id	Subject	Status	Created	Started	Doelgroep in	Deelnemer in/met (specifiek)	Incident klasse	Type incident	Type Melding
12741	RE: Wbni wordt misbruikt in phishing campagne	resolved	21-4-2015 09:55	21-4-2015 09:55	Vitaal	Energie	Gathering of Information	Phishing	Overige
13183	FW: Cryptolocker mail	resolved	11-5-2015 17:05	11-5-2015 17:05	Vitaal	Energie	Malware	Infection	(Inter)nationaal hulpverzoek
13517	FW: Poging tot aanmelden bij Wbni data server door onbevoegde	resolved	2-6-2015 10:15	2-6-2015 10:15	Vitaal	Energie	Intrusion attempt	Login attempt	Overige
14960	Melding 5x cryptoware besmetting energiesector	resolved	3-9-2015 17:08	3-9-2015 17:08	Vitaal	Energie	Malware	Infection	Overige
16606	Melding spearphishing Wbni dochter	resolved	12-12-2015 22:40	12-12-2015 22:40	Vitaal	Energie	Gathering of Information	Phishing	(Inter)nationaal hulpverzoek
16894	Internetstoring Wbni	resolved	4-1-2016 15:00	4-1-2016 15:00	Vitaal	Energie	Availability	DoS/DDoS	(Inter)nationaal hulpverzoek
16976	Information request regarding energy disruption	resolved	7-1-2016 13:40	7-1-2016 13:40	Internationaal	Energie	Malware	Infection	Overige
18145	Verdachte IP-adressen en netwerkverkeer Wbni	resolved	17-3-2016 23:13	17-3-2016 23:13	Vitaal	Energie	Other		(Inter)nationaal hulpverzoek
18806	FW: Computervirus ontdekt in Beierse kerncentrale	resolved	25-4-2016 21:43	25-4-2016 21:43	Internationaal	Energie	Malware	Infection	Overige
20069	melding datalek vitaal Wbni - vooruitlopend op voorgenomen meldplicht	resolved	12-7-2016 18:57	12-7-2016 18:57	Vitaal	Energie	Information Security	Unauthorised access	Overige
21121	FW: Phishing mail met vreemde link	resolved	27-9-2016 09:48	27-9-2016 09:48	Vitaal	Energie	Gathering of Information	Phishing	(Inter)nationaal hulpverzoek
21732	Incident Wbni	resolved	4-11-2016 17:27	4-11-2016 17:27	Vitaal	Energie	Other		(Inter)nationaal hulpverzoek
22456	FW: Geruchten nieuwe cyber aanval Ukraine	resolved	27-12-2016 15:19	27-12-2016 15:19	Internationaal	Energie	Availability	Sabotage	Overige
23870	Ransomwarem elding Wbni	resolved	10-3-2017 16:41	10-3-2017 16:41	Vitaal	Energie	Malware	Infection	(Inter)nationaal hulpverzoek
24808	DoS Wbni website	resolved	8-5-2017 10:14	8-5-2017 10:14	Vitaal	Energie	Availability	DoS/DDoS	(Inter)nationaal hulpverzoek
26120	Misconfigurati es op Wbni Wbni nl website	resolved	26-7-2017 10:02	26-7-2017 10:02	Overige	Energie		Exploitation of vulnerability	RD-melding
26215	Mogelijke ransomwarebe smetting Wbni	resolved	31-7-2017 21:02	31-7-2017 21:02	Privaat	Energie	Malware	Infection	Zelf gesignaleerd
26728	Incident Wbni	resolved	31-8-2017 20:49	31-8-2017 20:49	Privaat	Energie	Intrusion Information Security	Exploitation of vulnerability Unauthorised access	(Inter)nationaal hulpverzoek

28771	Wbni openstaande SharePoint	resolved	22-12-2017 16:52	22-12-2017 16:52	Privaat	Energie	Information Security	Unauthorised access	RD-melding
28887	FW: Vulnerability Report	resolved	29-12-2017 10:32	29-12-2017 10:32	Privaat	Energie	Other		RD-melding
28977	Request assistance in taking down a fraudulent web page: Wbn Wbni nl	resolved	2-1-2018 13:37	2-1-2018 13:37	Privaat	Energie	Fraud	Illegitimate use of the name of a third part	(Inter)national hulpverzoek
28979	Request assistance in taking down a fraudulent web page: Wbn Wbni nl	resolved	2-1-2018 14:42	2-1-2018 14:42	Privaat	Energie	Abusive content	Copyright	(Inter)national hulpverzoek
48057	IOC's GantCrab september al bekend?	resolved	30-9-2018 13:33	30-9-2018 13:33	Privaat	Energie	Malware	Distribution	(Inter)national hulpverzoek
48415	IOC (IP) hits bij Wbni	resolved	4-10-2018 13:20	4-10-2018 13:20	Privaat	Energie	Intrusion attempt		Ter informatie
55728	FW: frauduleuze mails Wb (C7085)	resolved	10-1-2019 17:38	10-1-2019 17:38	Privaat	Energie	Fraud		(Inter)national hulpverzoek
57967	vulnerability Report(server security misconfiguration) spf records Wbni .eu	resolved	10-2-2019 14:52	10-2-2019 14:52	Privaat	Energie	Fraud	Illegitimate use of the name of a third part	RD-melding
62888	Wbni Spectrum Power 4.7 scan	resolved	9-4-2019 17:29	9-4-2019 17:29	Overheid/Publiek	Energie	Gathering of Information		Zelf gesignaleerd
70840	ransomware johannesburg powerplant	resolved	25-7-2019 13:22	25-7-2019 13:22	Internationaal	Energie	Malware	Infection	Zelf gesignaleerd
74777	RD: Hulpverzoek RD bij Wbni	resolved	23-9-2019 17:40	23-9-2019 17:40	Privaat	Energie	Intrusion attempt	Exploitation of vulnerability	RD-melding
76024	vraag over fortigate	resolved	10-10-2019 17:45	10-10-2019 17:45	Privaat	Energie	Information Security		(Inter)national hulpverzoek
83422	Kaspersky Labs kwetsbaarheden in turbine control systemen	resolved	30-12-2019 13:37	30-12-2019 13:37	Privaat	Energie	Intrusion attempts	Exploitation of vulnerability	Ter informatie
87517	Internationale samenwerking 53 ongepatchte Russiche CVE`s voor Wbni Energie centrales	resolved	5-2-2020 11:06	5-2-2020 11:06	Vitale aanbieder Internationale partner	Energie	Vulnerable	Open for abuse	CVD-melding
93411	Informele melding van huidige manier van werken tijdens de COVID-19 pandemie	resolved	8-4-2020 14:51	8-4-2020 14:51	Vitale aanbieder	Energie	Other	Other	Ter informatie

94080	Vraag Wbni : RagnarLocker ransomware hits [redacted]	resolved	15-4-2020 13:14	15-4-2020 13:14	Nationale partner	Energie	Other	Other	(Inter)nationaal hulpverzoek
97961	Vraag Wbni [redacted] aanval	resolved	20-5-2020 15:21	20-5-2020 15:21	Vitale aanbieder	Energie	Intrusion attempts	Exploiting known vulnerabilities	Incident
99973	Mogelijke phishingmail naar Wbni	resolved	10-6-2020 11:38	10-6-2020 11:38	Vitale aanbieder	Energie	Fraud	Phishing	(Inter)nationaal hulpverzoek
100221	Vraag Wbni over context 3 IP adressen	resolved	12-6-2020 15:18	12-6-2020 15:18	Vitale aanbieder	Energie	Intrusion attempts		Overige
112486	melding DDOS - Wbni	resolved	24-9-2020 11:40	24-9-2020 11:40	Vitale aanbieder	Energie	Availability	DDoS	Ter informatie
113388	[#ERC-508-74163]: Smishing/phishing activity and domain trademark violation at Wbni direct	resolved	1-10-2020 19:22	1-10-2020 19:22	Vitale aanbieder	Energie	Fraud	Phishing	NTD-verzoek
113519	FW: [CONFIDENTIAL] - Betreft abuse melding Yahoo mailadres (CFO impersonation)	resolved	2-10-2020 22:09	2-10-2020 22:09	Vitale aanbieder	Energie	Fraud	Phishing	(Inter)nationaal hulpverzoek
114206	Kwetsbaarheden verholpen in Wbni Helpdesk	resolved	8-10-2020 11:27	8-10-2020 11:27	Vitale aanbieder	Energie	Other	Other	Ter informatie
121874	mogelijk spoofed website Wbni [redacted]	resolved	8-12-2020 12:19	8-12-2020 12:19	Vitale aanbieder	Energie	Fraud		Incident
127657	Hulpvraag Wbni 07 jan 2021	resolved	7-1-2021 17:55	7-1-2021 17:55	Vitale aanbieder	Energie	Other	Other	(Inter)nationaal hulpverzoek
127932	Vraag Wbni mbt uitval	resolved	11-1-2021 14:08	11-1-2021 14:08	Vitale aanbieder	Energie	Other	Other	(Inter)nationaal hulpverzoek
130013	Vraag emotetlijst	resolved	1-2-2021 14:33	1-2-2021 14:33	Vitale aanbieder	Energie	Other	Other	(Inter)nationaal hulpverzoek
133392	[Energie_vitaal] [TLP:GREEN] Vulnerabilities in Microsoft Exchange are actively exploited [ALSHAT]	resolved	9-3-2021 15:47	9-3-2021 15:47	Vitale aanbieder	Energie	Other	Other	Overige
139375	Mogelijk gecompromitteerd werkstation bij Wbni (vitaal)	resolved	14-4-2021 12:37	14-4-2021 12:37	Rijksoverheid	Energie	Intrusions		Incident
142759	Phishing slachtoffers (via CSIRT-DSP)	resolved	19-5-2021 14:32	19-5-2021 14:32	Overige	Energie	Information Gathering	Social engineering	Overige

145125	[TLP:AMBER][Oefening ISIDOOR 2021] Verdachte email bij [redacted]	resolved	1-6-2021 09:57	1-6-2021 09:57	Nationale partner	Energie	Fraud	Phishing	Oefening
147213	Ter info: vraag over procedure Melding Wbni [redacted]	resolved	11-6-2021 13:04	11-6-2021 13:04	Vitale aanbieder	Energie	Other	Other	(Inter)nationaal hulpverzoek
147671	WBNI melding: DDoS [redacted]	resolved	15-6-2021 15:19	15-6-2021 15:19	Vitale aanbieder	Energie	Availability	DDoS	WBNI-melding
148104	CVD Lemon Lizard - netgekoppelde omvormers voor zonnepanelen	resolved	18-6-2021 00:21	18-6-2021 00:21	Overige	Energie	Vulnerable	Open for abuse	CVD
151208	WBNI Melding [redacted] - reporting an incident	resolved	16-7-2021 12:50	16-7-2021 12:50	Vitale aanbieder	Energie	Other	Other	WBNI-melding
155219	[redacted] issue energiesector	resolved	24-8-2021 20:50	24-8-2021 20:50	Vitale aanbieder	Energie	Vulnerable	Open for abuse	RD-melding
157080	Zembla / [redacted]	resolved	13-9-2021 15:58	13-9-2021 15:58	Vitale aanbieder	Energie	Other	Other	Overige
158706	[TLP:AMBER] [redacted] Hulpdeskfraude	resolved	29-9-2021 10:43	29-9-2021 10:43	Vitale aanbieder	Energie	Information Gathering	Social engineering	Incident
158714	[redacted]: Verzoek tot advies bereiken leverancier die geraakt is door "hack":	resolved	29-9-2021 11:36	29-9-2021 11:36	Vitale aanbieder	Energie	Intrusions		Incident
161738	WBNI - [redacted] [vrijwillig]	resolved	1-11-2021 10:10	1-11-2021 10:10	Vitale aanbieder	Energie	Vulnerable	Open for abuse	WBNI-melding
164379	[redacted]	resolved	22-11-2021 18:17	22-11-2021 18:17	Privaat	Energie	Malicious code	Ransomware	Incident
166458	Melding incident WBNI - [redacted] - INC0036807	resolved	12-12-2021 15:30	12-12-2021 15:30	Privaat	Energie	Other	Other	WBNI-melding
167338	Ter info: DDOS aanval op Mobile gateway	resolved	20-12-2021 14:05	20-12-2021 14:05	Vitale aanbieder	Energie	Availability	DDoS	Incident
168231	Ter info: DDos [redacted]	resolved	1-1-2022 17:35	1-1-2022 17:35	Vitale aanbieder	Energie	Availability	DDoS	Ter informatie
169620	[redacted] melding van incident onder Wbni	resolved	17-1-2022 20:02	17-1-2022 20:02	Vitale aanbieder	Energie	Malicious code	Infection	Incident
170064	[Olie_vitaal] [TLP:AMBER Your Organization Only] [redacted] [redacted] mogelijk gecompromitteerde mailbox	resolved	21-1-2022 10:16	21-1-2022 10:16	Vitale aanbieder	Energie	Intrusions	Account Compromise	Incident

171482	CVD Sunray Salamander [redacted]	resolved	8-2-2022 10:50	8-2-2022 10:50	Overige	Energie	Vulnerable	Open for abuse	CVD
171546	FW: Blackcat IOCs (vanuit analyse bij 1 van de getroffen partijen)	resolved	8-2-2022 20:24	8-2-2022 20:24	Vitale aanbieder	Energie	Malicious code	Ransomware	Overige
171612	RD-melding: Kwetsbaarheid ssrf naar RCE bij [redacted] en [redacted]	resolved	9-2-2022 15:51	9-2-2022 15:51	Vitale aanbieder	Energie	Vulnerable	Open for abuse	RD-melding
172091	Grote Lijst IOC's energie/olie vanuit [redacted]	resolved	15-2-2022 22:14	15-2-2022 22:14	Vitale aanbieder	Energie	Other	Other	(Inter)national hulpverzoek
173835	Ter info: [redacted] Control Panels [FICORA #1186479]	resolved	3-3-2022 20:26	3-3-2022 20:26	Vitale aanbieder	Energie	Vulnerable	Open for abuse	Ter informatie
176270	Vraag over verdacht verkeer en meldingen bij [redacted]	resolved	25-3-2022 16:36	25-3-2022 16:36	Vitale aanbieder	Energie	Intrusion attempts	Login attempt	Incident
176486	RD: Open windmolen portaal via archive.org	resolved	28-3-2022 13:53	28-3-2022 13:53	Overige	Energie	Other	Other	RD-melding
176848	WBNI: Melding incident WBNI INC0038126 - [redacted]	resolved	31-3-2022 14:06	31-3-2022 14:06	Vitale aanbieder	Energie	Other	Other	WBNI-melding
176991	[redacted]: vraag inzake incident in supply chain	resolved	1-4-2022 16:32	1-4-2022 16:32	Vitale aanbieder	Energie	Other	Other	Incident
177003	Wbni melding [redacted] | 2022-04-01	resolved	1-4-2022 19:58	1-4-2022 19:58	Vitale aanbieder	Energie	Other	Other	WBNI-melding
177387	Dossier Windmolens/[redacted]	resolved	6-4-2022 14:03	6-4-2022 14:03	Overige	Energie	Other		Overige
178233	Berichtgeving over ICS SCADA malware	resolved	15-4-2022 09:53	15-4-2022 09:53	International partner	Energie	Other		Ter informatie
178873	[redacted] Botnet infectie	resolved	22-4-2022 16:23	22-4-2022 16:23	Vitale aanbieder	Energie	Intrusion attempts	Login attempt	Incident
178996	[Autoreporter 78b42ef7-ed51-4a5a-b6df-d6d3a0114c61] Unsecured wind turbine control portals on your constituent's/customer's networks (CERT-NL)	resolved	24-4-2022 12:04	24-4-2022 12:04	Vitale aanbieder	Energie	Vulnerable	Open for abuse	Incident

182344	TLP:AMBER. Second version of ACER's revision of the Draft Network Code for Cybersecurity Aspects of Cross-Border Flows of Electricity	resolved	1-6-2022 10:20	1-6-2022 10:20	Rijksoverheid	Energie	Other	Other	Ter informatie
182432	Hulpvraag [redacted]	resolved	2-6-2022 15:48	2-6-2022 15:48	Vitale aanbieder	Energie	Other	Other	(Inter)nationaal hulpverzoek
184563	[Autoreporter 58aee7a8-21f4-4cb6-b857-7ffc39b86410] Unsecured wind turbine control portals on your constituent's/customer's networks (CERT-NL)	resolved	23-6-2022 11:39	23-6-2022 11:39	Overige	Energie	Vulnerable	Open for abuse	Incident
185842	TLP Amber: ioc's energy organization attack Sweden	resolved	5-7-2022 14:26	5-7-2022 14:26	International partner	Energie	Other	Other	Ter informatie
186479	[redacted] mogelijk malafide IP addressen	resolved	12-7-2022 16:17	12-7-2022 16:17	Vitale aanbieder	Energie	Malicious code	C&C	Incident
186976	[redacted] breach hack of [redacted] E-mail account	resolved	18-7-2022 15:59	18-7-2022 15:59	Vitale aanbieder	Energie	Intrusions	Account Compromise	Incident
187956	CVD-report: broken-access-control	https://[redacted]	resolved	26-7-2022 19:11	#########	Vitale aanbieder	Energie	Information Gathering	RD-melding
190248	[redacted] besmetting (CERT-EU incident)	resolved	18-8-2022 14:02	18-8-2022 14:02	International partner	Energie	Other	Other	Incident
191302	Financial Cyber Attack - [redacted]	resolved	29-8-2022 13:58	29-8-2022 13:58	Vitale aanbieder	Energie	Intrusions		Incident
202589	[redacted]	Report on alleged threat against [redacted] in the Netherlands	resolved	27-11-2022 17:45	#########	Vitale aanbieder	Energie	Other	Other	Ter informatie
214934	Mogelijk compromittatie: Bestanden [redacted]	resolved	1-3-2023 22:18	1-3-2023 22:18	Privaat	Energie	Fraud	Unauthorized use of resources	Ter informatie
218490	Vraag over firewall sighting (telnet bruteforce)	resolved	27-3-2023 16:37	27-3-2023 16:37	Privaat	Energie	Information Gathering	Scanning	Overige

Van: Info (NCSC-NL)
Verzonden: vrijdag 5 maart 2021 17:56
Aan: 5.1 (2e) (NCSC-NL)
Onderwerp: RE: Beveiligingsadvies aan Wbni
Ha 5.1 (2e) ,

Ik heb het even gecontroleerd en alle onderstaande adviezen zijn naar de drie adressen zoals genoemd gemaild.
Zowel het originele bericht als de updates. We hebben ook geen bounce ontvangen.

Voor zover ik kan zien heeft Wbni deze adviezen dus gewoon op de juiste manier ontvangen.

Groet,
5.1 (2e)

-----Original Message-----
From: 5.1 (2e) (NCSC-NL)
Sent: vrijdag 5 maart 2021 14:00
To: Info (NCSC-NL)
Subject: Beveiligingsadvies aan Wbni

Beste collega,

Mijn contactpersoon bij Wbni heeft bij mij aangegeven het beveiligingsadvies van Wbni niet te hebben ontvangen terwijl zij als het goed is alle beveiligingsadviezen van ons ontvangen op de volgende adressen:

Wbni

Wbni

Wbni

Kunnen jullie voor mij nagaan of en zo ja wanneer en naar welke mailadressen dit beveiligingsadvies en de bijbehorende updates zijn gestuurd?

NCSC-2021-0080 [1.03]

NCSC-2021-0080 [1.02]

NCSC-2021-0080 [1.01]

NCSC-2021-0080 [1.00]

Met vriendelijke groet,

5.1 (2e)

5.1 (2e)

.....

Ministerie van Justitie en Veiligheid

Nationaal Cyber Security Centrum

Turfmarkt 147 | 2511 DP | Den Haag

Postbus 16950 | 2500 BZ | Den Haag

www.ncsc.nl <http://www.ncsc.nl/>

.....

5.1 (2e)

5.1 (2e)

E 5.1 (2e) @ncsc.nl>

Van: [redacted] (NCSC-NL)
Verzonden: vrijdag 1 oktober 2021 13:45
Aan: Info (NCSC-NL)
Onderwerp: RE: Geen H\H melding NCSC-2021-0801

Helder [redacted]. Dank je wel.
Fijn weekend gewenst alvast.
Met vriendelijke groet,

[redacted]

.....

Ministerie van Justitie en Veiligheid
Nationaal Cyber Security Centrum
Turfmarkt 147 | 2511 DP | Den Haag
Postbus 16950 | 2500 BZ | Den Haag
www.ncsc.nl
.....
T [redacted]
M [redacted]
E [redacted]

From: Info (NCSC-NL)
Sent: vrijdag 1 oktober 2021 11:46
To: [redacted] (NCSC-NL)
Subject: RE: Geen H\H melding NCSC-2021-0801

Ha [redacted],

Je deductie is helemaal correct.
Het klopt dat de [redacted] dit beveiligingsadvies niet heeft ontvangen omdat dit product niet op hun foto staat.
Dit is ook de reden dat zij niet zijn gebeld.
Als je daar verdere vragen over hebt of over wil sparren, dan kunnen we ook altijd bellen.
Met vriendelijke groet,

[redacted]

.....

Nationaal Cyber Security Centrum
Postbus 117 | 2501 CC | Den Haag | www.ncsc.nl
.....
E [redacted]@ncsc.nl
T [redacted] (algemeen)
M [redacted] (mobiel)
PGP [redacted]
.....
Bezoekadres:
Turfmarkt 147 | 2511 DP | Den Haag

From: [redacted] (NCSC-NL) <[redacted]@ncsc.nl>
Sent: vrijdag 1 oktober 2021 11:00
To: Info (NCSC-NL) <info@ncsc.nl>
Subject: FW: Geen H\H melding NCSC-2021-0801

Beste collega,

Wbni heeft de onderstaande vraag gesteld over het gemis van een melding over de H/H voor Azure (https://www.ncsc.nl/actueel/advisory?id=NCSC-2021-0801)
Ik kom na onderzoek voor een antwoord op de onderstaande vraag van Wbni tot de volgende conclusie:

- Wbni heeft een actueel contactformulier uit 2020, inclusief contact voor bellen bij H/H
- Wbni heeft een enigszins verouderde foto uit 2018, of het product uit het beveiligingsadvies daar tussen staat kan ik niet vaststellen

Ik wil jullie het volgende vragen:

- Klopt het dat Wbni geen notificatie heeft ontvangen van dit beveiligingsadvies?
- Als dit inderdaad klopt, wat is dan de reden dat zij dit niet hebben ontvangen?

Met vriendelijke groet,

5.1 (2e)
5.1 (2e)
.....
Ministerie van Justitie en Veiligheid
Nationaal Cyber Security Centrum
Turfmarkt 147 | 2511 DP | Den Haag
Postbus 16950 | 2500 BZ | Den Haag
www.ncsc.nl
.....
T 5.1 (2e)
M 5.1 (2e)
E 5.1 (2e)@ncsc.nl

From: Wbni < Wbni >
Sent: vrijdag 17 september 2021 08:00
To: 5.1 (2e) (NCSC-NL) < 5.1 (2e)@ncsc.nl>
Subject: Geen H\H melding NCSC-2021-0801

Goedemorgen 5.1 (2e),

Deze week zagen we op internet een kwetsbaarheid mbt de azure omgeving. Door andere energie leveranciers werd vermeld dat het NCSC met een H\H melding zou komen. Deze hebben wij bij Wbni niet ontvangen. Echter op de site van NCSC bij de beveiligsadviezen staat wel een melding https://www.ncsc.nl/actueel/advisory?id=NCSC-2021-0801
Kun jij nagaan of er iets mis is gegaan.

With regards,

Wbni
ICT Security

E: Wbni
M: 5.1 (2e)
I: 5.1 (2e)

Wbni
Wbni
Wbni
Wbni
Wbni
Wbni

[redacted]

Before printing, think about the environment.

En nog een aanvulling met mogelijke meer generieke impact op tal van sectoren.

From: [redacted]
Sent: donderdag 18 augustus 2022 13:51
To: [redacted] (NCSC-NL)
Subject: RE: Geomagnetisch storm

Mijn antwoord was natuurlijk alleen strikt stroom-technisch.
GPS kan natuurlijk wel een tik krijgen, wat hier en daar problemen met tijdssynchronisatie kan opleveren.
Maar daar behoord iedereen een backup voor geregeld te hebben (we zullen het zien)

Regards,

[redacted]

[redacted]

[redacted]

Postadres
[redacted]

[redacted]

[redacted]

Aanwezig: Alle werkdagen

[redacted]

From: [redacted] (NCSC-NL) <[redacted]@ncsc.nl>
Sent: donderdag 18 augustus 2022 13:49
To: [redacted] <[redacted]>
Subject: RE: Geomagnetisch storm

Dank je [redacted], helder.
Ik ben ook wel benieuwd wat de verrichtingen van het KNMI zijn in het afgeven van verwachtingen voor de toekomst. En daarbij ook hoe hier vanuit de overheid (Ministerie IenW) scenariovoorbereiding op wordt gepleegd.

Mocht ik daar iets wijzer over worden dan is dat misschien iets om in de ISAC terug te koppelen.

Met vriendelijke groet,

5.1 (2e)
5.1 (2e)
.....
Ministerie van Justitie en Veiligheid
Nationaal Cyber Security Centrum
Turfmarkt 147 | 2511 DP | Den Haag
Postbus 16950 | 2500 BZ | Den Haag
www.ncsc.nl
.....
T 5.1 (2e)
M 5.1 (2e)
E 5.1 (2e)

From: 5.1 (2e)
Sent: donderdag 18 augustus 2022 13:38
To: 5.1 (2e) (NCSC-NL) <5.1 (2e)@ncsc.nl>
Subject: RE: Geomagnetisch storm

Dit houden we in de gaten.
Vooralsnog heb je lange lijnen nodig (langer dan in europa voorkomt) om hier last van te hebben, of netten hebben die dichter bij de polen liggen.

Stukken noord amerika en australie kunnen wel eerder last van hebben. (australie deze keer niet; het gros komt deze keer noordelijk aan)

In de toekomst is wel de verwachting dat de stormen sterker kunnen worden.

Regards,

5.1 (2e)
5.1(2e)
5.1(2e)

Wbni
7 Wbni
Wbni
Wbni

Postadres
Wbni
Wbni
Wbni
Wbni
Wbni
Wbni
Wbni

Factuuradres
Wbni
Wbni
Wbni

Wbni
Aanwezig: Alle werkdagen

[redacted]

From: [redacted] (NCSC-NL) <[redacted]@ncsc.nl>
Sent: donderdag 18 augustus 2022 13:33
To: [redacted] <[redacted]>
Subject: Geomagnetisch storm

Hai [redacted],

In de media was in het onderstaande bericht te lezen dat bij een sterke geomagnetische reactie zelfs elektriciteitscentrales hinder kunnen ondervinden. Is dit dan ook iets waar jullie je op voorbereiden of rekening mee houden?
Er dendert een magnetische golf af op aarde: dit is wat het voor ons betekent | NU - Het laatste nieuws het eerst op NU.nl

In ons contact met KNMI hebben we begrepen dat zij sinds 3 jaar een afdeling Space Weather hebben die dit soort dingen in de gaten houdt (https://www.knmi.nl/kennis-en-datacentrum/uitleg/ruimteweer)
Zoals ik begreep is de wolk ingeschaald in categorie 3 (van schaal 1 tot 5) en dit is een lichte categorie waarbij geen uitval te verwachten is voor Nederland.

Wij nemen dit soort ontwikkelingen uiteraard wel mee in onze beeldvorming, maar kunnen bij eventuele verstoringen natuurlijk niets betekenen. Wel vroegen wij ons af of er specifieke acties zijn in de energiesector om hier op te anticiperen.

Met vriendelijke groet,

[redacted]
Senior Relatiemanager
.....
Ministerie van Justitie en Veiligheid
Nationaal Cyber Security Centrum
Turfmarkt 147 | 2511 DP | Den Haag
Postbus 16950 | 2500 BZ | Den Haag
www.ncsc.nl
.....
T [redacted]
M [redacted]
E [redacted]@ncsc.nl

Van: 5.1 (2e) (NCSC-NL)
Verzonden: maandag 6 februari 2023 13:24
Aan: Wbni (SOC)
CC: 5.1 (2e); 5.1 (2e); 5.1 (2e); Info (NCSC-NL)
Onderwerp: Info digitale aanval IT-leverancier

Beste 5.1 (2e),

Zojuist heb ik al even telefonisch contact gehad met Wbni voor afstemming naar aanleiding van een digitale aanval op een IT-leverancier uit Duitsland.
In de Duitse media is melding gemaakt van een digitale aanval op Adesso, een grote IT leverancier in Duitsland. (Zie: https://www.heise.de/news/Cyberattacke-auf-IT-Dienstleister-Adesso-Systeme-kompromittiert-Daten-kopiert-7477544.html) Adesso is gecompromitteerd n.a.v een digitale aanval en er is data gelekt. Adesso is een grote IT leverancier aan o.a. de Duitse overheid. Wbni wordt op de Duitse website van Adesso genoemd als klant. Uit ons eigen onderzoek kunnen wij concluderen dat klanten van Adesso o.a. On-premise software van deze leverancier gebruiken. Enkele klanten zijn reeds geïnformeerd door Adesso dat alleen de SAAS omgeving is geraakt. Meerdere klanten zouden door de digitale aanval momenteel hinder ondervinden.
We proberen ten aanzien van de info dat Wbni klant zou zijn bij Adesso het volgende te duiden:

- Zijn jullie geinformeerd door Adesso?
- Welke services gebruiken jullie/nemen jullie af?
- Welke technische verbindingen hebben jullie met deze leverancier (VPN)?

Mochten jullie antwoord kunnen geven op de bovenstaande vragen of zelf nog aanvullende vragen of informatie voor ons hebben dan is het verzoek deze te sturen naar info@ncsc.nl Via dat loket plegen onze collega's namelijk alle triage op de informatie die binnenkomt en kunnen zij jullie waar nodig van verdere duiding voorzien. Neem mij gerust mee in de cc. zo blijf ik op de hoogte en kan ik waar nodig ondersteunen.
Mocht Wbni behoefte hebben aan dringend contact dan kunnen de volgende contactgevens van het NCSC worden gebruikt:
In het geval van een (dreigend) cybersecurity incident is het NCSC 24 uur per dag, 7 dagen in de week bereikbaar. Doe een melding altijd zo spoedig mogelijk telefonisch via het NCSC-alarmnummer: 070 - 5.1(2i)
Meldingen kunnen ook versleuteld worden gestuurd naar cert@ncsc.nl. De PGP-jaarkey waarmee het NCSC een beveiligde e-mail kan worden gestuurd is te vinden op onze website [https://www.ncsc.nl/contact/pgp-key]. Deze key is dit kalenderjaar geldig.
E-mails naar dit adres worden 's avonds en in het weekend regelmatig gelezen. Het advies is de bovenstaande alarmnummers ook op te nemen in bijvoorbeeld de crisishandboeken.
Let wel: deze alarmnummers zijn NIET ter verdere verspreiding buiten de eigen organisatie, aangezien deze nummers gekoppeld zijn aan NCSC-medewerkers met 24/7 piketdiensten voor onze doelgroepen.
Met vriendelijke groet,

5.1 (2e)
5.1 (2e)
.....
Ministerie van Justitie en Veiligheid
Nationaal Cyber Security Centrum
Turfmarkt 147 | 2511 DP | Den Haag
Postbus 16950 | 2500 BZ | Den Haag
www.ncsc.nl

.....

T 5.1 (2e)
M 5.1 (2e)
E 5.1 (2e) @ncsc.nl

Van: 5.1 (2e) (NCSC-NL)
Verzonden: maandag 13 december 2021 08:47
Aan: Info (NCSC-NL)
Onderwerp: RE: Ter info: WBNI melding

Goed te weten 5.1 (2e).
Dank voor het delen.

Met vriendelijke groet,

5.1 (2e)
5.1 (2e)
.....
Ministerie van Justitie en Veiligheid
Nationaal Cyber Security Centrum
Turfmarkt 147 | 2511 DP | Den Haag
Postbus 16950 | 2500 BZ | Den Haag
www.ncsc.nl
.....
T 5.1 (2e)
M 5.1 (2e)
E 5.1 (2e) @ncsc.nl

-----Original Message-----
From: Info (NCSC-NL)
Sent: zondag 12 december 2021 17:46
To: 5.1 (2e) (NCSC-NL)
Subject: Ter info: WBNI melding

Hallo 5.1 (2e),

Vandaag heeft Wbni een WBNI-melding gedaan, zie onderstaande.

Wbni, Incident Repsons Manager OT-security Wbni),
Wbni
Gesproken over telefoon: ivm Log4j kwetsbaarheid zijn OT en IT omgeving losgekoppeld. Morgen wordt verder onderzocht wat de impact van de kwetsbaarheid is in het bedrijf. Voor nu geen vragen. Mochten er morgen wel vragen zijn dan nemen zij contact op met NCSC.

Het leek mij handig om jou als accounthouder op de hoogte te stellen.
Het calamiteitenteam is ook op de hoogte. Als er morgen vragen komen dan zullen zij die beantwoorden.

Met vriendelijke groet,

5.1 (2e)
5.1 (2e)
.....
Nationaal Cyber Security Centrum
Postbus 117 | 2501 CC | Den Haag | www.ncsc.nl .....
E 5.1 (2e) @ncsc.nl
T 5.1 (2e) (algemeen)
M 5.1 (2e) (mobiel)

5.1(2e)
.....
Bezoekadres:
Turfmarkt 147 | 2511 DP | Den Haag

Beste collega's,

Onderstaand bericht ontving ik gisteren van ons contactpersoon bij [redacted]. Deze casus was mij nog niet bekend.

Met vriendelijke groet,

[redacted]
.....
Ministerie van Justitie en Veiligheid
Nationaal Cyber Security Centrum
Turfmarkt 147 | 2511 DP | Den Haag
Postbus 16950 | 2500 BZ | Den Haag
www.ncsc.nl
.....
T [redacted]
M [redacted]
E [redacted]@ncsc.nl

Van: [redacted] <[redacted]>
Verzonden: woensdag 3 augustus 2022 11:06
Aan: [redacted] - BD/NCSC/SK <[redacted]@minjenv.nl>
CC: [redacted]; [redacted]
Onderwerp: threat Intel related to Wind Industry

- German power electronics manufacturer [redacted] has disclosed that it was hit by a ransomware attack that partially encrypted the company's network. [redacted] has over 3,000 employees in 24 offices and 8 production sites worldwide across Germany, Brazil, China, France, India, Italy, Slovakia, and the USA, with a turnover of around $461 million in 2020. It also says it's one of the world's leading power engineering component manufacturers, with 35% of the wind turbines installed each year operating with its technologies. More: **MailScanner has detected a possible fraud attempt from "eur02.safelinks.protection.outlook.com" claiming to be** https://www.bleepingcomputer.com/news/security/semiconductor-manufacturer-[redacted]-hit-by-lv-ransomware-attack/?fbclid=IwAR3rJJHoYeIfN5H3gUQVWWPzUds055hr1bFW_i6QmR76PmM5f3oYYz3mcSA

Hoi [redacted],
Bovenstaande is wellicht iets om te delen met onze vrienden van de diensten?
Wij zijn niet geraakt of gecompromitteerd geweest.

Met vriendelijke groet / Best regards

[redacted]

5.1 (2e)

Confidentiality: C2 - Internal

Goedemorgen collega,

Was ons de info uit dit nieuwsbericht al bekend?
Luxembourg energy companies struggling with alleged ransomware attack, data breach - The Record by Recorded Future

Met vriendelijke groet,

5.1 (2e)
5.1 (2e)
.....
Ministerie van Justitie en Veiligheid
Nationaal Cyber Security Centrum
Turfmarkt 147 | 2511 DP | Den Haag
Postbus 16950 | 2500 BZ | Den Haag
www.ncsc.nl
.....
T 5.1 (2e)
M 5.1 (2e)
E 5.1 (2e) @ncsc.nl

Thanks!

Met vriendelijke groet,

5.1 (2e)
5.1 (2e)
.....
Ministerie van Justitie en Veiligheid
Nationaal Cyber Security Centrum
Turfmarkt 147 | 2511 DP | Den Haag
Postbus 16950 | 2500 BZ | Den Haag
www.ncsc.nl
.....
T 5.1 (2e)
M 5.1 (2e)
E 5.1 (2e) @ncsc.nl

From: Info (NCSC-NL)
Sent: dinsdag 2 augustus 2022 15:17
To: 5.1 (2e) (NCSC-NL)
Subject: RE: Nieuwsbericht energiebedrijven Luxemburg

Hai 5.1 (2e),

Ik heb met LU-CIRCL contact gehad. Zij zijn op de hoogte van het incident en houden een oogje in het zeil. Daarnaast heeft hij een aantal MISP-events doorgegeven. Deze zijn op 25 juli door ons als gedeeld binnen het NDN.

Mochten er nog vragen zijn, dan lees ik die graag.

Gr, 5.1 (2e)

From: 5.1 (2e) (NCSC-NL) 5.1 (2e) @ncsc.nl>
Sent: dinsdag 2 augustus 2022 10:24
To: Info (NCSC-NL) <info@ncsc.nl>
Subject: RE: Nieuwsbericht energiebedrijven Luxemburg

Hai 5.1 (2e) ,

Hebben wij contacten bij onze evenknie in Luxemburg om eventueel nog nadere info te vragen? Of verwacht jij dat er niet meer info zal zijn dan dit bericht al geeft?

Met vriendelijke groet,

5.1 (2e)
5.1 (2e)
.....
Ministerie van Justitie en Veiligheid
Nationaal Cyber Security Centrum
Turfmarkt 147 | 2511 DP | Den Haag
Postbus 16950 | 2500 BZ | Den Haag
www.ncsc.nl
.....
T 5.1 (2e)
M 5.1 (2e)
E 5.1 (2e) @ncsc.nl

From: Info (NCSC-NL) <info@ncsc.nl>
Sent: dinsdag 2 augustus 2022 09:26
To: 5.1 (2e) (NCSC-NL) <5.1 (2e) @ncsc.nl>
Subject: RE: Nieuwsbericht energiebedrijven Luxemburg

Goedemorgen 5.1 (2e) ,

Dank je wel voor het doorgeven. Dit bericht hadden we nog niet eerder gezien.

Gr, 5.1 (2e)

From: 5.1 (2e) (NCSC-NL) <5.1 (2e) @ncsc.nl>
Sent: dinsdag 2 augustus 2022 07:47
To: Info (NCSC-NL) <info@ncsc.nl>
Subject: Nieuwsbericht energiebedrijven Luxemburg

Goedemorgen collega,

Was ons de info uit dit nieuwsbericht al bekend?
Luxembourg energy companies struggling with alleged ransomware attack, data breach - The Record by Recorded Future

Met vriendelijke groet,

5.1 (2e)
5.1 (2e)
.....
Ministerie van Justitie en Veiligheid
Nationaal Cyber Security Centrum
Turfmarkt 147 | 2511 DP | Den Haag
Postbus 16950 | 2500 BZ | Den Haag
www.ncsc.nl
.....
T 5.1 (2e)
M 5.1 (2e)
E 5.1 (2e) @ncsc.nl

Graag gedaan, 5.1 (2e).
Hot topic inderdaad. Houd het in de gaten :)

Gr, 5.1 (2e)

-----Original Message-----
From: 5.1 (2e) (NCSC-NL) <5.1 (2e)@ncsc.nl>
Sent: vrijdag 5 augustus 2022 11:42
To: Info (NCSC-NL) <info@ncsc.nl>
Subject: RE: Woningcorporaties melden datalek na cyberaanval op energiedienstverlener ista

Thanks 5.1 (2e), dit was mij nog niet bekend.
De energiesector is wel hot de laatste tijd.

Met vriendelijke groet,

5.1 (2e)
5.1 (2e)
.....
Ministerie van Justitie en Veiligheid
Nationaal Cyber Security Centrum
Turfmarkt 147 | 2511 DP | Den Haag
Postbus 16950 | 2500 BZ | Den Haag
www.ncsc.nl
.....
T 5.1 (2e)
M 5.1 (2e)
E 5.1 (2e)@ncsc.nl

-----Original Message-----
From: 5.1 (2e) (NCSC-NL) <5.1 (2e)@ncsc.nl>
Sent: donderdag 4 augustus 2022 12:58
To: 5.1 (2e) (NCSC-NL) <5.1 (2e)@ncsc.nl>
Subject: Woningcorporaties melden datalek na cyberaanval op energiedienstverlener ista

Hi 5.1 (2e),

ter info.

gr, 5.1 (2e)

Verschillende woningcorporaties waarschuwen huurders voor een datalek nadat energiedienstverlener ista vorige week het ...

More info:
https://www.security.nl/posting/763659/Woningcorporaties+melden+datalek+na+cyberaanval+op+energiedienstverlener+ista?channel=rss

Van: 5.1 (2e) (NCSC-NL) <5.1 (2e)@ncsc.nl>
Verzonden: dinsdag 4 april 2023 13:51
Aan: Wbni <Wbni>
CC: Info (NCSC-NL) <info@ncsc.nl>
Onderwerp: NCSC Duiding Vulkan bestanden

Ha5.1 (2e),

In navolging van ons telefoongesprek gisteren: het NCSC heeft een korte duiding van de Vulkan bestanden opgesteld die ik met je mag delen onder **TLP Amber+Strict.**

Bij verdere inhoudelijke vragen adviseer ik je contact op te nemen met ons Fusion Center (info@ncsc.nl). Daarmee heb je een meer directe lijn tot de operationele medewerkers van het NCSC dan via mij.

Ik hoop dat je hiermee bent geholpen!

Met vriendelijke groet,

5.1 (2e)
5.1 (2e)
.....
Ministerie van Justitie en Veiligheid
Nationaal Cyber Security Centrum
Turfmarkt 147 | 2511 DP | Den Haag
Postbus 16950 | 2500 BZ | Den Haag
www.ncsc.nl
.....
T 5.1 (2e)
M 5.1 (2e)
E 5.1 (2e)@ncsc.nl

TLP:AMBER+Strict

Duiding Vulkan bestanden

Essentie:

- Op 30 maart 2023 publiceerden diverse media een nieuwsartikel over meer dan 5000 gelekte documenten, afkomstig van NTC Vulkan, een in Moskou gevestigde softwareleverancier [1][2].
- De gelekte documenten geven deels inzage in de capaciteit van de Russische digitale oorlogsvoering en onthullen het bestaan van de softwaresystemen: Scan-V, Amesit en Krystal-2B. Ook de bijbehorende contracten zijn gelekt.
- Een van de documenten koppelt een van de softwaresystemen aan de Russische statelijke actor SANDWORM. Dit specifieke softwareproduct doorzoekt het internet naar potentiele doelwitten en kwetsbaarheiden voor initial access. Ook verwijzingen naar andere Russische statelijke actoren worden genoemd [1][2].
- Het gaat om een tijdsperiode van 2016 tot 2021. Het is onbekend of de systemen daadwerkelijk in gebruik zijn genomen, of in gebruik zijn.
- Het NCSC houdt rekening met een digitale dreiging vanuit Russische statelijke actoren. Dit is het meest recent beschreven in de “dreigingsscenario’s voor Nederland in relatie tot de oorlog in Oekraïne” van december 2022. De geanalyseerde documenten uit de Vulkan Files geven het NCSC **geen aanleiding** deze eerdere dreigingsanalyse bij te stellen.

Situatie:

Op 30 maart, 2023 hebben de nieuwsorganisaties Der Spiegel, the Guardian, Papertrail Media, Le Monde en de Washington Post een artikel gepubliceerd over meer dan 5000 gelekte documenten, afkomstig van NTC Vulkan, een in Moskou gevestigde softwareleverancier. De gelekte informatie onthult het bestaan van drie softwaresystemen, namelijk: Scan-V, Amesit en Krystal-2B.

Scan-V

Scan-V is de codenaam van een taak- planningsbeheersysteem ter ondersteuning van (des)informatie- en cyberoperaties. De uitgelekte documenten wijzen op een softwareonderdeel, dat zich richt op het maken en visueel weergeven van aanvalsscenario’s en grafieken in de vorm van bijvoorbeeld netwerktopologieën. Een tweede onderdeel lijkt te worden gebruikt voor het verzamelen en opslaan van (netwerk)gegevens en kwetsbaarheden in een database. Op basis van gelekte contracten en de ondertekenaars, wordt de Russische statelijke actor: SANDWORM genoemd als mogelijke opdrachtgever [1][2].

Capabilities: de mogelijkheden die worden beschreven in de documentatie kunnen het (deels) geautomatiseerd uitvoeren van de verkenningsfase en de algehele coördinatie bevorderen. De gelekte documenten bevatten niet voldoende informatie voor technische indicatoren of detectieve maatregelen [3].

Amesit-V

Amesit-V is een softwaresysteem meer zeer diverse mogelijkheden. Met één van de onderdelen is het mogelijk om neppe sociale media accounts aan te maken ter ondersteuning van desinformatiecampagnes. Met het tweede onderdeel is het mogelijk om internetverkeer te monitoren binnen de grenzen van Rusland. De derde functionaliteit richt zich op het identificeren van potentiele doelwitten, door kwetsbare systemen in kaart te brengen [3].

Capabilities: de mogelijkheden die worden beschreven in de documentatie van Amesit-V kunnen een volledige desinformatiecampagne ondersteunen. Van het monitoren van het medialandschap, creëren van content om een bepaald narratief te promoten, tot het tot stand brengen en verspreiden van de inhoud [3].

Krystal-2B

Krystal-2B is een trainingsprogramma wat gericht is op het aanvallen van IT/OT-netwerken, maar ook het verdedigen van deze netwerken. Krystal-2B lijkt op een trainingsprogramma in de vorm van een capture-the-flag, red-teaming en/of blue-teaming, maar toont de interesse van de Russische overheid in het gecoördineerd aanvallen van IT-OT-netwerken. De documenten beschrijven meerdere keren de term ICS (in het Russisch), het is onduidelijk of het gebruik van deze term ook doelt op OT-systemen [3].

Capabilities: Krystal-B biedt de mogelijkheid om operators te trainen in zowel het digitaal aanvallen van IT/OT-netwerken als het verdedigen van deze netwerken. Het trainingsprogramma bestaat uit een aantal publiek beschikbare softwareproducten als SNORT, Kali Linux en MetaSploit. Hoewel de nieuwsorganisaties en Mandiant specifiek OT-systemen noemen, kan het NCSC dit niet opmaken uit de gelekte documenten [3].

Duiding:

- Het is niet duidelijk of de genoemde softwaresystemen in gebruik zijn, nog ontwikkeld worden, of alleen besteld zijn door de Russische overheid [3].
- De gelekte documenten veranderen het dreigingsbeeld van het NCSC-NL niet. Het is algemeen bekend dat Russische statelijke actoren opzoek zijn naar manieren om toegang te verkrijgen tot (cruciale) infrastructuur [4]. De genoemde softwaresystemen zijn puur ter ondersteuning van dit doel, maar verhogen de dreiging niet.
- Energienetwerken en –systemen zijn in het verleden doelwit geweest van verstoringen door Russische statelijke actoren. Dergelijke aanvallen, met name als het gaat om het compromitteren van OT-systemen, zijn complex, vereisen training en worden vaak uitgevoerd door actoren met veel middelen. Het ligt in de lijn der verwachting dat hiervoor trainingsprogramma's worden gebruikt.
- Modus Operandi: de softwareproducten Scan-V en Amesit-V bevatten beide ondersteunende softwareonderdelen voor (de coördinatie) van informatie- en cyber-operaties. De overlap hierin is sterk aanwezig en laat zien dat de Russische overheid beide inzet, als een gecombineerd middel en wellicht ook ziet als één middel [3].
- Gezien het volume en de complexiteit van de gelekte informatie is het mogelijk dat er meer technisch details met betrekking tot de exacte reikwijdte van de Vulkan-programma's en hun implicaties gepubliceerd gaan worden.

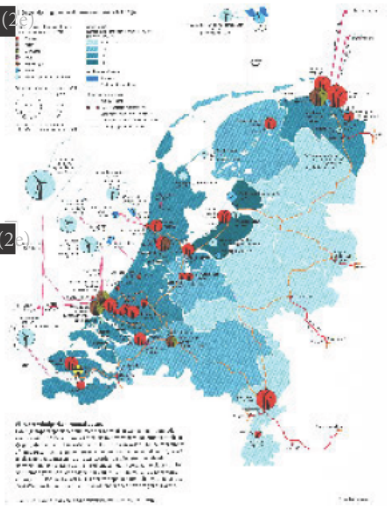
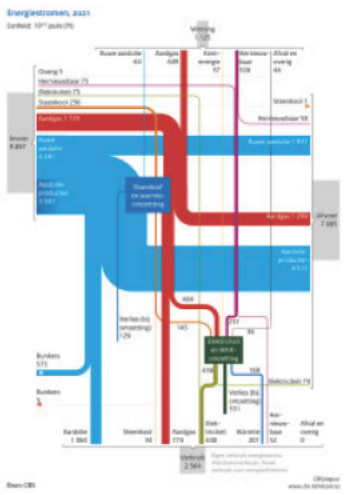
[1] https://www.theguardian.com/technology/2023/mar/30/vulkan-files-leak-reveals-putins-global-and-domestic-cyberwarfare-tactics

[2] https://www.washingtonpost.com/national-security/2023/03/30/takeaways-vulkan-files-investigation/

[3] Gelekte NTC Vulkan documenten

[4] https://www.aivd.nl/documenten/publicaties/2022/11/28/dreigingsbeeld-statelijke-actoren-dbsa-2

Energie

Relatiemanager	5.1(2	**Energiebeeld NL 2030** *(klik en zoom in)* 	**Energie NL in cijfers 2022** *(klik en zoom in)* A4-digitaa .pdf	**Energiestromen NL 2021** *(klik en zoom in)* 	**Stake** 20
Achtervang RM	5.1(2				
Adviseurs &K					
Expert IRON					
Expertise CTI					
Dossierhouder FC					
Tags	energie				

Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

Start cybersecurity overzicht

Maandelijks doelgroepbeeld Energie - 2022

	31 Mar 2023 [redacted] **(NCSC-NL)**

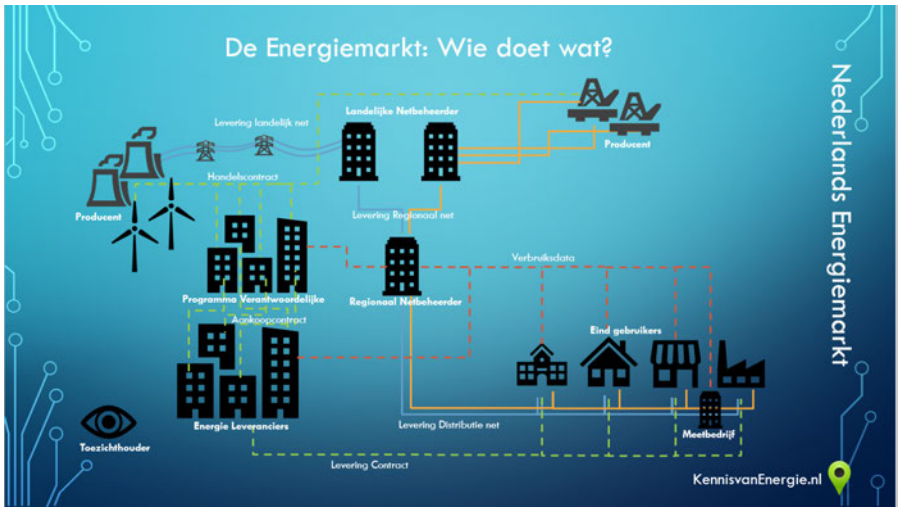
1 Dreigingen	• *Reconnaissance*
	  • (4 oktober 2022) - **TLP: AMBER** [redacted] ziet sinds 24-09-2022 een verandering van het dreigingsbeeld. De dreigingen lijken meer gericht (DOS, (spear-)phishing, scans). Mitigatie volstaat.
	  • (25 november 2022) - 'Russische hackers hebben het gemunt op Nederlandse gasinstallaties' | RTL Nieuws/ Dit is waarom onze LNG-terminals interessant zijn voor hackers | RTL Nieuws
	• *Verstoring & sabotage*:
	  • (januari 2022) Verschillende energiepart jen geven aan scenariovoorbereidingen te treffen naar aanleiding van de situatie in de Oekraïne. Netbeheerders bereiden zich voor op voorzorgsmaatregelen gekoppeld aan het dreigingsniveau. De mogelijke voorzorgsmaatregelen richten zich op detectie & monitoring, beperken van bedienen op afstand, freeze op kritieke systemen, overschakelen naar 'eilandbedrijf'.
	  • (april 2022) Industroyer2 richt zich op ICS-systemen van Oekraïens energiebedrijf. B j de aanval op een Oekraïens energiebedrijf is deze nieuwe ICS-malware ontdekt. Geen aanwijzingen bekend over een eventuele impact op Nederland.
	  • (april 2022) Nieuwe malware richt zich op ICS/SCADA-apparatuur. CISA, Mandiant en Dragos rapporteren over een nieuwe set malware (PIPEDREAM en INCONTROLLER benoemd) die zich richt op ICS/SCADA-apparatuur. Deze malware is nog niet aangetroffen bij een daadwerkel jke aanval. De malware richt zich volgens Dragos op vloeibaar gas- en stroomvoorzienings-omgevingen, maar kan aangepast worden op andere omgevingen.
	  • (2022) Meerdere incidenten in de energiesector hebben betrekking gehad op de supply chain, zoals fabrikanten van turbines en semiconductors en bedrijven voor onderhoud en beheer.
	  • (16 maart 2023) - Microsoft: Russische hackers werken aan groot offensief met cyberaanvallen - NRC
	• *(Economische) Spionage*:
	  • (februari 2022) Jaarrapportage meldplicht datalekken 2021 gepubliceerd door AP. In 2021 zag de AP opnieuw een explosieve toename van het aantal meldingen van datalekken veroorzaakt door cyberaanvallen. Dit aantal is in 2021 bijna verdubbeld ten opzichte van het jaar daarvoor. Overzichten datalekken | Autoriteit Persoonsgegevens
	• *Cybercrime*:
	  • Ransomware: volgens Mandiant bestaan er 7 Ransomware families die ook ICS process kill lists bevatten. Financially Motivated Actors Are Expanding Access Into OT: Analysis of Kill Lists That Include OT Processes Used With Seven Malware Families | Mandiant
	  • Ransomware: er wordt sinds 2017 een toename waargenomen van ransomware aanvallen op zowel IT als OT die gericht z jn op het ontregelen van industriële processen. Ransomware Against the Machine: How Adversaries are Learning to Disrupt Industrial Production by Targeting IT and OT | Mandiant

2 Belangen	• Territoriale veiligheid/ Continuïteit samenleving - Productie, transmissie en distributie van elektriciteit en gas. Geredeneerd vanuit de ketenafhankelijkheden is continuïteit/ leverzekerheid het kernbelang. • Economische veiligheid/ intellectueel eigendom - Ontwikkelingen aangaande deze belangen vloeien o.a. voort uit de geopolitiek van de energietransitie (innovatie groene technologieën) en de internationale afhankelijkheden op het gebied van energie (gaswinning en Europees electriciteitsnet) Energie en Geopolitiek - HCSS
3 Weerbaarheid	• Signalen van diverse partijen in de energiesector dat schaarste in de capaciteit (kennis & ervaring cyber security) in toenemende mate van invloed zijn op de ambities. Een groot aantal vacatures voor Cyber Security functies staat langere t jd open.

4 Incidenten *(afgelopen 12 maanden)*	• (19 november 2021) - Wbni: Third update on cyber incident Wbni .com) • (24 februari 2022) – Satellite disruption, Wbni Service News Detail Wbni .de) • (4 april) **TLP: AMBER** Onderzoek van Finse CERT heeft uitgewezen dat ook in NL enkele windturbines benaderbaar zijn via het publieke internet. Alhoewel wel heel veel details van deze windturbines en de onderliggende systemen vr j geraadpleegd kunnen worden, is niet duidelijk wie de eigenaar is. Hierop is CSIRT-DSP gewezen op deze situatie met het verzoek via de betreffende DSP de eigenaar van de windturbines te verwittigen. Bron: Finse CERT • (31 maart 2022) - Wbni: Update on cyber security incident - Wbni Wbni .com) • (11 april 2022) - Wbni: Press information of Wbni Wbni .com) • (25 april 2022 - Article, The Wall Street Journal: European Wind-Energy Sector Hit in Wave of Hacks - WSJ • (13 juni 2022) Twee Duitse energiebedrijven geraakt door Blackcat ransomware. Bronnen: CERT Bund, Hackers knock out two German energy suppliers | Cybernews, Heise.de • (juli 2022) - Energiebedrijf in Zweden getroffen door aanval, met dataextractie en afpersing ten gevolge. Bron: Zweedse CERT, zonder naam van het getroffen bedr jf. • (juli 2022) - Twee energiebedr jven in Luxemburg getroffen door ransomware. Bronnen: The Record Media, Security.nl • (juli 2022) - Duitse energiedienstverlener Wbni getroffen door een cyberaanval, met datalek voor woningcorporaties in NL ten gevolge. Security.nl • (4 augustus 2022) - Wbni Duitse fabrikant van semiconductors voor energiesystemen getroffen door een ransomwareaanval met dataextractie. Bron: Media Statement • (29 augustus 2022) - **TLP: AMBER** Wbni meldt b j NCSC de compromittatie van een Outlook-account middels spearphishing met fraude in betalingsverkeer ten gevolge. • (26 oktober 2022) - Duits regionaal energiebedr jf getroffen door cyberaanval. IT-Störung bei enercity • (27 december 2022) - Hackers stole data from multiple electric utilities in recent ransomware attack | CNN Politics • (31 januari 2023) - IT Army of Ukraine gained access to 1.5GB archive from GazpromSecurity Affairs • (31 januari 2023) - New Report Reveals NikoWiper Malware That Targeted Ukraine Energy Sector (thehackernews.com) • (10 maart 2023) - Kaspersky ziet aanvalsgolf in energiesector | Computable.nl
5 Thema's	• **Laadpaalinfrastructuur** vormt door het gezamelijke vermogen een aanzienl jk risico voor de stabiliteit van het Electriciteitsnet. Er is gezamenlijk overleg tussen de departementen IenW en EZK, het Agentschap Telecom, de sector, ELaadNL en het NCSC. • **Slimme meters** vormen een (IoT) risico, voornamelijk op het gebied van privacy en data-integriteit. Netbeheerder worden in toenemende mate geconfronteerd met de uitdagingen in de beveiliging van de slimme meter en de energiedata. De ontw kkelingen op het gebied van regulering, normeringen en toezichthouder vragen de aandacht en capaciteit van energiepart jen. • **Zonnepanelen** en dan in concreto (Chinese) omvormers zouden beveiligingslekken bevatten (juli 2022), waardoor de veiligheid van de stroomvoorziening in gevaar komt. Dit onderwerp is zowel in de sector als in de media een terugkerend onderwerp van aandacht. In juli 2022 z jn kamervragen gesteld naar aanleiding van de publicatie van een kwetsbaarheid in Chinese omvormers. (Security.nl) De kwetsbaarheid is inmiddels verholpen. NCSC heeft hierin haar rol vervuld als coördinator van de CVD. • **Windturbines** z jn sinds eind 2021 prominent in beeld gekomen door ransomware aanvallen op de twee grootste fabrikanten in Europa Wbni) en één van de grootste onderhoudspartijen in Europa Wbni) (juli 2022) De casus Wbni (ransomware aanval op windturbinefabrikant) heeft politieke aandacht gekregen en geleid tot kamervragen. Ook in de community is de cyberveiligheid van windturbines als vitale infra onder de aandacht. (Cybersecurity blogger)
6 Politiek	• (juli 2022) Kamervragen over het hacken via Chinese zonnepanelen (Verslag Tweede Kamer) (Security.nl) • (augustus 2022) Kamervragen over het hacken van windturbines (Verslag Tweede Kamer, (Security.nl) • (februari 2023) Minister: gasleveranciers zelf verantwoordelijk voor digitale weerbaarheid - Security.NL (Antwoord op vragen van het lid Bontenbal over het bericht 'Russische hackers hebben het gemunt op Nederlandse gasinstallaties' | Tweede Kamer der Staten-Generaal)
7 Regelgeving	• (14 januari 2022) Entsoe levert conform planning het voorstel voor de 'European Network Code on Cybersecurity' op aan ACER. Meer info: Cybersecurity (entsoe.eu) • Om de veerkracht tegen cyberrisico's in het elektriciteitssysteem te vergroten, is de Europese Commissie voornemens om (samen met ACER, ENTSB-E en de EU DSB-entiteit) een gedelegeerde handeling voor te stellen in de vorm van een netcode voor cyberbeveiligingsaspecten van grensoverschrijdende elektriciteitsstromen, die voortvloeit uit de eisen van artikel 59, lid 2, punt e), van de elektriciteitsverordening, met inbegrip van regels inzake gemeenschappelijke minimumeisen, planning, monitoring, rapportering en crisisbeheer, met het oog op vaststelling begin 2023. • EZK en AT nemen deel in werkgroepen waarin de Network Code wordt besproken. Midden juli begint de comitologie waar lidstaten verder onderhandelen over de Netcode. De verordening zal in januari 2023 van kracht worden, en is dan gel jk van toepassing in de lidstaten. Er is dus geen uitvoerings- of implementatiewet nodig (zoals bij de Wbni van de NIB). • Na 6 tot 9 maanden zijn de eerste entiteiten geïdentificeerd en kunnen deze dus kunnen ze dan al aangesloten worden op CSIRT. De crisis structuren moeten wel na 6 maanden al staan (zonder dat het nog echt operationeel is). • (november 2022) Ter voorbereiding op de implementatie van de 'European Network Code on Cybersecurity' is er een werkgroep actief bestaande uit NCSC, EZK en AT. Doel is een advies hoe de CSIRT-taken uit de Network Code in Nederland te beleggen. • (november 2022) Europese Commissie presenteert EU-actieplan voor de digitalisering van het energiesysteem | Expertisecentrum Europees Recht (minbuza.nl) • (6 december 2022) Kamerbrief over aanbieders essentiële diensten in de gas- en oliesector ter bevordering van de digitale veiligheid | Kamerstuk | Rijksoverheid.nl • (maart 2023) EZK heeft een BBNI-wijziging voorgesteld op basis waarvan laadpaalexploitanten aangewezen kunnen worden als AAVA ('andere aangewezen vitale aanbieder'). Hiermee zouden zij wel een meldplicht krijgen, maar geen zorgplicht. De schatting is dat dit tussen de 6 - 10 CPO's (Charging Point Operators = laadpaalexploitanten) gaat betreffen. Zoals de verwachting nu is afgegeven zal deze aanw jzing per juli 2023 van kracht zijn.

8 Samenwerking	• (januari 2022) T jdens een drietal Infosessie's (2xNL, 1xENG) van het NCSC hebben 11 nieuwe AED's uit de energiesector een toelichting gekregen op de rol en taken van het NCSC en de wijze waarop de samenwerking met de doelgroeppartijen kan worden opgestart en uitgebouwd. Hoofddoelstelling voor deze partijen de primaire aansluiting (intake) in gang te zetten is behaald. • (16 maart 2022) In samenwerking met Netbeheer Nederland heeft een verdiepende sessie Incidenthandling plaatsgevonden. Dit is een vervolg op een sessie in 2021. Netbeheer Nederland en NCSC hebben uitgesproken de samenwerking voor incidenthandling verder te verdiepen en ontwikkelen. • (6 april 2022) De CISO's van de landelijke en regionale netbeheerders hebben tijdens een strategische sessie met het NCSC en de NCTV verschillende onderwerpen besproken. Aan de orde z jn gekomen: Crisispreparatie NCSC en de visie op samenwerking, de uitwisseling van dreigingsbeelden en –scenario's waarop de sector maatregelen kan bepalen, de ontw kkeling van het cyberstelsel in NL. • (oktober 2022) Samen met Netbeheer Nederland worden in het najaar van 2022 enkele sessie's gepland. O.a. op 4/10 MASKER ten behoeve van een sectoraal dreigingsbeeld voor de netbeheerders. En op 28/11 een verdiepingssessie Meldingproces WBNI en ondersteuning NCSC. • (oktober 2022) Topsector Energie, actief op de thema's digitalisering en energietransitie. Met de programmadirecteur Topsector Energie Digitalisering een verkenning gestart voor nadere samenwerking. In oktober zal een bijdrage worden geleverd aan de webinar verdiepingsessie Cybersecurity. Tevens lopen de initiatieven tot het oprichten van ISAC's voor verschillende sub-sectoren (laapalen, windenergie, zonne-energie). Verkenning gestart naar samenwerking cybersecurity binnen energiesector | Topsector Energie
9 Ontwikkelingen	• Vitaliteitsbeoordeling voor olie en gas in opdracht van EZK momenteel in uitvoering door Clingendael. Uitkomsten van beide vitaliteitsbeoordelingen vormen de basis voor AED-aanw jzing door EZK. Verwachting is medio 2022 een uitbreiding van flink aantal AED's in de sector petrochemie/ gas (opslag, verwerking).
10 Onderzoeken	• **Opdrachtgever**: Topsector Energie, **Thema**: Digitale innovaties energietransitie, **Termijn**: september 2022 resultaten met vervolgstappen voor 2023, **Toelichting**: Adviesbureau Baringa heeft de afgelopen maanden een uitgebreid onderzoek gedaan naar de voorwaarden en bouwstenen voor een referentie-architectuur voor de Nederlandse energie-infrastructuur. • **Opdrachtgever**: TU Delft, **Thema**: Control Room of the future, **Termijn**: NN, **Toelichting**: TU Delft's Control Room of the Future maakt elektriciteitsnet digitaal weerbaar. • **Opdrachtgever**: Agentschap Telecom & Topsector Energie, programma Digitalisering, **Thema**: Risico's connectiviteit hoogvermogensystemen achter de meter, **Termijn**: NN, **Toelichting**: NN • **Opdrachtgever**: NN, **Thema**: NN, **Termijn**: NN, **Toelichting**: NN
11 Agenda	• 04 Oct 2022 MASKER Netbeheer Nederland, 5.1 (2e) (NCSC-NL) 5.1 (2e) (NCSC-NL) 5.1 (2e) (NCSC-NL) • 24 Mar 2023 Tweede sessie MASKER Netbeheer Nederland, 5.1 (2e) (NCSC-NL) 5.1 (2e) (NCSC-NL) 5.1 (2e) 5.1 (2e) (NCSC-NL) 5.1 (2e) (NCSC-NL) • medio mei Risicomanagement MASKER Netbeheer Nederland, 5.1 (2e) (NCSC-NL) 5.1 (2e) (NCSC-NL) 5.1 (2e) (NCSC-NL) • 16 May 2023 Energy ISAC 5.1 (2e) (NCSC-NL) • 04 Jul 2023 Energy ISAC 5.1 (2e) (NCSC-NL) • 12 Sep 2023 Energy ISAC gezamenlijk met Water ISAC 5.1 (2e) (NCSC-NL) 5.1 (2e) (NCSC-NL) • 28 Nov 2023 Energy ISAC 5.1 (2e) (NCSC-NL)
12 Nuttige contacten *(contactinfo in CRM)*	• 5.1 (2e) betrokken en daadkrachtige ingang voor de connectie met de netbeheerders, tevens goed zicht en contact met kritieke ketenpartners. • 5.1 (2e) kennisdrager security i.r.t. het nationale energienet en grensoverschrijdende elektriciteitsstromen. • 5.1 (2e) - technisch kennisdrager OT-security in de energiesector en toegang tot netwerk SOC's van de netbeheerders. • 5.1 (2e) - kennisdrager security i.r.t. het nationale gasnet en grensoverschrijdend gastransport/ LNG-terminals. • 5.1 (2e) - ingang voor nadere info omtrent windparken op zee.

Wie doet wat NL	**Regio's Netbeheerders Electriciteit (Landelijk Netbe**



WBNI >NIS2 transitie	Sector	Aanbieder	Essentiële dienst	Aantal doelgroeppartij (-en) onder WBNI	NIS2
	Energie: elektriciteit	De netbeheerder van het landelijk hoogspanningsnet, aangewezen op grond van artikel 10, tweede lid, of 14 van de Elektriciteitswet 1998	Transmissie en distributie van elektriciteit	1 [redacted]	
	Energie: elektriciteit + gas	De regionale ne beheerders, aangewezen op grond van artikel 10 negende lid, 13 eerste lid, of 14 van de Elektriciteitswet 1998 De regionale ne beheerders, aangewezen krachtens artikel 2, achtste lid, of 5 van de Gaswet	Transmissie en distributie van elektriciteit Transmissie en distributie van gas	6	
	Energie: elektriciteit	[redacted]	Transmissie van elektriciteit (landsgrensoverschrijdend)	1 [redacted]	
	Energie: elektriciteit	Een elektriciteitsbedrijf als bedoeld in Bijlage II van de NIB-richtlijn, dat één of meerdere productie-installaties als bedoeld in artikel 1, eerste lid, onder ah, van de Elektriciteitswet 1998, beheert met een cumulatief nominaal vermogen van ten minste 100 MegaWatt	Productie van elektriciteit	22	
	Energie: elektriciteit	De bij besluit van Onze Minister van Economische Zaken en Klimaat aangewezen elektriciteitsbedrijven, als bedoeld in Bijlage II van de NIB-richtlijn	Levering of aankoop van elektriciteit	0	
	Energie: elektriciteit	Exploitanten van oplaadpunten met een totaal opgesteld laadvermogen van minimaal 300 megawatt (300.000 kilowatt)	Beheer en de exploitatie van een oplaadpunt dat een laaddienst levert aan particuliere en/of zakelijke eindgebruikers, onder meer namens en voor rekening van een aanbieder van mobiliteitsdiensten	tussen de 5 en 10 laadpaalexploitanten	
	Energie: gas	De netbeheerder van het landelijk gastransportnet, aangewezen op grond van artikel 2, eerste lid, of 5 van de Gaswet	Transmissie en distributie van gas	1 [redacted]	
	Energie: gas	[redacted]	Het opsporen en winnen van gas op basis van de concessie voor de aardgaswinning uit het Groningenveld op grond van het koninklijk besluit van 30 mei 1963, nr. 39 (Stcrt. 1963, 126) Het opslaan van gas op basis van de opslagvergunning «Norg» van 31 maart 2003 (Stcrt. 2003, 68)	1 [redacted]	
	Energie: gas	De bij besluit van Onze Minister van Economische Zaken en Klimaat aangewezen leveringsbedrijven, als bedoeld in Bijlage II van de NIB-richtlijn	Levering van gas	0	
	Energie: gas	De bij besluit van Onze Minister van Economische Zaken en Klimaat aangewezen opslagsysteembeheerders, als bedoeld in Bijlage II van de NIB-richtlijn	Opslag van gas	0	
	Energie: gas	De bij besluit van Onze Minister van Economische Zaken en Klimaat aangewezen LNG-systeembeheerders, als bedoeld in Bijlage II van de NIB-richtlijn	Het vloeibaar maken van aardgas of de invoer, de verlading en de hervergassing van LNG	0	
	Energie: gas	De bij besluit van Onze Minister van Economische Zaken en Klimaat aangewezen aardgasbedrijven, als bedoeld in Bijlage II van de NIB-richtlijn	Productie of aankoop van aardgas, met inbegrip van LNG	1	

	Energie: gas	De bij besluit van Onze Minister van Economische Zaken en Klimaat aangewezen exploitanten van voorzieningen voor de raffinage en behandeling van aardgas, als bedoeld in Bijlage II van de NIB-richtlijn	Raffinage of behandeling van aardgas	0	
NIS2	(a) Elektricite it	Benoemde elektriciteitsmarktbeheerders als bedoeld in artikel 2, punt 8, van Verordening (EU) 2019/943(2) 20 en 59, van Richtlijn (EU) 2019/944	xxx	xxx	?
NIS2	(a) Elektricite it	Marktdeelnemers op de elektriciteitsmarkt als bedoeld in artikel 2, punt 25, van Verordening (EU) 2019/943 die aggrega ie verrichten of vraagrespons- of energieopslagdiensten verstrekken als bedoeld in artikel 2, punten 18, 20 en 59, van Richtlijn (EU) 2019/944	xxx	xxx	?
NIS2	(b) Stadsver warming en - koeling	Stadsverwarming of stadskoeling als bedoeld in artikel 2, punt 19, van Richtlijn (EU) 2018/2001(3) ter bevordering van het gebruik van energie uit hernieuwbare bronnen	xxx	xxx	?
NIS2	(e) Waterstof	Exploitanten van voorzieningen voor de produc ie, opslag en transport van waterstof	xxx	xxx	?

Belangen

Title	Belangen: TBB	Belangen: Aanwijzing tot doelgroep	Belangen: TBB's en ketenafhankelijkheid	Belangen: Toelichting op belanghebbenden
Wbni	Het gaat hierb j altijd om varianten op: 1. Vertrouwelijkheid data (persoonsgegevens, bedr jfsgeheimen, (staats) geheimen, intellectueel eigendom) 2. Integriteit /betrouwbaarheid (authenticiteit) data 3. Ongehinderde doorgang processen en systemen (=besch kbaarheid)	**Vitale infrastructuur, categorie B** Vitale processen: Regionale distributie elektriciteit, Regionale distributie gas. **Aanbieder Essentiële Dienst (AED)** Aanbieder: • De regionale netbeheerders, aangewezen op grond van artikel 10, negende lid, 13, eerste lid, of 14 van de Elektriciteitswet 1998. • De regionale netbeheerders, aangewezen krachtens artikel 2, achtste lid, of 5 van de Gaswet Dienst: Transmissie en distributie van elektriciteit en gas	Denk aan cascade effecten, afnemers/gebruikers van data, diensten en producten. Met bijzondere aandacht voor andere vitale processen.	Wie wordt waardoor negatief geraakt? Denk aan: burgers, onderdelen van de R jksoverheid, bedrijven, bewindspersonen.
Wbni	Het gaat hierb j altijd om varianten op: 1. Vertrouwelijkheid data (persoonsgegevens, bedr jfsgeheimen, (staats) geheimen, intellectueel eigendom) 2. Integriteit /betrouwbaarheid (authenticiteit) data 3. Ongehinderde doorgang processen en systemen (=besch kbaarheid)	**Vitale infrastructuur, categorie B** Vitale processen: Regionale distributie elektriciteit, Regionale distributie gas. **Aanbieder Essentiële Dienst (AED)** Aanbieder: • De regionale netbeheerders, aangewezen op grond van artikel 10, negende lid, 13, eerste lid, of 14 van de Elektriciteitswet 1998. • De regionale netbeheerders, aangewezen krachtens artikel 2, achtste lid, of 5 van de Gaswet Dienst: Transmissie en distributie van elektriciteit en gas	Denk aan cascade effecten, afnemers/gebruikers van data, diensten en producten. Met bijzondere aandacht voor andere vitale processen.	Wie wordt waardoor negatief geraakt? Denk aan: burgers, onderdelen van de R jksoverheid, bedrijven, bewindspersonen.

Wbni	Het gaat hierb j altijd om varianten op: 1. Vertrouwelijkheid data (persoonsgegevens, bedr jfsgeheimen, (staats) geheimen, intellectueel eigendom) 2. Integriteit /betrouwbaarheid (authenticiteit) data 3. Ongehinderde doorgang processen en systemen (=besch kbaarheid)	**Vitale infrastructuur, categorie B** Vitale processen: Regionale distributie elektriciteit, Regionale distributie gas. **Aanbieder Essentiële Dienst (AED)** Aanbieder: • De regionale netbeheerders, aangewezen op grond van artikel 10, negende lid, 13, eerste lid, of 14 van de Elektriciteitswet 1998. • De regionale netbeheerders, aangewezen krachtens artikel 2, achtste lid, of 5 van de Gaswet Dienst: Transmissie en distributie van elektriciteit en gas	Denk aan cascade effecten, afnemers/gebruikers van data, diensten en producten. Met bijzondere aandacht voor andere vitale processen.	Wie wordt waardoor negatief geraakt? Denk aan: burgers, onderdelen van de R jksoverheid, bedrijven, bewindspersonen.
Wbni	Het gaat hierb j altijd om varianten op: 1. Vertrouwelijkheid data (persoonsgegevens, bedr jfsgeheimen, (staats) geheimen, intellectueel eigendom) 2. Integriteit /betrouwbaarheid (authenticiteit) data 3. Ongehinderde doorgang processen en systemen (=besch kbaarheid)	**Vitale infrastructuur, categorie A** Gasproductie, landelijk transport en distr butie gas **Aanbieder Essentiële Dienst (AED)** Aanbieder: De netbeheerder van het landel jk gastransportnet, aangewezen op grond van artikel 2, eerste lid, of 5 van de Gaswet Dienst: Transmissie en distributie van gas	Denk aan cascade effecten, afnemers/gebruikers van data, diensten en producten. Met bijzondere aandacht voor andere vitale processen.	Wie wordt waardoor negatief geraakt? Denk aan: burgers, onderdelen van de R jksoverheid, bedrijven, bewindspersonen.
Wbni	Het gaat hierb j altijd om varianten op: 1. Vertrouwelijkheid data (persoonsgegevens, bedr jfsgeheimen, (staats) geheimen, intellectueel eigendom) 2. Integriteit /betrouwbaarheid (authenticiteit) data 3. Ongehinderde doorgang processen en systemen (=besch kbaarheid)	**Vitale infrastructuur, categorie A** Gasproductie, landelijk transport en distr butie gas. **Aanbieder Essentiële Dienst (AED)** Aanbieder: De Nederlandse Aardolie Maatschappij B.V. (art. 2 BBNI) Essentiële dienst: Het opsporen en winnen van gas op basis van de concessie voor de aardgaswinning uit het Groningenveld op grond van het koninklijk besluit van 30 mei 1963, nr. 39 (Stcrt. 1963, 126)	Denk aan cascade effecten, afnemers/gebruikers van data, diensten en producten. Met bijzondere aandacht voor andere vitale processen.	Wie wordt waardoor negatief geraakt? Denk aan: burgers, onderdelen van de R jksoverheid, bedrijven, bewindspersonen.
Wbni	Het gaat hierb j altijd om varianten op: 1. Vertrouwelijkheid data (persoonsgegevens, bedr jfsgeheimen, (staats) geheimen, intellectueel eigendom) 2. Integriteit /betrouwbaarheid (authenticiteit) data 3. Ongehinderde doorgang processen en systemen (=besch kbaarheid)	**Vitale infrastructuur, categorie B** Vitale processen: Regionale distributie elektriciteit, Regionale distributie gas. **Aanbieder Essentiële Dienst (AED)** Aanbieder: • De regionale netbeheerders, aangewezen op grond van artikel 10, negende lid, 13, eerste lid, of 14 van de Elektriciteitswet 1998. • De regionale netbeheerders, aangewezen krachtens artikel 2, achtste lid, of 5 van de Gaswet Dienst: Transmissie en distributie van elektriciteit en gas	Denk aan cascade effecten, afnemers/gebruikers van data, diensten en producten. Met bijzondere aandacht voor andere vitale processen.	Wie wordt waardoor negatief geraakt? Denk aan: burgers, onderdelen van de R jksoverheid, bedrijven, bewindspersonen.

Wbni	Het gaat hierb j altijd om varianten op: 1. Vertrouwelijkheid data (persoonsgegevens, bedr jfsgeheimen, (staats) geheimen, intellectueel eigendom) 2. Integriteit /betrouwbaarheid (authenticiteit) data 3. Ongehinderde doorgang processen en systemen (=besch kbaarheid)	**Vitale infrastructuur, categorie B** Vitale processen: Regionale distributie elektriciteit, Regionale distributie gas. **Aanbieder Essentiële Dienst (AED)** Aanbieder: • De regionale netbeheerders, aangewezen op grond van artikel 10, negende lid, 13, eerste lid, of 14 van de Elektriciteitswet 1998. • De regionale netbeheerders, aangewezen krachtens artikel 2, achtste lid, of 5 van de Gaswet Dienst: Transmissie en distributie van elektriciteit en gas	Denk aan cascade effecten, afnemers/gebruikers van data, diensten en producten. Met bijzondere aandacht voor andere vitale processen.	Wie wordt waardoor negatief geraakt? Denk aan: burgers, onderdelen van de R jksoverheid, bedrijven, bewindspersonen.
Wbni	Het gaat hierb j altijd om varianten op: 1. Vertrouwelijkheid data (persoonsgegevens, bedr jfsgeheimen, (staats) geheimen, intellectueel eigendom) 2. Integriteit /betrouwbaarheid (authenticiteit) data 3. Ongehinderde doorgang processen en systemen (=besch kbaarheid)	**Vitale infrastructuur, categorie A** Landelijk transport en distributie elektriciteit **Aanbieder Essentiële Dienst (AED)** Aanbieder: De netbeheerder van het landel jk hoogspanningsnet, aangewezen op grond van artik el 10, tweede lid, of 14 van de Elektriciteitswet 1998 Dienst: Transmissie en distributie van elektriciteit	Denk aan cascade effecten, afnemers/gebruikers van data, diensten en producten. Met bijzondere aandacht voor andere vitale processen.	Wie wordt waardoor negatief geraakt? Denk aan: burgers, onderdelen van de R jksoverheid, bedrijven, bewindspersonen.
Wbni	Het gaat hierb j altijd om varianten op: 1. Vertrouwelijkheid data (persoonsgegevens, bedr jfsgeheimen, (staats) geheimen, intellectueel eigendom) 2. Integriteit /betrouwbaarheid (authenticiteit) data 3. Ongehinderde doorgang processen en systemen (=besch kbaarheid)	**Vitale infrastructuur, categorie B** Vitale processen: Regionale distributie elektriciteit, Regionale distributie gas. **Aanbieder Essentiële Dienst (AED)** Aanbieder: • De regionale netbeheerders, aangewezen op grond van artikel 10, negende lid, 13, eerste lid, of 14 van de Elektriciteitswet 1998. • De regionale netbeheerders, aangewezen krachtens artikel 2, achtste lid, of 5 van de Gaswet Dienst: Transmissie en distributie van elektriciteit en gas	Denk aan cascade effecten, afnemers/gebruikers van data, diensten en producten. Met bijzondere aandacht voor andere vitale processen.	Wie wordt waardoor negatief geraakt? Denk aan: burgers, onderdelen van de R jksoverheid, bedrijven, bewindspersonen.

Dreigingen

Title	Dreigingen: vastgesteld	Dreigingen: voorstelbaar	Samenwerking op cybergebied

Wbni	- *Manifestaties (onderkende aanvallen)* - *Bekende actoren die het voorzien hebben op de doelgroeporganisaties / sector* o *Relevante doelen / ambities* o *TTPs: tactieken, technieken en procedures relevant voor de doelgroeporganisatie*	*Hierbij combineer je de te beschermen belangen met bekende of voorstelbare dreigingsactoren met hun bekende of voorstelbare drijfveren / ambities en strategieën.*	Op we ke manier werkt de organisatie samen met het NCSC? Welke verbanden zijn er al ook buiten het NCSC? Wat wil de organisatie qua samenwerking? Dit goed begrijpen helpt om focus te krijgen op waar samenwerking nog meer mogelijk en wenselijk is. Met een beter beeld van de belangen, dreigingen en weerbaarheidsvraagstukken geeft dit richting aan het gesprek en de afspraken voor de toekomst. Samenwerkingsaspecten: · Samenwerkingsverbanden NCSC en eigen netwerk: IRB lid · Gremia, lid Energie ISAC NL · Producten en diensten (b jv. NDN): Advisory (email), Advisory (XML), CSBN, Kwartaal dreigingsanalyse, End-of-Week (email), Maandmonitor Amber, Monitoring meldingen, NDN update Vitaal NDN aansluiting MISP · Onderzoek / pilots · Wensen m.b.t. samenwerking en beelden bij samenwerking met NCSC en daarbuiten
Wbni	- *Manifestaties (onderkende aanvallen)* - *Bekende actoren die het voorzien hebben op de doelgroeporganisaties / sector* o *Relevante doelen / ambities* o *TTPs: tactieken, technieken en procedures relevant voor de doelgroeporganisatie*	*Hierbij combineer je de te beschermen belangen met bekende of voorstelbare dreigingsactoren met hun bekende of voorstelbare drijfveren / ambities en strategieën.*	Op we ke manier werkt de organisatie samen met het NCSC? Welke verbanden zijn er al ook buiten het NCSC? Wat wil de organisatie qua samenwerking? Dit goed begrijpen helpt om focus te krijgen op waar samenwerking nog meer mogelijk en wenselijk is. Met een beter beeld van de belangen, dreigingen en weerbaarheidsvraagstukken geeft dit richting aan het gesprek en de afspraken voor de toekomst. Samenwerkingsaspecten: · Samenwerkingsverbanden NCSC en eigen netwerk · Gremia · Producten en diensten (b jv. NDN): Advisory (email), CSBN, Kwartaal dreigingsanalyse, End-of-Week (email), Maandmonitor Amber, Monitoring meldingen · Onderzoek / pilots · Wensen m.b.t. samenwerking en beelden bij samenwerking met NCSC en daarbuiten
Wbni	- *Manifestaties (onderkende aanvallen)* - *Bekende actoren die het voorzien hebben op de doelgroeporganisaties / sector* o *Relevante doelen / ambities* o *TTPs: tactieken, technieken en procedures relevant voor de doelgroeporganisatie*	*Hierbij combineer je de te beschermen belangen met bekende of voorstelbare dreigingsactoren met hun bekende of voorstelbare drijfveren / ambities en strategieën.*	Op we ke manier werkt de organisatie samen met het NCSC? Welke verbanden zijn er al ook buiten het NCSC? Wat wil de organisatie qua samenwerking? Dit goed begrijpen helpt om focus te krijgen op waar samenwerking nog meer mogelijk en wenselijk is. Met een beter beeld van de belangen, dreigingen en weerbaarheidsvraagstukken geeft dit richting aan het gesprek en de afspraken voor de toekomst. Samenwerkingsaspecten: · Samenwerkingsverbanden NCSC en eigen netwerk · Gremia: Lid (voorzitter) Energie ISAC NL · Producten en diensten (b jv. NDN): Advisory (email), CSBN, Kwartaal dreigingsanalyse, End-of-Week (email), Maandmonitor Amber, NDN update Vitaal, NDNupdateVitaal · Onderzoek / pilots · Wensen m.b.t. samenwerking en beelden bij samenwerking met NCSC en daarbuiten

Wbni	- *Manifestaties (onderkende aanvallen)* - *Bekende actoren die het voorzien hebben op de doelgroeporganisaties / sector* o *Relevante doelen / ambities* o *TTPs: tactieken, technieken en procedures relevant voor de doelgroeporganisatie*	*Hierbij combineer je de te beschermen belangen met bekende of voorstelbare dreigingsactoren met hun bekende of voorstelbare drijfveren / ambities en strategieën.*	Op we ke manier werkt de organisatie samen met het NCSC? Welke verbanden zijn er al ook buiten het NCSC? Wat wil de organisatie qua samenwerking? Dit goed begrijpen helpt om focus te krijgen op waar samenwerking nog meer mogelijk en wenselijk is. Met een beter beeld van de belangen, dreigingen en weerbaarheidsvraagstukken geeft dit richting aan het gesprek en de afspraken voor de toekomst. Samenwerkingsaspecten: · Samenwerkingsverbanden NCSC en eigen netwerk: lid NCSC council, IRB lid · Gremia: lid Energie ISAC NL · Producten en diensten (b jv. NDN): Advisory (email), Advisory (XML), CSBN, Kwartaal dreigingsanalyse, End-of-Week (email), Maandmonitor Amber, Monitoring meldingen, NDN update Vitaal · Onderzoek / pilots · Wensen m.b.t. samenwerking en beelden bij samenwerking met NCSC en daarbuiten

Wbni	- *Manifestaties (onderkende aanvallen)* - *Bekende actoren die het voorzien hebben op de doelgroeporganisaties / sector* o *Relevante doelen / ambities* o *TTPs: tactieken, technieken en procedures relevant voor de doelgroeporganisatie*	*Hierbij combineer je de te beschermen belangen met bekende of voorstelbare dreigingsactoren met hun bekende of voorstelbare drijfveren / ambities en strategieën.*	Op we ke manier werkt de organisatie samen met het NCSC? Welke verbanden zijn er al ook buiten het NCSC? Wat wil de organisatie qua samenwerking? Dit goed begrijpen helpt om focus te krijgen op waar samenwerking nog meer mogelijk en wenselijk is. Met een beter beeld van de belangen, dreigingen en weerbaarheidsvraagstukken geeft dit richting aan het gesprek en de afspraken voor de toekomst. Samenwerkingsaspecten: · Samenwerkingsverbanden NCSC en eigen netwerk · Gremia · Producten en diensten (b jv. NDN): Advisory (email), Advisory (XML), End-of-Week (email), NDN update Vitaal · Onderzoek / pilots · Wensen m.b.t. samenwerking en beelden bij samenwerking met NCSC en daarbuiten

Wbni	- *Manifestaties (onderkende aanvallen)* - *Bekende actoren die het voorzien hebben op de doelgroeporganisaties / sector* o *Relevante doelen / ambities* o *TTPs: tactieken, technieken en procedures relevant voor de doelgroeporganisatie*	*Hierbij combineer je de te beschermen belangen met bekende of voorstelbare dreigingsactoren met hun bekende of voorstelbare drijfveren / ambities en strategieën.*	Op we ke manier werkt de organisatie samen met het NCSC? Welke verbanden zijn er al ook buiten het NCSC? Wat wil de organisatie qua samenwerking? Dit goed begrijpen helpt om focus te krijgen op waar samenwerking nog meer mogelijk en wenselijk is. Met een beter beeld van de belangen, dreigingen en weerbaarheidsvraagstukken geeft dit richting aan het gesprek en de afspraken voor de toekomst. Samenwerkingsaspecten: · Samenwerkingsverbanden NCSC en eigen netwerk · Gremia: lid Energie ISAC NL · Producten en diensten (b jv. NDN): Advisory (email), CSBN, Kwartaal dreigingsanalyse, End-of-Week (email), Maandmonitor Amber, Monitoring meldingen, NDN update Vitaal · Onderzoek / pilots · Wensen m.b.t. samenwerking en beelden bij samenwerking met NCSC en daarbuiten

Wbni	- *Manifestaties (onderkende aanvallen)* - *Bekende actoren die het voorzien hebben op de doelgroeporganisaties / sector* o *Relevante doelen / ambities* o *TTPs: tactieken, technieken en procedures relevant voor de doelgroeporganisatie*	*Hierbij combineer je de te beschermen belangen met bekende of voorstelbare dreigingsactoren met hun bekende of voorstelbare drijfveren / ambities en strategieën.*	Op we ke manier werkt de organisatie samen met het NCSC? Welke verbanden zijn er al ook buiten het NCSC? Wat wil de organisatie qua samenwerking? Dit goed begrijpen helpt om focus te krijgen op waar samenwerking nog meer mogelijk en wenselijk is. Met een beter beeld van de belangen, dreigingen en weerbaarheidsvraagstukken geeft dit richting aan het gesprek en de afspraken voor de toekomst. Samenwerkingsaspecten: · Samenwerkingsverbanden NCSC en eigen netwerk · Gremia: Lid Energie ISAC NL · Producten en diensten (b jv. NDN): Advisory (email), Advisory (XML), CSBN, Kwartaal dreigingsanalyse, End-of-Week (email), Maandmonitor Amber, Monitoring meldingen, NDN update Vitaal · Onderzoek / pilots · Wensen m.b.t. samenwerking en beelden bij samenwerking met NCSC en daarbuiten
Wbni	- *Manifestaties (onderkende aanvallen)* - *Bekende actoren die het voorzien hebben op de doelgroeporganisaties / sector* o *Relevante doelen / ambities* o *TTPs: tactieken, technieken en procedures relevant voor de doelgroeporganisatie*	*Hierbij combineer je de te beschermen belangen met bekende of voorstelbare dreigingsactoren met hun bekende of voorstelbare drijfveren / ambities en strategieën.*	Op we ke manier werkt de organisatie samen met het NCSC? Welke verbanden zijn er al ook buiten het NCSC? Wat wil de organisatie qua samenwerking? Dit goed begrijpen helpt om focus te krijgen op waar samenwerking nog meer mogelijk en wenselijk is. Met een beter beeld van de belangen, dreigingen en weerbaarheidsvraagstukken geeft dit richting aan het gesprek en de afspraken voor de toekomst. Samenwerkingsaspecten: · Samenwerkingsverbanden NCSC en eigen netwerk: lid DSC overleg en IRB lid · Gremia: lid Energie ISAC NL · Producten en diensten (b jv. NDN): Advisory (email), Advisory (XML), CSBN, Kwartaal dreigingsanalyse, End-of-Week (email), Maandmonitor Amber, Monitoring meldingen, NDN update Vitaal · Onderzoek / pilots · Wensen m.b.t. samenwerking en beelden bij samenwerking met NCSC en daarbuiten
Wbni	- *Manifestaties (onderkende aanvallen)* - *Bekende actoren die het voorzien hebben op de doelgroeporganisaties / sector* o *Relevante doelen / ambities* o *TTPs: tactieken, technieken en procedures relevant voor de doelgroeporganisatie*	*Hierbij combineer je de te beschermen belangen met bekende of voorstelbare dreigingsactoren met hun bekende of voorstelbare drijfveren / ambities en strategieën.*	Op we ke manier werkt de organisatie samen met het NCSC? Welke verbanden zijn er al ook buiten het NCSC? Wat wil de organisatie qua samenwerking? Dit goed begrijpen helpt om focus te krijgen op waar samenwerking nog meer mogelijk en wenselijk is. Met een beter beeld van de belangen, dreigingen en weerbaarheidsvraagstukken geeft dit richting aan het gesprek en de afspraken voor de toekomst. Samenwerkingsaspecten: · Samenwerkingsverbanden NCSC en eigen netwerk · Gremia: Lid Energie ISAC NL · Producten en diensten (b jv. NDN): Advisory (email), CSBN, Kwartaal dreigingsanalyse, End-of-Week (email), Maandmonitor Amber, Monitoring meldingen, NDN update Vitaal · Onderzoek / pilots · Wensen m.b.t. samenwerking en beelden bij samenwerking met NCSC en daarbuiten

Weerbaarheid

Title	Weerbaarheid: identify	Weerbaarheid: protect	Weerbaarheid: detect	Weerbaarheid: respond

Wbni	· *Assetmanagement* · *Business environment* · *Governance* · *Risk Assessment* · *Risk Management Strategy*	· *Awareness Control* · *Awareness and training* · *Data Security* · *Info Protection and procedures* · *Maintenance* · *Protective technology*	· *Anomalies and events* · *Security continuous monitoring* · *Detection process*	· *Response planning* · *Communications* · *Analysis* · *Mitigation* · *Improvements*
Wbni	· *Assetmanagement* · *Business environment* · *Governance* · *Risk Assessment* · *Risk Management Strategy*	· *Awareness Control* · *Awareness and training* · *Data Security* · *Info Protection and procedures* · *Maintenance* · *Protective technology*	· *Anomalies and events* · *Security continuous monitoring* · *Detection process*	· *Response planning* · *Communications* · *Analysis* · *Mitigation* · *Improvements*
Wbni	· *Assetmanagement* · *Business environment* · *Governance* · *Risk Assessment* · *Risk Management Strategy*	· *Awareness Control* · *Awareness and training* · *Data Security* · *Info Protection and procedures* · *Maintenance* · *Protective technology*	· *Anomalies and events* · *Security continuous monitoring* · *Detection process*	· *Response planning* · *Communications* · *Analysis* · *Mitigation* · *Improvements*
Wbni	· *Assetmanagement* · *Business environment* · *Governance* · *Risk Assessment* · *Risk Management Strategy*	· *Awareness Control* · *Awareness and training* · *Data Security* · *Info Protection and procedures* · *Maintenance* · *Protective technology*	· *Anomalies and events* · *Security continuous monitoring* · *Detection process*	· *Response planning* · *Communications* · *Analysis* · *Mitigation* · *Improvements*
Wbni	· *Assetmanagement* · *Business environment* · *Governance* · *Risk Assessment* · *Risk Management Strategy*	· *Awareness Control* · *Awareness and training* · *Data Security* · *Info Protection and procedures* · *Maintenance* · *Protective technology*	· *Anomalies and events* · *Security continuous monitoring* · *Detection process*	· *Response planning* · *Communications* · *Analysis* · *Mitigation* · *Improvements*
Wbni	· *Assetmanagement* · *Business environment* · *Governance* · *Risk Assessment* · *Risk Management Strategy*	· *Awareness Control* · *Awareness and training* · *Data Security* · *Info Protection and procedures* · *Maintenance* · *Protective technology*	· *Anomalies and events* · *Security continuous monitoring* · *Detection process*	· *Response planning* · *Communications* · *Analysis* · *Mitigation* · *Improvements*

Wbni	· *Assetmanagement* · *Business environment* · *Governance* · *Risk Assessment* · *Risk Management Strategy*	· *Awareness Control* · *Awareness and training* · *Data Security* · *Info Protection and procedures* · *Maintenance* · *Protective technology*	· *Anomalies and events* · *Security continuous monitoring* · *Detection process*	· *Response planning* · *Communications* · *Analysis* · *Mitigation* · *Improvements*
Wbni	· *Assetmanagement* · *Business environment* · *Governance* · *Risk Assessment* · *Risk Management Strategy*	· *Awareness Control* · *Awareness and training* · *Data Security* · *Info Protection and procedures* · *Maintenance* · *Protective technology*	· *Anomalies and events* · *Security continuous monitoring* · *Detection process*	· *Response planning* · *Communications* · *Analysis* · *Mitigation* · *Improvements*
Wbni [redacted]	· *Assetmanagement* · *Business environment* · *Governance* · *Risk Assessment* · *Risk Management Strategy*	· *Awareness Control* · *Awareness and training* · *Data Security* · *Info Protection and procedures* · *Maintenance* · *Protective technology*	· *Anomalies and events* · *Security continuous monitoring* · *Detection process*	· *Response planning* · *Communications* · *Analysis* · *Mitigation* · *Improvements*

Stukken die bijdragen aan cybersecurity overzicht van de sector

	Wat	Wanneer	Link	Relevantie van bron	Gepubliceerd door?
E1	**Dreigings analyse**	**2020 Q4**	**TLP-GREEN-2020Q4-Sectoral-Energy-v1.0.pdf**		
E2	**BBNI (besluit beveiliging netwerk- en informatie systemen)**	**2021, maart**	**https://zoek.officielebekendmakingen.nl/stb-2021-160.html**	**aanwijzing AED's, nota van toelichting heel relevant en consultatie partijen (veel energiepartijen, goed om hun reacties te lezen). Agentschap Telecom heeft uitvoerbaarheid en handhaafbaarheidstoets (U&H toets) gedaan (ook in opgenomen)**	**Staatsb;lad 2021, 160**
E3					
E4					

E5	**ENISA rapport over dreigingen tav energieleveranciers**	**2020, mei**	**https://www.enisa.europa.eu/news/enisa-news/dependency-of-energy-operators-on-time-sensitive-services**	**This publication describes the threats against energy providers' services which depend on the availability of precise timing and communication networks. It provides a typical architecture which supports the time measurement service. Then it describes the threats as well as the attacks against the CIA (confidentiality, integrity, availability) of the service and it provides a set of mitigation measures. Finally, it concludes with some recommendations to technology vendors and energy operators**	**ENISA**
E6	**ENISA rapport over o.a. CSIRT capabilities en uitdagingen in relatie tot energie en gaat in op de NIB richtlijn**	**2020, december**	**https://www.enisa.europa.eu/publications/sectoral-csirt-capabilities-energy-and-air-transport**	**The report focuses on trends in Energy and Air Transport Incident Response (IR) Capabilities, procedures, processes and tools. It also offers insights on current challenges and gaps facing IR communities. The analysis aimed to focus on: current IRC of Air Transport and Energy sectors, the recent changes in the context of the Covid-19 pandemic, the upcoming revision of the NIS Directive, and to draw practical recommendations for the IR community.**	**ENISA**
E7	**ENISA rapportage over smart grid**	**2013 (wel oud, nog geen recenter rapport gevonden)**	**https://www.enisa.europa.eu/topics/threat-risk-management/threats-and-trends/enisa-thematic-landscapes/sgtl**		**ENISA**

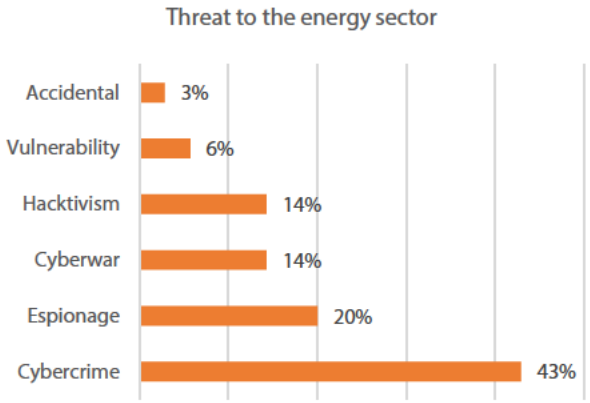
E8	**CBS-rapport 2020 Cybersecurity monitor**	**2021**	**https://www.cbs.nl/nl-nl/publicatie/2021/18/cybersecuritymonitor-2020**	**Jaarlijks rapport over ICT enquete onder 20.000 a-select getrokken Nederlandse bedrijven. Energie vormt samen met water en afvalbeheer een categorie. Incident dat vaakst voorkomt in deze categorie is uitval ICT dienst door veiligheidsincident. Top 3 meest gebruikte ICT maatregel in deze categorie: 1. antivirussoftware, 2. updaten software /besturingssysteem, 3. gegevens op andere fysieke locatie.** **NB Let op: elk jaar is er een andere selectie van bedrijven, vandaar dat het kan verschillen per jaar.Daarnaast zit energie met water en afvalbeheer in dezelfde categorie, dus niet exclusief energie.**	**CBS**

Sectoral Threat Landscape: Energy

TLR 2020Q3 - Date: 09/10/2020 - Version: 1.0
TLP:GREEN

Key points

- At least 9 organisations in the energy sector became victims of ransomware attacks, with 5 of them in Europe. The most observed ransomware families in this sector have been Netwalker (4 cases), Maze (2 cases), DoppelPaymer, Netfilim, and REvil (1 case each).
- The Russian APT28 threat actor carried out a broad cyber operation against US targets from December 2018 until at least May 2020. Some victims belong to the energy sector.
- In July, several reports suggested that Iran and Israel are engaged in cyber operations of a continuous nature, with some of them allegedly affecting solar energy systems.
- There has been an increase in targeted attacks against Middle East based supply chain organisations in the oil and gas sector.
- Researchers have found a vulnerability affecting an industrial module widely used in the energy sector.



Cybercrime

Ransomware

During 2020Q3, at least 9 organisations in the energy sector became victims of ransomware attacks. Five of these incidents affected European entities. The most observed ransomware families in this sector have been Netwalker (4 cases), Maze (2 cases), DoppelPaymer, Netfilim, and REvil (1 case each). In the case of the breach of K-Electric, the sole electricity provider for Karachi, Pakistan, the attack reportedly caused the disruption of billing and online services.

The table below provides a more complete list of ransomware victims in the energy sector.

Date	Ransomware	Country	Victim	Activities
Sep	Netwalker	Pakistan	Wbni	Power utility
Sep	DoppelPaymer	Italy	Wbni	Smart utility for the integrated offer of energy
Aug	Netfilim	France	Wbni	Technical services - energy and communications
Aug	Netwalker	US	Wbni	Retail energy company
Aug	Netwalker	France	Wbni	Smart battery systems for sustainable electric transport
Aug	Revil	US	Wbni	Catalyst services for refineries, gas processing facilities, petrochemical, and chemical plants
Aug	Maze	Germany	Wbni	Machines and accessories for the underground installation and renewal of pipelines
Aug	Maze	Middle East	Wbni	Construction / oil & gas, refineries, petrochemicals and power industries
July	Netwalker	France	Wbni	Conversion of oil and biomass

Cyberespionage / Targeted intrusions

Middle East

According to a research, since July 2020, there has been an increase in **targeted attacks** against several **Middle East** based **supply chain** organisations in the **oil and gas sector**. Multiple instances of malicious PDF files have been sent as email attachments and were used to distribute an information-stealing trojan, AZORult, to these organisations.

North America

According to the US FBI, the **Russia-based APT28** threat actor carried out a broad cyber operation against **US targets** from December 2018 until at least May 2020. The identified victims belong to the state and federal government, education as well as **energy** sectors. To penetrate into their targets' IT networks, APT28 attempted to breach mail servers, VPN servers, and Microsoft Office 365 and email accounts. See details in TM-20-091.

Cyberwar and hacktivism

On June 27, two **Iranian hacktivist groups** claimed that they carried out a cyber-intrusion into an **Israeli gas company**. The groups stated that they had comprised one of the company's servers and shared media depicting their efforts. The hacktivists claimed their action was a response to rumours that an explosion near an Iranian military base, reported several days before, was the result of an Israeli cyberattack.

In July, several reports suggested that **Iran** and **Israel** are engaged in **cyber operations of a continuous nature**. Hacktivist cyberattacks hit agriculture, drinking water and **energy infrastructures** in Israel. More specifically, on June 30, on their Facebook page, a hacking collective calling itself the Jerusalem Electronic Army (JEA) claimed the compromise of an Israeli **solar energy** system. In April, JEA had posted screenshots on their Facebook page of an allegedly compromised Sunny WebBox of remote monitoring and diagnostic tools for solar energy systems. Hacktivists also claimed breaching a military surveillance system. See details in TM-20-093.

Early July, **Iran**'s Atomic Energy Organisation (AEOI) announced that an explosion had occurred at the Natanz **nuclear site** resulting in significant damage. Several speculative reports regarding the cause of the explosion emerged, including claims of state-backed sabotage, and a cyberattack. However, no evidence has been presented to support any of these assertions.

On August 21, the **Arabic-speaking** actor Spider Team claimed to compromise a **Russian nuclear research institute**, allegedly obtaining "**secret documents**" they promised to publish soon. The breach appears to be part of OpRussia, a hacktivist campaign marking the August 21, 2013, Ghouta chemical attack in Syria.

Vulnerabilities

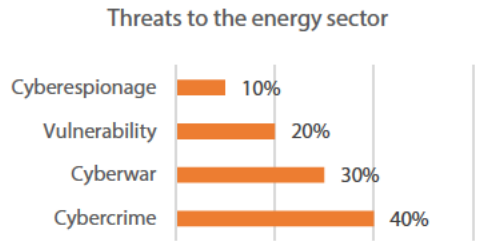
A new **vulnerability** (tracked as CVE-2020-15858) was discovered on August 19 in widely used **Thales components**. This module is embedded in millions of "critical" connected devices used by the automotive, **energy**, telecommunications, and medical sectors. The vulnerability can let attackers bypass security controls protecting files and operational code of the device, stealing data or affecting its operation. In some cases, the flaw is even remotely exploitable over 3G.

Sectoral Threat Landscape: Energy

TLR 2020Q4 - Date: 11/01/2021- Version: 1.0
TLP:GREEN

Key points

- At least eight companies of the energy sector have become victims of ransomware attacks, with 3 of them in Europe. The most observed ransomware family has been DoppelPaymer.
- Japan's Nuclear Regulation Authority (NRA) disclosed it suffered a suspected cyberattack.
- A cyberattack is possibly the origin of a power outage in India.
- The National Iranian Gas Company was targeted in a cyberattack that disabled a "large part" of its distribution network.



- An UK-based energy company disclosed a data breach potentially affecting 270.000 customers' personal data.

Cybercrime

- During 2020Q4, at least eight companies of the energy sector became victims of ransomware attacks.
- This companies are responsible for a variety of activities including electric power distribution, gas supply and petroleum services.
- Victims are located in Spain, Italy, France, Brazil, the US, and Japan.
- DoppelPaymer is the most observed piece of ransomware in the energy sector.
- Unspecified entities in the energy sector also became victims of a spear phishing campaign targeting the distribution of COVID-19 vaccines in developing countries.

On October 7, a Brazilian petrochemical company known for producing thermoplastic resins reported to the Brazilian securities commission that they suffered a security breach. In a press release, the company said the breach temporarily stalled its operations as they worked to resolve the impacted servers and software.

On October 19, media reporting indicated that energy multinational Endesa disrupted a ransomware operation by an unknown cybercrime actor.

In October, IT networks of the Italian energy giant Enel were compromised by the Netwalker ransomware. The cybercriminals asked for a $14 million ransom. Attackers also said they had downloaded 5 terabytes of data. In June 2020, Enel Group was already confronted with a ransomware attack involving the Ekans ransomware (aka Snake). At that time, the company claimed they had prevented the malware from causing significant damage. See details in TM 20-139.

On December 25, a ransomware attack affected servers belonging to Companhia Energética de Minas Gerais (CEMIG). CEMIG is a major Brazilian power company, responsible for the generation, transmission and distribution of electricity mainly in Minas Gerais.

A list of publicly known victims of ransomware attacks in the energy sector is provided in the table below.

Date	Ransomware	Country	Victim	Activities
Dec	Unspecified	Brazil	Wbni	Electric power distribution
Nov	DoppelPaymer	US	Wbni	Petroleum equipment and service
Nov	DoppelPaymer	US	Wbni	Gas provider
Nov	DoppelPaymer	Japan	Wbni	Petroleum
Nov	Egregor	France	Wbni	Electric power transmission and distribution
Oct	Revil	Brazil	Wbni	Petrochemical
Oct	Unspecified	Spain	Wbni	Energy
Oct	Netwalker	Italy	Wbni	Electricity and gas generation and distribution

According to a report released in December, a spear phishing campaign targeted executives in several organisations (in the government, supply chain, healthcare, energy, manufacturing sectors) in multiple countries. The campaign used a sophisticated lure related to the distribution of COVID-19 vaccines to developing countries. The goal is highly likely to gather information on the COVID-19 vaccine distribution process at international and national levels. See details in TA 20-050.

Cyberespionage / Targeted intrusions

- Japan's Nuclear Regulation Authority (NRA) disclosed it had suffered a suspected cyberattack.
- A cyberattack was possibly the origin of a power outage in India.
- The National Iranian Gas Company was targeted in a cyberattack that disabled a "large part" of its distribution network.

On November 3, Japan's Nuclear Regulation Authority (NRA) disclosed it had suffered a suspected cyberattack during which attackers gained access to its networks. In response, the NRA disabled its email systems. In addition, the JRNA website became inaccessible for five and a half hours, before JNRA was able to restore it. According to media reporting, there is no indication that any data was exfiltrated from NRA systems.

In November, Indian authorities said they were investigating cyber threat activity as a potential cause of a power outage that occurred on October 12 in Mumbai. According to media reports that cite government sources, the investigators identified suspicious logins and malware on relevant systems at a dispatch centre.

In November, according to Iranian authorities the National Iranian Gas Company (NIGC) was targeted in a cyberattack that disabled a "large part" of its distribution network. The attack forced NIGC to divert gas from industrial to domestic networks used for home consumption. However, other officials later refuted the claim. In Iranian state media, there were also allusions to the potential involvement of Israel and vows of retaliation if proven true.

Data leaks

- An Edinburgh-based energy company disclosed a data breach potentially affecting 270.000 customers' personal information.

In December, People's Energy, an Edinburgh-based energy company, disclosed a data breach potentially affecting more than 270.000 customers' personal data. Potentially compromised information includes names, addresses, dates of birth, phone numbers, and tariff and energy meter numbers.

EUROPEAN UNION AGENCY
FOR CYBERSECURITY

ANNUAL ENERGY THREAT LANDSCAPE 2021

ABOUT ENISA

The European Union Agency for Cybersecurity (ENISA) has been working to make Europe cyber secure since 2004. ENISA works with the EU, its Member States, the private sector and Europe's citizens to develop advice and recommendations on good practices in information security. It assists the EU Member States in implementing relevant EU legislation and works to improve the resilience of Europe's critical infrastructure and networks.

More information about ENISA and its work can be found at www.enisa.europa.eu

AUTHORS

Konstantinos Moulinos

Ricardo Figueiredo

Policy Development and Implementation Unit

LEGAL NOTICE

COPYRIGHT NOTICE

Document Handling

This Document is marked as TLP AMBER

COLOR	HOW MAY IT BE SHARED?
TLP:AMBER  Limited disclosure, restricted to participants' **EE-ISAC ONLY**.	Recipients may only share TLP:AMBER information with members of the EE-ISAC, and should not use publicly available channels or for public disclosure.

Acknowledgements

This report has been prepared in the scope of the collaboration of ENISA within the EE-ISAC. We would like to thank those who have provided support and guidance in its development, namely the Board of Directors and Applied Risk.

Table of Contents

1 INTRODUCTION

The energy sector is undergoing an accelerated period of digital transformation, thanks to the increasingly widespread use of technology throughout the entire supply chain. While capturing the value of such technologies for streamlining business operations and remain competitive, the industry has exposed itself to vulnerabilities that such technologies could potentially create.

The threat landscape of today is ever changing and more sophisticated as the number, magnitude, frequency and impact of cybersecurity incidents are increasing. In particular, SCADA, IoT, DCS and ICS' cyber threats have risen exponentially, and dramatically increased security risks worldwide for the energy sector, a critical infrastructure which continues on the forefront of the essential functioning of society and economy.

Objective

Within the spirit of EE-ISAC, this document focuses on reporting cybersecurity incidents and detections while raising awareness on current and emerging trends thus contributing to a more secure European Energy sector.

Data sources

This report is based on information made available from EE-ISAC MISP Platform, open sources (OSINT) as well as on internal restricted energy sector threat assessment reports provided to ENISA by third parties.

2 ANALYSIS

2.1 2021 Attacks Overview

Overall, the number of identified incidents totalled 75 entries plus 450 detections registered on the MISP platform. The analysis of the incidents shows that threat types gravitate mostly around ransomware and data breaches/exfiltration on a global scale, with some of the attacks being conducted by APTs and nation state groups. Some of the most notable attacks of 2021 include:

- Colonial pipeline disruption of operations
- Saudi Aramco data breach
- Disruption of Iranian Fuel POS Infrastructure
- A set of campaigns targeting Italian companies throughout the year

Although the levels of activity from relevant actors are on the rise on a global scale, most of the incidents did not result in an immediate impact on services or downtime. In some particular cases campaigns appear to be focused on industrial and intellectual property espionage (mostly from Chinese actors), hence not to be further leveraged for disruptive attacks.

The following table summarizes the main incidents that could be identified through the previously mentioned information sources, for the period starting in January until November 2021.

THREAT TYPE	THREAT ACTOR	AFFECTED ORGANISATION	DATE	GEOGRAPHICAL AREA	COMPROMISED ASSETS
Ransomware	Conti Group	[redacted] Wbni	Nov-21	Italy	Unknown
Ransomware	Pysa	[redacted] Wbni	Nov-21	Italy	Unknown
DoS		[redacted] Wbni	Oct-21	Iran	Petrol distribution computer system - POS
Ransomware	Conti Group	[redacted] Wbni	Oct-21	United States	Unknown
Exploitation	ChamelGang	Energy and transportation companies	Sep-21	Global	Unknown
Exfiltration/ Data leakage/Breach		[redacted] Wbni	Sep-21	United States	Unknown
Ransomware	Conti	[redacted] Wbni	Sep-21	Spain, South America	Unknown
Exploitation	Unknown ATP	Various energy sector companies	Sep-21	Italy	Unknown
Exfiltration/ Data leakage/Breach	Darkweb persona	Undisclosed water, energy, food and environmental organisation	Sep-21	China, Japan	Unknown
Exfiltration/ Data leakage/Breach	Darkweb persona	Undisclosed Chinese energy company	Sep-21	China	Unknown
Exfiltration/ Data leakage/Breach	Darkweb persona	[redacted] Wbni	Sep-21	Oman	Unknown
Exfiltration/ Data leakage/Breach	Marketo	[redacted] Wbni	Sep-21	Unknown	Unknown
Ransomware	LockBit	[redacted] Wbni	Aug-21	Italy	ICT infrastructure
Breach/Intrusion	Unknown	Energy sector companies in general	Aug-21	Southeast Asia	Databases and relevant information for nation-state intelligence purposes
Ransomware	Unknown	[redacted] Wbni [municipality consortium for local energy distribution]	Aug-21	Italy	Datacenter
Fraud/Impersonation/ Counterfeit	Unknown	Companies likely to work with the USDOT, including from the energy sector	Aug-21	United States	Personal credentials
Exfiltration/ Data leakage/Breach	Darkweb persona	[redacted] Wbni	Aug-21	Iran	Unknown
Exfiltration/ Data leakage/Breach	Darkweb persona	South American Energy company	Aug-21	South America	Unknown
Exfiltration/ Data leakage/Breach	Darkweb persona	[redacted] Wbni	Aug-21	United States	Unknown

THREAT TYPE	THREAT ACTOR	AFFECTED ORGANISATION	DATE	GEOGRAPHICAL AREA	COMPROMISED ASSETS
Exfiltration/ Data leakage/Breach	Darkweb persona	[redacted]	Aug-21	Unknown	Unknown
Spyware	APT	Org operating in the energy sector in Asia	Aug-21	ASIA	Unknown
Ransomware	LockBit	Energy sector companies in general	Jul-21	Global	unknown
Credential harvesting	APT28	Energy sector companies in general	Jul-21	Europe and United States	unknown
Exfiltration/ Data leakage/Breach	ZeroX	[redacted]	Jul 21	Middle East	Databases
Ransomware	Unknown	[redacted]	Jul-21	United States	Databases
Ransomware	Unknown	[redacted]	Jul-21	Norway	Databases
Ransomware	XingLocker	[redacted]	Jul-21	United States	Databases
Exfiltration/ Data leakage/Breach	Darkweb persona	[redacted]	Jul-21	Saudi Arabia	Unknown
Ransomware	Conti Group	[redacted]	Jun-21	Europe	Databases
Ransomware	Revil	[redacted]	Jun-21	Unknown	Download of "4 TB of sensitive data including projects, contracts, and NDAs"
DDoS	Unknown	[redacted]	Jun-21	South America	Client portal and mobile app unavailable
RAT	Unknown	Energy companies in general	Jun-21	Southeast and Central Asia	Networks assets
DDoS	Unknown	[redacted]	Jun-21	Puerto Rico	Unknown
DDoS	Fancy Lazarus	Organisations in the energy, financial, insurance, manufacturing, public utilities and retail sectors	Jun-21	United States	Unknown
Ransomware	Revil	[redacted]	Jun-21	United States	Unknown
Spyware	Suspected Pakistan actor	Government and energy infrastructure	Jun-21	India	Unknown
Exfiltration/ Data leakage/Breach	Kimsuky	[redacted]	May-21	South Korea	Unknown
Ransomware	Darkside Group	[redacted]	May-21	United States	Critical systems causing the shutdown of operations
Ransomware	Avaddon	Energy sector companies in general	May-21	Global	Networks assets

THREAT TYPE	THREAT ACTOR	AFFECTED ORGANISATION	DATE	GEOGRAPHICAL AREA	COMPROMISED ASSETS
Ransomware	Ryuk	[redacted]	May-21	Norway	Unknown
Exfiltration/ Data leakage/Breach	Darkweb persona	[redacted]	Apr-21	China	Unknown
DoS	Israel (nation state)	[redacted]	Apr-21	Iran	Unknown
Exfiltration/ Data leakage/Breach	Darkweb persona	Undisclosed Energy company	Mar-21	UK	Proprietary data
Exfiltration/ Data leakage/Breach	Darkweb persona	Undisclosed Energy company	Mar-21	Italy	Access credentials
Ransomware	RansomExx	[redacted]	Mar-21	Indonesia	Linux systems
Ransomware	REvil	[redacted]	Mar-21	United States	Proprietary data
Exfiltration/ Data leakage/Breach	Clop	[redacted]	Mar-21	Netherlands	Unknown
Exfiltration/ Data leakage/Breach	Darkweb persona	Undisclosed leading energy and infrastructures company	Mar-21	Israel	Unknown
Exfiltration/ Data leakage/Breach	Darkweb persona	Group on energy companies	Mar-21	Italy	Unknown
Ransomware	Unknown	[redacted]	Feb-21	Brazil	Over 1 TB of sensitive data and Active Directory (AD) data
Ransomware	Darkside Group	[redacted]	Feb-21	Brazil	Administrative network servers
Ransomware	Clop	[redacted]	Feb-21	Netherlands	Internal networks
Ransomware	Avaddon	[redacted]	Feb-21	United States	Business confidential data
Exfiltration/ Data leakage/Breach	Darkweb persona	[redacted]	Feb-21	Brazil	Unknown
Exfiltration/ Data leakage/Breach	Hafnium	Various energy companies, including [redacted] in Korea; Romania's [redacted] of Azerbaijan Republic; [redacted] Jordan's [redacted]	Jan-21	Middle East, Asia and Eastern Europe	Databases
Exfiltration/ Data leakage/Breach	Darkweb persona	[redacted]	Jan-21	United States	Unknown

2.2 Attacks' Analysis

As previously mentioned ransomware and data breaches/exfiltration take the lead when it comes to the threat types that energy companies faced in 2021. Available data shows that the combined weight of such threats accounts for 71% of the total, with 40% for data breaches/exfiltration and 31% for ransomware activity.

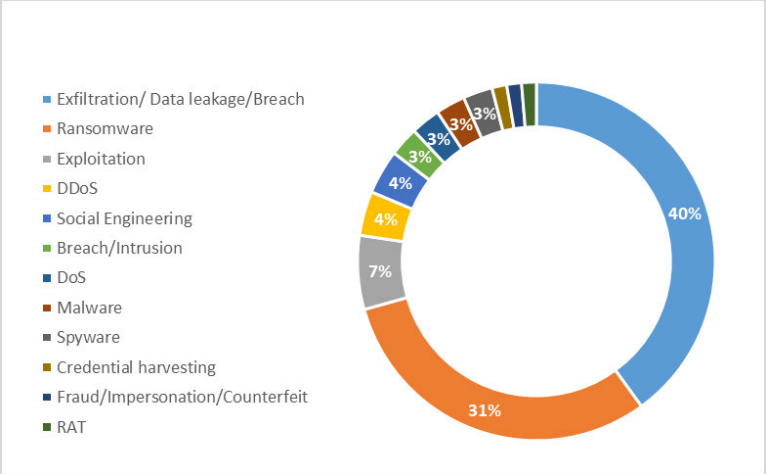


Chart 1 – Threat Type

Due to the lack of information regarding many attacks (and the nature of cyberspace itself), it is often difficult to fully grasp the scope and reach of the incidents in terms of geographical areas and companies affected. Concerning reported incidents per country/geographical area, data suggests that they mostly occurred in the United States – 16, but almost as many attacks had a global reach – 12, thus probably associated with most countries. On the other hand, for as much as 12 incidents, it was impossible to know which particular country or countries were affected, as shown in the follwing chart:

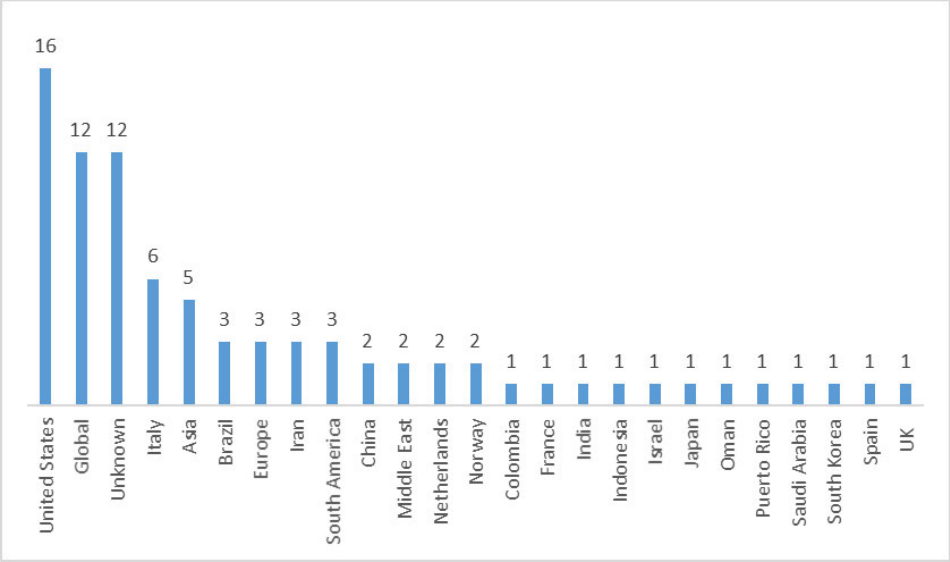


Chart 2 – Incidents per Country/Geographical Area

Threat actors are diverse, ranging from personas posting on dark web forums and DLS (Data Leak Sites) to sophisticated and resourceful APTs. In 33% of the analysed incidents, the threat actor was identified as a dark web persona (see image below). This may come as “no surprised” considering that data breaches/exfiltration is the most common threat in this analysis, and as such, these criminals typically will use posts and blogs to advertise/sell compromised data or credentials.

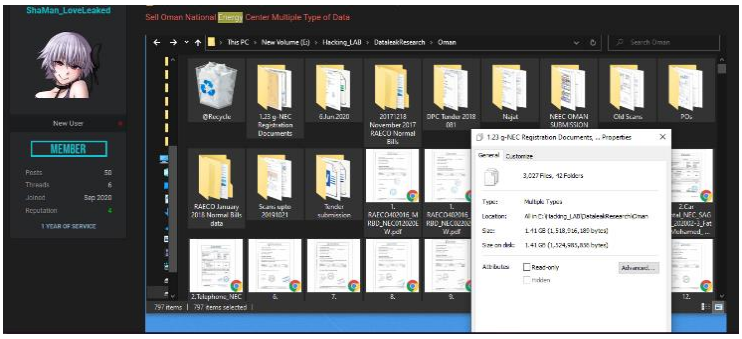


Image 1 – printscreen from a darkweb data leaks forum selling Oman’s [redacted]

In 12% of the cases the attack could be directly linked to an APT, mostly of Russian and Chinese origin such as APT 27, APT28, ATP29 and APT30.

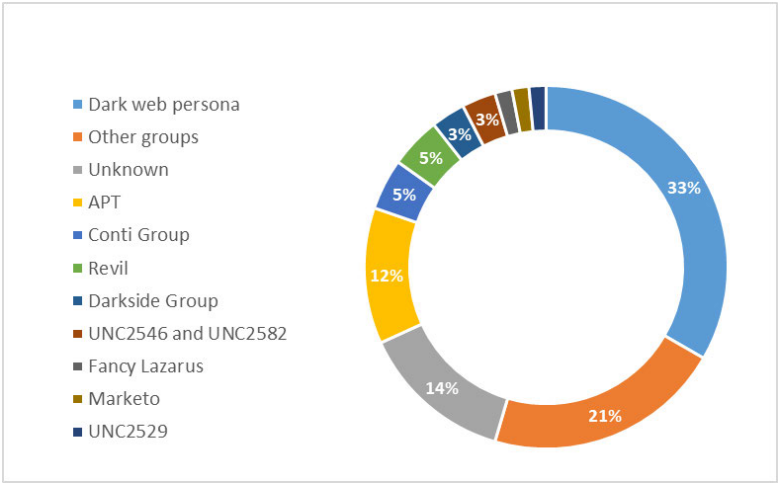


Chart 3 – Threat actors

Other groups in general together with unknown actors make for 35% of the attacks. A final note a couple of very active “well known” groups for their TTPs, as for example “Darkside Group” (claimed to be responsible for the Colonial Pipeline attack) and “Conti Group”. Conti is a particularly ruthless actor as characterized in some cyber community blogs – “*The group has spent more than a year attacking organizations where IT outages can have life-threatening consequences: hospitals, emergency carriers, emergency medical services, and law enforcement*. […] *The FBI has linked Conti to more than 400*

cyberattacks against organizations around the world, three-quarters of which are based in the United States, with claims of up to $25 million. This makes Conti one of the most avid groups ever."[1]

3 GENERAL RECOMMENDATIONS

3.1 Ransomware

The use of weak passwords in combination with a lack of MFA can have severe consequences for organizations. MITRE provides mitigations against the use of valid accounts as initial access vector. MFA should be enabled on all accounts to provide additional security. It is not known how the attackers accessed the data. However, stringent data loss prevention (DLP) measures can increase the chances of detecting data leaving the network in an unauthorised fashion. For additional information and guidance on guarding against ransomware information visit https://www.enisa.europa.eu/publications/ransomware and also NCSC, ANSSI and CISA websites.

Follow the Europol initiative NO MORE RANSOM. https://www.europol.europa.eu/activities-services/public-awareness-and-prevention-guides/no-more-ransom-do-you-need-help-unlocking-your-digital-life.

3.2 Supply Chain

Supply chain attacks have been a concern for information security experts for many years because the chain reaction triggered by one attack on a single supplier can compromise a network of providers. The joint advisory offers detection and mitigation advice, which centres around deploying MFA, locking out accounts after several failed attempts, password complexity, encrypted authentication, network segmentation, and log auditing. According to the recent ENISA report 'Threat Landscape for Supply Chain Attacks', strong security in no longer enough for organizations when attackers have already shifted their attention to suppliers.

3.3 Phishing

Education is the best prevention against social engineering tactics. Given that this campaign featured highly targeted lures, it is likely that even individuals that are trained to spot phishing attempts will be tricked. As such, operational intelligence, can significantly reduce risk. Fileless malware was used in the operation, and it is vital to ensure that organisations' security products have the capability to detect this type of threat.

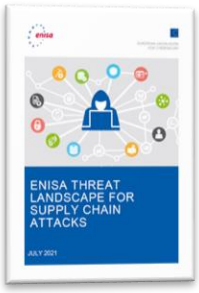
Training and awareness (the "human firewall") is considered to be one of the best prevention tools against social engineering tactics. Given that this campaign featured highly targeted lures and fileless malware, it is likely that even individuals that are trained to spot phishing attempts were tricked. As

[1] https://www.redhotcyber com/post/attacco-all-energia-elettrica-italiana-conti-colpisce-argos-connect-energy

such, operational cyber-intelligence can help increase the capability to detect this type of threat and significantly reduce risk

4 SUGGESTED READINGS FROM ENISA

Threat Landscape for Supply Chain Attacks – This report aims at mapping and studying the supply chain attacks that were discovered from January 2020 to early July 2021. It is estimated that there will be four times more supply chain attacks in 2021 than in 2020. With half of the attacks being attributed to Advanced Persistence Threat (APT) actors, their complexity and resources greatly exceed the more common non-targeted attacks, and, therefore, there is an increasing need for new protective methods that incorporate suppliers in order to guarantee that organizations remain secure.



ENISA Threat Landscape 2020 - Ransomware – The report outlines the findings on ransomware, provides a description and analysis of the domain and lists relevant recent incidents. A series of proposed actions for mitigation is provided.