Sentinel Report - November 2022

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

November 2022 report brings You a very unusual set of passwords. A very popular password seems to be **mx#** on ten single-digit variations. This might suggest raising interest in gaining access to the mail exchange servers, so beware if you are running some of those. Simple password attacks might not be the only reason the mailservers are targets. The use of numbered 123... passwords appears to have declined between October and November. In spite of this fact, passwords ***123456*** and ***123456789*** are still on top.

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.

78 818

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.

10 017

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?

4 211

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.

21

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
51413	UDP	69 038	65 451	–5%	N/A
445	TCP	25 800	32 554	26%	Microsoft-DS (Directory Services) Active Directory, | Microsoft-DS (Directory Services) SMB
62882	UDP	64	31 095	48 486%	N/A
55555	UDP	37 423	26 033	–30%	N/A
443	TCP	15 645	16 326	4%	Hypertext Transfer Protocol Secure (HTTPS)HTTP/3 uses QUIC,
8828	UDP	0	11 995	0.00%	N/A
23	TCP	14 849	11 400	–23%	Telnet protocol—unencrypted text communications
39115	UDP	5 537	11 149	101%	N/A
1433	TCP	9 340	10 924	17%	Microsoft SQL Server database management system (MSSQL) server
2323	TCP	13 338	10 851	–19%	N/A
8080	TCP	10 682	10 600	–1%	Alternative port for HTTP. See also ports 80 and 8008. | Apache Tomcat | Atlassian JIRA applications
21336	UDP	2	9 873	493 550%	N/A
27032	UDP	20 100	9 407	–53%	Steam (In-Home Streaming)
5555	TCP	8 115	8 248	2%	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
7881	UDP	32	6 041	18 778%	N/A
5353	UDP	6 209	5 410	–13%	League of Legends, a multiplayer online battle arena video game | Multicast DNS (mDNS)
60345	UDP	0	5 389	0.00%	Range from which Mosh – a remote-terminal application similar to SSH – typically assigns ports for ongoing sessions between Mosh servers and Mosh clients.

Port	Protocol	Previous	Last	Growth	Description
81	TCP	4 831	5 366	11%	TorPark onion routing
6379	TCP	5 316	4 934	–7%	Redis key-value data store
6881	UDP	12 342	4 926	–60%	BitTorrent beginning of range of ports used most often
8443	TCP	4 565	4 366	–4%	SW Soft Plesk Control Panel | Apache Tomcat SSL | Promise WebPAM SSL | iCal over SSL | MineOs WebUi
3306	TCP	2 589	4 098	58%	MySQL database system
37215	TCP	5 018	4 082	–19%	N/A
8000	TCP	4 309	3 895	–10%	Commonly used for Internet radio streams such as SHOUTcastIcecastiTunes Radio | DynamoDB Local | Django Development Webserver | Python 3 http.server
49160	TCP	66	3 884	5 785%	Certificate Management over CMS | Palo Alto Networks' Panorama.
21336	TCP	9	3 859	42 778%	N/A
8888	TCP	4 143	3 820	–8%	HyperVM over HTTPS | Freenet web UI (localhost only) | Default for IPythonJupyter | MAMP
49160	UDP	0	3 715	0.00%	Palo Alto Networks' Panorama.
27032	TCP	6 081	3 569	–41%	N/A
6881	TCP	2 025	3 545	75%	BitTorrent beginning of range of ports used most often
3389	TCP	3 138	3 522	12%	Microsoft Terminal Server (RDP) officially registered as Windows Based Terminal (WBT)
8081	TCP	3 085	3 391	10%	Sun Proxy Admin Service
22	TCP	4 479	3 269	–27%	Secure Shell (SSH),file transfers (scp, sftp) and port forwarding
5432	TCP	2 835	3 236	14%	PostgreSQL
9200	TCP	2 881	3 005	4%	Elasticsearch
5678	UDP	3 073	2 940	–4%	N/A
2375	TCP	3 167	2 904	–8%	Docker REST API (plain)
123	UDP	2 114	2 806	33%	Network Time Protocol (NTP), used for time synchronization
7443	TCP	3 324	2 778	–16%	N/A
39115	TCP	1 026	2 765	169%	N/A
139	TCP	2 620	2 666	2%	NetBIOS Session Service
80	TCP	2 874	2 579	–10%	Hypertext Transfer Protocol (HTTP)HTTP/3 uses QUIC,

Port	Protocol	Previous	Last	Growth	Description
9000	TCP	2 448	2 385	–3%	SonarQube Web Server | ClickHouse default port | DBGp | SqueezeCenter web server & streaming | UDPCast | Play Framework web server | Hadoop NameNode default port | PHP-FPM default port | QBittorrent's embedded torrent tracker default port
8090	TCP	2 034	2 382	17%	Atlassian Confluence | Coral Content Distribution Network (legacy; 80 and 8080 now supported) | Matrix identity server
27017	TCP	2 472	2 363	–4%	Unturned, a survival game | Steam (downloads) | MongoDB daemon process (mongod) and routing service (mongos)
8181	TCP	2 090	2 248	8%	N/A
51413	TCP	5 353	2 247	–58%	Certificate Management over CMS
57000	UDP	2	2 221	110 950%	N/A
2222	TCP	2 100	2 214	5%	EtherNet/IP implicit messaging for IO data | DirectAdmin Access | ESET Remote administrator
8088	TCP	1 795	2 141	19%	Asterisk management access via HTTP
88	TCP	1 885	2 082	10%	Kerberos
7547	TCP	1 993	2 039	2%	CPE WAN Management Protocol (CWMP) Technical Report 069
5060	UDP	2 187	2 031	–7%	League of Legends, a multiplayer online battle arena video game | Session Initiation Protocol (SIP)
4443	TCP	2 063	2 006	–3%	N/A
3000	TCP	2 547	1 938	–24%	Ruby on Rails development default | Meteor development default | Resilio Sync, | Create React App, script to create single-page React applications | Gogs (self-hosted GIT service) | Grafana
5900	TCP	1 850	1 935	5%	Remote Frame Buffer protocol (RFB) | Virtual Network Computing (VNC) Remote Frame Buffer RFB protocol
2000	TCP	1 825	1 934	6%	Cisco Skinny Client Control Protocol (SCCP)
873	TCP	1 786	1 810	1%	rsync file synchronization protocol
102	TCP	1 749	1 803	3%	ISO Transport Service Access Point (TSAP) Class 0 protocol;
5984	TCP	1 790	1 803	1%	CouchDB database server
1434	UDP	1 937	1 802	–7%	Microsoft SQL Server database management system (MSSQL) monitor
53	TCP	1 477	1 796	22%	Domain Name System (DNS)

Port	Protocol	Previous	Last	Growth	Description
389	TCP	1 729	1 791	4%	Lightweight Directory Access Protocol (LDAP)
83	TCP	1 644	1 774	8%	mit-ml-dev (MIT ML Device)
2376	TCP	2 113	1 738	–18%	Docker REST API (SSL)
10443	TCP	1 697	1 738	2%	N/A
161	UDP	1 767	1 732	–2%	Simple Network Management Protocol (SNMP)
137	UDP	1 655	1 727	4%	NetBIOS Name Service, used for name registration and resolution
8880	TCP	2 445	1 720	–30%	Alternate port of CDDB (Compact Disc Database) protocol, used to look up audio CD (compact disc) information over the Internet. | IBM WebSphere Application Server SOAP connector
5985	TCP	1 462	1 662	14%	Windows PowerShell Default psSession PortWindows Remote Management Service (WinRM-HTTP)
1723	TCP	1 583	1 616	2%	KDE Connect | Point-to-Point Tunneling Protocol (PPTP)
3128	TCP	1 190	1 611	35%	Squid caching web proxy
5986	TCP	1 573	1 596	1%	Windows PowerShell Default psSession PortWindows Remote Management Service (WinRM-HTTPS)
631	TCP	1 568	1 572	0.26%	Internet Printing Protocol (IPP) | Common Unix Printing System (CUPS) administration console (extension to IPP)
11211	TCP	1 555	1 572	1%	memcached
465	TCP	1 433	1 571	10%	SMTP over implicit SSL (obsolete) | URL Rendezvous Directory for Cisco SSM (primary usage assignment) | Authenticated SMTPTLS/SSL (SMTPS) (alternative usage assignment)
502	TCP	1 484	1 561	5%	Modbus Protocol
1911	TCP	1 566	1 551	–1%	N/A
60632	UDP	0	1 549	0.00%	Range from which Mosh – a remote-terminal application similar to SSH – typically assigns ports for ongoing sessions between Mosh servers and Mosh clients.
8008	TCP	1 408	1 544	10%	Alternative port for HTTP. See also ports 80 and 8080. | IBM HTTP Server administration default | iCal, a calendar application by Apple | Matrix homeserver federation over HTTP

Port	Protocol	Previous	Last	Growth	Description
9443	TCP	1 394	1 531	10%	VMware Websense Triton console (HTTPS port used for accessing and administrating a vCenter Server via the Web Management Interface) | NCSA Brown Dog Data Tilling Service
50512	UDP	4	1 527	38 075%	N/A
143	TCP	1 416	1 522	7%	Internet Message Access Protocol (IMAP),electronic mail messages on a server
2083	TCP	1 479	1 517	3%	Secure RADIUS Service (radsec) | cPanel default SSL
82	TCP	1 303	1 505	16%	xfer (XFER Utility) | TorPark control
110	TCP	1 376	1 496	9%	Post Office Protocol, version 3 (POP3)
3790	TCP	2 125	1 485	–30%	N/A
5901	TCP	1 469	1 477	1%	N/A
5672	TCP	1 419	1 473	4%	Advanced Message Queuing Protocol (AMQP)
1900	UDP	1 535	1 471	–4%	Simple Service Discovery Protocol (SSDP),UPnP devices
7001	TCP	1 369	1 444	5%	Avira Server Management Console | Default for BEA WebLogic Server's HTTP server, though often changed during installation
4567	TCP	1 351	1 433	6%	Sinatra default server port in development mode (HTTP)
1521	TCP	1 418	1 429	1%	nCUBE License Manager | Oracle database default listener, in future releases
8001	TCP	1 235	1 428	16%	N/A
993	TCP	1 406	1 426	1%	Internet Message Access Protocol over TLS/SSL (IMAPS)
5938	TCP	1 328	1 424	7%	TeamViewer remote desktop protocol
1080	TCP	1 347	1 413	5%	SOCKS proxy
2082	TCP	1 326	1 407	6%	cPanel default
4444	TCP	1 180	1 401	19%	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

Port	Protocol	Previous	Last	Growth	Description
5001	TCP	1 269	1 398	10%	Slingbox and Slingplayer | Iperf (Tool for measuring TCP and UDP bandwidth performance) | Synology Inc. Secured Management Console, File Station, Audio Station | 3CX Phone System Management Console/Web Client (HTTPS)

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	207 398	171 403	–17%
123456789	172 717	167 797	–3%
123	133 770	158 211	18%
1234567890	127 869	149 739	17%
1111	127 365	149 332	17%
1	185 236	140 965	–24%
000000	126 716	107 379	–15%
12345	186 717	100 108	–46%
1234	185 236	99 769	–46%
123123	160 252	68 241	–57%
1011	12 840	51 229	299%
101010	12 992	50 585	289%
test	226 276	49 458	–78%
mx9	8	47 194	589 825%
mx0	42	47 179	112 231%
mx5	12	46 964	391 267%
mx2	25	46 285	185 040%
mx3	14	45 648	325 957%
mx6	25	45 330	181 220%
mx4	24	45 184	188 167%
mx7	26	44 495	171 035%
mx8	6	43 897	731 517%
112233	65 955	42 783	–35%
Lu5ei35	5 671	42 552	650%
1012	12 852	41 631	224%
111111	48 064	41 540	–14%
xR1i4YUARcX	7 020	40 988	484%
2oA69kPz0	6 440	40 816	534%
111	1 296	40 020	2 988%
11111	906	39 638	4 275%
RTg0CUI4	7 032	39 384	460%
11	959	39 314	3 999%

TURRIS

Password	Previous Month	Last Month	Growth
11111111	948	39 114	4 026%
10	26 199	39 035	49%
1111111	437	38 869	8 795%
111111111	143	38 802	27 034%
11223344	380	38 772	10 103%
111222	148	38 748	26 081%
szx69VQ8R44	6 217	38 744	523%
1111111111	159	38 728	24 257%
1010	16 161	38 626	139%
1100	4	38 620	965 400%
111aaa	17	38 605	226 988%
1122	43	38 592	89 649%
112112	25	38 574	154 196%
112233445566	203	38 563	18 897%
1110	9	38 507	427 756%
1004	25 690	38 489	50%
1092	3 079	35 437	1 051%
1123	50	34 894	69 688%
eR3WSfF1y	4 798	33 879	606%
12345678	193 991	33 735	–83%
mx1	41	32 004	77 959%
IUvO6O	4 487	31 308	598%
mzIYdQFAmy	6 083	30 917	408%
1.q	25 684	29 650	15%
sU4h6twZ	3 059	29 078	851%
12	2 568	28 804	1 022%
5wMat8C	2 977	28 532	858%
eXTw6nP	4 612	28 224	512%
Gb8ki3UaiP	3 008	28 118	835%
m6wX8	4 652	28 062	503%
102030	14 336	27 475	92%
19h8sxw8X7	3 174	27 341	761%
SUV77Z49D9ZmWlH	3 342	27 306	717%
9iFJM9sD	3 226	26 970	736%
J9Qen97n9uXs	4 600	26 948	486%
2bZ7T2Z58e	3 105	26 858	765%
3LEGz5	3 270	26 785	719%

Password	Previous Month	Last Month	Growth
Q9JfmH5	2 899	26 713	821%
osOeRuuYO728Su	3 048	26 704	776%
X4w0907089Q	2 945	26 178	789%
2Ng6d43	3 002	26 113	770%
cZ9I89b6MW	2 823	26 041	822%
WmEO71259N	5 629	25 813	359%
1-Abc	38 502	25 734	–33%
1029384756	12 878	25 733	100%
113355	23	25 718	111 717%
1133	25	25 702	102 708%
10203040	12 845	25 689	100%
1-Ab	34 678	25 680	–26%
6dGj19Dr	121	25 675	21 119%
114477	26	25 673	98 642%
1!@#456	31 184	25 655	–18%
1148	2	25 650	1 282 400%
1-q	36 803	25 639	–30%
1029	12 830	25 638	100%
q7p5i6raui	2 571	25 468	891%
1234567	25 420	25 316	–0.41%

Most Used Passwords Wordcloud