Reconnaissance activity against entities in the oil and gas sector

This report is updated on 24 October 2022.

Executive Summary

NORMA Cyber has received information about network reconnaissance activity against entities in the oil and gas sectors, and possibly entities involved in transportation of Liquefied Natural Gas (LNG).

The threat actor is unknown, but in light of the current geo-political situation, and similar warnings received earlier, it is **LIKELY** that the threat actor is linked to Russia.

NORMA Cyber encourage members, and particular those with assignments related to oil and gas, to search firewall and access logs from Internet facing servers for network traffic originating from Cactus VPN exit nodes.

Background

[NORMA Cyber source] On 13 October 2022, NORMA Cyber received a warning from one of our partners that an unknown threat actors has conducted network reconnaissance activity against entities in the oil and gas sector, and possibly entities involved in transportation of Liquefied Natural Gas (LNG). The reconnaissance activity has included port scanning, accessing web pages, as well as automated login attempts to VPN services. The threat actors has used the Cactus VPN service to anonymize the activity. The activity has been ongoing from June 2022 until September 2022.

COMMENT: Cactus VPN[1] is a small VPN provider with servers in 22 countries. According to SPUR[2] there is approximate 110 IP addresses used as Cactus VPN exit nodes, with an

[1] https://www.cactusvpn.com/

[2] https://spur.us/

average of 4 devices per IP address, so this is not a very polular VPN service. COMMENT ENDS

We have also received reports of similar reconnaissance activity from international partners.

Assessment

The reconnaissance activity has been ongoing from June until September, but it is **LIKELY** that the activity is still be ongoing.

We have no information about the threat actor, but in light of the current geo-political situation, and a similar warning received earlier this summer, it is **LIKELY** that the threat actor is linked to Russia.

The results from the reconnaissance activity can **LIKELY** be used for further exploitation of vulnerabilities in Internet facing servers or remote access with credentials acquired through the automated login attemts (password spraying).

TTPs / Indicators of Compromise

The following Cactus VPN exit nodes have been observed used in reconnaissance activity in the past months, but not specifically against the oil and gas sector:

Type	Value	Description
IP	162.248.94[.]37	Cactus VPN, US Port scanning
IP	104.153.109[.]218	Cactus VPN, US Port scanning
IP	88.150.154[.]3	Cactus VPN, GB Web scanning and password spraying against VPN endpoint
IP	69.197.182[.]90	Cactus VPN, US

		Port scanning and Web scanning
IP	88.198.133[.]24	Cactus VPN, DE Port scanning
IP	179.43.145[.]246	Cactus VPN, AU Port scanning
IP	139.99.248[.]110	Cactus VPN, AU Port scanning and Web scanning

See Appendix 1 for a list of known IP addresses used as Cactus VPN exit nodes.

Recommendations

NORMA Cyber encourage members, and particular those with assignments related to oil and gas, to search firewall and access logs from Internet facing servers for network traffic originating from Cactus VPN exit nodes (see Appendix 1 for a list of known IP addresses). In particularly access logs from web servers and VPN solutions should be examined. The search should include logs from June until today.

NORMA Cyber appreciate the following information if you have observed any network traffic from Cactus VPN exit nodes in the period:

- Are there any particular web pages that has been accesses (e.g. related to names or e-mail addresses for employees, particular projects, etc)?
- Which "User-Agent:"[3] has been used?
- Which ports has been scanned?
- Date and time for the activity

[3] https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/User-Agent

Definitions and standardisation

The threat: The threat assessed by NORMA Cyber is based on our understanding of known threat actors' capabilities, hostile intentions and opportunities to cause harm directly towards vessels/units and their crew today and in the future, limited to defined areas. The threat could also be of an indirect nature, caused as collateral damage when vessels/units plausibly could be affected by an attack by mistake or by coincidence.

Words of estimative probability (confidence levels): Words of estimative probability (WEP) are terms used to convey the likelihood/probability of a future event occurring. In this product, the following WEPs are used:

HIGHLY LIKELY – LIKELY – (EVEN CHANCE) – UNLIKELY – HIGHLY UNLIKELY

Threat levels: Threat levels are designed to conclude the assessment of each threat. In this product, the following Threat Levels are used (NATO and Norwegian standards) with the defined level of probability/confidence:

- **LOW** means attack against member is **UNLIKELY**
- **MODERATE** means attack against member is **LIKELY**
- **HIGH** means attack against member is **HIGHLY LIKELY**
- **CRITICAL** means attack against member is expected imminently

The NORMA Cyber Monthly Threat Assessment is valid only from the date of dissemination and until a revised Threat Assessment is disseminated by NORMA Cyber. Outdated Threat Assessments should never be used as inputs to Security Risk Assessments or as any kind of decision support on security matters.

Traffic Light Protocol

The Traffic Light Protocol (TLP) was created in order to facilitate greater sharing of information. TLP is a set of designations used to ensure that sensitive information is shared with the appropriate audience. It employs four colours to indicate expected sharing boundaries to be applied by the recipient(s).

NORMA Cyber uses the FIRST definition TLP.[4]

TLP:RED

= Not for disclosure, restricted to participants only.

Sources may use TLP:RED when information cannot be effectively acted upon by additional parties, and could lead to impacts on a party's privacy, reputation, or operations if misused. Recipients may not share TLP:RED information with any parties outside of the specific exchange, meeting, or conversation in which it was originally disclosed. In the context of a meeting, for example, TLP:RED information is limited to those present at the meeting. In most circumstances, TLP:RED should be exchanged verbally or in person.

TLP:AMBER

= Limited disclosure, restricted to participants' organisations.

Note that TLP:AMBER+STRICT restricts sharing to the organisation only. Sources may use TLP:AMBER when information requires support to be effectively acted upon, yet carries risks to privacy, reputation, or operations if shared outside of the organisations involved. Recipients may only share TLP:AMBER information with members of their own organisation, and with clients or customers who need to know the information to protect themselves or prevent further harm. Sources are at liberty to specify additional intended limits of the sharing: these must be adhered to.

TLP:GREEN

= Limited disclosure, restricted to the community.

[4] https://www.first.org/tlp/

Sources may use TLP:GREEN when information is useful for the awareness of all participating organisations as well as with peers within the broader community or sector. Recipients may share TLP:GREEN information with peers and partner organisations within their sector or community, but not via publicly accessible channels. Information in this category can be circulated widely within a particular community. TLP:GREEN information may not released outside of the community.

TLP:CLEAR

= Disclosure is not limited.

Sources may use TLP:CLEAR when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release. Subject to standard copyright rules, TLP:CLEAR information may be distributed without restriction.

Specifications and contact details

Information Cut-Off: 21 October 2022

NORMA Cyber Operations Centre Contact details:

Duty Officer e-mail: ops@normacyber.no

Duty Officer mobile: +47 909 89 737

Caveats

This report has been compiled from multiple sources. NORMA Cyber does not accept responsibility for verifying information provided in this document, nor for the outcome of action taken or not taken as a result of information provided, our comments and/or advice.

Appendix 1 – List of known Cactus VPN exit nodes

1.234.58.165
103.20.212.22
103.20.214.113
103.75.117.53
104.153.109.173
104.153.109.218
104.237.193.52
109.169.22.73
109.169.22.74
109.169.22.75
109.169.22.84
109.169.22.85
109.169.22.87
111.90.149.156
121.50.45.15
139.99.238.43
139.99.248.110
139.99.30.162
149.56.182.0
149.56.182.1
149.56.182.2
149.56.182.3
15.235.142.145
158.69.26.89
162.248.94.37
163.172.124.146
179.43.145.245
179.43.145.246
185.101.107.124
185.15.23.16
185.15.23.36
185.176.221.124
185.176.221.28
185.176.221.68
188.127.224.27
188.127.249.91
192.223.24.121
192.223.24.125
192.95.36.1
195.154.56.103
195.154.56.115
195.231.67.141
195.231.67.193
198.251.84.18
198.50.251.184
198.50.251.185
201.131.126.58
209.250.242.95
45.124.137.81
45.148.120.246
45.148.121.197
45.148.123.106
45.162.230.219
45.162.230.220
45.77.103.66
46.246.97.104
46.246.97.105
5.182.209.57
5.182.210.46
50.7.177.162
50.7.177.163
50.7.177.164
54.38.198.240
54.38.58.142
54.38.58.143
69.197.143.178
69.197.143.179
69.197.143.180
69.197.143.181
69.197.143.182
69.197.182.90
69.197.182.91
74.91.112.207
74.91.112.234
74.91.117.168
74.91.124.187
74.91.125.245
74.91.126.205
74.91.126.209
82.102.26.226
82.102.26.228
82.102.26.229
82.102.26.230
88.150.154.17
88.150.154.2
88.150.154.27
88.150.154.3
88.150.154.4
88.150.154.5
88.198.133.23
88.198.133.24
88.198.142.155
89.38.145.40
93.114.194.145
93.114.194.168
95.179.177.222