EMERGING THREATS TO THE GRID

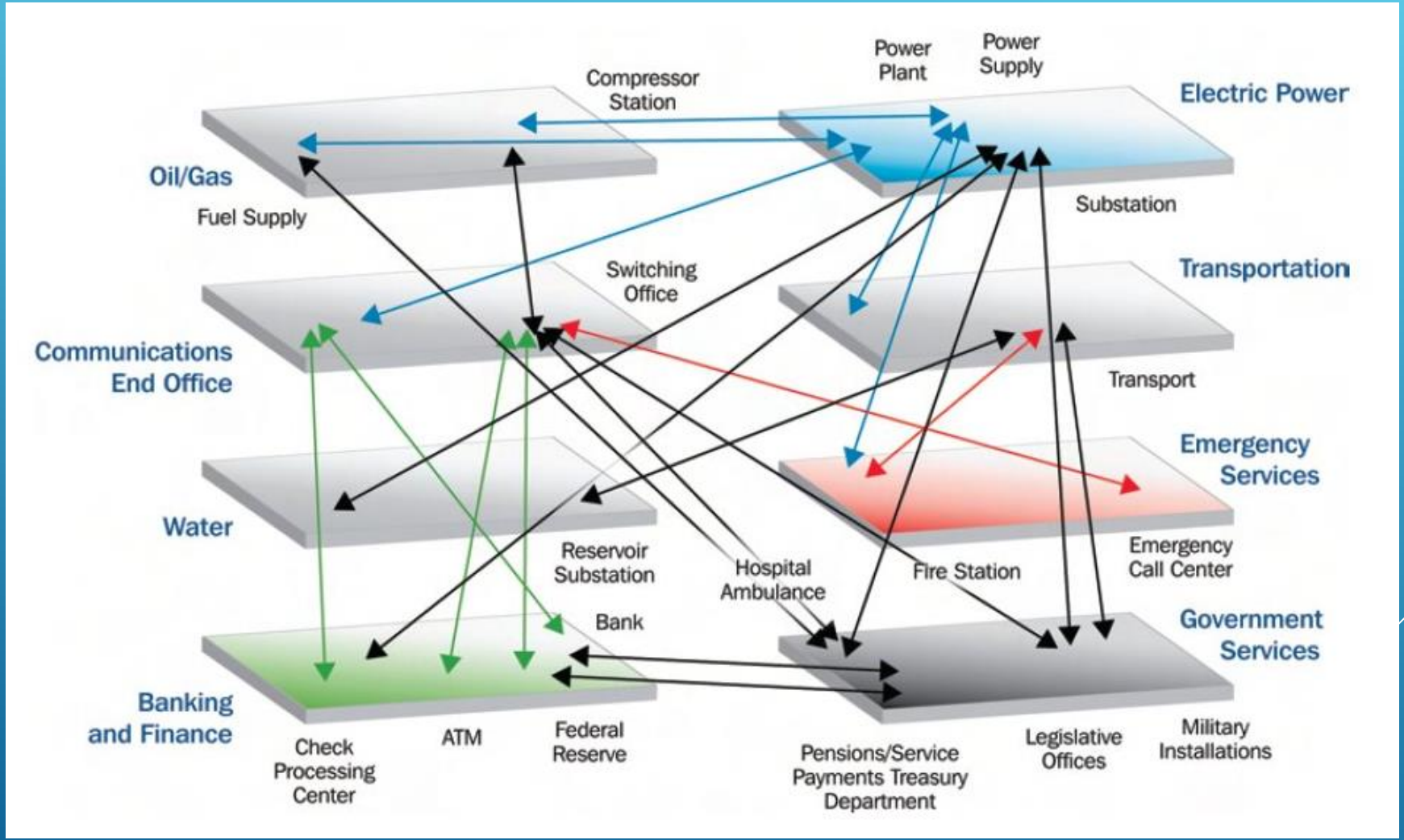
Marcus Sachs, Research Director, McCrary Institute, Auburn University

NAEMA Virtual Presentation

March 10, 2021

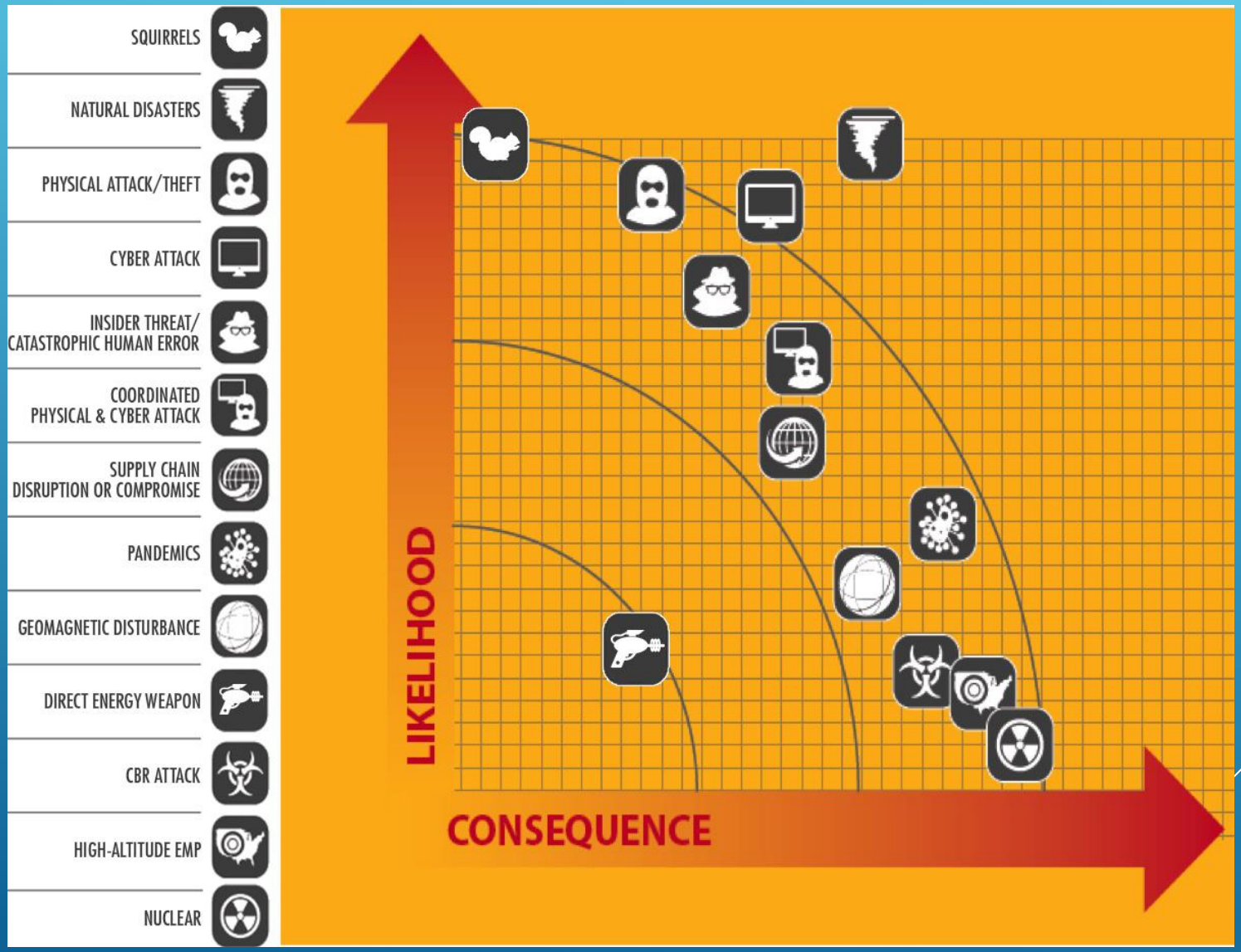

Government Operations
Gas & Oil Storage and Delivery
Emergency Services
Water Supply Systems
Critical Infrastructures
Telecommunications
Banking & Finance
Electrical Energy
Transportation

CRITICAL INFRASTRUCTURE DEPENDENCIES



HIDDEN INFRASTRUCTURE DEPENDENCIES

ELECTRICITY THREAT LANDSCAPE



MOST COMMON THREAT AGENTS

Agent	Success
Squirrel	1252
Bird	639
Snake	117
Raccoon	115
Rat	53
Cat	28
Marten	25
Jellyfish	13
Monkey	12
Human/Cyber	3

http://cybersquirrel1.com/

"I don't think paralysis [of the electrical grid] is more likely by cyberattack than by natural disaster. And frankly the number-one threat experienced to date by the US electrical grid is squirrels." – John C. Inglis, Former Deputy Director, National Security Agency
July 9, 2015

NATURAL THREATS – LIGHTNING

NATURAL THREATS – FLOODING

PHYSICS THREATS – METAL FATIGUE

OPERATIONAL THREATS – FIRE

MAN-MADE THREATS – LOOSE NAVY BLIMP

HUMAN THREATS

TARGETED THREATS – PIPE BOMBS

TARGETED THREATS – IEDS

TARGETED THREATS – GUN SHOTS

TARGETED THREATS – VANDALISM

CRIMINAL THREATS – COPPER THEFT

CY“BEAR” THREATS

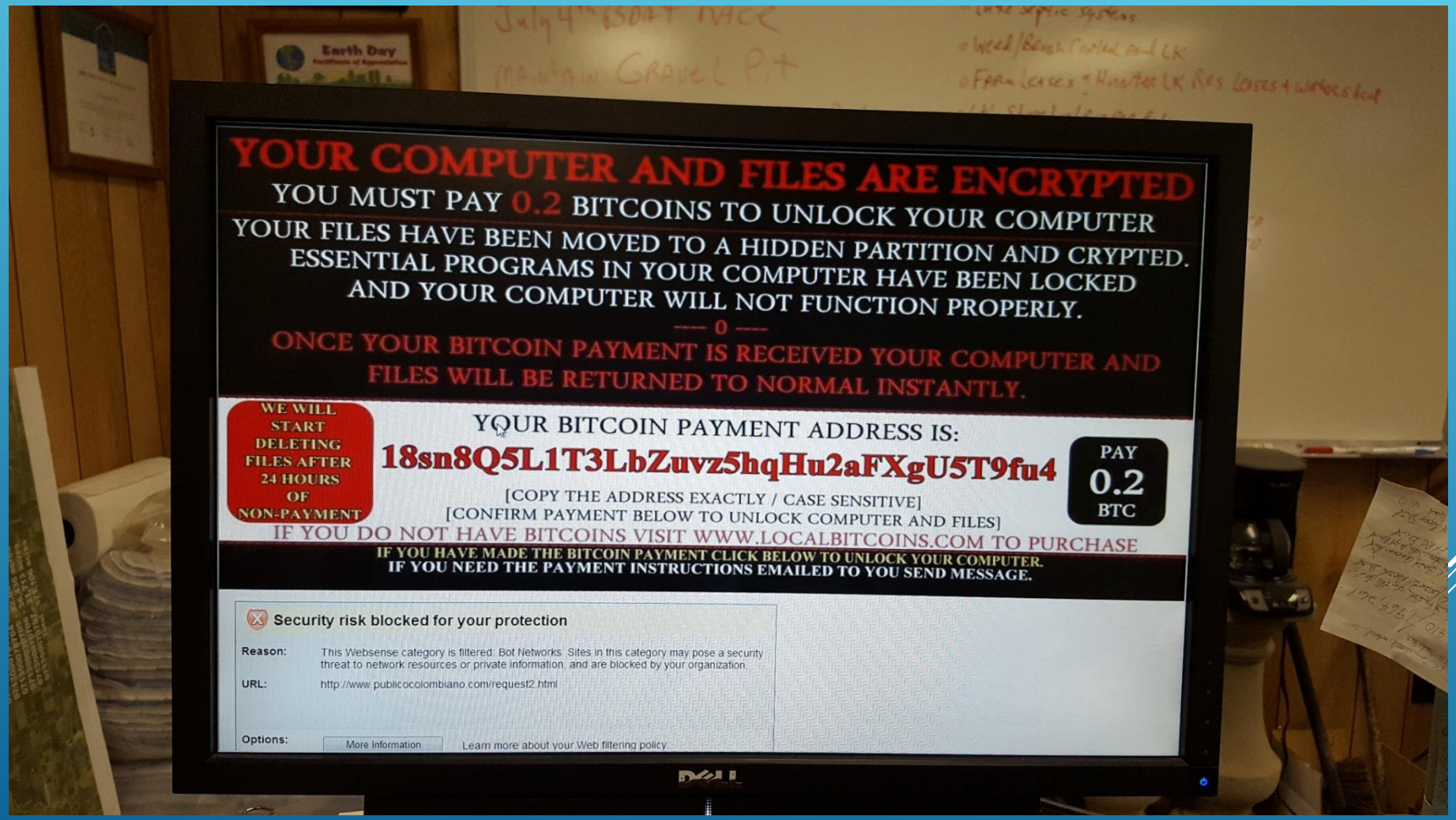
INCREASING LEVELS OF CYBER THREATS

- Reputation damage
  - Website defacement
  - Phishing attacks against customers
- Theft of intellectual property
  - Employee or customer financial data (credit cards, etc.)
  - Corporate intellectual property (plans, financials, blueprints, etc.)
- Ransomware
  - Encrypts sensitive data then demands payment for decryption
  - Might install persistent access for later use

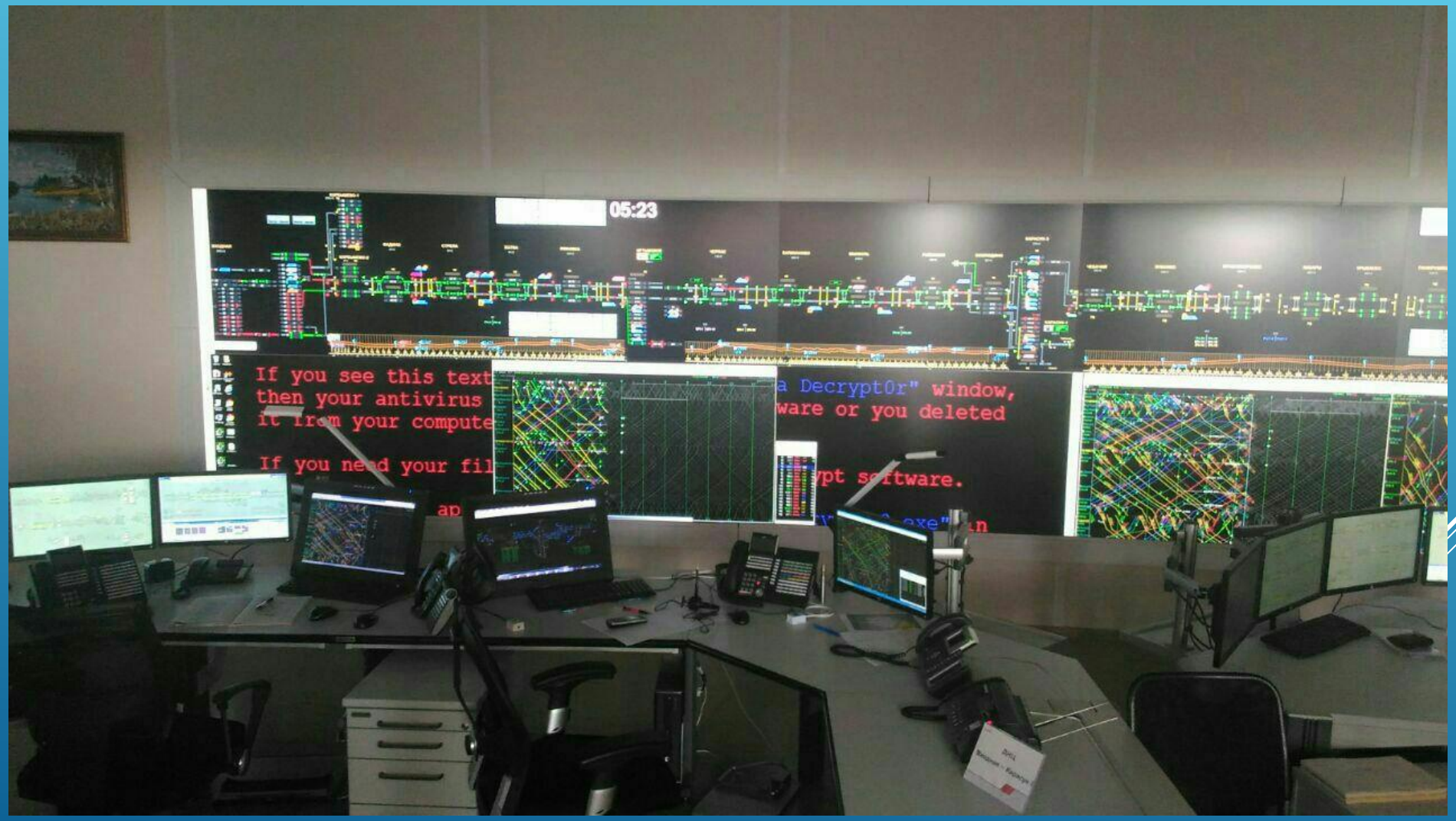
DANGEROUS LEVELS OF CYBER THREATS

- Direct manipulation of control systems
  - Jumps the boundary between enterprise (IT) systems and plant (OT) systems
  - Disruptive, not destructive
- Mechanical or logical damage
  - Destructive to system components
  - "Bricking" a computer or protective relay
  - Aurora-style damage to generators via remote manipulation of breakers

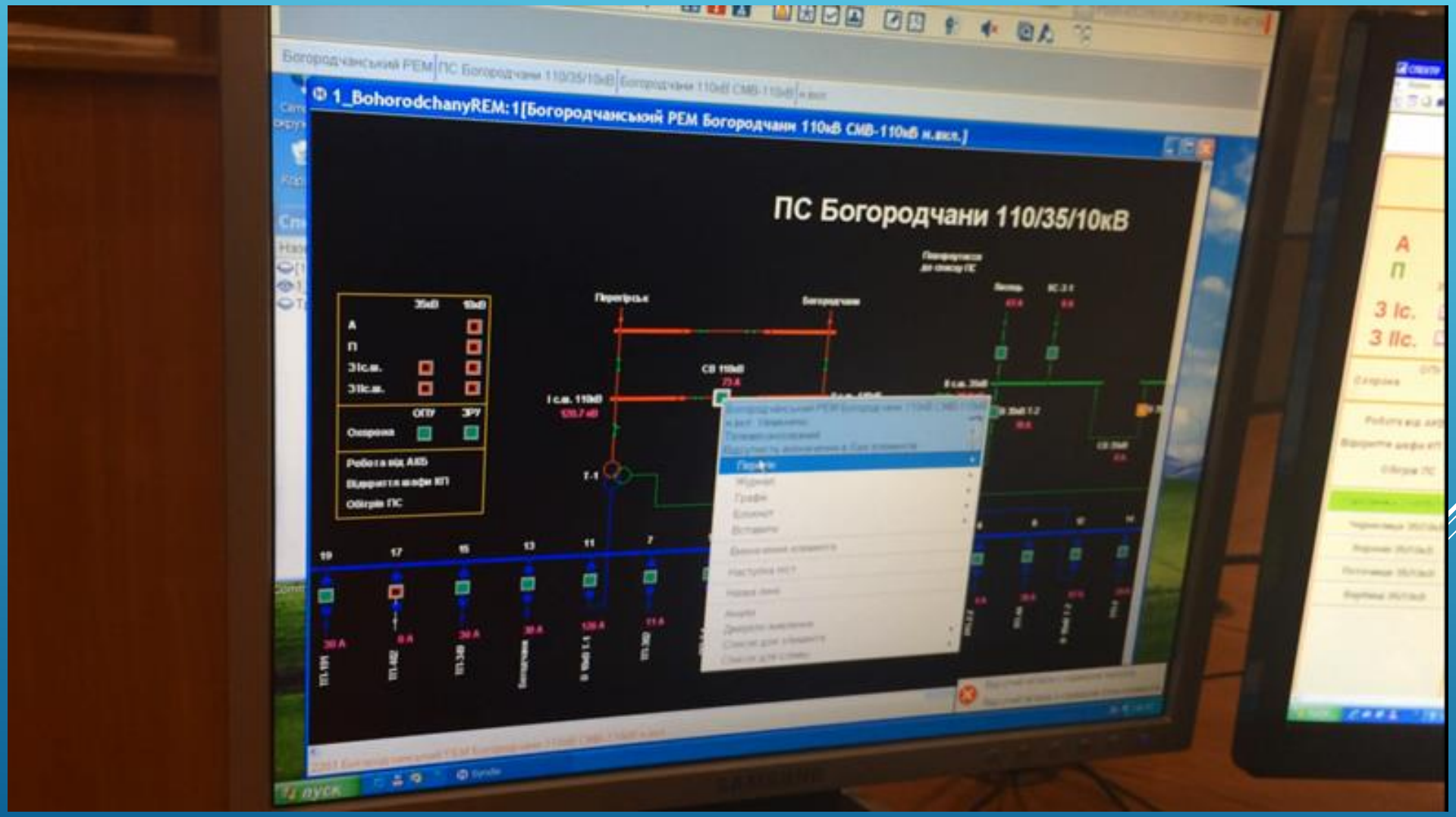
MOST LIKELY CYBER THREAT TO ELECTRIC UTILITIES



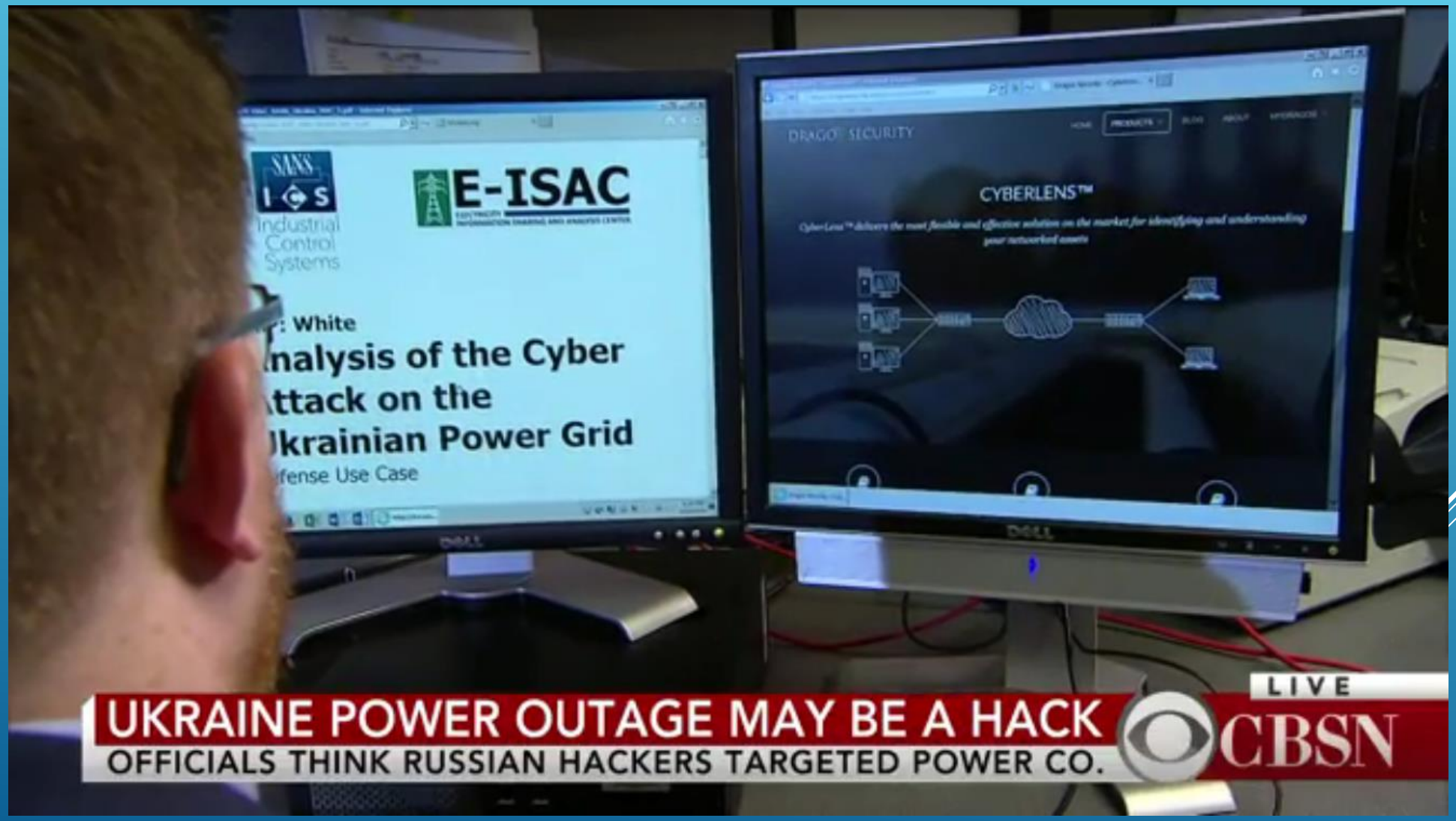
RANSOMWARE IN A CONTROL CENTER



LEAST COMMON CYBER THREAT

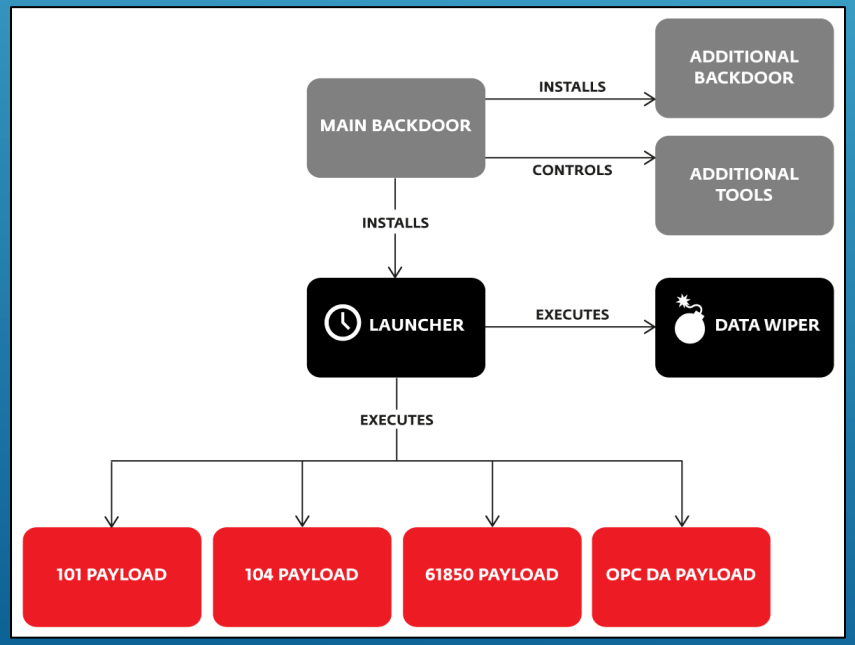


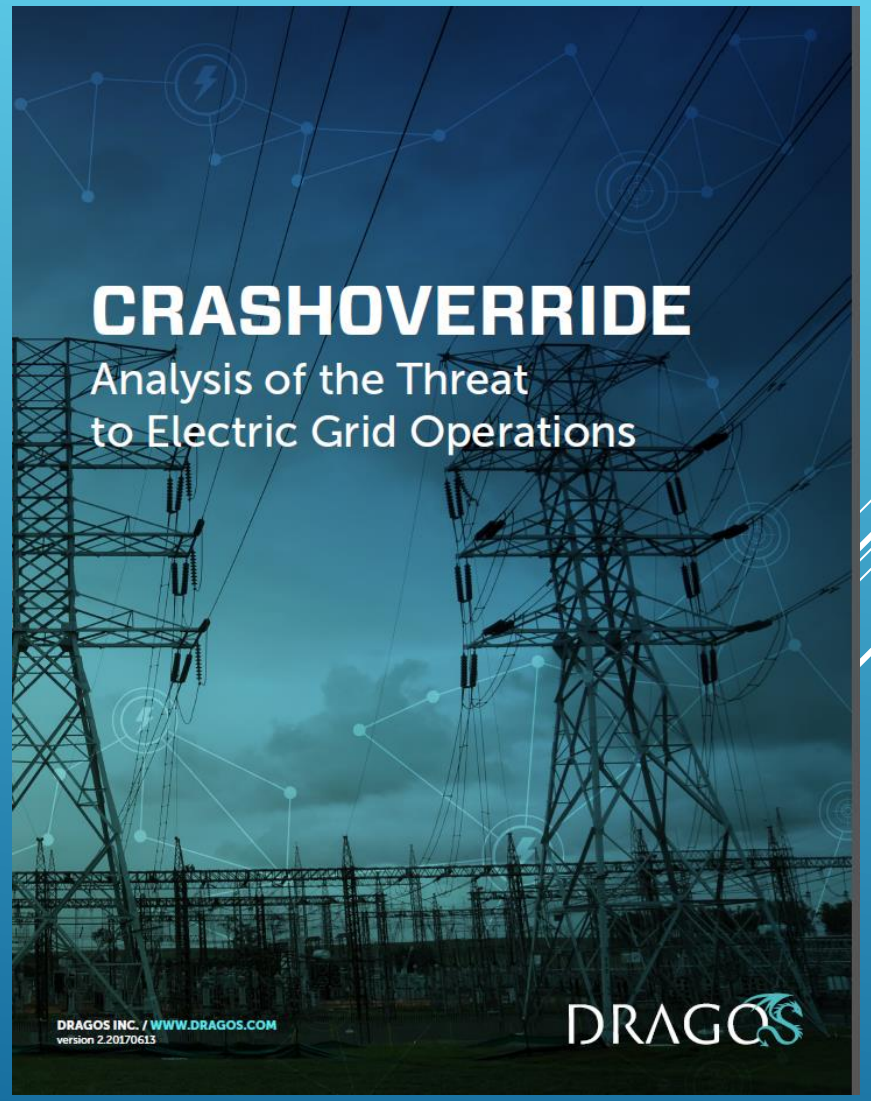
E-ISAC ANALYSIS OF THE UKRAINE ATTACKS



INDUSTROYER/CRASHOVERRIDE

- Investigation by two private sector research companies
  - Reports released on June 12, 2017
- Reportedly used in Ukraine





HACKING IS EASY – SHODAN.IO

File Edit View History Bookmarks Tools Help

Shodan

https://www.shodan.io/?language=None

Search

Shodan Developers Book View All... Show API Key Help Center

SHODAN

Explore Downloads Reports Enterprise Access Contact Us

My Account Upgrade

The search engine for Security

Shodan is the world's first search engine for Internet-connected devices.

Create a Free Account Getting Started

67.20.69.105
50.87.75.184
104.18.61.231

Explore the Internet of Things

Use Shodan to discover which of your devices are connected to the Internet, where they are located and who is using them.

See the Big Picture

Websites are just one part of the Internet. There are power plants, Smart TVs, refrigerators and much more that can be found with Shodan!

Monitor Network Security

Keep track of all the computers on your network that are directly accessible from the Internet. Shodan lets you understand your digital footprint.

Get a Competitive Advantage

Who is using your product? Where are they located? Use Shodan to perform empirical market intelligence.

56% of Fortune 100

1,000+ Universities

Shodan is used around the world by researchers, security professionals, large enterprises, CERTs and everybody in between.

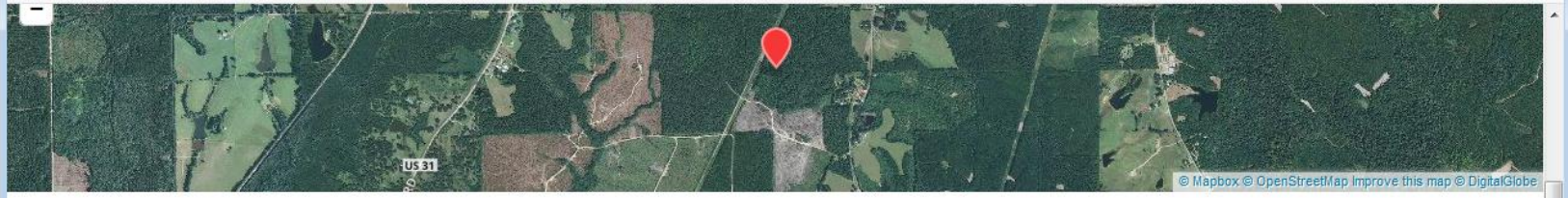
FUEL TANK STATUS OPEN TO THE PUBLIC

File Edit View History Bookmarks Tools Help

208.111.119.39

https://www.shodan.io/host/208.111.119.39

Search



208.111.119.39 host-208-111-119-39.htcnet.net View Raw Data

Industrial Control System

City	Greenville
Country	United States
Organization	Hayneville Telephone Company
ISP	Hayneville Telephone Company
Last Update	2021-01-16T00:10:50.973936
Hostnames	host-208-111-119-39.htcnet.net
ASN	AS33623

Ports

10001

Services

10001
tcp
automated-tank-gauge

```
PINEBELT FUELS
GREENVILLE BYPASS


IN-TANK INVENTORY

TANK PRODUCT             VOLUME TC VOLUME   ULLAGE   HEIGHT    WATER     TEMP
  1  REGULAR UNLEADED      1335      1330     6623    21.54     0.00    63.96
  2  DIESEL 8000           1442      1439     6516    22.75     0.00    64.69
  3  DIESEL 20000          4407      4400    15616    32.64     0.00    63.50
```

SEARCH FOR WEBCAMS

File Edit View History Bookmarks Tools Help

amcrest - Shodan Search

https://www.shodan

Search

Shodan Developers Book View All... Show API Key Help Center

SHODAN amcrest

Explore Downloads Reports Enterprise Access Contact Us My Account Upgrade

Exploits Maps Share Search Download Results Create Report

TOTAL RESULTS

989

TOP COUNTRIES

United States	811
Canada	31
Panama	22
United Kingdom	18
Korea, Republic of	14

TOP SERVICES

8081	241
3702	177
Splunk	57
Synology	43

184.12.43.38

static-184-12-43-38.drr01.nrwl.oh.frontiernet.net

Frontier Communications

Added on 2018-02-25 18:17:22 GMT

United States

Details

```
HTTP/1.1 200 OK
CONNECTION: close
Date: Sun, 25 Feb 2018 13:17:20 GMT
Last-Modified: Sat, 20 May 2017 18:47:04 GMT
Etag: "1495306024:4485"
CONTENT-LENGTH: 17541
CACHE-CONTROL: max-age=0
CONTENT-TYPE: text/html

<!DOCTYPE html> <html> <head> <title></title> <meta charset="UTF-8"> <meta ht...
```

104.190.138.190

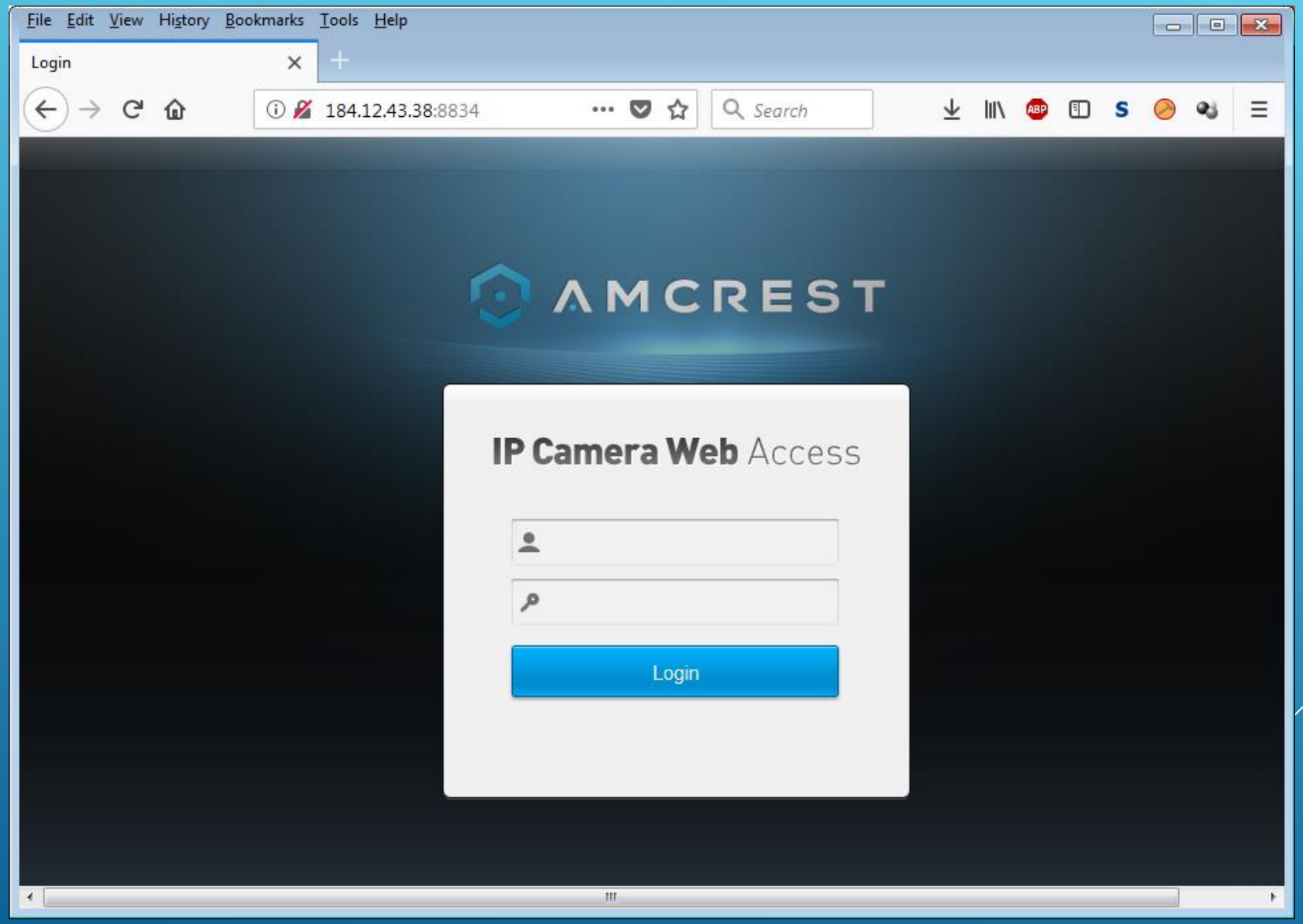
AT&T Internet Services

Added on 2018-02-25 17:45:34 GMT

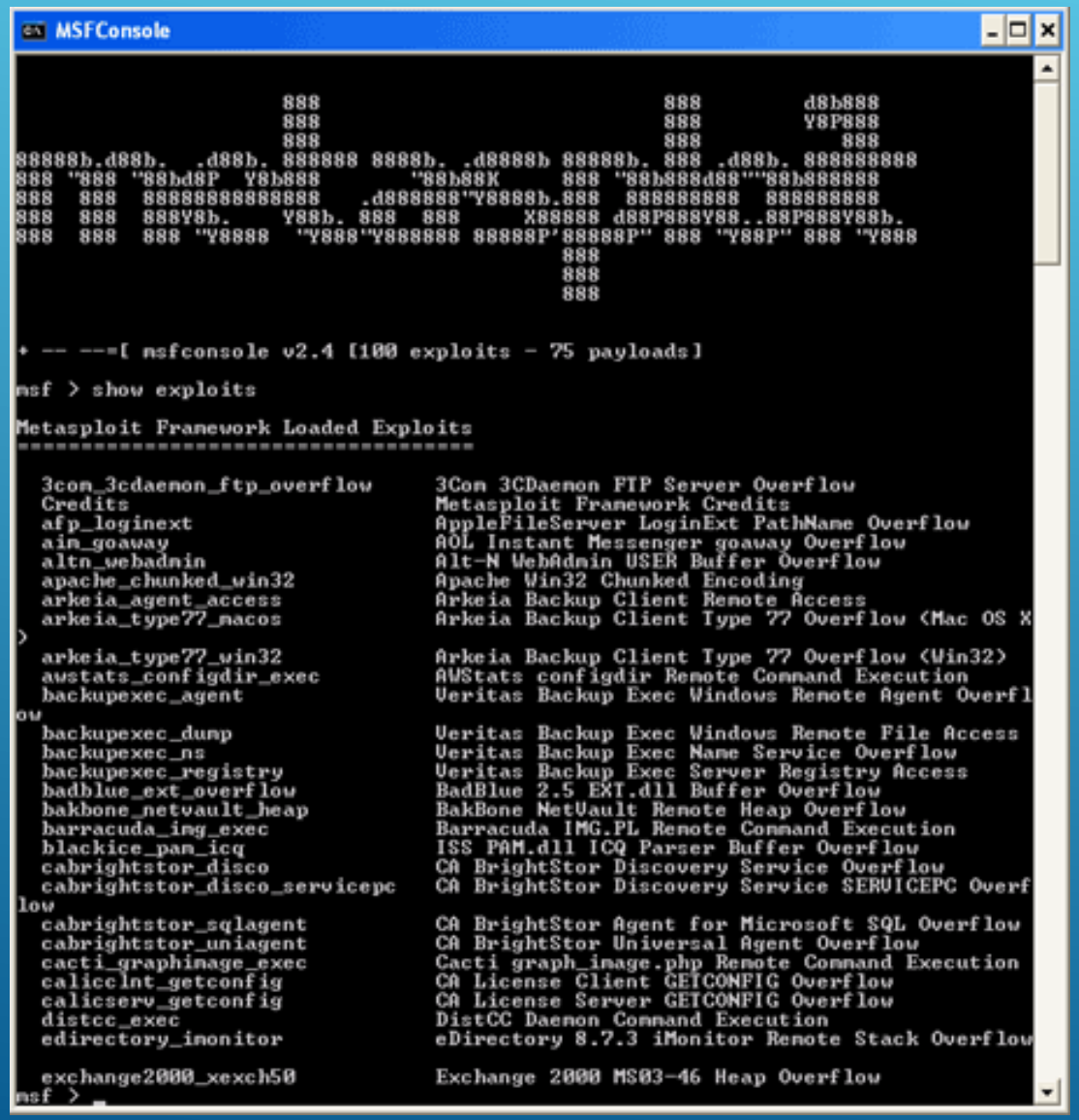
United States, Austin

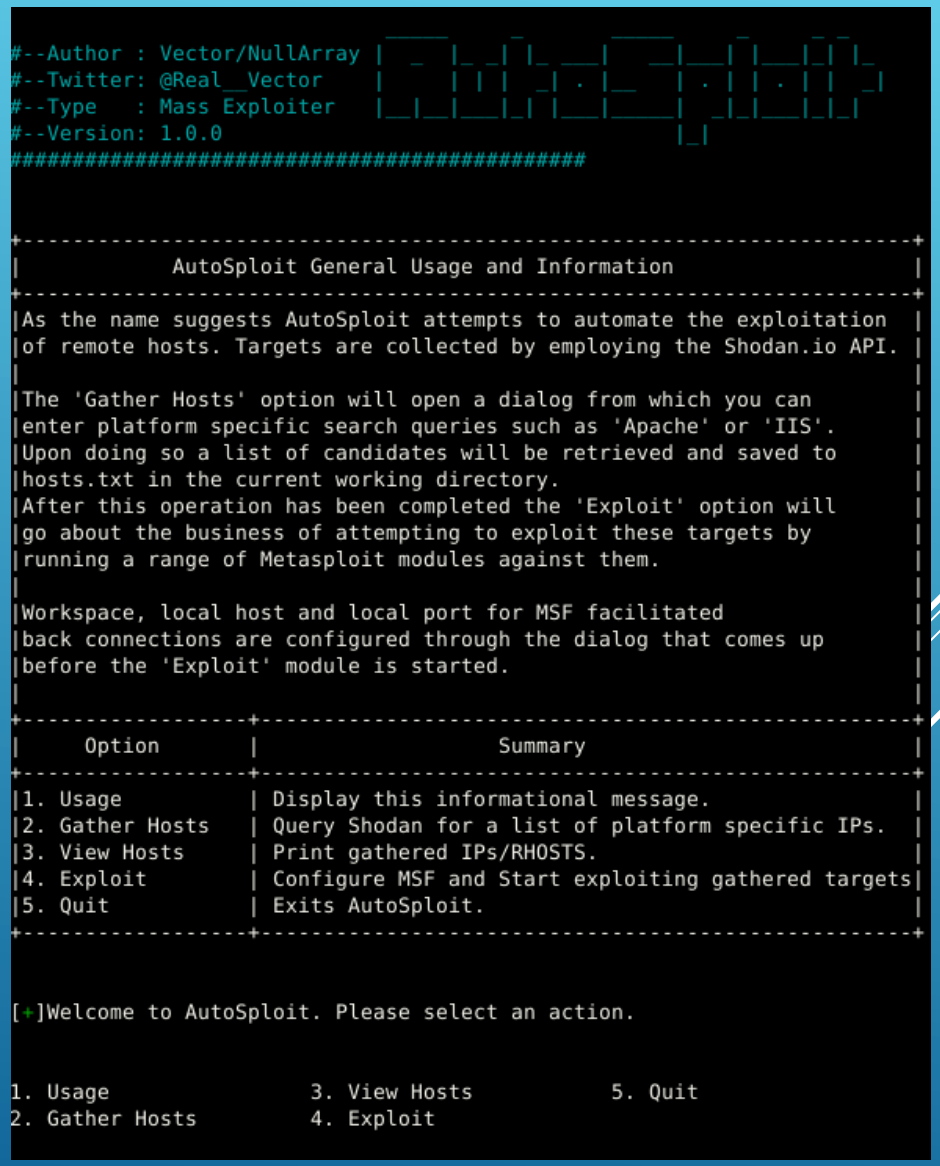
Details

ANYBODY KNOW THE DEFAULT PASSWORD?



IT GETS WORSE





SOLARWINDS INCIDENT

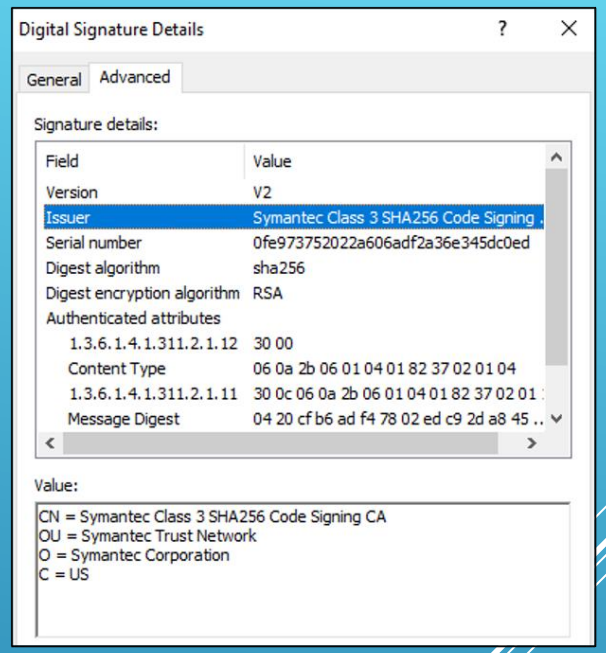
- Story broke on December 13, 2020
  - US Departments of Treasury and Commerce were victims of a very sophisticated cyber attack
  - FireEye previously announced on December 8th that they were breached
- Over 18,000 victims
  - Government, consulting, technology, telecom, and oil and gas companies in North America, Europe, Asia and the Middle East
  - All were breached through the update server of a network management system made by the firm SolarWinds


Sections
The Washington Post
Democracy Dies in Darkness
Sign in
National Security Foreign Policy Justice Military

National Security

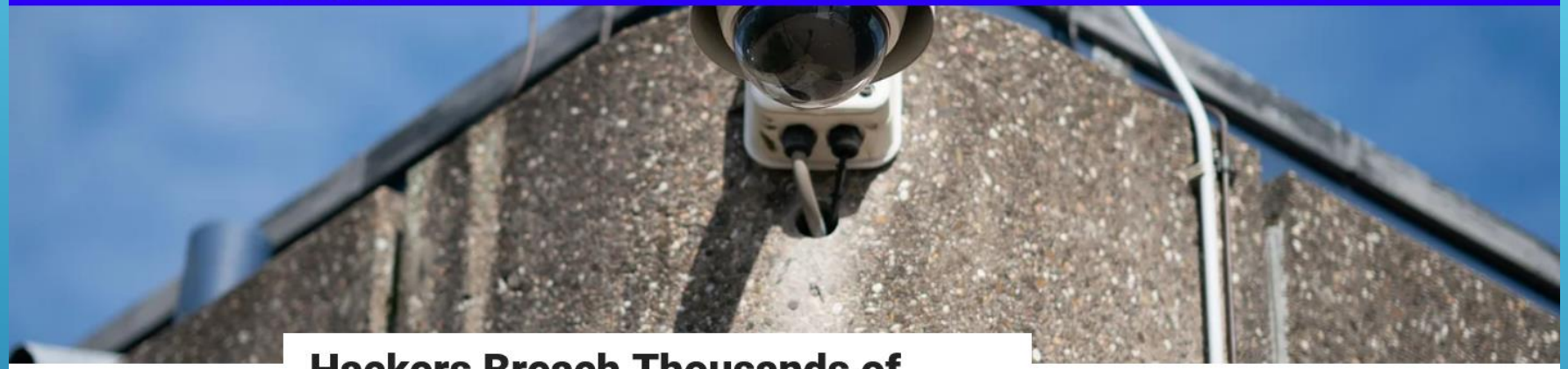
Russian government hackers are behind a broad espionage campaign that has compromised U.S. agencies, including Treasury and Commerce

SOLARWINDS IMPACT



- Attackers are "APT 29" – also known as Cozy Bear
  - Part of Russia's foreign intelligence service, the SVR
  - Same Russian group hacked the State Department's and the White House's email servers during the Obama administration
  - Microsoft believes that over 1000 coders were involved on the Russian side
- Attackers gained access to victims through updates to SolarWinds' Orion network monitoring software
  - Orion is widely used by hundreds of thousands of organizations
  - As organizations updated their Orion software, they added a "feature" that gave the SVR access to internal networks

VERKADA CAMERA INCIDENT



Hackers Breach Thousands of Security Cameras, Exposing Tesla, Jails, Hospitals

William Turton

Published on March 10 2021, 3:02 AM
Last Updated on March 10 2021, 10:51 PM

(Bloomberg) -- A group of hackers say they breached a massive trove of security-camera data collected by Silicon Valley startup Verkada Inc., gaining access to live feeds of 150,000 surveillance cameras inside hospitals, companies, police departments, prisons and schools.

Companies whose footage was exposed include carmaker Tesla Inc. and software provider Cloudflare Inc. In addition, hackers were able to view video from inside women's health clinics, psychiatric hospitals and the offices of Verkada itself. Some of the cameras, including in hospitals, use facial-recognition technology to identify and categorize people captured on the footage. The hackers say they also have access to the full video archive of all Verkada customers.

AURORA TEST – MARCH 4, 2007

USA TODAY

Home | News | Travel | Money | Sports | Life | Tech | Weather

Technology ▪ Technology Live ▪ Science Fair ▪ Science & Space ▪ Products ▪ Gaming ▪ Wi-Fi Center

U.S. video shows hacker hit on power grid

Updated 9/27/2007 9:33 AM | Comment | Recommend

E-mail | Print | RSS

Enlarge Dept. of Homeland Security via AP

In this image from video released by the Department of Homeland Security, smoke pours from an expensive electrical turbine during a March 4, 2007, demonstration by the Idaho National Laboratory, which was simulating a hacker attack against the U.S. electrical grid.

WASHINGTON (AP) — A government video shows the potential destruction caused by hackers seizing control of a crucial part of the U.S. electrical grid: an industrial turbine spinning wildly out of control until it becomes a smoking hulk and power shuts down.

The video, produced for the Homeland Security Department and obtained by the Associated Press on Wednesday, was marked "Official Use Only." It shows commands quietly triggered by simulated hackers having such a violent reaction that the enormous turbine shudders as pieces fly apart and it belches black-and-white smoke.

The video was produced for top U.S. policymakers by the Idaho National Laboratory, which has studied the little-understood risks to the specialized electronic equipment that operates power, water and chemical plants. Vice President Dick Cheney is among those who have watched the video, said one U.S. official, speaking on condition of anonymity because this official was not authorized to publicly discuss such high-level briefings.

Mixx it

Other ways to share:

Digg

del.icio.us

Newsvine

Reddit

Facebook

What's this?

CHANGING THREAT LANDSCAPE

- Near-term (0-2 years)
  - Nation state threats, advanced persistent threats, Internet of Things (IoT), Distributed Denial of Service (DDoS) attacks, and ransomware
  - Data breaches and intellectual property theft
  - Insiders, physical damage, coordinated attacks, and third-party risks
- Mid-term (3-5 years)
  - Increased reliance on gas generation
  - Distribution system vulnerabilities via networked control systems
  - Growth of demand response technologies with low security
  - Distributed energy resources
  - Reliability of communications networks

CORPORATE SECURITY MINDSET

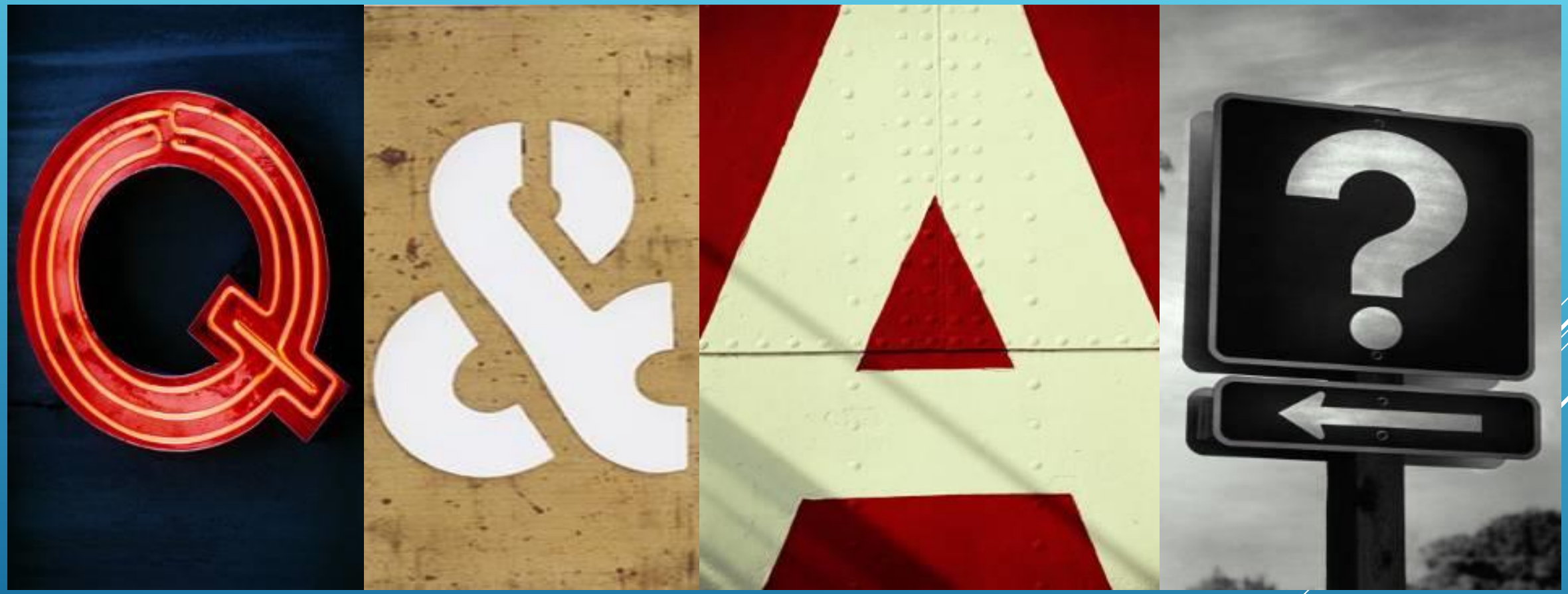
- Security layers should be invisible
- Security controls should not ***prevent proper*** behavior
  - They should however ***detect improper*** behavior
- Think of information technology as the oxygen supporting creativity
  - Information security keeps the air clean, and warns when pollution or pathogens are detected
  - Infected devices are like infected people – you don't want them in the same room spreading their disease

PRACTICE GREAT CORPORATE SECURITY

- Starts with executive involvement and commitment
  - C-level leaders
  - Directors and advisors
- Develop a strong corporate policy
  - Include explicit statements of what is, and is not, permissible
  - Set a baseline for employees and managers
  - Provide a framework for disciplinary or legal action
  - Can be more restrictive than public laws and regulations
  - Include guidance for incident handling and recovery

EXPECTATIONS OF EMPLOYEES

- Treat security seriously
  - Expect to be a target
  - A bit of paranoia is OK
- Use locks and barriers to protect physical property
  - Use a VPN to protect virtual property
- Keep phones, laptops, and tablets updated
- Use antivirus software and endpoint security
- Avoid putting company information on personal systems
- Watch for security issues and call for help


Q
&
A
?