Global og lokal cybertrussel i VA

VA-dagene 03.04.2024

kraftCERT

infraCERT

KraftCERT/InfraCERT

- Et initiativ fra Nasjonal sikkerhetsmyndighet og NVE etablert i 2014
- Uavhengig, non-profit selskap
- Er sektor-CERT, og er med i flere beredskaps- og interesseorganisasjoner
- Har medlemmer i alle størrelser innen kraft, gjenvinning, petroleum, vann og avløp.
- Noen leverandører er også medlem

- ***Vi har alle sårbare kjernesystemer og står overfor mer eller mindre det samme trusselbildet***

Sektoren

- Vann og avløp er del av kritisk infrastruktur
  - Har fått større fokus av både trusselaktører og det offentlige i det siste
- Ingen god nasjonal lovgivning
- Modenheten er, som i alle bransjer varierende, ikke minst på grunn av størrelsesvariasjon.
- Frihet til å velge infrastruktur kan være begrenset
- Investeringer i cyber kan være tungt å få innvilget

Spørsmål

Hvordan kommer vi til å bli angrepet?

Hvilke av våre teknologier vil bli angrepet?

Hva gjør oss og verdikjedene våre til mål?

Hvordan vil vårt trusselbilde påvirkes av nasjonal og internasjonal sikkerhetspolitikk?

Globalt

Overordnet trusselbilde

- Russland vil samle informasjon, ikke bare gjennom nettverksoperasjoner, men også fysisk og hybrid
- Kina er ute etter teknologi, og bedriver operasjoner i det stille; i motsetning til mange andre aktører har de lite behov for oppmerksomhet.
- Fremtidige aktører i kriger vil ha et cyberelement.
- Leverandørkjedeangrep er fremdeles svært aktuelt; angriperne blir stadig mer klar over potensialet her.

Hendelser

- Det har vært mange kompromitterte selskap i VA verden rundt, med dertil hørende panikk
- Kinesiske trusselaktører
- Iranske trusselaktører som ser sitt snitt
- Andre, opportunistiske trusselaktører

nathan Greig
y 3rd, 2023

overnment | News

ybercrime

Italian w
with ran

An Italian com
experiencing

Alto Calore Se

Jonathan Greig
February 21st, 2023

Malware | News Briefs

Cybercrime | Technology

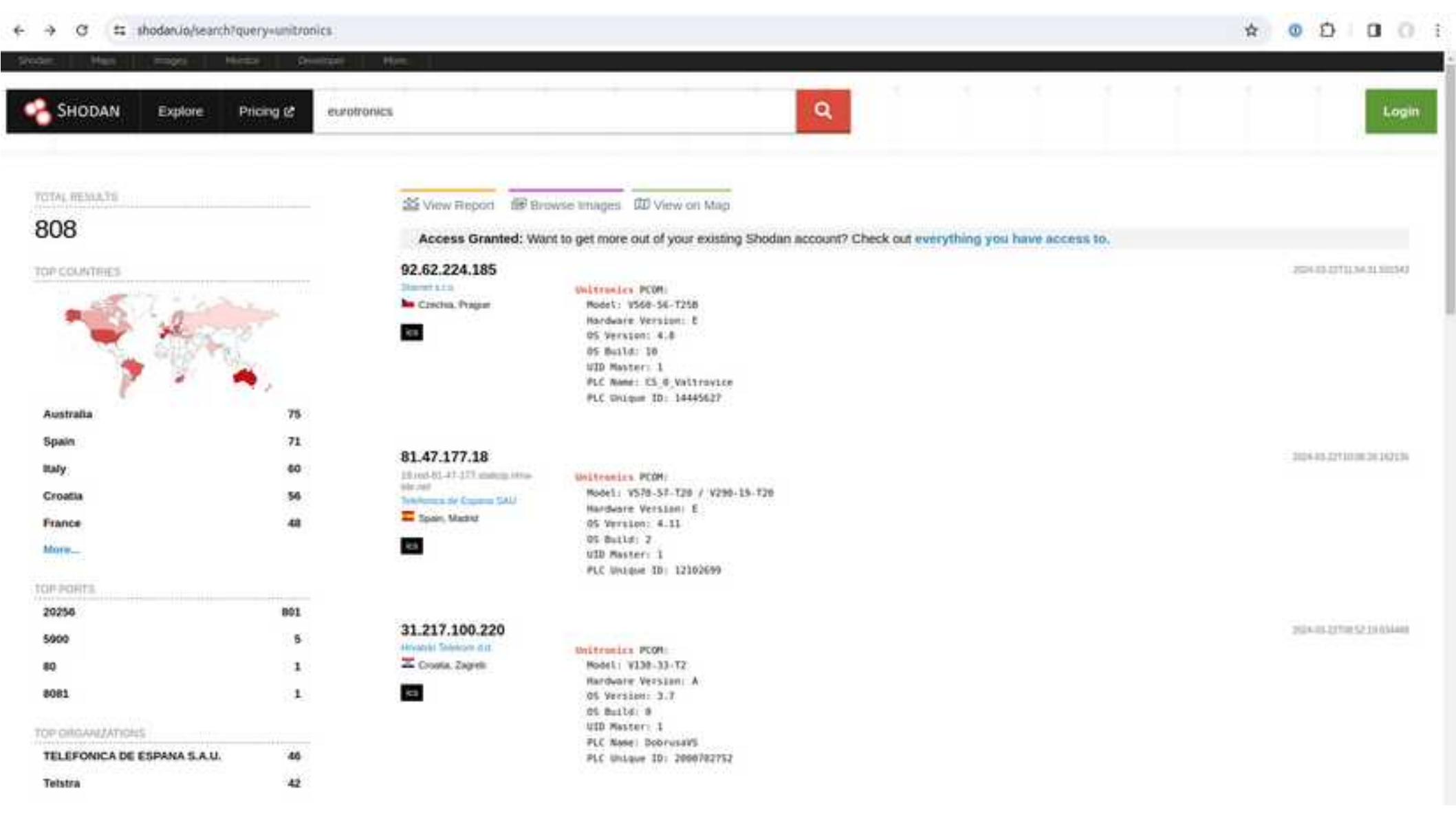
LockBit gang takes credit for attack on water utility in Portugal

The LockBit ransomware group has taken credit for an attack on the water utility of Porto, Portugal's second-largest city.

Hva vil de?

- Skaffe seg fotfeste, bevege seg innover
- Gjøre endringer, markere at de har vært der
- Sabotere
- Kryptere eller drive annen utpresning


YOU HAVE BEEN
HACKED
DOWN WITH ISRAEL
الموت لإسرائيل
EVERY EQUIPMENT
"MADE IN ISRAEL"
IS CYBER AV3NGERS
LEGAL TARGET
V570


shodan.io/search?query=unitronics
SHODAN
Explore
Pricing
eurotronics
Login
TOTAL RESULTS
808
TOP COUNTRIES
Australia 75
Spain 71
Italy 60
Croatia 56
France 48
More...
TOP PORTS
20256 801
5900 5
80 1
8081 1
TOP ORGANIZATIONS
TELEFONICA DE ESPANA S.A.U. 46
Telstra 42
View Report
Browse Images
View on Map
Access Granted: Want to get more out of your existing Shodan account? Check out everything you have access to.
92.62.224.185
Czechia, Prague
Unitronics PCOM:
Model: V560-56-T25B
Hardware Version: E
OS Version: 4.8
OS Build: 10
UID Master: 1
PLC Name: CS_0_Valtrovice
PLC Unique ID: 14445627
81.47.177.18
Telefónica de España SAU
Spain, Madrid
Unitronics PCOM:
Model: V570-57-T20 / V290-19-T20
Hardware Version: E
OS Version: 4.11
OS Build: 2
UID Master: 1
PLC Unique ID: 12102699
31.217.100.220
Hrvatski Telekom d.d.
Croatia, Zagreb
Unitronics PCOM:
Model: V130-33-T2
Hardware Version: A
OS Version: 3.7
OS Build: 0
UID Master: 1
PLC Name: DobrusaVS
PLC Unique ID: 2000782752

Hvem tar de?

- Vannverk
- Kommunale vann- og avløp
- Relevante myndigheter

Lokalt

Mest sannsynlige trussel:
Følgeskade fra utpresningsangrep fra kriminelle er den mest sannsynlige trusselen mot produksjonsprosesser/ kontrollsystem.

Mest alvorlige trussel:
Avanserte oppdragsstyrte aktører jobber kontinuerlig for å utvikle evne til destruktive eller driftsforstyrrende angrep.

Trusselaktørutvikling

- Ytterligere profesjonalisering:
  det er nesten bare aksess-selgere i de initielle fasene
- Vet man da egentlig hvem som står bak et angrep?
- En angrepsadresse: er det samme angriper som sist
  - Infrastrukturer selges, de hackes, og ofte vil angriper at du tror det er noen andre.

Industrielle kontrollsystemer

- Fjernaksess, VPN, filoverføring og brannmurer er svært populære angrepsmål
- Aktører vil stjele informasjon industrielle systemer for å nå langsiktig mål om å angripe kontrollsystem
- Dette kan f.eks. gjelde data lekket fra IoT, data lekket fra leverandører, data lekket i overføringer til annet bruk, eller data tatt i cyberinnbrudd.

Fremover

- Man vil se mye hacktivisme, ekte eller ei
- Det vil være mye industrispionasje i det stille
- Leverandørkjedeangrep er blitt med tilgjengelig for trusselaktører
- Trusselaktører blir bedre på sky- og hybridløsninger
- KI
  - Avanserte angrep; sensitiv informasjon, sette sammen informasjon til relevant angrepsinformasjon
- Krypteringsskadevare: det er rom for mere og flere metoder

Fremover

- Dagens eksport av data skaper morgendagens destruktive angrep
- Dagens usikre integrasjoner og trafikk skaper morgendagens driftsforstyrrende angrep
- Vi kan ikke forvente forvarsel
- Nasjonalt trusselbilde må følges opp med lokal analyse
- Leverandørkjeder er en stor utfordring
- Grunnsikring er viktigere enn reaktiv sikring

Spørsmål?

Margrete Raaum,
Margrete.raaum@kraftcert.no
cert@kraftcert.no
Tlf: +47 95201798

kraftCERT

infraCERT