The Rising Tide
Threats to Industrial Control Systems

INFOWARCON 2018

Joe Slowik

Dragos, Inc. | October 2018

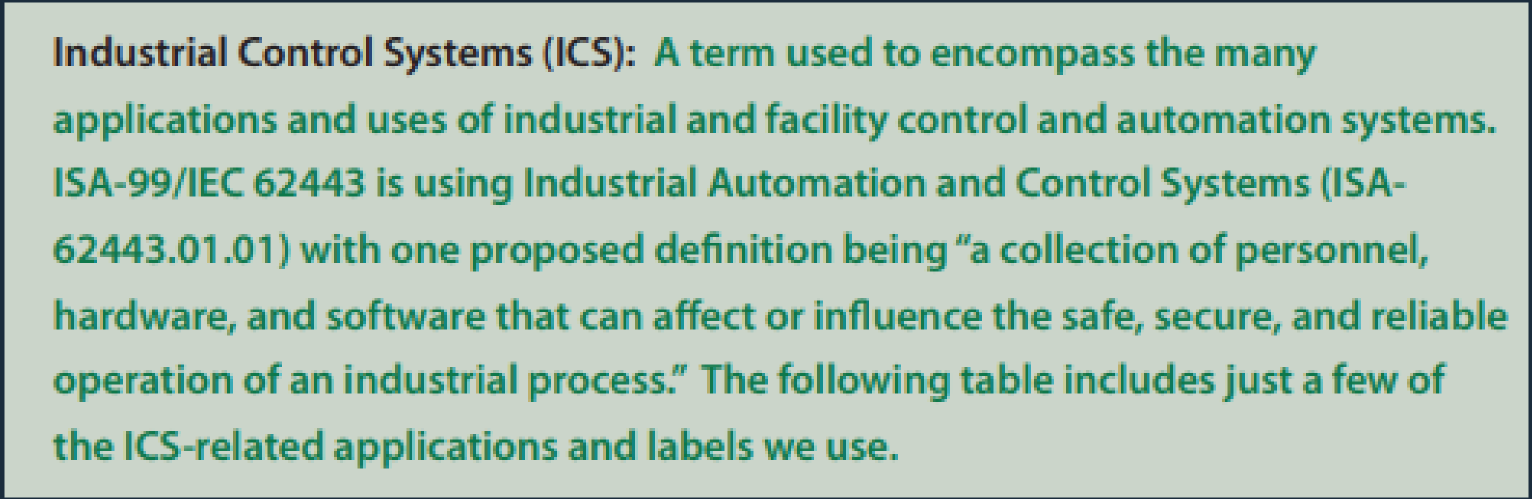
Agenda

1. ICS in Context
2. High Profile Attacks
3. Current Operations
4. Future Expectations

WHOAMI – ICS Defender!

...But on My Terms!

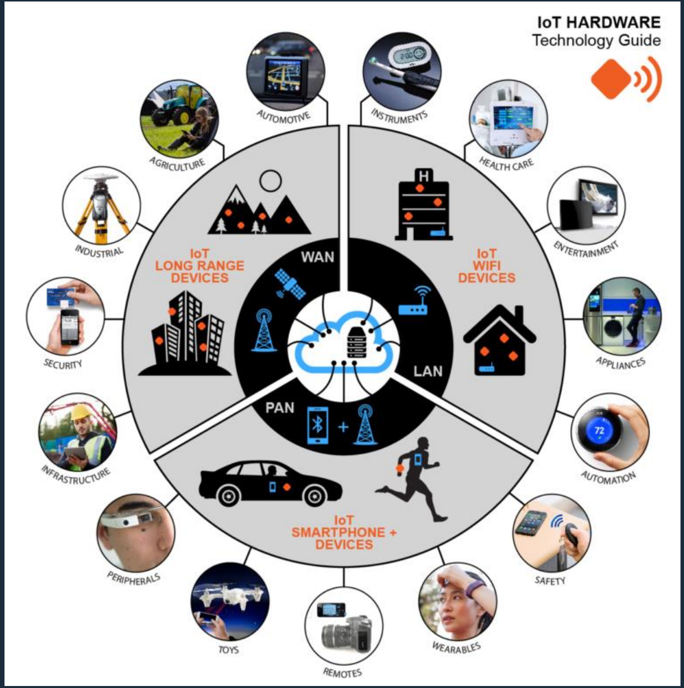
What is ICS?



Industrial Control Systems (ICS): A term used to encompass the many applications and uses of industrial and facility control and automation systems. ISA-99/IEC 62443 is using Industrial Automation and Control Systems (ISA-62443.01.01) with one proposed definition being "a collection of personnel, hardware, and software that can affect or influence the safe, secure, and reliable operation of an industrial process." The following table includes just a few of the ICS-related applications and labels we use.

https://ics.sans.org/media/An-Abbreviated-History-of-Automation-and-ICS-Cybersecurity.pdf

What ICS is NOT

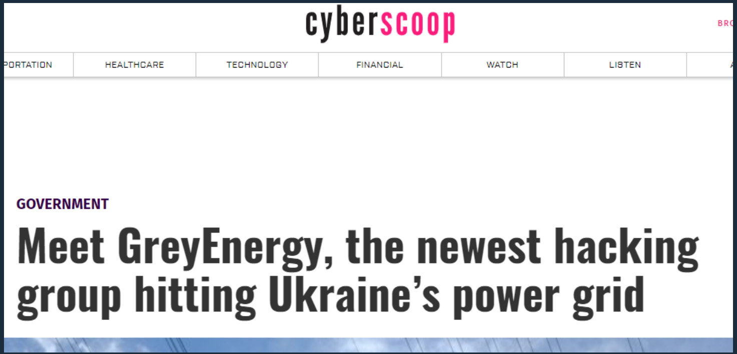


http://www.a2n.net/site/wp-content/uploads/2017/03/IoT_04.png

What is an 'Attack'?

- Focusing specifically on ICS context:
  - Event that degrades, disrupts, or destroys an ICS process
  - Preparatory actions to an attack
  - Separate from IT-specific impacts
- General reconnaissance, intelligence gathering, and IP theft are separate concerns

Not ICS Attacks

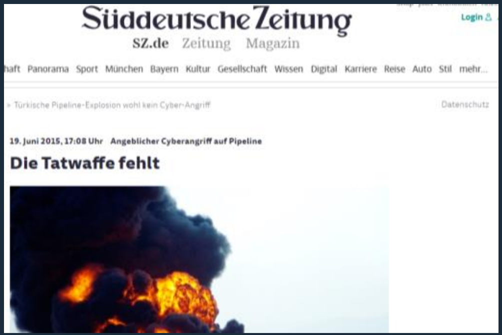


cyberscoop

PORTATION | HEALTHCARE | TECHNOLOGY | FINANCIAL | WATCH | LISTEN

GOVERNMENT

Meet GreyEnergy, the newest hacking group hitting Ukraine's power grid



Süddeutsche Zeitung

SZ.de Zeitung Magazin

Login

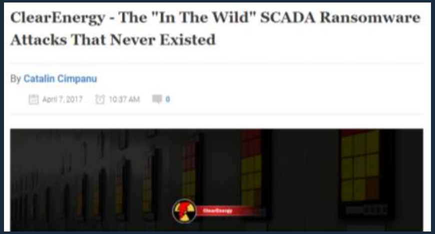
haft Panorama Sport München Bayern Kultur Gesellschaft Wissen Digital Karriere Reise Auto Stil mehr...

» Türkische Pipeline-Explosion wohl kein Cyber-Angriff

Datenschutz

19. Juni 2015, 17:08 Uhr Angeblicher Cyberangriff auf Pipeline

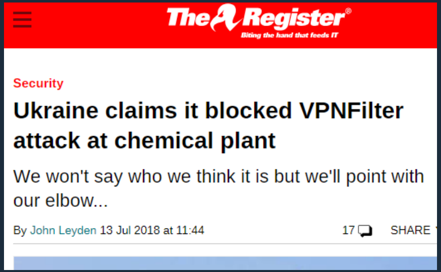
Die Tatwaffe fehlt



ClearEnergy - The "In The Wild" SCADA Ransomware Attacks That Never Existed

By Catalin Cimpanu

April 7, 2017 10:37 AM 0



The Register
Biting the hand that feeds IT

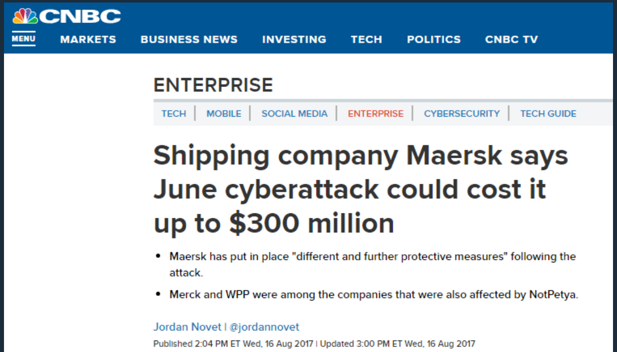
Security

Ukraine claims it blocked VPNFilter attack at chemical plant

We won't say who we think it is but we'll point with our elbow...

By John Leyden 13 Jul 2018 at 11:44

17 SHARE



CNBC

MENU MARKETS BUSINESS NEWS INVESTING TECH POLITICS CNBC TV

ENTERPRISE

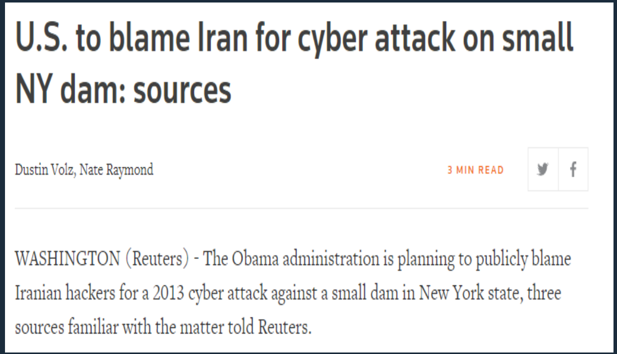
TECH | MOBILE | SOCIAL MEDIA | ENTERPRISE | CYBERSECURITY | TECH GUIDE

Shipping company Maersk says June cyberattack could cost it up to $300 million

- Maersk has put in place "different and further protective measures" following the attack.
- Merck and WPP were among the companies that were also affected by NotPetya.

Jordan Novet | @jordannovet

Published 2:04 PM ET Wed, 16 Aug 2017 | Updated 3:00 PM ET Wed, 16 Aug 2017



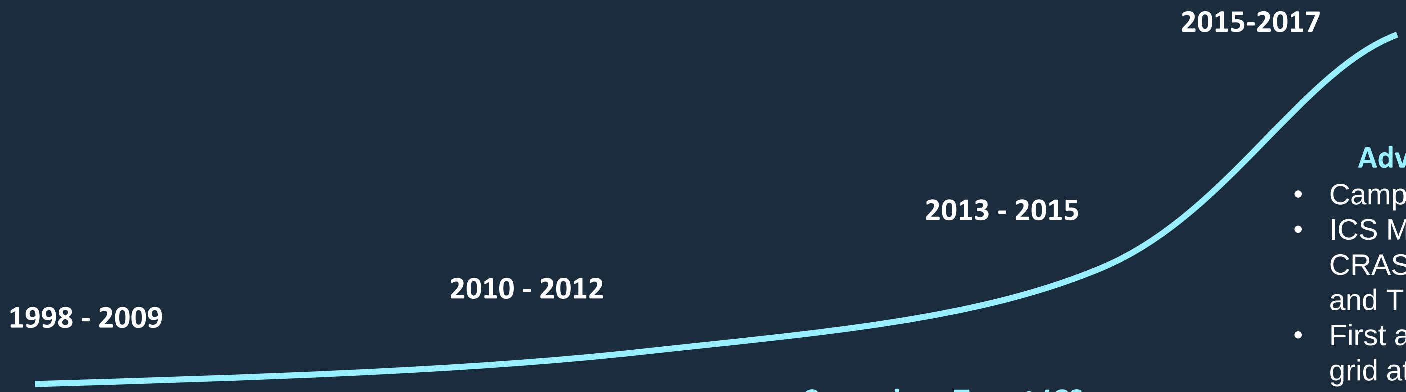
U.S. to blame Iran for cyber attack on small NY dam: sources

Dustin Volz, Nate Raymond

3 MIN READ

WASHINGTON (Reuters) - The Obama administration is planning to publicly blame Iranian hackers for a 2013 cyber attack against a small dam in New York state, three sources familiar with the matter told Reuters.

ICS Interest Over Time



Lack of Collection

- Campaigns: APT1
- ICS Malware: None

New Interest in ICS

- Campaigns: Sandworm
- ICS Malware: Stuxnet

Campaigns Target ICS

- Campaigns: Dragonfly
- ICS Malware: BlackEnergy 2 and Havex
- First attack to cause physical destruction on civilian infrastructure (German Steel)

Adversaries Disrupt ICS

- Campaigns: 10 Unique
- ICS Malware: CRASHOVERRIDE and TRISIS
- First and second ever electric grid attacks that disrupt power
- First malware to target human life

ICS Attacks & Malware in Context

ICS-Focused Malware

- STUXNET
- HAVEX
- BLACKENERGY2
- CRASHOVERRIDE
- TRISIS

ICS Disruptive Events

- 2005-2010 (?): STUXNET
- 2014: German Steel Mill Attack
- 2015: Ukraine BLACKENERGY3
- 2016: Ukraine CRASHOVERIDE
- 2017: Saudi Arabia TRISIS

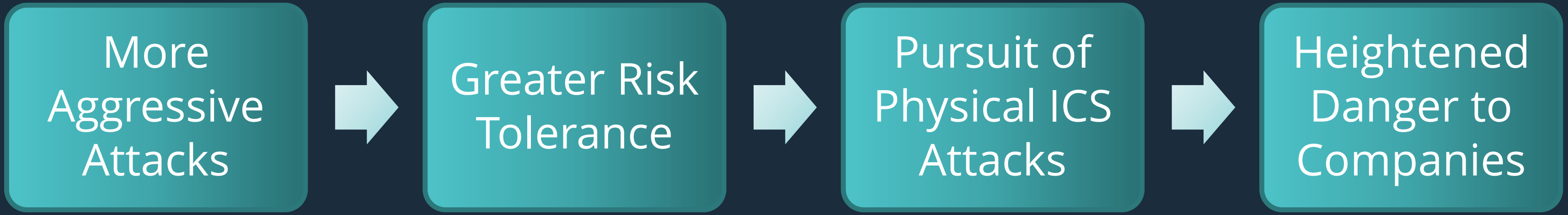
Disruptive/Destructive Malware

- STUXNET
- CRASHOVERRIDE
- TRISIS

ICS Threat Evolution

STUXNET	•Automated spread and impact •Outlier
Havex	• Automated information gathering, manual deployment • No “effects” portion
BlackEnergy2	• Modified BlackEnergy code • Used for HMI reconnaissance
BlackEnergy3	•Implants designed to facilitate access •ICS operations all manual
CRASHOVERRIDE	• Manual deployment • Effects modules codify specialist knowledge
TRISIS	• Manually deployed • ICS logic encoded in malware

Concerning Trends



More Aggressive Attacks

Greater Risk Tolerance

Pursuit of Physical ICS Attacks

Heightened Danger to Companies

Headline Attacks

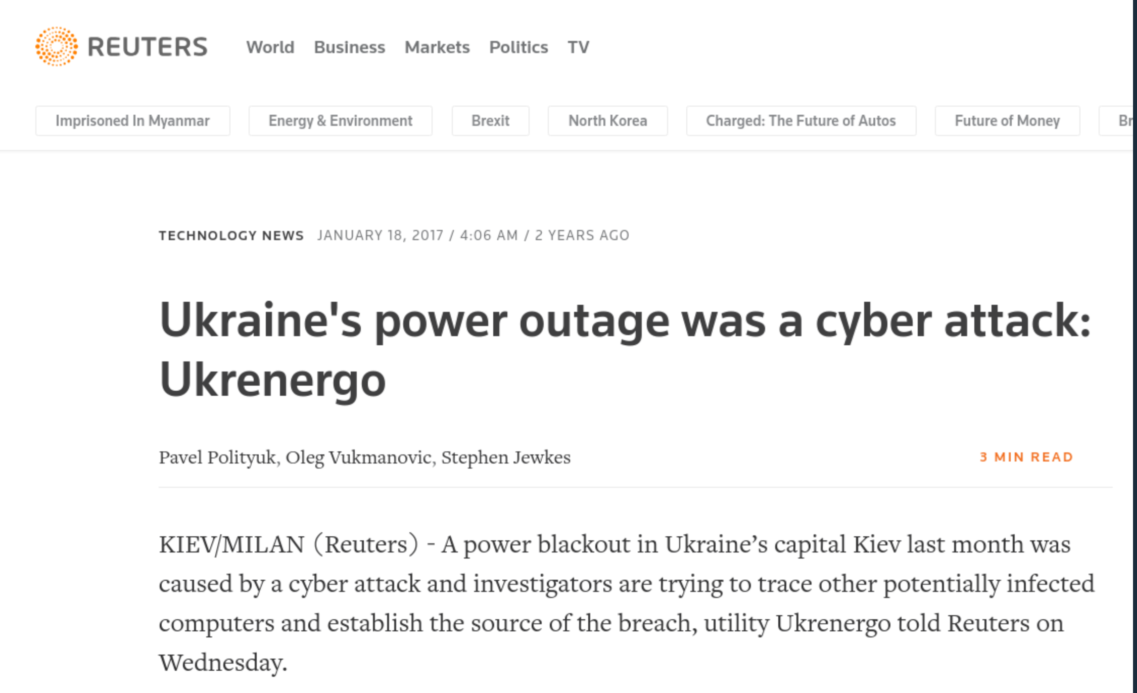
2016: CRASHOVERRIDE

- Evolution in Ukraine Attacks
- ICS Manipulation via Malware

2017: TRISIS

- First Known Case Targeting Safety Systems
- Accepts Risk to Human Life

2016 Ukraine



TECHNOLOGY NEWS JANUARY 18, 2017 / 4:06 AM / 2 YEARS AGO

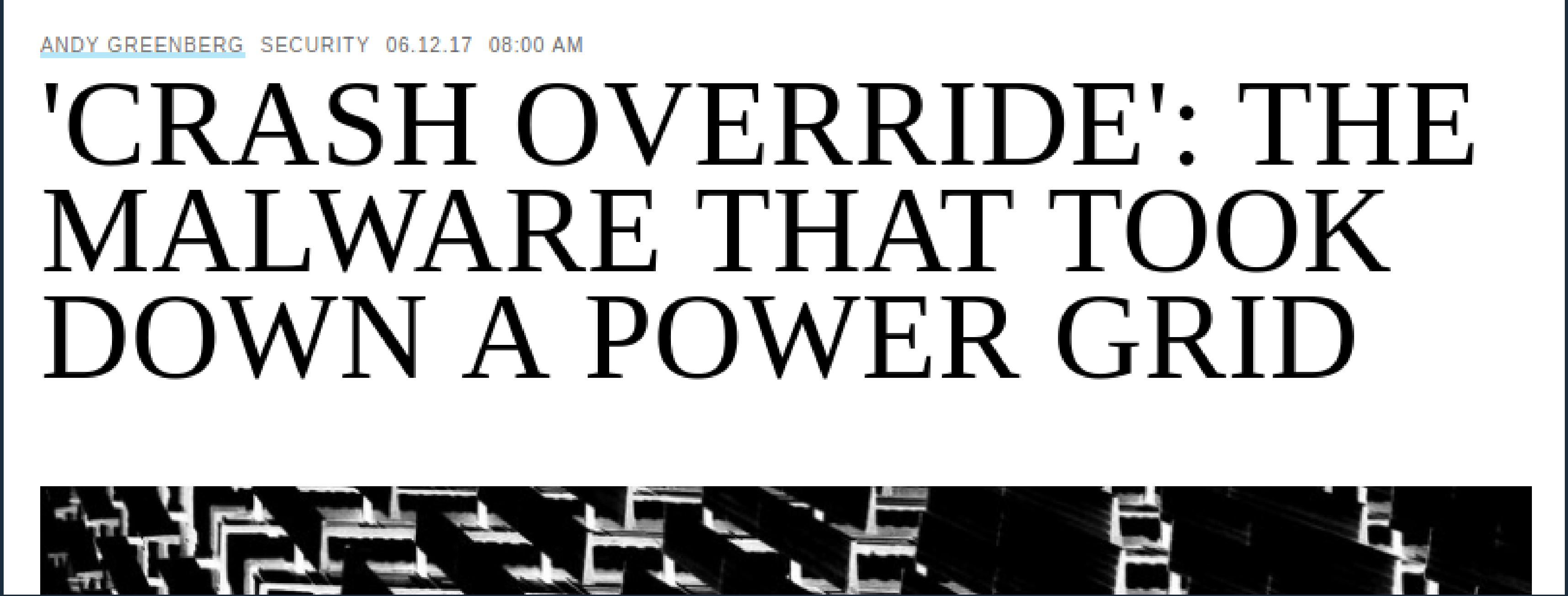
Ukraine's power outage was a cyber attack: Ukrenergo

Pavel Polityuk, Oleg Vukmanovic, Stephen Jewkes

3 MIN READ

KIEV/MILAN (Reuters) - A power blackout in Ukraine's capital Kiev last month was caused by a cyber attack and investigators are trying to trace other potentially infected computers and establish the source of the breach, utility Ukrenergo told Reuters on Wednesday.

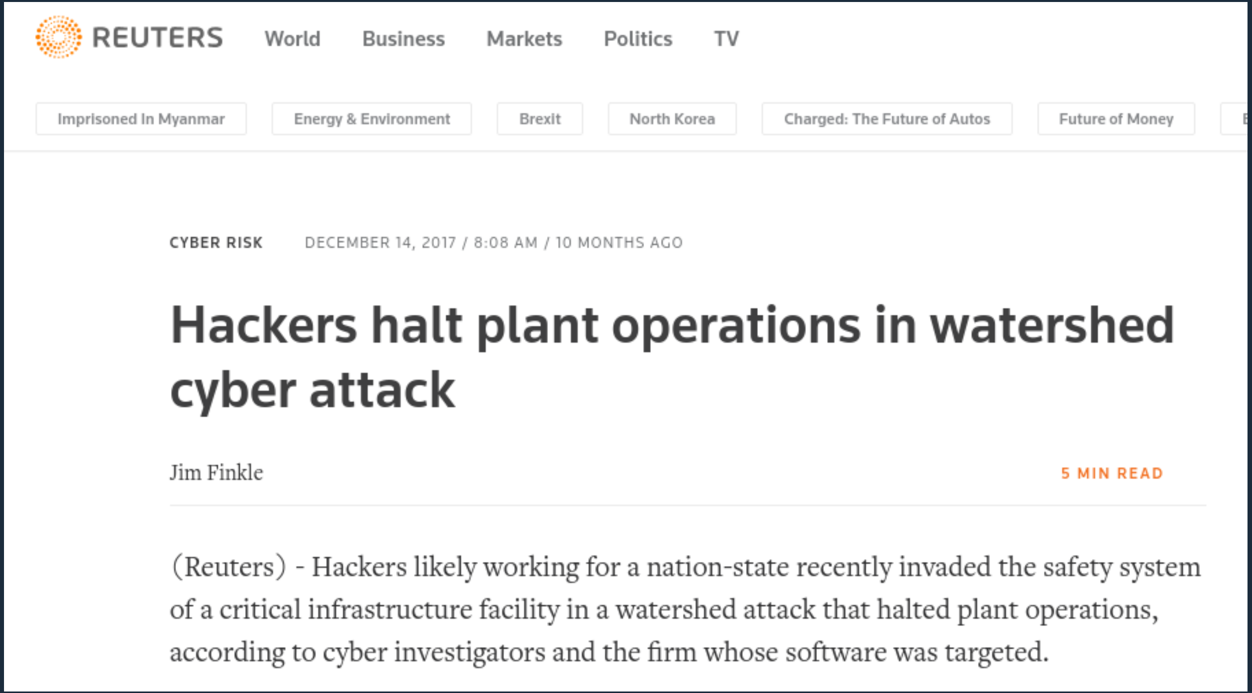
CRASHOVERRIDE Malware



ANDY GREENBERG SECURITY 06.12.17 08:00 AM

'CRASH OVERRIDE': THE MALWARE THAT TOOK DOWN A POWER GRID

2017 Saudi Arabia



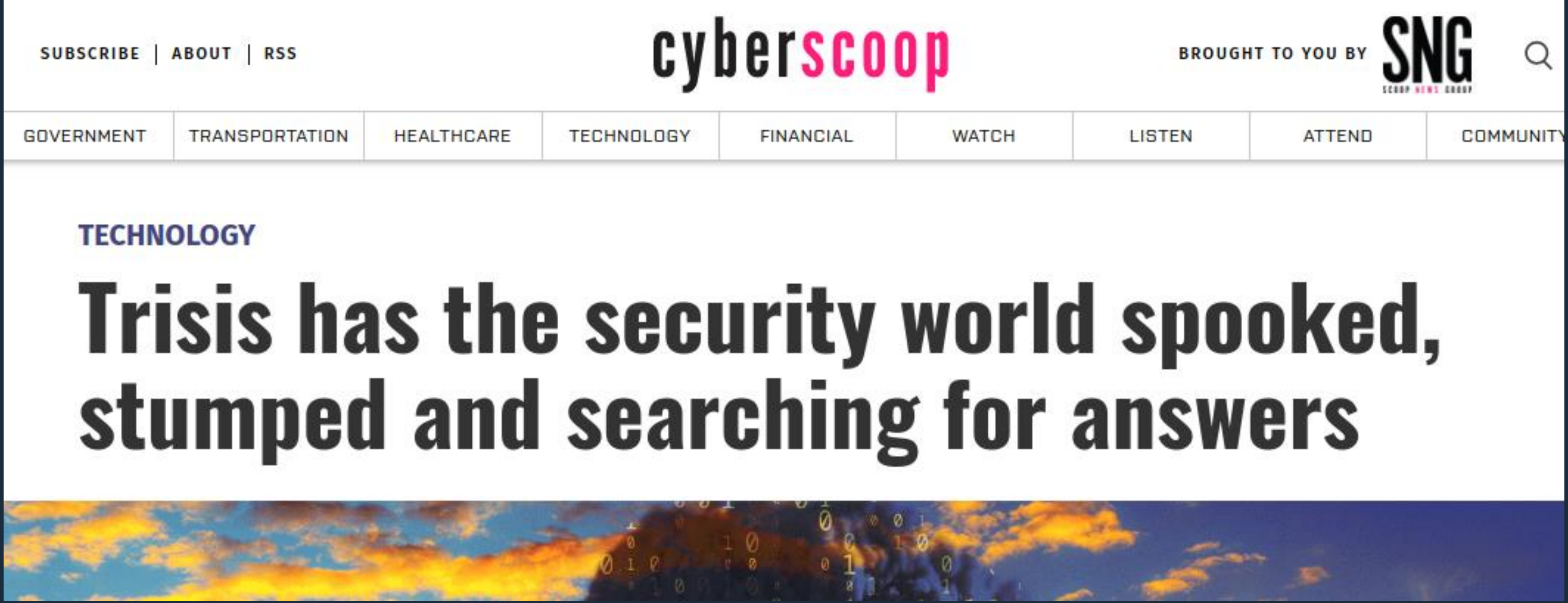
CYBER RISK DECEMBER 14, 2017 / 8:08 AM / 10 MONTHS AGO

Hackers halt plant operations in watershed cyber attack

Jim Finkle 5 MIN READ

(Reuters) - Hackers likely working for a nation-state recently invaded the safety system of a critical infrastructure facility in a watershed attack that halted plant operations, according to cyber investigators and the firm whose software was targeted.

TRISIS Rootkit



TECHNOLOGY

Trisis has the security world spooked, stumped and searching for answers

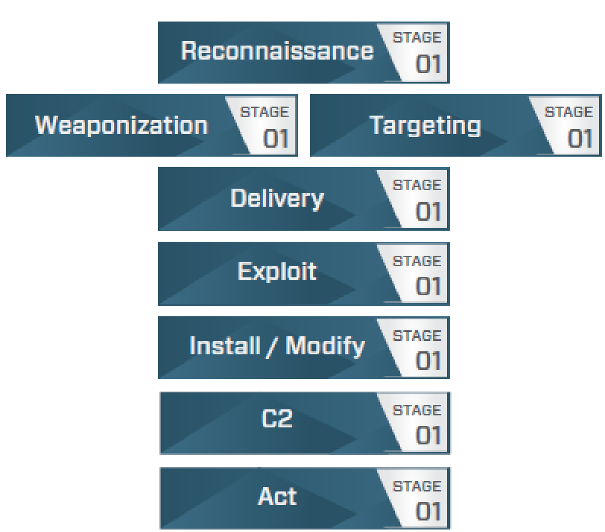
CONTEXT ATTACKS OPERATIONS FUTURE

Beyond Disruptive & Destructive

- ICS Operations are not “Bolts from the Blue”
- Attacks Require Capability Development
- Delivery Requires Access
- Execution Demands Control

Orienting to Kill Chain

PHASE 1 - IT



Reconnaissance STAGE 01

Weaponization STAGE 01

Targeting STAGE 01

Delivery STAGE 01

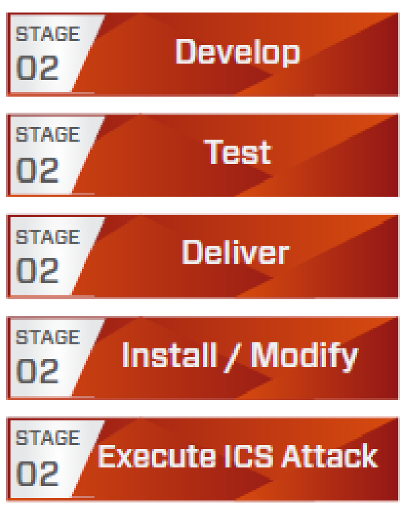
Exploit STAGE 01

Install / Modify STAGE 01

C2 STAGE 01

Act STAGE 01

PHASE 2 - ICS



STAGE 02 Develop

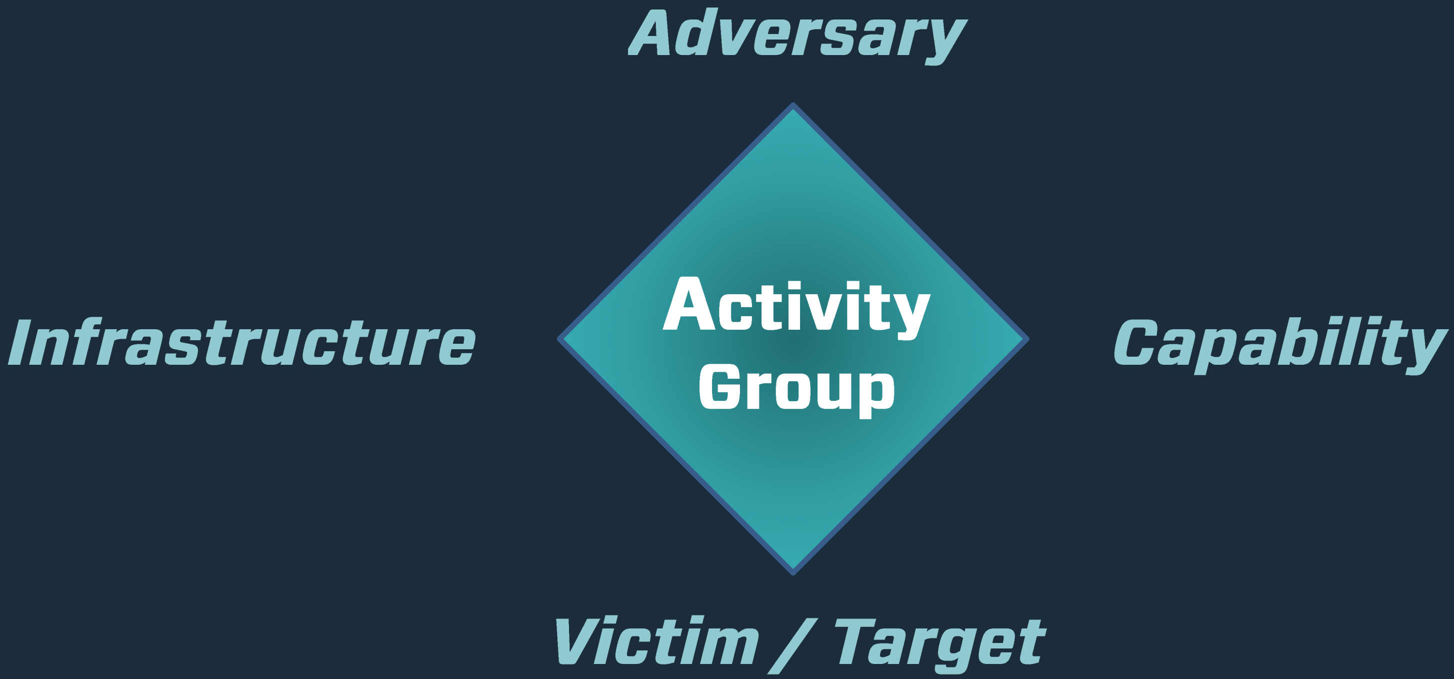
STAGE 02 Test

STAGE 02 Deliver

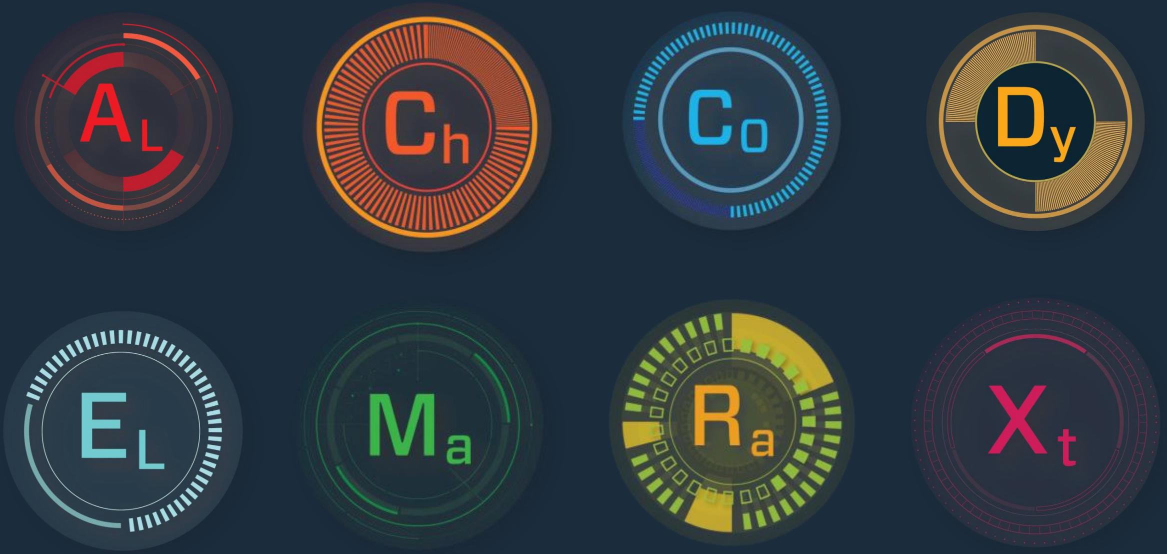
STAGE 02 Install / Modify

STAGE 02 Execute ICS Attack

Tracking Adversaries by Behavior



ICS Targeting Activity Groups



Initial Access & Recon

Initial Access & Recon

- Stage 1 Kill Chain activity
- Pre-requisite for Stage 2 operations
- Focus on:
  - Identifying access to ICS environment
  - Determining target technologies and attack surface

CHRYSENE Oil & Gas Targeting

SHAMOON Relationship

- Code Overlap with Shamoon Activity
- Relationship with Disruptive Attacks

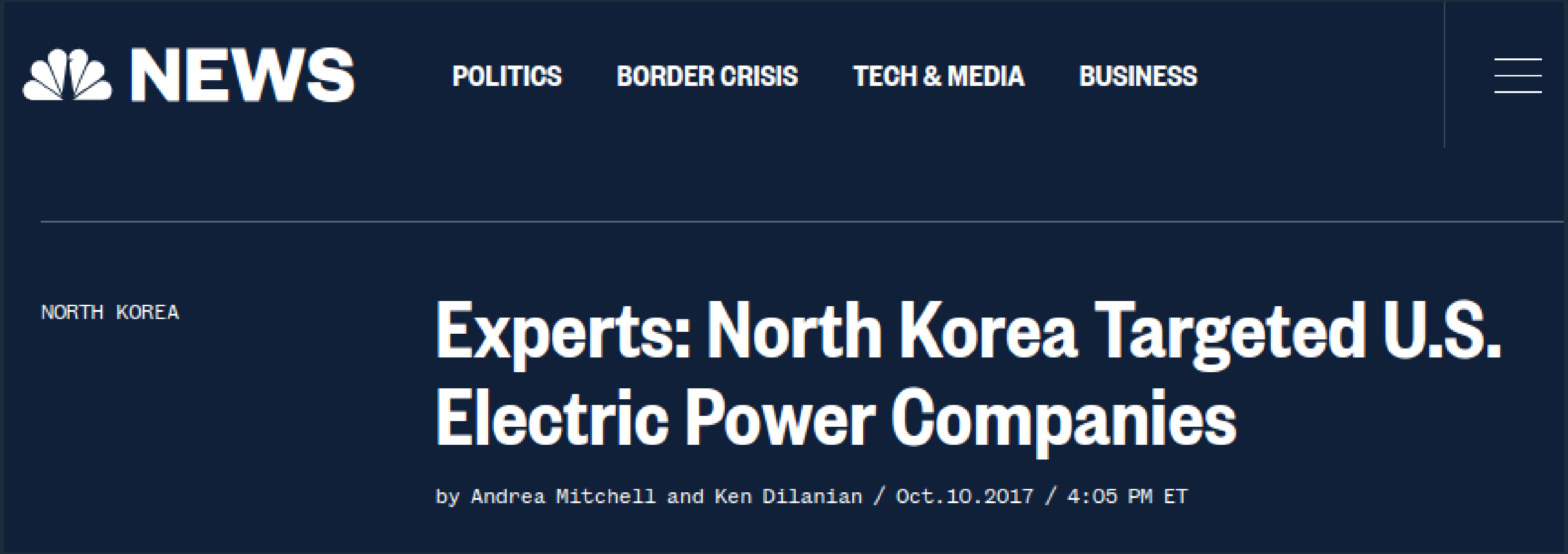
Targeting Profile

- Largely Focused on Middle East
- Indications of Targeting Expansion to North America

Goals & Intentions

- Information Gathering and Establishing Access
- Can be Used for Future Disruptive Attacks

COVELLITE US Power Intrusions

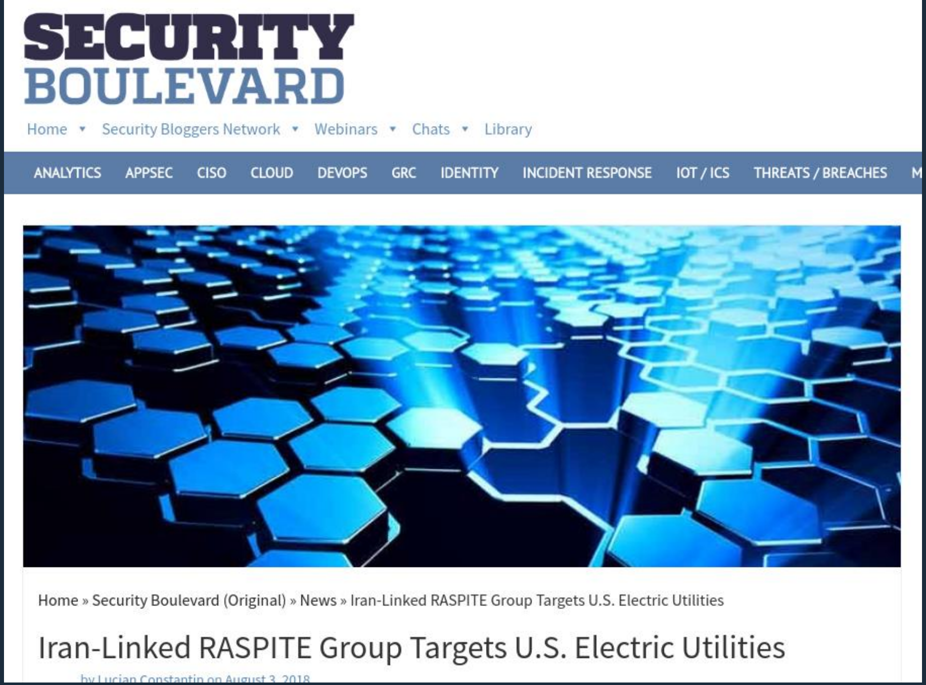


NORTH KOREA

Experts: North Korea Targeted U.S. Electric Power Companies

by Andrea Mitchell and Ken Dilanian / Oct.10.2017 / 4:05 PM ET

RASPITE Grid Investigation



Home » Security Boulevard (Original) » News » Iran-Linked RASPITE Group Targets U.S. Electric Utilities

Iran-Linked RASPITE Group Targets U.S. Electric Utilities

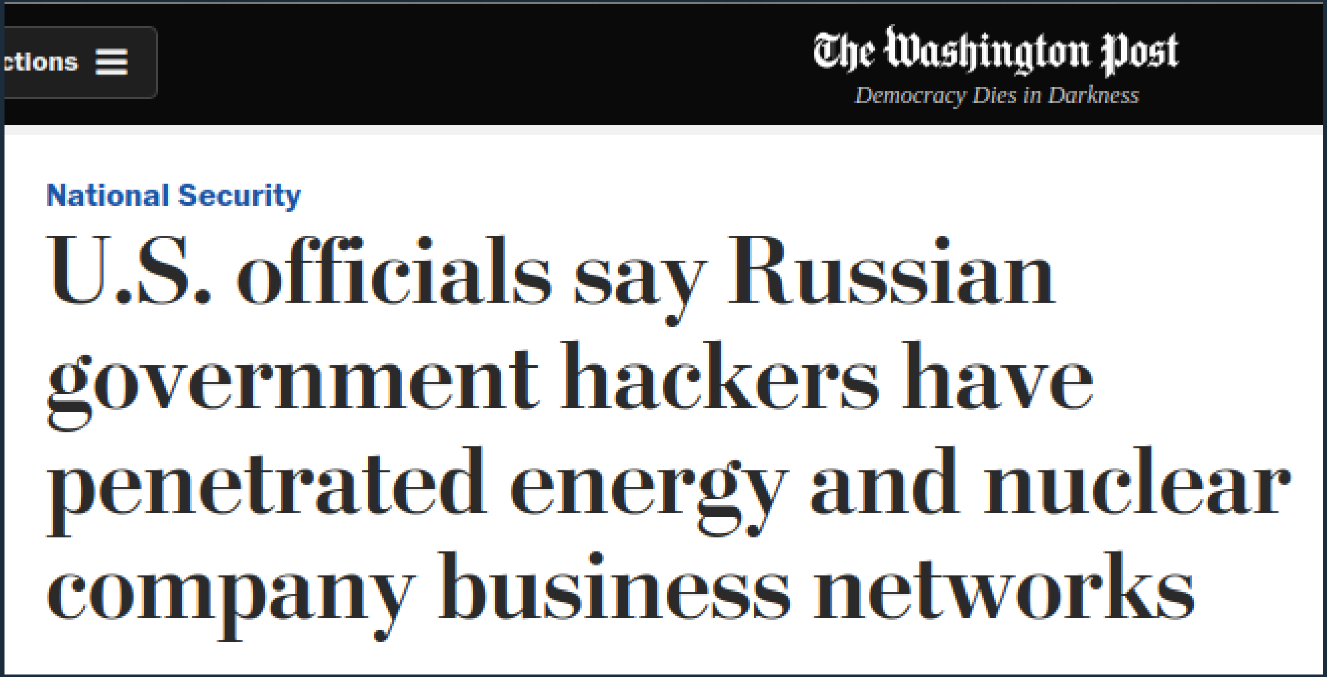
by Lucian Constantin on August 3, 2018

ICS Survey and Development

ICS Survey and Development

- Initial Stage 2 Kill Chain activity
- ICS environment accessed
- Focus on:
    - Enumerating ICS environment
    - Prerequisite to attack development and deployment

US & UK Electric Grid Probing



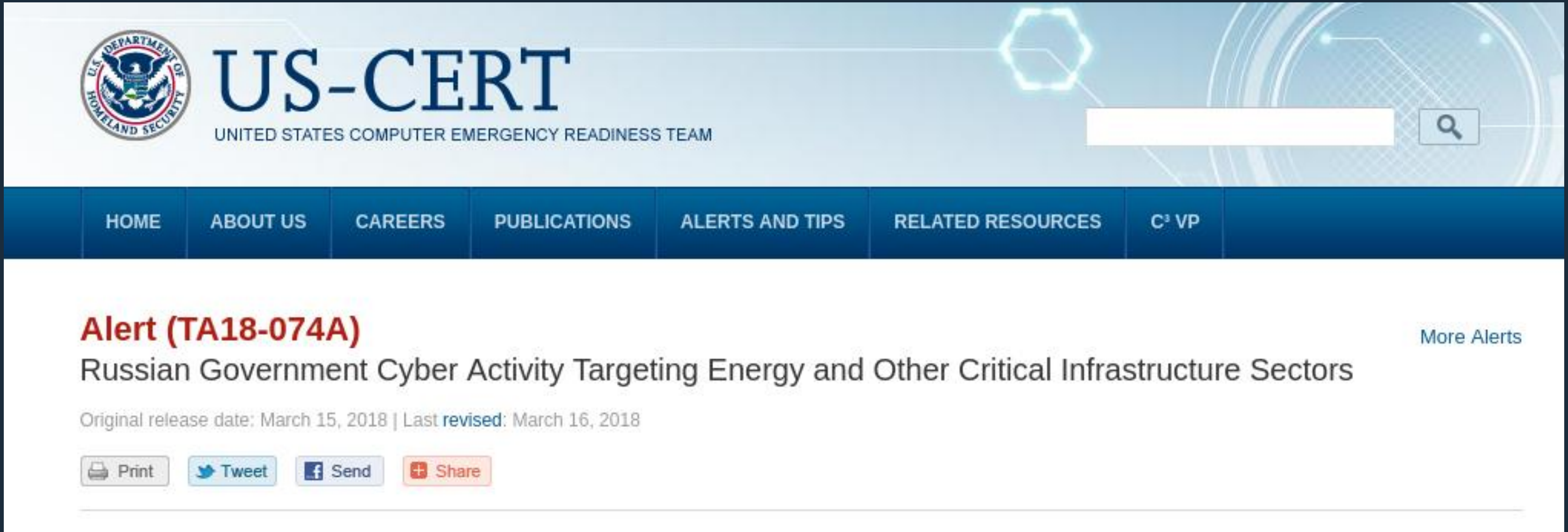
The Washington Post

Democracy Dies in Darkness

National Security

U.S. officials say Russian government hackers have penetrated energy and nuclear company business networks

US & UK Electric Grid Probing

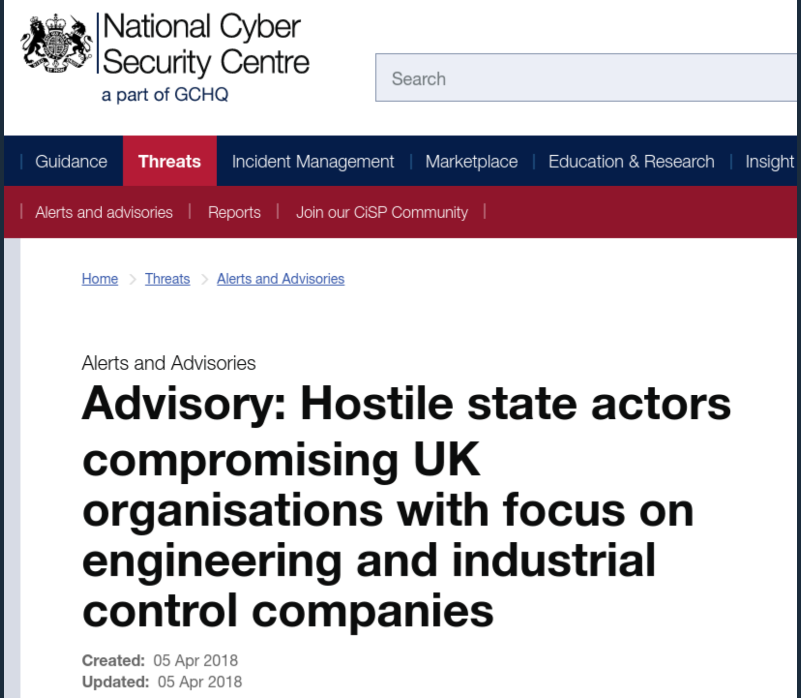


Alert (TA18-074A)

Russian Government Cyber Activity Targeting Energy and Other Critical Infrastructure Sectors

Original release date: March 15, 2018 | Last revised: March 16, 2018

US & UK Electric Grid Probing



Alerts and Advisories

Advisory: Hostile state actors compromising UK organisations with focus on engineering and industrial control companies

Created: 05 Apr 2018
Updated: 05 Apr 2018

Sustained Campaigns

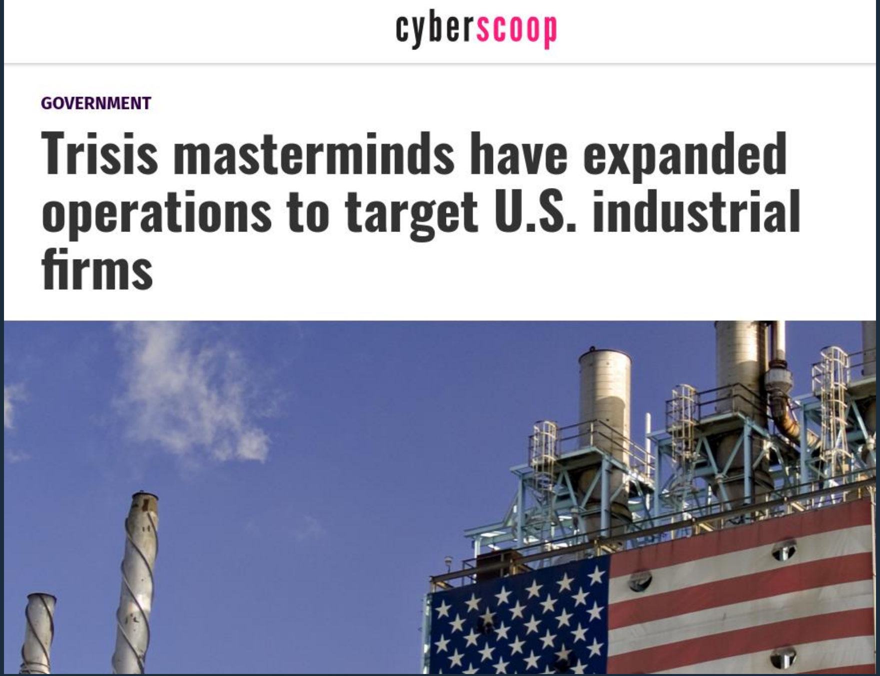
	DRAGONFLY	DYMALLOY	ALLANITE
Active	2013-2014	Late 2015 – ?	Mid 2017 - ?
Target Geography	Europe North America	Turkey Europe North America	USA UK
Infection Vector	Phishing w/PDF, Watering Hole, Trojanized Softare	Phishing w/Doc	Phishing w/Doc, Watering Hole
Persistence Mechanism	HERIPLOR, KARAGANY Malware	Various Malware and Backdoors	Create User Accounts, Credential Harvesting
ICS Impact	OPC-focused Malware Family	Survey and Screenshots via Malware	Survey and Screenshots vis System Tools

ICS Attack Capable

ICS Attack Capable

- Final Stage 2 Kill Chain ICS impact
- Environment is reasonably known
- Attack developed and in place
- Execution of disruptive/destructive attack

XENOTIME Attack Development

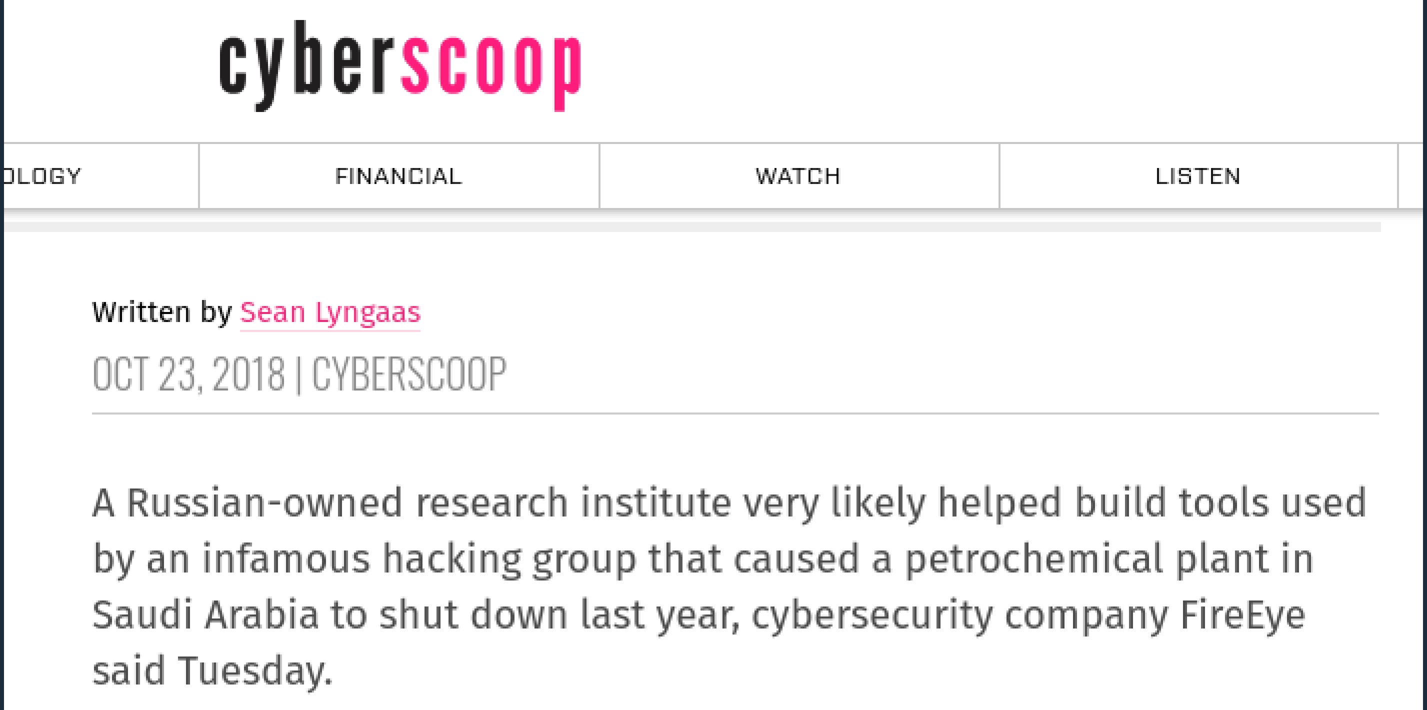


cyberscoop

GOVERNMENT

Trisis masterminds have expanded operations to target U.S. industrial firms

XENOTIME Attribution?



Written by Sean Lyngaas

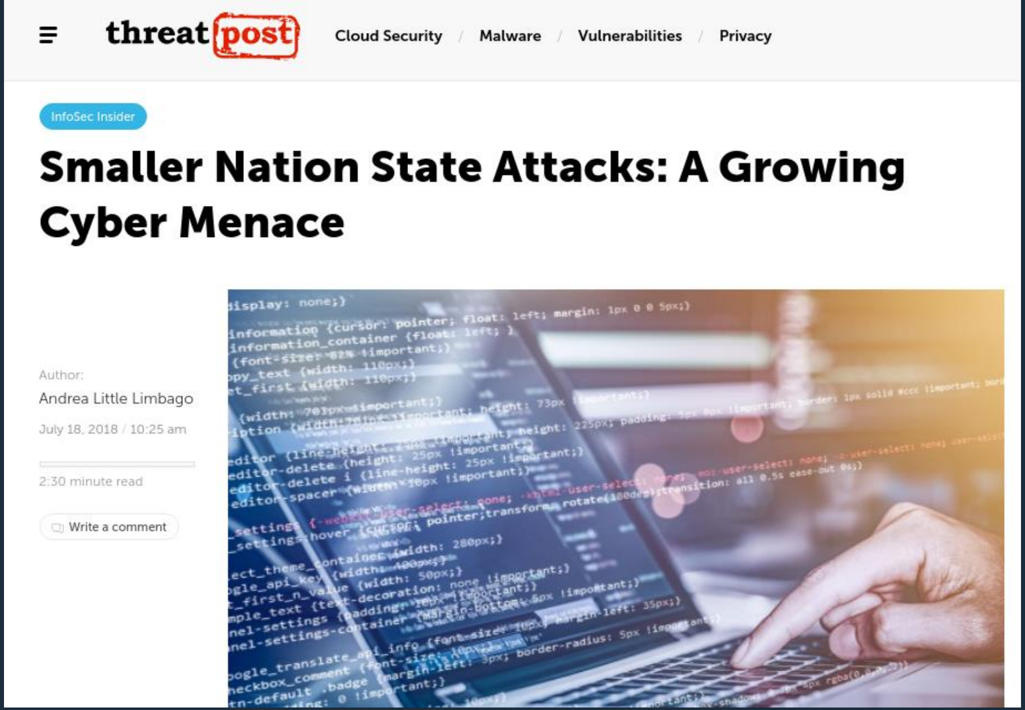
OCT 23, 2018 | CYBERSCOOP

A Russian-owned research institute very likely helped build tools used by an infamous hacking group that caused a petrochemical plant in Saudi Arabia to shut down last year, cybersecurity company FireEye said Tuesday.

Where Do We Go from Here?

http://abcnews.go.com/images/US/abc_texas_chemical_fire_ll_111003_wblog.jpg

Expect More Adversaries



threatpost

Cloud Security / Malware / Vulnerabilities / Privacy

InfoSec Insider

Smaller Nation State Attacks: A Growing Cyber Menace

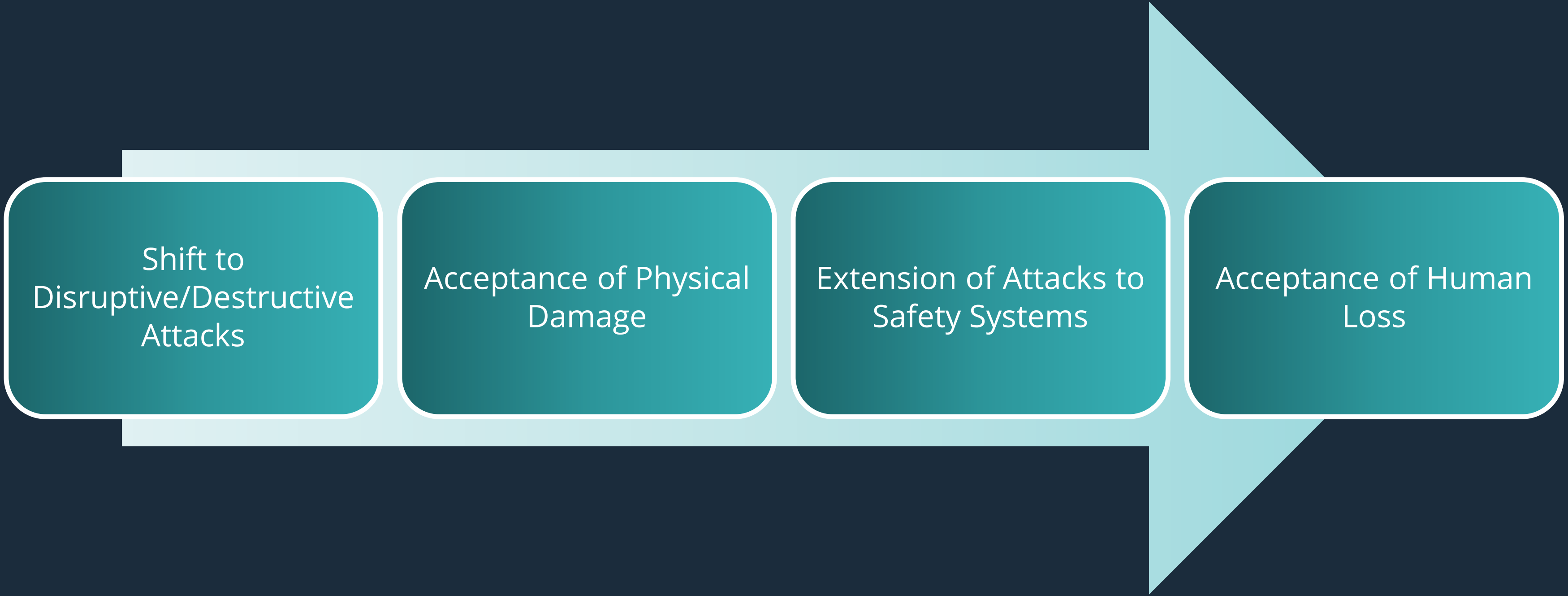
Author:
Andrea Little Limbago

July 18, 2018 / 10:25 am

2:30 minute read

Write a comment

Greater Adversary Risk Tolerance



Shift to Disruptive/Destructive Attacks

Acceptance of Physical Damage

Extension of Attacks to Safety Systems

Acceptance of Human Loss

ICS Attacks as Strategic Messaging

https://alochonaa.files.wordpress.com/2014/03/ukraine.png

http://rawabetcenter.com/en/wp-content/uploads/2016/07/IRAN-VS-KSA-768x506.jpg

Concerns in ICS Targeting

- Potential for Errors and Mistakes
- Miscalculation and Control of Events
- Indeterminate Response and Proportionality
- Physical Disruption Equating to Physical Attack

Expectations

- More Attacks to Come
- Greater Likelihood of Physical Destruction
- Increased Threat Adversary Activity
- Possibility Initial Access and Info Gathering Results in Accident

Further Reading

- An Abbreviated History of Automation & Industrial Controls Cyber Security – SANS Institute
- Analysis of the Cyber Attack on the Ukrainian Power Grid – SANS Institute
- Russian Government Cyber Activity Targeting Energy and Other Critical Infrastructure Sectors – US-CERT
- Dragonfly: Cyberespionage Attacks Against Energy Suppliers – Symantec
- Dragonfly: Western Energy Sector Targeted by Sophisticated Attack Group – Symantec
- CRASHOVERRIDE: Analysis of the Threat to Electric Grid Operations – Dragos
- TRISIS Malware: Analysis of Safety System Targeted Malware – Dragos
- Anatomy of an Attack: Detecting and Defeating CRASHOVERRIDE – Dragos
- Industrial Control System Threats Year in Review, 2017 – Dragos
- Attackers Deploy New ICS Attack Framework “TRITON” – FireEye

Questions?

@jfslowik
jslowik@dragos.com
dragos.com / pylos.co

DRAGOS