NAKIT

Národní agentura pro
komunikační a informační
technologie, s. p.

BEZPEČNOST KRITICKÉ INFRASTRUKTURY MĚST ČR

15. 5. 2018

Praha

Vladimír ROHEL

Žijeme v době, kdy:

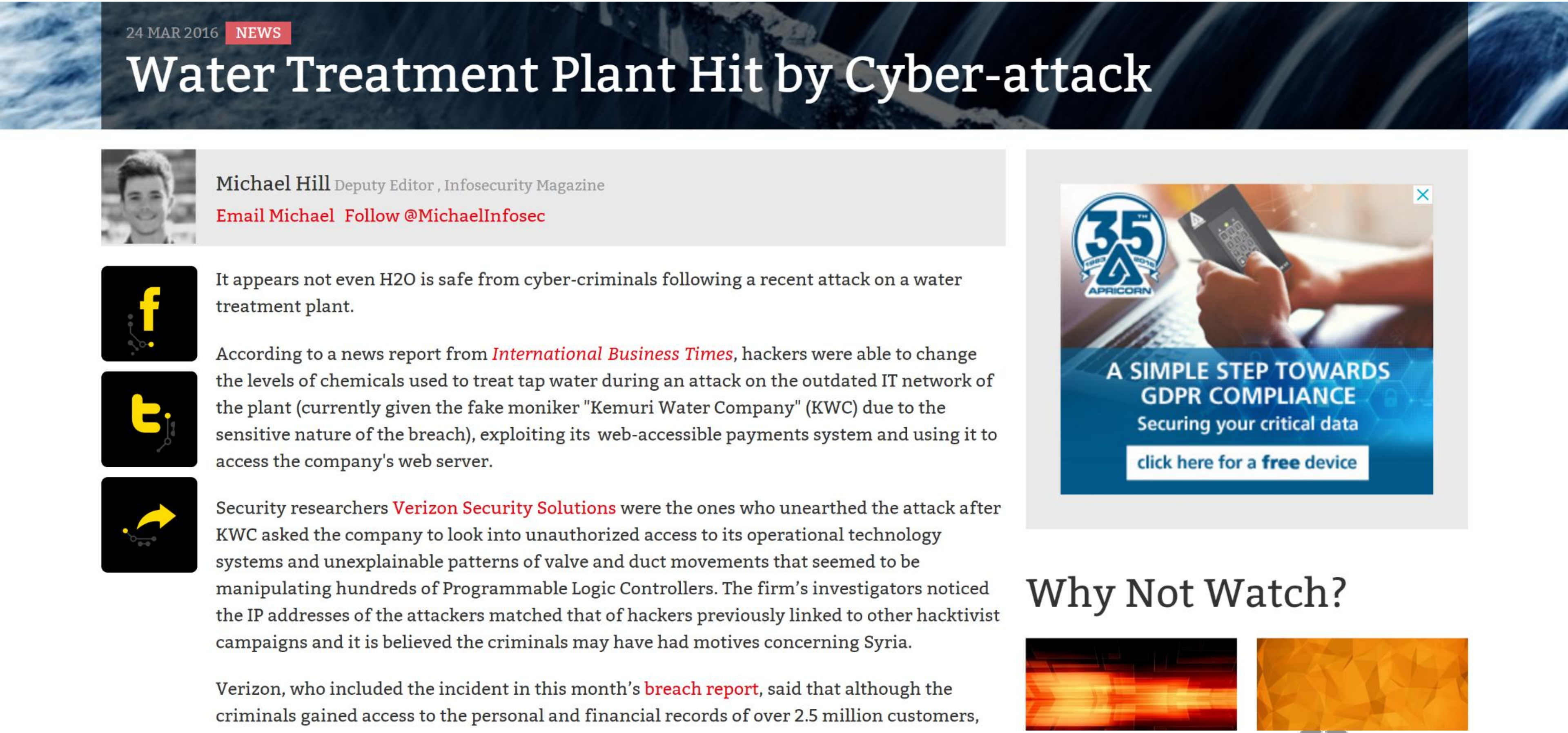
- Roste naše závislost na IT
- IT pronikají do oblastí, kde dříve nebyly
- Svět se stále více propojuje a vše se zrychluje
- Do internetu a sítí se připojují technologie a zařízení, která s tím nikdy v návrhu nepočítala – bezpečnost
- Takováto zařízení jsou často využívána v sítích KI
- Roste kvalifikovanost a technické schopnosti útočníků
- Do útoků se zapojují noví hráči
- Dochází k vývoji obchodních modelů i na hackerské scéně (CaaS)

Reakce ČR na současný stav –> z 181/2014 Sb.

- Zákon o kybernetické bezpečnosti reaguje na situaci v KI od roku 2014
- Novely zákona z roku 2017:
  - Reagují na zkušenosti ze 3 let účinnosti zákona
  - Zavádějí soulad s evropskou směrnicí NIS
  - Definují nová odvětví:
    - 1. energetika,
    - 2. doprava,
    - 3. bankovnictví,
    - 4. infrastruktura finančních trhů,
    - 5. zdravotnictví,
    - 6. **vodní hospodářství,**
    - 7. digitální infrastruktura,
    - 8. chemický průmysl,
  - Zavádějí nový pojem základní služba, jejíž poskytování je závislé na sítích elektronických komunikací nebo informačních systémech a jejíž narušení by mohlo mít významný dopad na zabezpečení společenských nebo ekonomických činností v některém z těchto odvětví. (vazba na KII)

Proč je to důležité?

- Kybernetické útoky na KI každoročně přibývají a roste jejich závažnost
- V oblasti kybernetických útoků se stále více angažují státní aktéři – jiná motivace, jiné cíle, jiné možnosti financování
- Časté jsou ale i útoky s kriminální podstatou – typicky v poslední době Ransomware
- Některé státy již zřizují speciální týmy na bezpečnost těchto systémů – specifičnost prostředí
- NATO a CCDCoE zařadily pravidelně do svých cvičení KB oblast „SCADA“ systémů; vazby mezi IT a OT



24 MAR 2016 NEWS

Water Treatment Plant Hit by Cyber-attack

Michael Hill Deputy Editor , Infosecurity Magazine
Email Michael Follow @MichaelInfosec

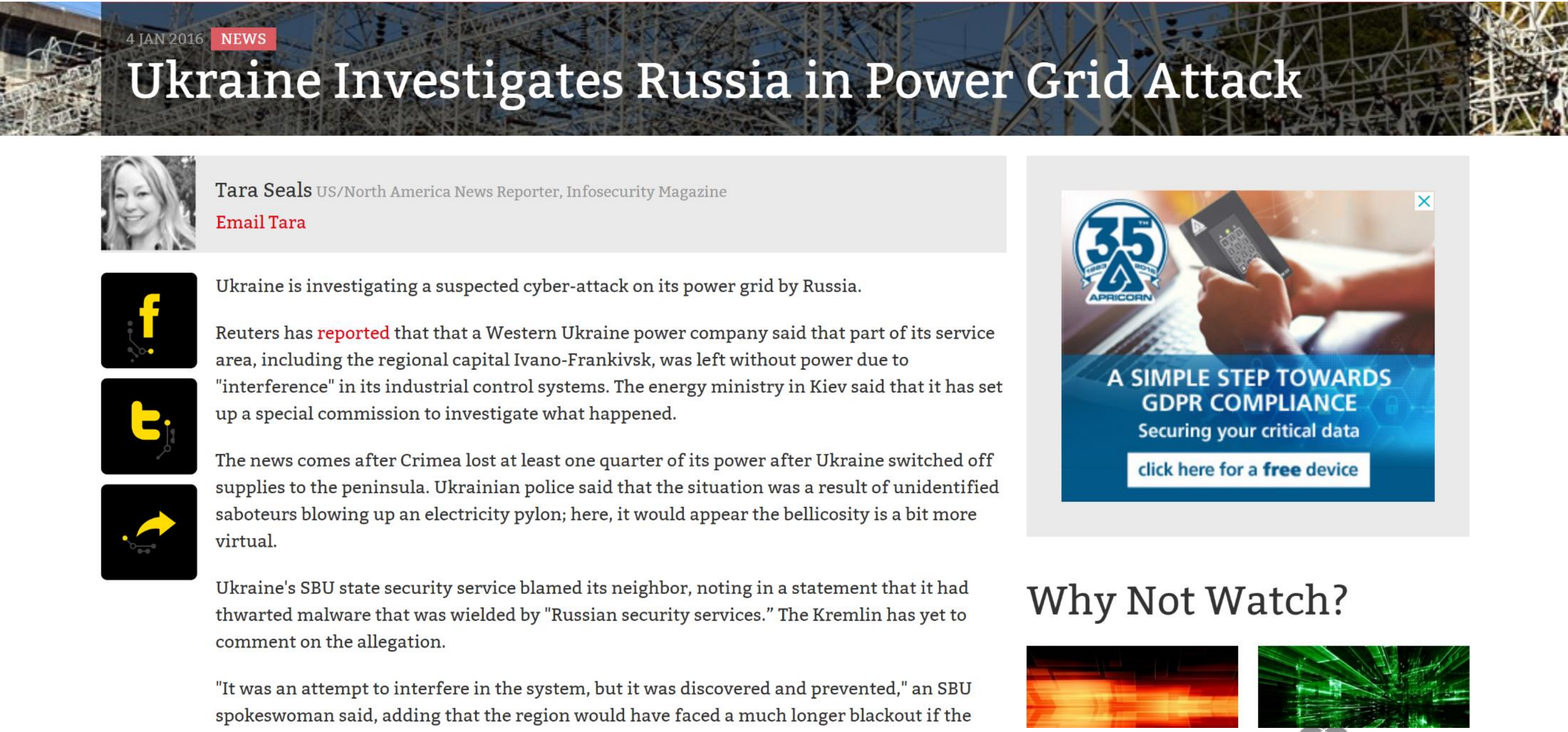
It appears not even H2O is safe from cyber-criminals following a recent attack on a water treatment plant.

According to a news report from *International Business Times*, hackers were able to change the levels of chemicals used to treat tap water during an attack on the outdated IT network of the plant (currently given the fake moniker "Kemuri Water Company" (KWC) due to the sensitive nature of the breach), exploiting its web-accessible payments system and using it to access the company's web server.

Security researchers Verizon Security Solutions were the ones who unearthed the attack after KWC asked the company to look into unauthorized access to its operational technology systems and unexplainable patterns of valve and duct movements that seemed to be manipulating hundreds of Programmable Logic Controllers. The firm's investigators noticed the IP addresses of the attackers matched that of hackers previously linked to other hacktivist campaigns and it is believed the criminals may have had motives concerning Syria.

Verizon, who included the incident in this month's breach report, said that although the criminals gained access to the personal and financial records of over 2.5 million customers,

Why Not Watch?



4 JAN 2016 NEWS

Ukraine Investigates Russia in Power Grid Attack

Tara Seals US/North America News Reporter, Infosecurity Magazine

Email Tara

Ukraine is investigating a suspected cyber-attack on its power grid by Russia.

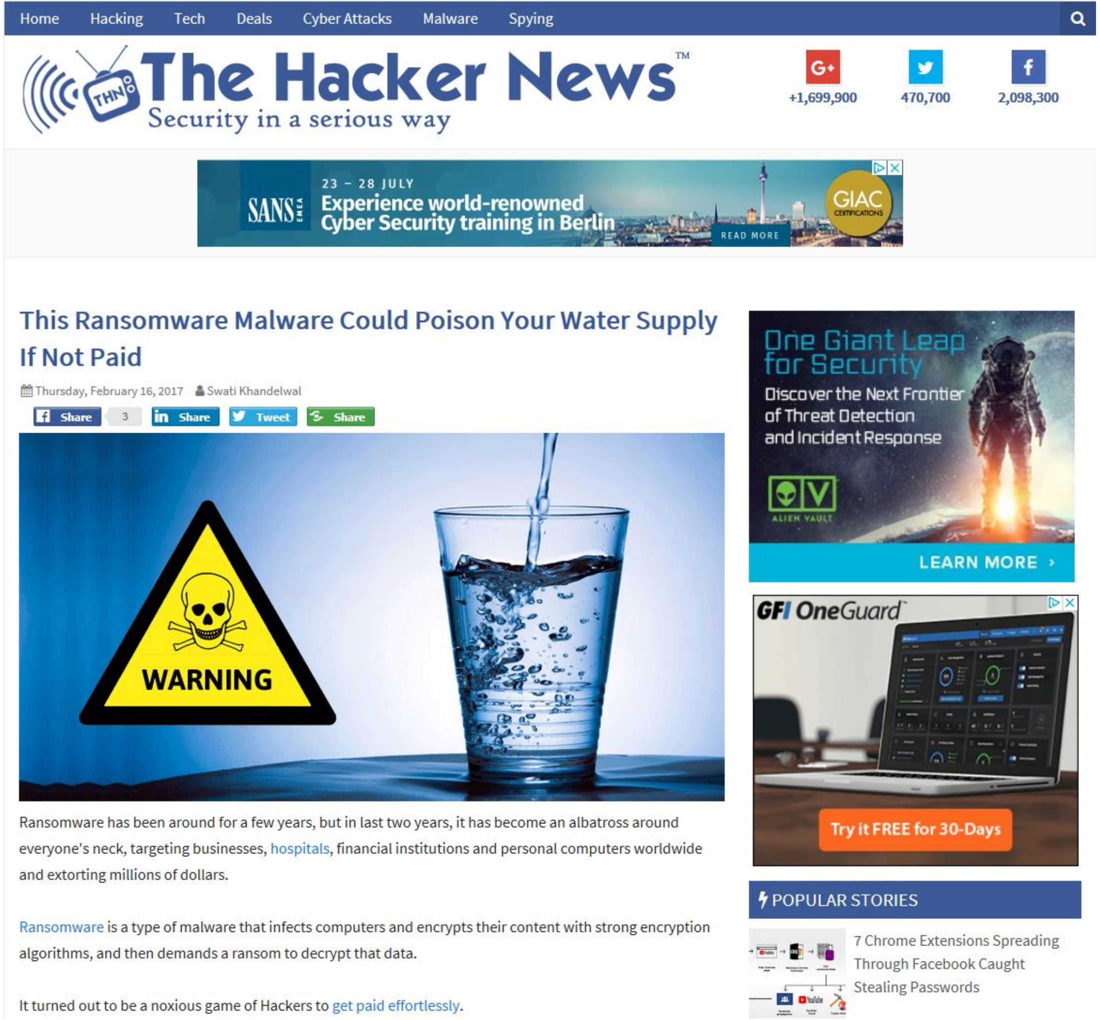
Reuters has reported that that a Western Ukraine power company said that part of its service area, including the regional capital Ivano-Frankivsk, was left without power due to "interference" in its industrial control systems. The energy ministry in Kiev said that it has set up a special commission to investigate what happened.

The news comes after Crimea lost at least one quarter of its power after Ukraine switched off supplies to the peninsula. Ukrainian police said that the situation was a result of unidentified saboteurs blowing up an electricity pylon; here, it would appear the bellicosity is a bit more virtual.

Ukraine's SBU state security service blamed its neighbor, noting in a statement that it had thwarted malware that was wielded by "Russian security services.” The Kremlin has yet to comment on the allegation.

"It was an attempt to interfere in the system, but it was discovered and prevented," an SBU spokeswoman said, adding that the region would have faced a much longer blackout if the

Why Not Watch?



The Hacker News™
Security in a serious way

This Ransomware Malware Could Poison Your Water Supply If Not Paid

Thursday, February 16, 2017 Swati Khandelwal

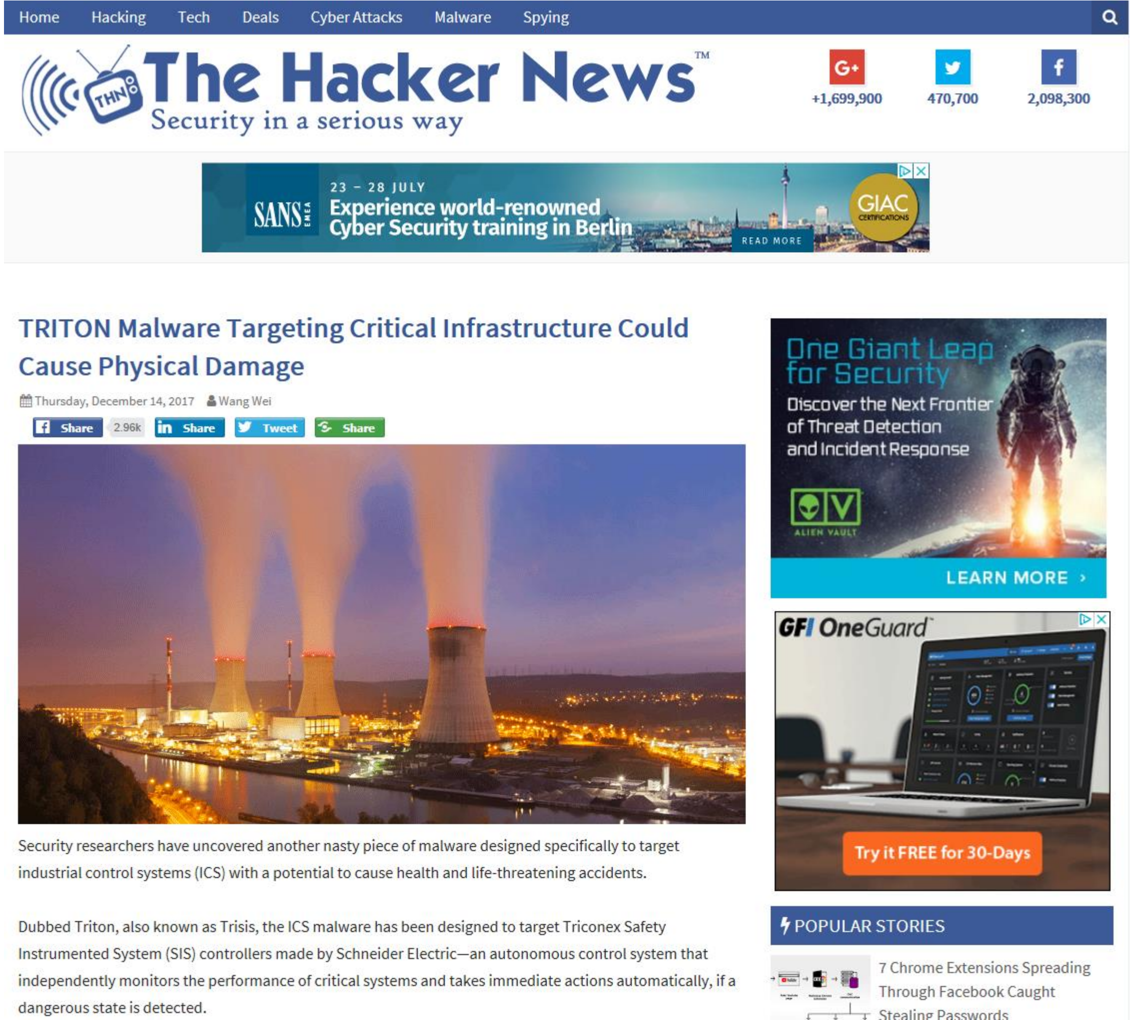
Ransomware has been around for a few years, but in last two years, it has become an albatross around everyone's neck, targeting businesses, hospitals, financial institutions and personal computers worldwide and extorting millions of dollars.

Ransomware is a type of malware that infects computers and encrypts their content with strong encryption algorithms, and then demands a ransom to decrypt that data.

It turned out to be a noxious game of Hackers to get paid effortlessly.

POPULAR STORIES

7 Chrome Extensions Spreading Through Facebook Caught Stealing Passwords



TRITON Malware Targeting Critical Infrastructure Could Cause Physical Damage

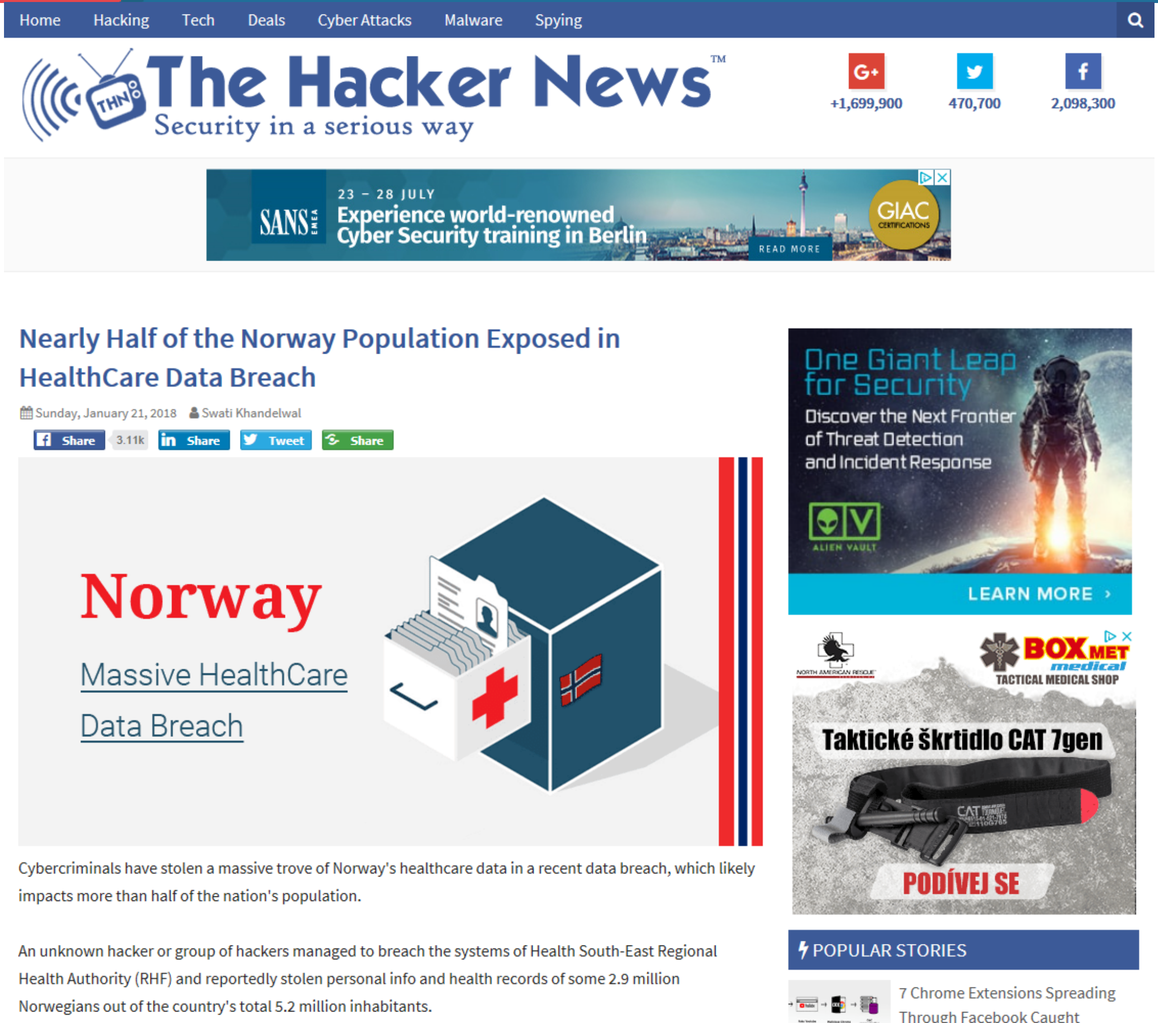
Thursday, December 14, 2017 Wang Wei

Security researchers have uncovered another nasty piece of malware designed specifically to target industrial control systems (ICS) with a potential to cause health and life-threatening accidents.

Dubbed Triton, also known as Trisis, the ICS malware has been designed to target Triconex Safety Instrumented System (SIS) controllers made by Schneider Electric—an autonomous control system that independently monitors the performance of critical systems and takes immediate actions automatically, if a dangerous state is detected.

POPULAR STORIES

7 Chrome Extensions Spreading Through Facebook Caught Stealing Passwords



Nearly Half of the Norway Population Exposed in HealthCare Data Breach

Sunday, January 21, 2018 Swati Khandelwal

Cybercriminals have stolen a massive trove of Norway's healthcare data in a recent data breach, which likely impacts more than half of the nation's population.

An unknown hacker or group of hackers managed to breach the systems of Health South-East Regional Health Authority (RHF) and reportedly stolen personal info and health records of some 2.9 million Norwegians out of the country's total 5.2 million inhabitants.

POPULAR STORIES

7 Chrome Extensions Spreading Through Facebook Caught

Utilities statistics

91% of power generation organizations have experienced a cyber attack[5]

159 vulnerabilities reported, with most of them impacting systems used in the energy sector[6]

38% of reported attacks are against power and water[6]

79 energy incidents were reported[6]

14 water incidents were reported[6]

NAKIT

Národní agentura pro komunikační a informační technologie, s. p.

Děkuji

Vladimír Rohel
Ředitel sekce Bezpečnost

+420 725 755 418

vladimir.rohel@nakit.cz