | 849 649 | –42% |
| 1234567 | 4 127 879 | 828 192 | –80% |
| user | 641 294 | 754 186 | 18% |
| root | 617 108 | 716 651 | 16% |
| P@ssword | 19 696 771 | 711 824 | –96% |
| admin@123 | 472 514 | 669 217 | 42% |
| passwd123 | 209 708 | 621 809 | 197% |
| test | 487 772 | 612 432 | 26% |
| %null% | 161 010 | 611 858 | 280% |
| admin123 | 568 728 | 549 886 | –3% |
| 123qwe!@# | 294 889 | 545 329 | 85% |
| scan | 385 616 | 494 271 | 28% |
| p@ssword | 400 553 | 483 106 | 21% |
| passwd | 375 891 | 476 887 | 27% |
| 1111 | 494 888 | 475 713 | –4% |
| abc | 384 580 | 469 783 | 22% |
| P@ssword1 | 351 108 | 467 864 | 33% |
| !QAZ2wsx | 393 006 | 466 378 | 19% |
| | 343 372 | 430 140 | 25% |
| Admin2017 | 6 728 | 418 165 | 6 115% |
| abc@123 | 38 136 | 416 402 | 992% |
| Admin123 | 401 571 | 373 755 | –7% |
| 123qweASD | 195 804 | 354 090 | 81% |
| Qwerty123 | 399 644 | 351 271 | –12% |
| 123456aA | 9 181 179 | 343 078 | –96% |
| abcd1234 | 400 018 | 340 660 | –15% |
| passw0rd | 388 574 | 339 127 | –13% |
| 123321 | 341 861 | 335 651 | –2% |
| ! | 461 780 | 325 884 | –29% |
| qwe123 | 407 491 | 325 455 | –20% |
| 1qazxsw2 | 1 140 862 | 323 111 | –72% |
| qq123456 | 209 565 | 317 994 | 52% |
| 111 | 256 350 | 300 161 | 17% |

| Password | Previous | Last | Growth |
|---|---|---|---|
| 888888 | 129 781 | 281 348 | 117% |
| p@ssw0rd1 | 3 119 | 270 596 | 8 576% |
| P@$$w0rd | 29 247 | 270 030 | 823% |
| abcd@123 | 3 891 | 268 083 | 6 790% |
| root@123 | 10 390 | 267 240 | 2 472% |
| !QAZ1qaz | 26 152 | 266 091 | 917% |
| qwe123!@# | 23 110 | 263 723 | 1 041% |
| admin123# | 1 463 | 263 166 | 17 888% |
| Admin123!@# | 1 358 | 263 158 | 19 278% |
| root123!@# | 22 | 261 665 | 1 189 286% |
| !QAZxsw2 | 3 952 | 261 129 | 6 508% |
| abc123! | 24 136 | 260 540 | 979% |
| huawei@123 | 18 | 256 549 | 1 425 172% |
| P@ssw0rd1234 | 25 840 | 255 725 | 890% |
| adminHW | 345 915 | 249 472 | –28% |
| f7q1kgv9x@123 | 0 | 240 183 | N/A |
| 620715S7iPs9@123 | 0 | 234 639 | N/A |
| 98hfE8GP@123 | 0 | 233 535 | N/A |
| ■ | 33 292 | 220 512 | 562% |
| 666666 | 201 686 | 213 208 | 6% |
| Y4lHTYDp0zF@123 | 0 | 188 318 | N/A |
| 0 | 92 416 | 179 827 | 95% |
| pass | 196 039 | 172 231 | –12% |
| Password01! | 25 639 | 162 958 | 536% |
| Admin@123 | 32 532 | 162 272 | 399% |
| Passw0rd | 49 058 | 157 357 | 221% |
| info | 114 900 | 157 083 | 37% |
| Welcome@123 | 190 492 | 156 523 | –18% |
| 159753 | 398 687 | 154 775 | –61% |
| Abcd1234 | 41 880 | 152 447 | 264% |
| Passw0rd1 | 32 456 | 151 399 | 366% |

## Most Used Passwords Wordcloud