ICS Network Activity Report: July 25–31, 2022

Critical Infrastructure (CI) | Fusion (FS)

August 1, 2022 08:54:23 PM, 22-00018050, Version: 1

Executive Summary

- Mandiant leverages open and internal sources to identify network activity indicative of control systems targeting and scanning.
- It is important to note that this activity may also represent nefarious/non-malicious scanning activity. Additionally, IP addresses used as indicators can have a "shelf-life" or time in which it is still relevant to the activity in this report. Over time these IP addresses may be reused or rotated and therefore may be benign.
- Forty-nine of the 4,372 suspicious Internet Protocol (IP) addresses identified connecting to industrial control system (ICS) ports during the reporting period are likely malicious based on our analysis.
- The top three ICS ports targeted were TCP/55555 (325 reports), TCP/20000 (294 reports), TCP/4000 (120 reports).
- For more information about this report's methodology, use cases, and a full list of tracked ICS ports, please refer to our reference report (18-00015181).

Threat Detail

Updated Version: This version of the ICS Network Activity Report (NAR) was developed using a new methodology that evaluates findings against the Mandiant Score. We will continue to improve and adjust the report as needed.

Key Definitions

- Source: IP address that issued the communications
- Report: Number of times the Source issued communications to ICS ports
- Target: Endpoint or end IP address with which the Source communicated

Activity Summary

The following table presents a list of the top 10 most reported IP addresses we identified this week:

Source IP Addresses	Source Organization/Whois	Number of Reports	Moderate- and High-Fidelity Ports	Country of Origin
193[.]142[.]146[.]204	AS208046 HostSlick	282	TCP/55555	NL
81[.]218[.]45[.]231	AS8551 Bezeq International	154	TCP/20000	IL

89[.]248[.]168[.]197	AS202425 IP Volume inc	52	TCP/4000	NL
154[.]89[.]5[.]81	AS141167 AgotoZ HK Limited	48	TCP/20000	HK
196[.]3[.]97[.]71	AS31960 EMUNET	47	TCP/102, TCP/1089	MZ
5[.]39[.]216[.]167	AS57043 Hostkey B.v.	43	TCP/20000	NL
185[.]133[.]241[.]0	AS200474 CRFreeNet, z.s.	35	TCP/5094	CZ
107[.]152[.]46[.]186	AS11878 TZULO	31	UDP/1090	US
80[.]66[.]66[.]14	AS51765 Oy Crea Nova Hosting Solution Ltd	24	TCP/4000	RU
204[.]232[.]132[.]236	AS27357 RACKSPACE	20	TCP/5450	US

Table 1: Top weekly scanners

Source IP Addresses Country of Origin

Figure 1 presents the origin country of the source IP addresses contributing to the reported spikes this week:

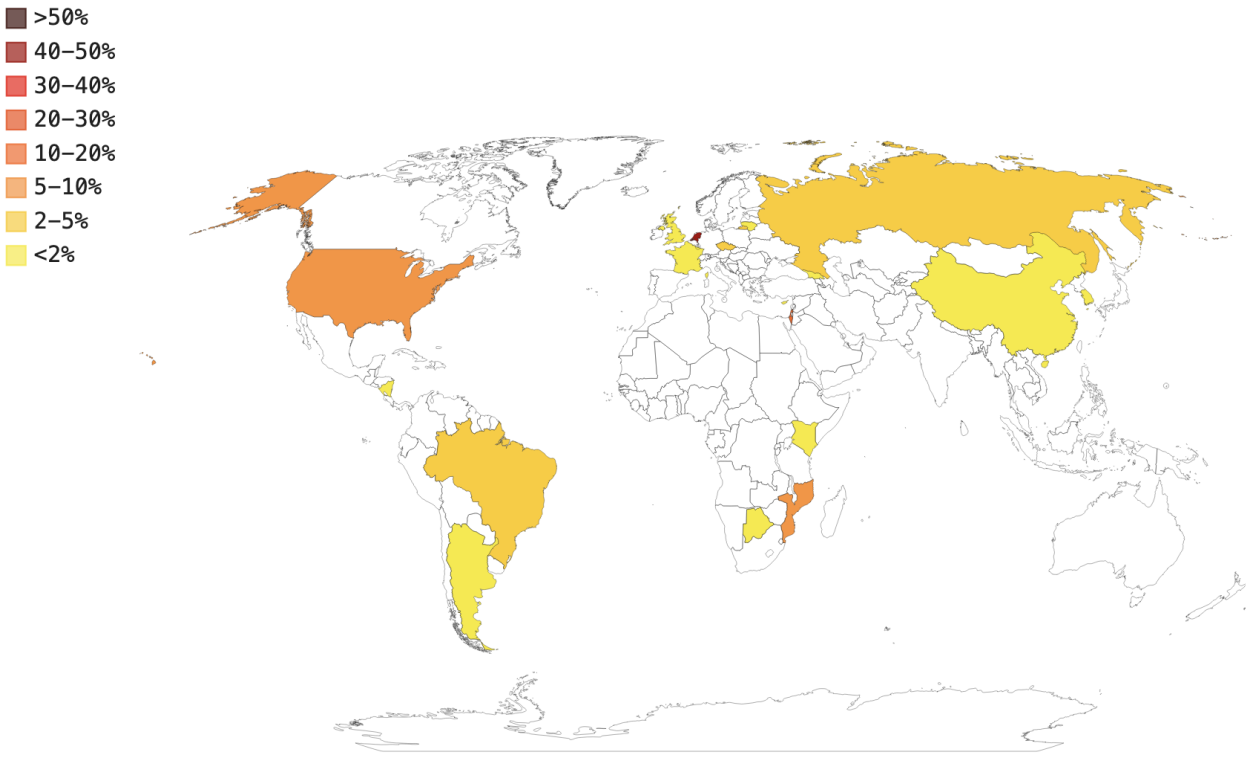

Figure 1: Distribution of Sources by Country of Origin

IP Addresses Potentially Targeting ICS Ports

Analyzing our data feeds, we examined 49 unique IP addresses that suspiciously communicated with high-fidelity control systems-related ports. The addresses listed in Table 2 originated from potentially malicious IP addresses.

Where possible, we assign each IP address a Mandiant Score value based on additional context that represents (from 1 through 100) how confident we are that the source is conducting some sort of malicious activity. Any IP address with an Indicator Confidence score of 80 or higher, Mandiant deems that source IP

potentially malicious. A detailed explanation of Mandiant Score can be found the Mandiant Advantage documentation page.

IP Address	ICS Port(s)	Origin	ASN	Mandiant Score
5[.]39[.]216[.]167	TCP/20000	NL	AS57043 Hostkey B.v.	100
152[.]32[.]162[.]95	TCP/20000	HK	AS135377 UCLOUD INFORMATION TECHNOLOGY HK LIMITED	100
101[.]68[.]211[.]3	TCP/502, TCP/4712, TCP/4840	CN	AS4837 CHINA UNICOM China169 Backbone	100
195[.]154[.]235[.]110	UDP/4000	FR	AS12876 Online S.a.s.	100
89[.]248[.]165[.]52	TCP/20000	NL	AS202425 IP Volume inc	100
154[.]89[.]5[.]81	TCP/20000	HK	AS141167 AgotoZ HK Limited	100
123[.]160[.]221[.]18	TCP/20000	CN	AS137687 Luoyang, Henan Province, P.R. China.	100
62[.]204[.]41[.]56	TCP/20000	RU	AS59425 Horizon LLC	100
123[.]160[.]221[.]8	TCP/20000	CN	AS137687 Luoyang, Henan Province, P.R. China.	99
154[.]89[.]5[.]214	TCP/20000	HK	AS141167 AgotoZ HK Limited	99
154[.]89[.]5[.]73	TCP/20000	HK	AS141167 AgotoZ HK Limited	99
89[.]248[.]168[.]197	TCP/4000	NL	AS202425 IP Volume inc	99
183[.]136[.]225[.]14	TCP/20000	CN	AS58461 CT-HangZhou-IDC	99
45[.]227[.]254[.]55	TCP/1089	LT	AS267784 Flyservers S.A.	99
193[.]142[.]146[.]204	TCP/55555	NL	AS208046 HostSlick	99
154[.]89[.]5[.]100	TCP/20000	HK	AS141167 AgotoZ HK Limited	98
190[.]120[.]191[.]21	UDP/34964	AR	AS52409 COSEIDI S.A.	97
197[.]218[.]241[.]234	TCP/4000	MZ	AS37342 MOVITEL	97
41[.]209[.]43[.]93	TCP/1091, TCP/1089	KE	AS9129 KE-NET2000	97
193[.]142[.]146[.]216	TCP/55555	NL	AS208046 HostSlick	97
87[.]228[.]185[.]240	TCP/5002	CY	AS6866 Cyprus	97

			Telecommunications Authority	
165[.]98[.]224[.]34	TCP/18000	NI	AS18840 EQUIPOS Y SISTEMAS S.A.	97
81[.]218[.]45[.]231	TCP/20000	IL	AS8551 Bezeq International	96
177[.]70[.]65[.]78	TCP/55555	BR	AS262544 Sulcom Informatica Ltda	96
198[.]54[.]128[.]69	TCP/55555	US	AS11878 TZULO	96
195[.]154[.]169[.]176	UDP/4000	FR	AS12876 Online S.a.s.	96
185[.]108[.]105[.]82	TCP/5002	GB	AS203020 HostRoyale Technologies Pvt Ltd	95
196[.]3[.]97[.]71	TCP/102, TCP/1089	MZ	AS31960 EMUNET	95
217[.]147[.]228[.]15	UDP/55555	GE	AS20545 Georgian Research and Educational Networking Association (GRENA)	95
82[.]202[.]68[.]3	TCP/5094	CZ	AS25512 CD-Telematika a.s.	94
168[.]167[.]26[.]162	TCP/4000	BW	AS14988 BTC-GATE1	94
200[.]73[.]137[.]2	UDP/4000	AR	AS10481 Telecom Argentina S.A.	94
107[.]152[.]46[.]186	UDP/1090	US	AS11878 TZULO	94
80[.]66[.]66[.]14	TCP/4000	RU	AS51765 Oy Crea Nova Hosting Solution Ltd	93
78[.]156[.]44[.]203	TCP/5094	CZ	AS43507 RETE internet, s.r.o.	93
92[.]255[.]85[.]155	TCP/4000	RU	AS57523 Chang Way Technologies Co. Limited	93
92[.]255[.]85[.]181	TCP/4000	RU	AS57523 Chang Way Technologies Co. Limited	93
185[.]133[.]241[.]0	TCP/5094	CZ	AS200474 CRFreeNet, z.s.	93
185[.]122[.]204[.]39	TCP/4000	RU	AS50340 OOO Network of data-centers Selectel	93
165[.]90[.]88[.]130	TCP/4000	MZ	AS37110 moztel-as	93
165[.]90[.]83[.]150	TCP/4000	MZ	AS37110 moztel-as	93
104[.]243[.]45[.]45	UDP/1090	US	AS23470 RELIABLESITE	93

204[.]232[.]132[.]236	TCP/5450	US	AS27357 RACKSPACE	92
195[.]154[.]200[.]29	UDP/4000	FR	AS12876 Online S.a.s.	92
1[.]215[.]138[.]43	UDP/4000	KR	AS3786 LG DACOM Corporation	92
209[.]14[.]68[.]113	UDP/4000	BR	AS268581 QNAX LTDA	89
64[.]227[.]107[.]14	UDP/1090	US	AS14061 DIGITALOCEAN-ASN	86
186[.]125[.]169[.]112	UDP/4000	AR	AS7303 Telecom Argentina S.A.	84
45[.]180[.]248[.]10	TCP/20000	BR	AS269210 Espaco Livre Informatica Ltda ME	82

Table 2: IP addresses targeting ICS ports during the reporting period

Known Research Activity Scanning ICS Ports

Table 3 presents known research organizations that we recognized scanning ICS ports during the week. When possible, we provided the subnets they used.

Attribution	Origin	ICS Port(s)	Number of Addresses	IP Subnets
binaryedge[.]ninja	US	TCP/5007	3	204[.]48[.]26[.]0/24
censys[.]io	US	TCP/20000, TCP/2404, TCP/502, TCP/102	102	167[.]94[.]138[.]0/24, 167[.]248[.]133[.]0/24, 162[.]142[.]125[.]0/24, 167[.]94[.]146[.]0/24
openportstats[.]com	NL	TCP/4000	52	89[.]248[.]168[.]0/24
shadowserver[.]org	US	UDP/9600	3	74[.]82[.]47[.]0/24
shodan[.]io	NL	TCP/20000, TCP/20547	16	185[.]142[.]236[.]0/24, 94[.]102[.]49[.]0/24

Table 3: Research organizations scanning ICS ports during the reporting period

Please rate this product by taking a short four question survey

First Version Publish Date

August 1, 2022 08:54:23 PM

Threat Intelligence Tags

Affected Industries

- Aerospace & Defense
- Chemicals & Materials
- Construction & Engineering
- Energy & Utilities

- Governments
- Healthcare
- Manufacturing
- Oil & Gas
- Pharmaceuticals
- Transportation

Affected Systems

- Control Systems and Applications
- Equipment Under Control
- Operations Management
- Safety Protection
- Regulatory and Supervisory Control
- Communication Infrastructure
- Industrial Network Protocols
- Industrial Internet of Things

Intended Effects

- Interference with ICS
- Disruption
- Destruction

Motivations

- Opportunistic

Source Geographies

- Global

Tactics, Techniques And Procedures (TTPs)

- Network Reconnaissance

Target Geographies

- Global

Version Information

Version:1, August 1, 2022 08:54:23 PM