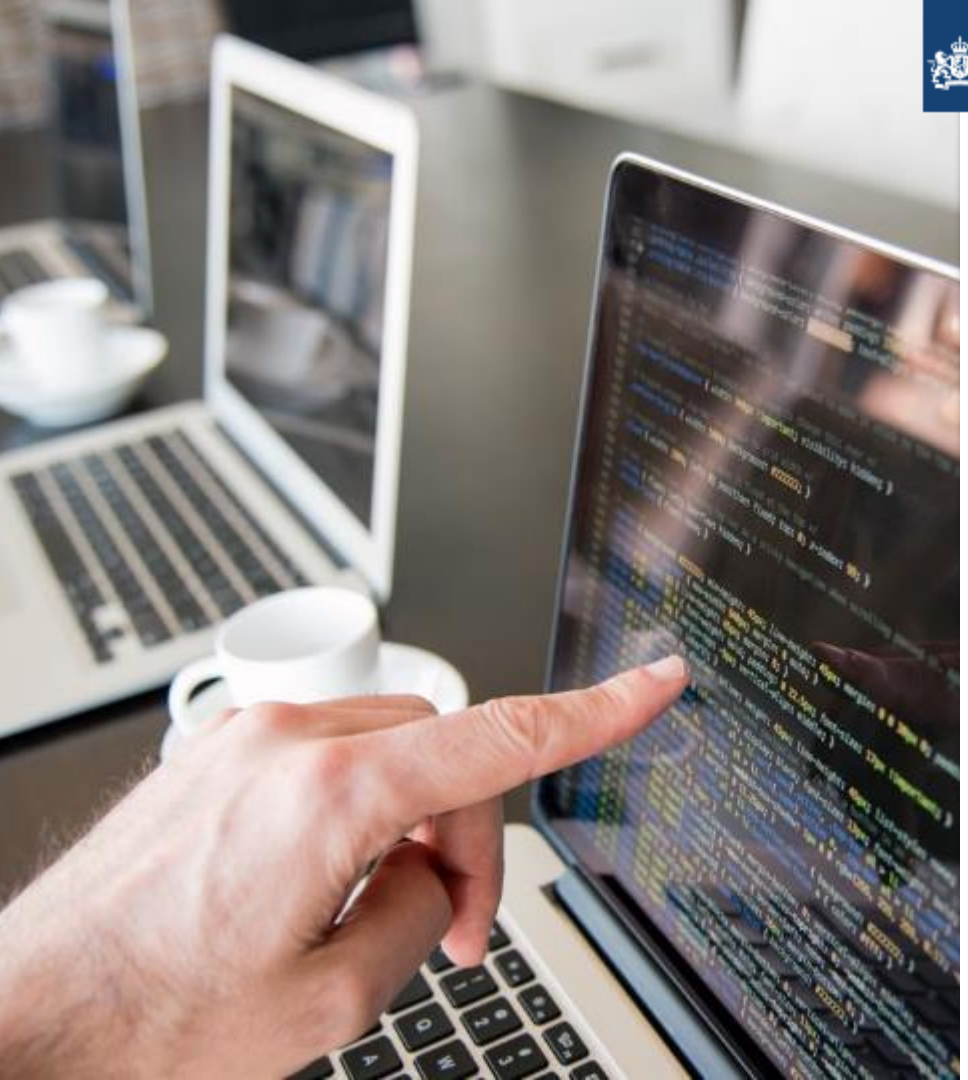
National Cyber Security Centre
Ministry of Justice and Security

Dreigingslandschap OT

Ivan Flos, Dreigingsanalist NCSC

10 februari 2022

NCSC



Agenda

1. Introductie
2. Historische incidenten in vogelvlucht
3. Huidige dreigingsbeeld
4. 2022: waar moeten we op letten


Waarom is OT-security relevant?

Waarom hebben we het over OT-security?

OT-systemen zijn van fundamenteel belang voor de continuïteit van vitale processen.

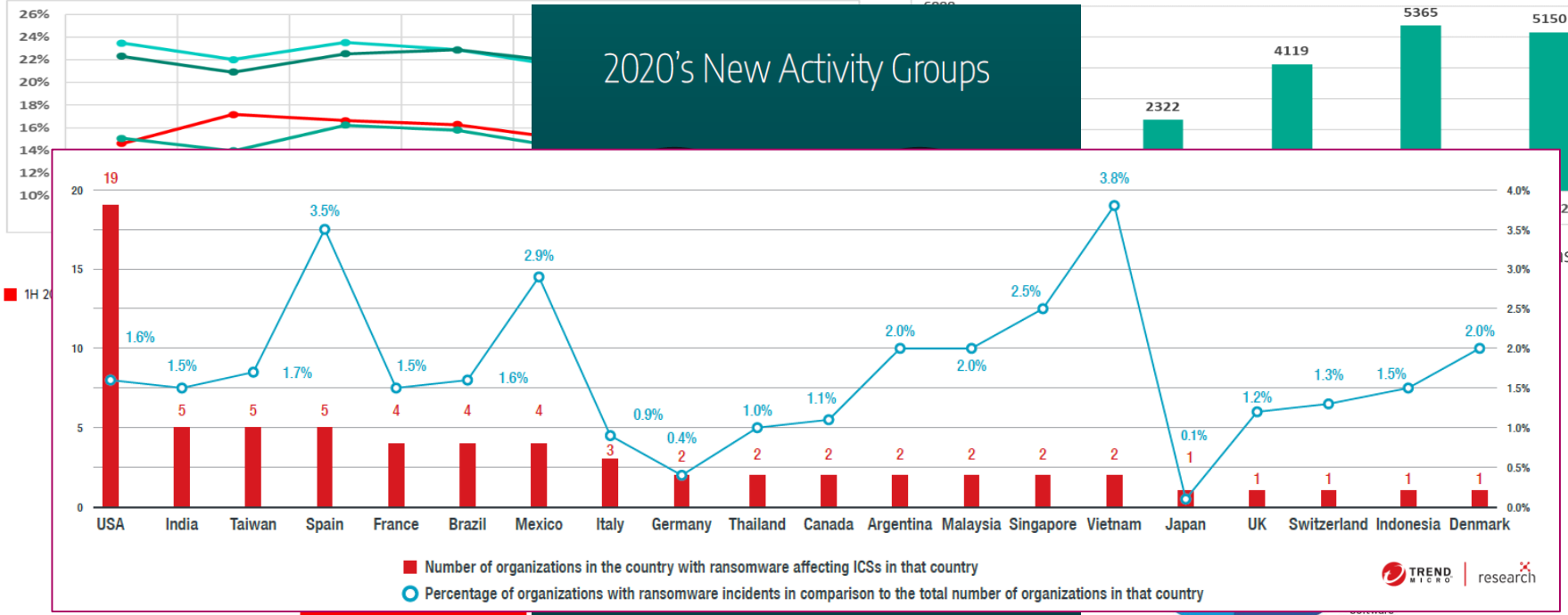
Uitval kan leiden tot:

- **Maatschappelijke onrust**
- **Economische schade**
- **Verlies van vertrouwen in digitalisering**

OT-security is geen sinecure

IT/OT steeds meer verweven

Aanhoudende dreiging...



...maar ook toenemend bewustzijn

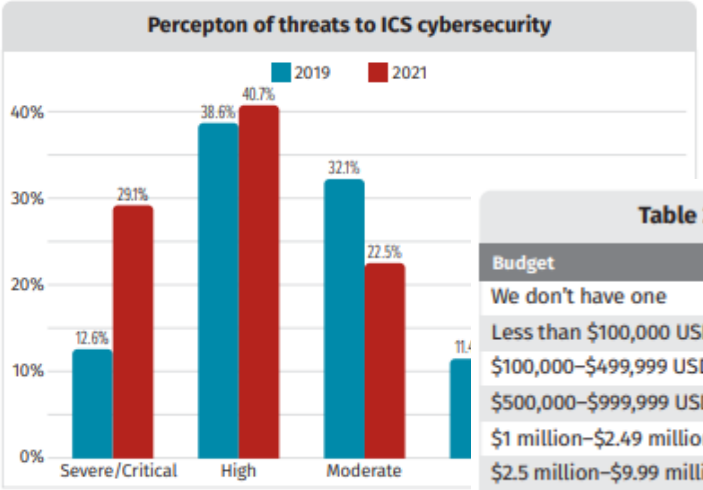
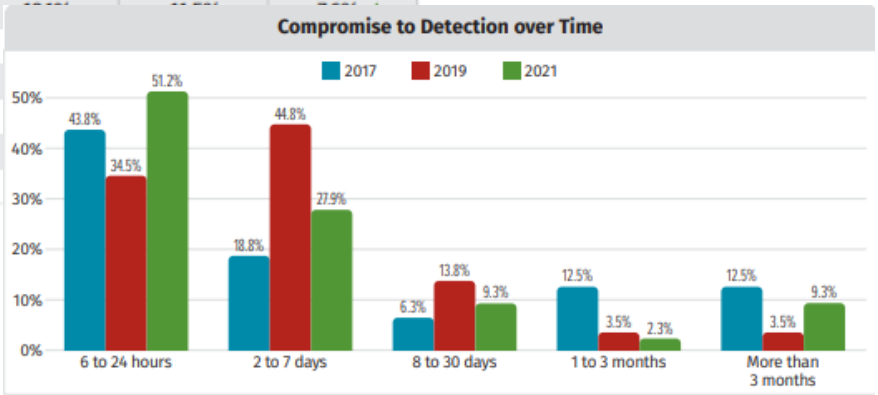


Table 2. 2021 vs. 2019 Budget Comparison

Budget	2021	2019	% Change
We don't have one	23.7%	9.9%	13.8% ▲
Less than $100,000 USD			
$100,000–$499,999 USD			
$500,000–$999,999 USD			
$1 million–$2.49 million USD			
$2.5 million–$9.99 million USD			
Greater than $10 million USD			

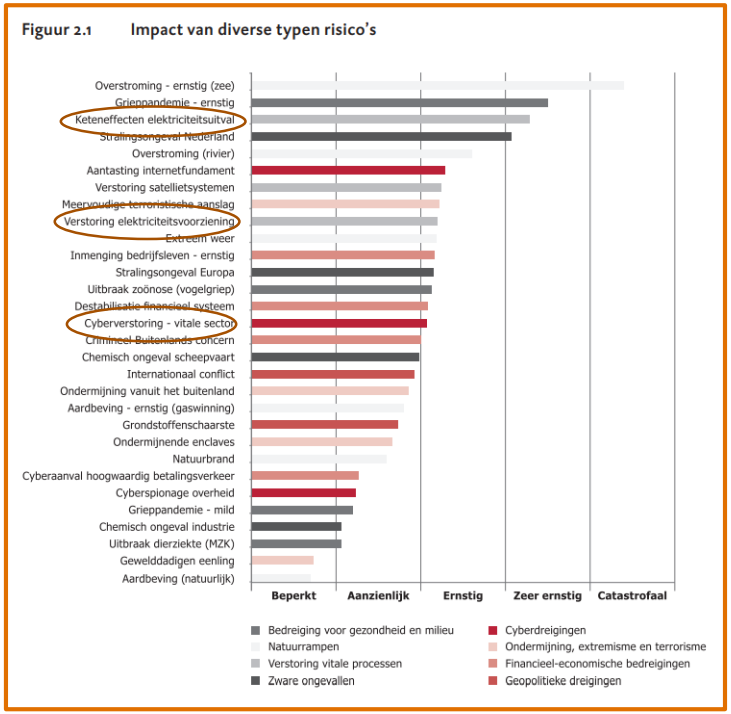


Bron: A SANS 2021 Survey: OT/ICS Cybersecurity

OT-security is ook voor Nederland relevant

De afgelopen jaren zijn er meerdere rapporten verschenen die het belang van OT-security voor Nederland onderschrijven:

- **WRR waarschuwt voor mogelijke digitale ontwrichting**
- **En de Algemene Rekenkamer stelt dat "Cybersecurity vitale waterwerken niet waterdicht" is**
- **Ook volgens de CSR is er "werk aan de winkel" op het gebied van OT-beveiliging**
- **Onderzoek van de Universiteit Twente heeft aangetoond dat het relatief makkelijk is met het internet verbonden OT-systemen in Nederland te vinden**
- **Een recente rondgang bij gemeenten toont aan dat er grote zorgen zijn over industriële controlesystemen waarmee riolering, sluizen en verkeerslichtsystemen worden aangestuurd**



Historische OT-incidenten

Stuxnet

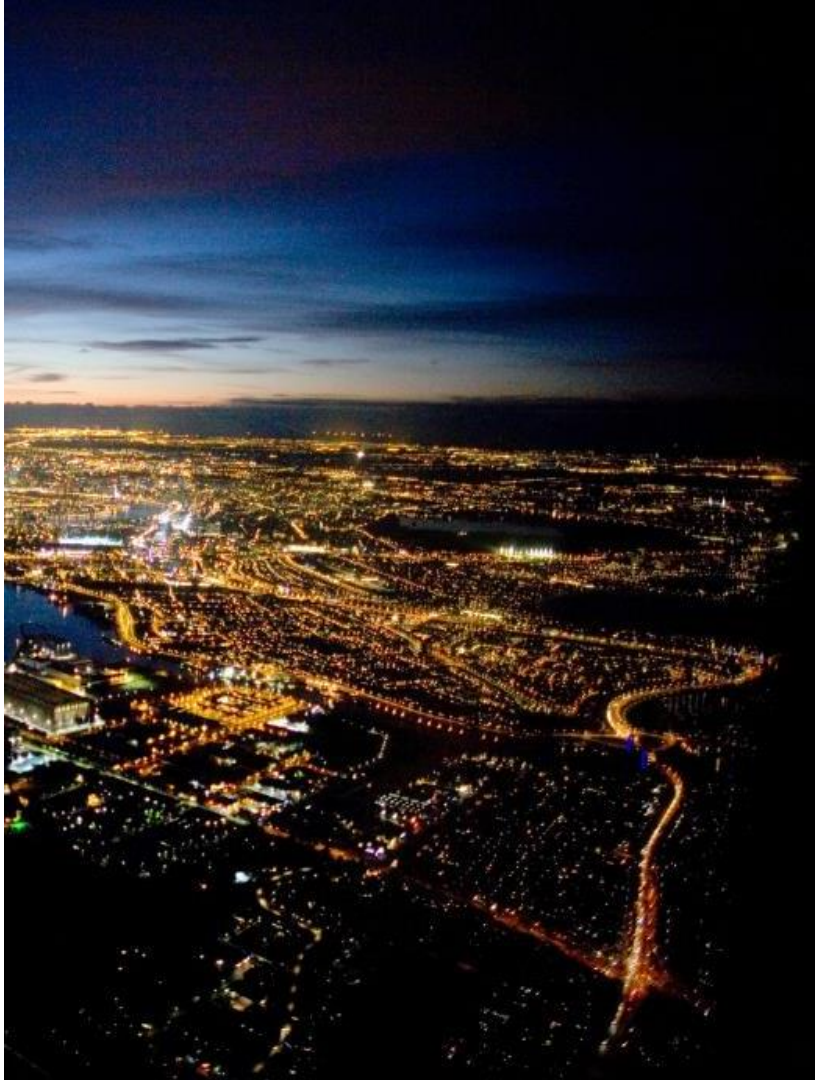
- **Een van de meest geavanceerde cyberaanvallen ooit**
- **Ingezet tegen uranium verrijkingsinstallatie Natanz (Iran):**
  - **Versie 1: compromittatie Siemens PLC's om uitlaatkleppen dicht te houden**
  - **Versie 2: automatische verspreiding gericht op ontwrichting toerental centrifuges**
- **Gericht op frustreren en vertragen van verrijkingsprogramma**

Havex

- **Verzamelen van inlichtingen in energiesector**
- **Remote Access Trojan (RAT) voor beheer van ICS-systemen**
- **Supply chain aanval → updates ICS-software**
- **Nieuwe campagne 2015: voorbereidingshandelingen t.o.v. sabotage**

BlackEnergy/Industroyer/NotPetya

- **BlackEnergy (2015): hackers zorgen voor het eerst voor een stroomuitval**
- **Industroyer/CrashOverride (2016): eerste malware specifiek ontworpen gericht op elektriciteitsnet**
- **NotPetya (2017): wiperware verpakt als ransomware richt grote (internationale) schade aan (niet gericht op OT maar wel grote operationele gevolgen)**

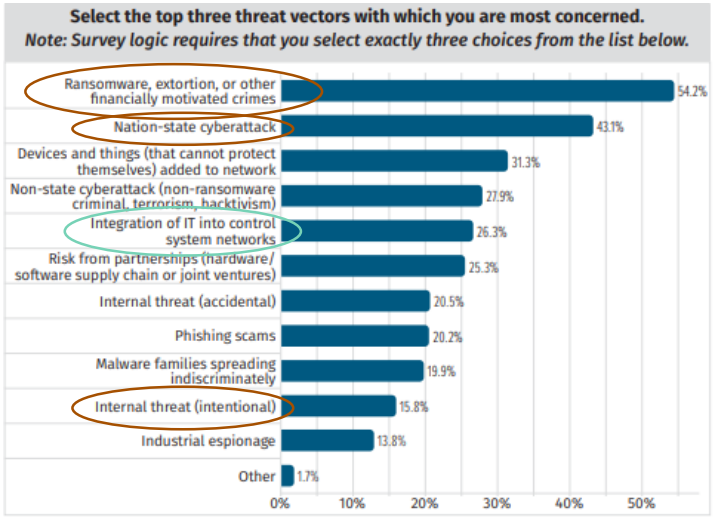


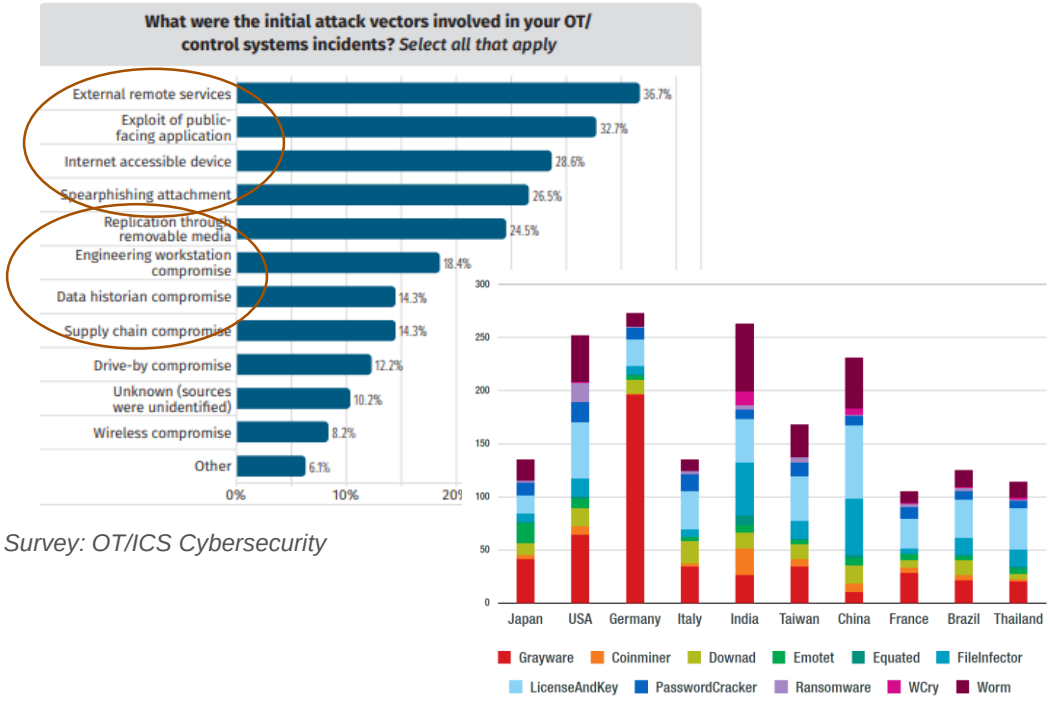
TRITON/TRISIS

- **Eerste malware die zich richt op aantasting veiligheidssystemen**
  (herprogrammering van het noodstopsysteem van Schneider Electric's Triconex Safety Instrumented System (SIS) controllers)
- **Aanval (2017) op olieraffinaderij Saudi-Arabië mislukt en productiefaciliteiten worden stilgelegd**
- **VS legt sancties op aan het Russische "Central Scientific Research Institute of Chemistry and Mechanics"**


Huidig
dreigingslandschap

Dreigingsperceptie, aanvalsvectoren en malware





Bron: A SANS 2021 Survey: OT/ICS Cybersecurity

TREND MICRO | research

Statelijke actoren

CSBN 2020/2021:

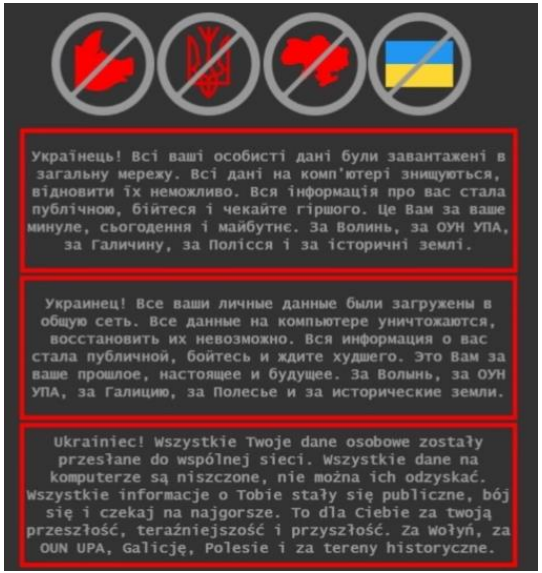
- **Digitale dreiging is permanent**
- **Sabotage een van de grootste cyberdreigingen**
- **Voorbereidende handelingen maar geen intentie om over te gaan tot sabotage**

Dreigingsbeeld statelijke actoren:

- **China, Iran, Rusland hebben een offensief cyberprogramma**
- **Beschikken over een breed palet aan middelen**

Statelijke actoren

- **Rusland probeert structureel toegang te krijgen tot essentiële en vitale infrastructuur van bondgenoten (Bron: DBSA 2021)**
- **In het verleden gezien dat Rusland over de juiste capaciteiten beschikt**
- **Rekening houden met mogelijk veranderende intentie ten tijde van escalatie**
- **Wat we hebben gezien in Oekraïne tot nu toe:**
  - **Defacement-aanval**
  - **Wiperware (geen worm)**
  - **Wit-Russische cyberpartizanen**



Statelijke actoren

Iran

- **Mogelijke nevenschade van activiteiten**
- **Aanvallen passen binnen geopolitieke context**
  - **Shamoon (2012/2016/2018)**
  - **Verkenningen in scheepsvaart en olie- en gassector**
  - **Toegang tot drinkwatervoorzieningen Israël**
  - **Maar ook aanvallen *op* Iran, recentelijk op tankstations**

China

- **Nederlandse afhankelijk van Chinese technologie**

> Retouradres Postbus 16950 2500 BZ Den Haag

Aan de Voorzitter van de Tweede Kamer
der Staten-Generaal
Postbus 20018
2500 EA DEN HAAG

Turfmarkt 147
2511 DP Den Haag
Postbus 16950
2500 BZ Den Haag
www.nctv.nl

Ons kenmerk
2665986

Uw kenmerk
2019Z15162

Bij beantwoording de datum en ons kenmerk vermelden. Wilt u slechts één zaak in uw brief behandelen.

Datum 16 september 2019
Onderwerp Antwoorden Kamervragen over 'Het advies van de AIVD over de nationale veiligheid en veiling 5G'

In antwoord op uw brief van 16 juli 2019 deel ik u mede namens de Minister van Binnenlandse Zaken en Koninkrijksrelaties en de Minister van Defensie mee dat de schriftelijke vragen van de leden Buitenweg en Bromet (beiden GroenLinks) over het advies van de AIVD over de nationale veiligheid en veiling 5G worden beantwoord zoals aangegeven in de bijlage van deze brief.

De Minister van Justitie en Veiligheid,

Ferd Grapperhaus

Criminele organisaties en ICS

- **CSBN 2020 waarschuwt voor toenemende dreiging criminele actoren t.o.v. ICS**
- **Aantrekkelijk doelwit vanwege consequenties downtime**
- **EKANS-ransomware lijkt hier specifiek op in te spelen (opvolger van MegaCortex?)**
- **Mogelijke slachtoffers zijn Honda en Enel, precieze impact onduidelijk**
- **Vrij stil sinds 2020… Is ICS-focus wel noodzakelijk?**

Appendix A – EKANS Targeted Processes

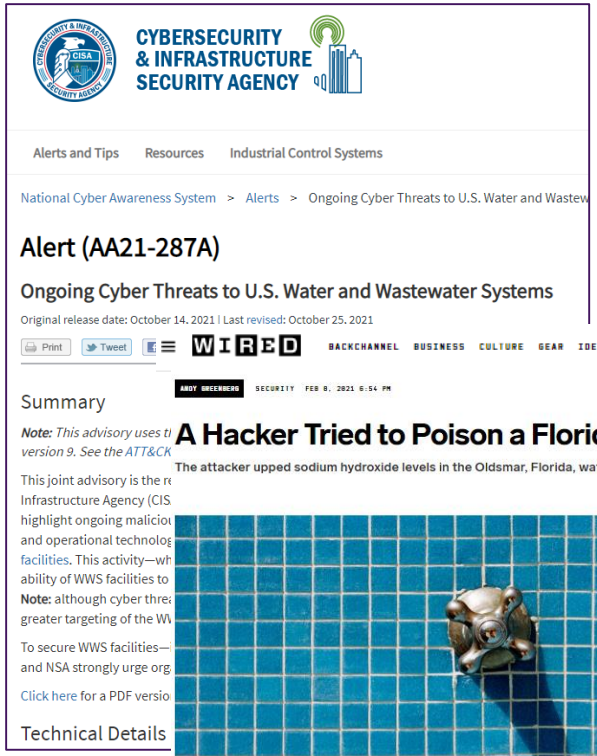
Process	Description
bluestripecollector.exe	BlueStripe Data Collector
ccflic0.exe	Proficy Licensing
ccflic4.exe	Proficy Licensing
cdm.exe	Nimsoft Related
certificateprovider.exe	Ambiguous
client.exe	Ambiguous
client64.exe	Ambiguous
collwrap.exe	BlueStripe Data Collector
config_api_service.exe	ThingWorx Industrial Connectivity Suite, Ambiguous
dsmcsvc.exe	Tivoli Storage Manager Client
epmd.exe	RabbitMQ Server (SolarWinds)
erlsrv.exe	Erlang
fnplicensingservice.exe	FLEXNet Licensing Service
hasplmv.exe	Sentinel Hasp License Manager
hdb.exe	Honeywell HMIWeb
healthservice.exe	Microsoft SCCM
ilicensevc.exe	GE Fanuc Licenseing
inet_gethost.exe	Erlang
keysvc.exe	Ambiguous
managementagenthost.exe	VMWare CAF Management Agent Service
monitoringhost.exe	Microsoft SCCM

Ransomware en operationele processen

- **Dragos: 500% toename ransomware-aanvallen 2018-2020**
- **Veelal IT-gericht, maar grote gevolgen voor operationele processen**
- **CSBN 2021: ransomware is risico voor nationale veiligheid**
- **Recente cases:**
  - **Norsk Hydro**
  - **"Kaas-hack"**
  - **Colonial Pipeline**
  - **JBS**
  - **Terminals DE/BE/NL**

Insider Threat

- **Meerdere (ransomware-)aanvallen op riolering- en waterzuiveringsbedrijven in VS in 2021**
- **Toegang door spearfishing, RDP en VPN**
- **Maar ook insider threat (Oldsmar):**
  - **Toegang tot SCADA-systeem middels TeamViewer**
  - **Gedeeld ww/Windows7/Internet**
  - **Verhoging chemicaliën tot dodelijk niveau**



CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY

Alerts and Tips Resources Industrial Control Systems

National Cyber Awareness System > Alerts > Ongoing Cyber Threats to U.S. Water and Wastew

Alert (AA21-287A)

Ongoing Cyber Threats to U.S. Water and Wastewater Systems

Original release date: October 14, 2021 | Last revised: October 25, 2021

Print Tweet

Summary

Note: This advisory uses t
version 9. See the ATT&CK

This joint advisory is the r
Infrastructure Agency (CIS
highlight ongoing maliciou
and operational technolog
facilities. This activity—wh
ability of WWS facilities to
Note: although cyber threa
greater targeting of the WW

To secure WWS facilities—
and NSA strongly urge org

Click here for a PDF versio

Technical Details

WIRED BACKCHANNEL BUSINESS CULTURE GEAR IDEAS SCIENCE SECURITY

ANDY GREENBERG SECURITY FEB 8, 2021 6:54 PM

A Hacker Tried to Poison a Florida City's Water Supply

The attacker upped sodium hydroxide levels in the Oldsmar, Florida, water supply to extremely dangerous levels.

The cursor began clicking through the water treatment plant's controls. Within seconds, the intruder was attempting to change the water supply's levels of sodium hydroxide. PHOTOGRAPH: GETTY IMAGES

Waar moeten we op letten in 2022

1. Aanhoudende ransomware-aanvallen
2. Toenemende verbondenheid IT/OT
3. Oplopende spanningen Oekraine
4. Nozomi: verschuiving digitale aanvallen VS naar EU
5. Kaspersky: ICS-aanvallen moeilijker te detecteren
6. Vergeet ook Log4j niet

Vragen?