# Sentinel Report - January 2023

This document is the monthly report from the Turris Sentinel 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 monthly 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

In January, we encountered slightly more attackers than in December. But overall, behavior stays the same. The number of attackers per device and victims per attacker didn't change much. Looking back at our first report, we also had about the same amount of victims per attacker but more attackers per device. The trend for the last three months is to target about 20 Turris devices on average if you are an attacker.
We see a rising number of attempts on BitTorrent in port scans, but those might be just clients misconfigured. The first relevant port that gained popularity is Samba, aka Microsoft file sharing. No surprise there; that is quite a logical service to target. More interesting is the popularity of port 1035, which has been used in the past by various trojans. That might suggest that there is a new derivate of those spreading around.
In passwords, we see a continuing trend of randomly looking passwords. After the last report, we investigated those further, and they are all attacks on SMTP, and they try multiple random passwords. Majority of those come from one IP segment - from one Iranian ISP. There are also a few extra IPs from around the world. But based on the IP allocations, those belong to various hosting providers, so the primary source of those attempts is Iran, with bounces via various hosting services worldwide.

## 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.

**85 747**

#### 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.

**10 862**

## Incident Statistics

In the previous section, we described some globalized views on attackers this month. Now let's drill down into more details. How dangerous was it to be online this month?

#### 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 month?

**3 683**

**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 attacker tried to attack on average.

**20**

## Port Trends

This section shows monthly trends in port scans for port-protocol combinations. 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 |
|---|---|---|---|---|---|
| 6881 | UDP | 1 765 408 | 3 021 685 | 71% | BitTorrent beginning of range of ports used most often |
| 51413 | UDP | 2 187 664 | 2 687 364 | 23% | N/A |
| 6889 | UDP | 554 057 | 644 139 | 16% | BitTorrent continuation of range of ports used most often |
| 27032 | UDP | 460 683 | 451 247 | –2% | Steam (In-Home Streaming) |
| 7881 | UDP | 371 969 | 450 975 | 21% | N/A |
| 445 | TCP | 296 093 | 378 736 | 28% | Microsoft-DS (Directory Services) Active Directory, \| Microsoft-DS (Directory Services) SMB |
| 51413 | TCP | 332 979 | 333 875 | 0.27% | Certificate Management over CMS |
| 64541 | UDP | 177 587 | 260 024 | 46% | N/A |
| 1024 | UDP | 164 085 | 236 620 | 44% | Reserved |
| 1035 | UDP | 6 098 | 210 628 | 3 354% | N/A |
| 51000 | UDP | 88 596 | 206 070 | 133% | N/A |
| 64541 | TCP | 63 991 | 188 904 | 195% | Certificate Management over CMS |
| 6881 | TCP | 110 802 | 186 896 | 69% | BitTorrent beginning of range of ports used most often |
| 23 | TCP | 118 796 | 168 138 | 42% | Telnet protocol—unencrypted text communications |
| 1 | UDP | 94 795 | 161 349 | 70% | TCP Port Service Multiplexer (TCPMUX). Historic. Both TCP and UDP have been assigned to TCPMUX by IANA, |
| 29047 | UDP | 60 | 159 140 | 265 133% | N/A |
| 56736 | UDP | 38 123 | 155 567 | 308% | N/A |

| Port | Protocol | Previous | Last | Growth | Description |
|---|---|---|---|---|---|
| 443 | TCP | 95 188 | 143 860 | 51% | Hypertext Transfer Protocol Secure (HTTPS)HTTP/3 uses QUIC, |
| 47514 | UDP | 108 358 | 141 286 | 30% | N/A |
| 16881 | UDP | 36 483 | 122 689 | 236% | 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 | 89 803 | 116 592 | 30% | Alternative port for HTTP. See also ports 80 and 8008. \| Apache Tomcat \| Atlassian JIRA applications |
| 6886 | UDP | 26 577 | 116 528 | 338% | BitTorrent beginning of range of ports used most often |
| 2457 | UDP | 82 222 | 112 181 | 36% | N/A |
| 27032 | TCP | 98 041 | 110 160 | 12% | N/A |
| 7477 | UDP | 20 | 108 044 | 540 120% | N/A |
| 21742 | UDP | 30 424 | 106 680 | 251% | N/A |
| 5555 | TCP | 77 305 | 105 910 | 37% | 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 |
| 60731 | UDP | 112 563 | 105 392 | –6% | Range from which Mosh – a remote-terminal application similar to SSH – typically assigns ports for ongoing sessions between Mosh servers and Mosh clients. |
| 49001 | UDP | 40 773 | 105 028 | 158% | N/A |
| 16881 | TCP | 21 306 | 95 854 | 350% | N/A |
| 1892 | UDP | 43 283 | 89 362 | 106% | N/A |
| 6882 | UDP | 142 724 | 88 935 | –38% | BitTorrent beginning of range of ports used most often |
| 59492 | UDP | 1 872 | 83 590 | 4 365% | N/A |
| 55555 | UDP | 72 790 | 80 730 | 11% | N/A |
| 51412 | UDP | 18 758 | 78 634 | 319% | N/A |
| 1 | TCP | 32 384 | 78 515 | 142% | TCP Port Service Multiplexer (TCPMUX). Historic. Both TCP and UDP have been assigned to TCPMUX by IANA, |

| Port | Protocol | Previous | Last | Growth | Description |
|---|---|---|---|---|---|
| 64716 | UDP | 39 | 78 290 | 200 644% | N/A |
| 23197 | UDP | 49 | 75 255 | 153 482% | N/A |
| 55859 | UDP | 1 678 | 72 972 | 4 249% | N/A |
| 61345 | UDP | 20 621 | 71 880 | 249% | N/A |
| 24588 | UDP | 58 069 | 69 616 | 20% | N/A |
| 6901 | UDP | 29 800 | 68 557 | 130% | Windows Live Messenger (Voice) \| BitTorrent continuation of range of ports used most often |
| 62734 | UDP | 49 400 | 68 110 | 38% | N/A |
| 1433 | TCP | 55 296 | 66 263 | 20% | Microsoft SQL Server database management system (MSSQL) server |
| 22 | TCP | 30 602 | 65 941 | 115% | Secure Shell (SSH),file transfers (scp, sftp) and port forwarding |
| 13651 | UDP | 40 | 63 306 | 158 165% | 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. |
| 6888 | UDP | 20 184 | 62 112 | 208% | MUSE \| BitTorrent continuation of range of ports used most often |
| 2323 | TCP | 34 951 | 62 105 | 78% | N/A |
| 62882 | UDP | 116 512 | 62 050 | –47% | N/A |
| 56424 | UDP | 100 | 61 621 | 61 521% | N/A |
| 30303 | UDP | 42 198 | 60 951 | 44% | N/A |
| 43076 | UDP | 98 615 | 59 526 | –40% | N/A |
| 60023 | TCP | 26 754 | 57 533 | 115% | Certificate Management over CMS |
| 9091 | UDP | 32 565 | 56 629 | 74% | Openfire Administration Console (SSL Secured) \| Transmission (BitTorrent client) Web Interface |
| 1539 | UDP | 9 535 | 55 362 | 481% | N/A |
| 80 | TCP | 34 459 | 54 355 | 58% | Hypertext Transfer Protocol (HTTP)HTTP/3 uses QUIC, |
| 1025 | TCP | 12 447 | 54 155 | 335% | Teradata database management system (Teradata) server |
| 12701 | UDP | 44 551 | 52 821 | 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. |
| 62319 | UDP | 57 | 51 610 | 90 444% | N/A |

| Port | Protocol | Previous | Last | Growth | Description |
|---|---|---|---|---|---|
| 4444 | UDP | 37 242 | 50 534 | 36% | 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 \| OpenOCD (Telnet) \| I2P HTTP/S proxy |
| 1026 | UDP | 55 586 | 50 330 | –9% | N/A |
| 48803 | UDP | 1 431 | 50 187 | 3 407% | N/A |
| 1024 | TCP | 4 742 | 48 159 | 916% | Reserved |
| 11516 | UDP | 53 | 47 915 | 90 306% | 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. |
| 7332 | UDP | 12 | 47 885 | 398 942% | N/A |
| 37388 | UDP | 10 307 | 46 527 | 351% | N/A |
| 42018 | UDP | 43 | 46 346 | 107 681% | N/A |
| 53 | UDP | 62 214 | 46 085 | –26% | Domain Name System (DNS) |
| 54728 | UDP | 32 099 | 45 641 | 42% | N/A |
| 40318 | UDP | 11 872 | 45 567 | 284% | N/A |
| 9006 | UDP | 36 591 | 44 524 | 22% | Tomcat in standalone mode |
| 31402 | TCP | 26 549 | 43 664 | 64% | N/A |
| 21336 | UDP | 27 824 | 42 918 | 54% | N/A |
| 13188 | UDP | 165 | 42 240 | 25 500% | 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. |
| 32016 | UDP | 44 828 | 42 139 | –6% | N/A |
| 7676 | TCP | 6 932 | 40 290 | 481% | N/A |
| 81 | TCP | 34 783 | 39 661 | 14% | TorPark onion routing |
| 1030 | UDP | 939 | 39 584 | 4 116% | N/A |
| 32862 | UDP | 9 768 | 39 310 | 302% | N/A |
| 2222 | TCP | 9 928 | 39 032 | 293% | EtherNet/IP implicit messaging for IO data \| DirectAdmin Access \| ESET Remote administrator |

| Port | Protocol | Previous | Last | Growth | Description |
|---|---|---|---|---|---|
| 14981 | UDP | 44 | 38 599 | 87 625% | 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. |
| 15593 | UDP | 68 | 38 439 | 56 428% | 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. |
| 57017 | UDP | 108 951 | 38 419 | –65% | N/A |
| 9091 | TCP | 26 853 | 37 427 | 39% | Openfire Administration Console (SSL Secured) \| Transmission (BitTorrent client) Web Interface |
| 39841 | UDP | 28 945 | 37 422 | 29% | N/A |
| 52786 | UDP | 89 | 37 245 | 41 748% | N/A |
| 7680 | TCP | 28 389 | 37 142 | 31% | Delivery Optimization for Windows 10 |
| 16018 | UDP | 41 | 37 098 | 90 383% | 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. |
| 1034 | UDP | 120 354 | 36 951 | –69% | N/A |
| 59622 | UDP | 15 899 | 36 938 | 132% | N/A |
| 1031 | UDP | 693 | 35 965 | 5 090% | N/A |
| 59144 | UDP | 77 | 35 752 | 46 331% | N/A |
| 1033 | UDP | 4 963 | 35 697 | 619% | N/A |
| 3813 | UDP | 82 | 35 177 | 42 799% | N/A |
| 50319 | UDP | 17 933 | 34 955 | 95% | N/A |
| 48804 | UDP | 20 404 | 34 606 | 70% | N/A |
| 3687 | UDP | 52 | 34 456 | 66 162% | N/A |
| 27015 | UDP | 2 604 | 33 473 | 1 185% | Steam (game client traffic) \| GoldSrc and Source engine dedicated server port \| Unturned, a survival game \| Steam (matchmaking and HLTV) \| Steam (downloads) |
| 54728 | TCP | 32 818 | 33 387 | 2% | Certificate Management over CMS |
| 6890 | UDP | 31 462 | 33 291 | 6% | BitTorrent continuation of range of ports used most often |

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 month in comparison to the month before. The data are ordered by count last month, and the last column contains the difference against the previous month 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 Month | Last Month | Growth |
|---|---|---|---|
| 123456 | 275 673 | 189 767 | –31% |
| 12345 | 297 788 | 182 080 | –39% |
| test | 319 359 | 134 384 | –58% |
| 1234 | 231 878 | 115 828 | –50% |
| 1111 | 25 257 | 96 860 | 283% |
| L9BTvj | 0 | 94 303 | N/A |
| F7Nd1c0c | 0 | 94 160 | N/A |
| y5hVk2z9WJ | 0 | 84 126 | N/A |
| K06z4G | 0 | 83 409 | N/A |
| r3q196nbs | 0 | 83 385 | N/A |
| 34Y5HYf2AwLy | 0 | 83 299 | N/A |
| 723B4Rv | 0 | 83 287 | N/A |
| 1 | 89 466 | 82 597 | –8% |
| 5cU3Fq | 0 | 79 715 | N/A |
| 123456789 | 201 728 | 78 397 | –61% |
| 123 | 227 748 | 75 722 | –67% |
| 000000 | 2 074 | 71 576 | 3 351% |
| 48v7G1idBSen | 0 | 68 406 | N/A |
| kwdfj3 | 0 | 68 399 | N/A |
| 2ugj1Ys | 0 | 68 347 | N/A |
| Mhl94r7 | 0 | 68 236 | N/A |
| RbJnyv37ML | 0 | 66 511 | N/A |
| ye95158 | 0 | 66 415 | N/A |
| gh8xw76 | 0 | 66 395 | N/A |
| GhXFGm | 0 | 66 055 | N/A |
| clhHx55C | 0 | 65 995 | N/A |
| 1kRBQ | 0 | 65 588 | N/A |
| Uj0Vhu62 | 0 | 65 510 | N/A |
| vpP96124 | 0 | 65 497 | N/A |
| eX93JCZf90 | 0 | 65 469 | N/A |
| nSyT8x | 0 | 65 452 | N/A |
| Ir2l8k | 0 | 64 928 | N/A |

TURRIS

| Password | Previous Month | Last Month | Growth |
|---|---|---|---|
| mg0nSM | 0 | 64 808 | N/A |
| 6ikLmE8cw | 0 | 64 609 | N/A |
| XYcJp8Q1 | 0 | 62 606 | N/A |
| MgO2V | 0 | 62 459 | N/A |
| 3aw7a2 | 0 | 61 556 | N/A |
| 1234567890 | 151 412 | 59 988 | –60% |
| 8Tcu6zl2 | 0 | 59 076 | N/A |
| 8V1lfH | 0 | 57 026 | N/A |
| 5WrYW3sA | 0 | 52 427 | N/A |
| BYkc19dCd | 0 | 52 355 | N/A |
| EwTzrQrmKD14 | 61 923 | 48 623 | –21% |
| Bqko5TaS5 | 56 472 | 48 602 | –14% |
| ANW5HTaz8 | 64 963 | 48 566 | –25% |
| b8iGkZvevX56 | 68 613 | 48 523 | –29% |
| KaBMGeJwP2 | 0 | 48 375 | N/A |
| s8V79 | 0 | 48 329 | N/A |
| ZX0kmM | 43 874 | 48 311 | 10% |
| D8aFL | 62 232 | 48 297 | –22% |
| 0h8GZaaY | 64 497 | 48 286 | –25% |
| 2p1uilHR1zry | 24 276 | 48 231 | 99% |
| iD0M187 | 61 028 | 48 196 | –21% |
| 9V0U8kZ6 | 0 | 47 249 | N/A |
| 9mV5R | 0 | 47 081 | N/A |
| dzO9O447 | 0 | 47 058 | N/A |
| sf6Hv89z | 0 | 47 050 | N/A |
| nm0nv | 0 | 47 032 | N/A |
| Upivmc9YAdA | 0 | 47 022 | N/A |
| 5TO4i65k47Z1 | 0 | 46 910 | N/A |
| sX897SR2l0R0hl | 0 | 46 842 | N/A |
| 3XE6ug3Wtv | 0 | 46 822 | N/A |
| SFT9DfA | 0 | 46 446 | N/A |
| P84Pq8 | 0 | 46 380 | N/A |
| u9nMu197B | 0 | 46 276 | N/A |
| l9omB2v | 0 | 46 257 | N/A |
| 81uZaUv | 59 878 | 46 202 | –23% |
| 0PQY3 | 0 | 46 139 | N/A |
| s7t8Dx2 | 0 | 46 134 | N/A |

| Password | Previous Month | Last Month | Growth |
|---|---|---|---|
| l1P4Od3w | 0 | 46 094 | N/A |
| 57gLCz4bP | 69 209 | 46 085 | –33% |
| Bp3Jh312eM7 | 0 | 46 077 | N/A |
| jHa0SpD9 | 0 | 46 065 | N/A |
| 0UfsA | 0 | 46 058 | N/A |
| 29vf6ydPV | 0 | 46 049 | N/A |
| 0C2viC0xfx | 0 | 46 045 | N/A |
| eFwRS89xu | 0 | 46 019 | N/A |
| PjZ9ewMSHo | 0 | 45 983 | N/A |
| rA9xDjD47cdY4a | 33 453 | 45 980 | 37% |
| 9707OA5I6Co | 0 | 45 946 | N/A |
| kclfFEU | 0 | 45 943 | N/A |
| 33JdNZ548xk | 66 141 | 45 838 | –31% |
| efk9qrSPP | 0 | 45 827 | N/A |
| b48Cav72IZ | 0 | 45 698 | N/A |
| Ajp1D15c7L1u | 0 | 45 661 | N/A |
| ODvAS7V49K | 0 | 45 498 | N/A |
| QqCkC1T8O9 | 42 202 | 45 390 | 8% |
| 3ReliMatt | 0 | 45 375 | N/A |
| rwzdb8yzN | 67 733 | 45 357 | –33% |
| KM2cw5k6ogJ | 0 | 45 291 | N/A |
| qws5DU6Bg | 0 | 45 214 | N/A |
| 6mjf1 | 0 | 45 187 | N/A |
| IOJr6W4 | 0 | 45 186 | N/A |
| 8070c5d2 | 0 | 45 180 | N/A |
| 96Zw0p6K4m | 0 | 45 160 | N/A |
| 0p6QPO0vYz | 0 | 45 114 | N/A |
| rE1rmxp | 0 | 45 108 | N/A |
| 6i3d942 | 0 | 44 916 | N/A |
| ud8ZLg8 | 0 | 44 873 | N/A |
| 4T4IYgvE | 0 | 44 707 | N/A |

## Most Used Passwords Wordcloud