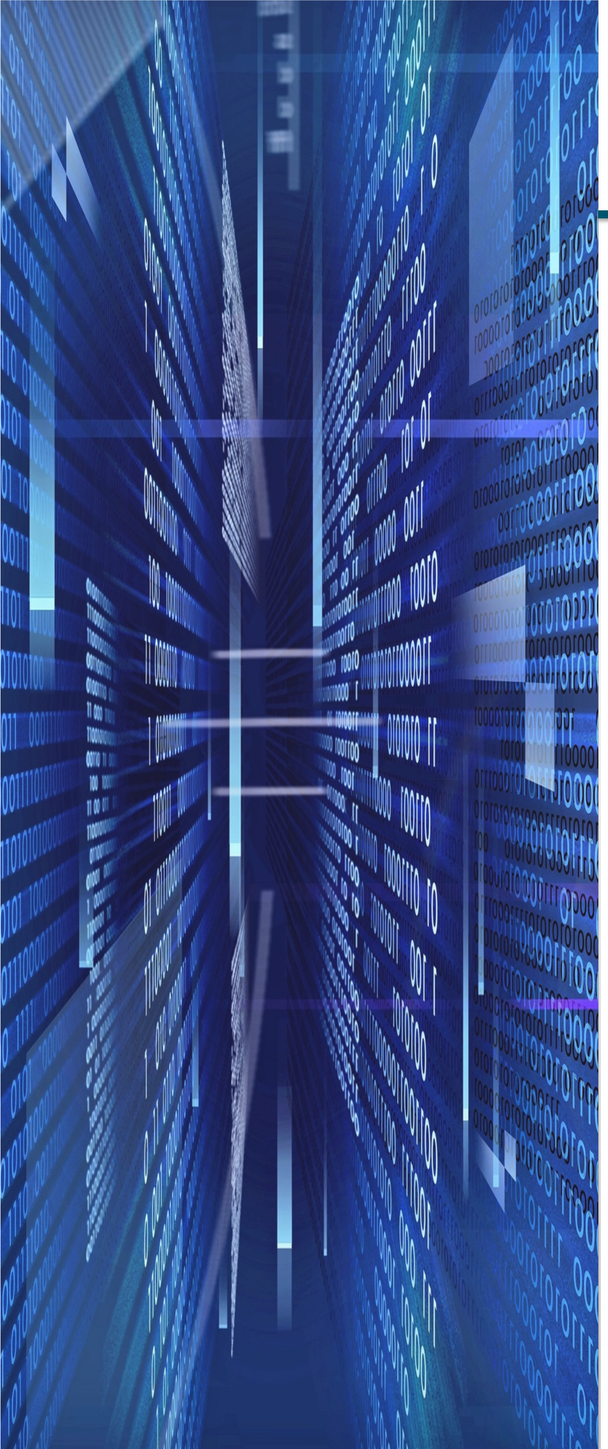


Attacks to Critical Infrastructures
Cyber War

Prof. Federica Paci

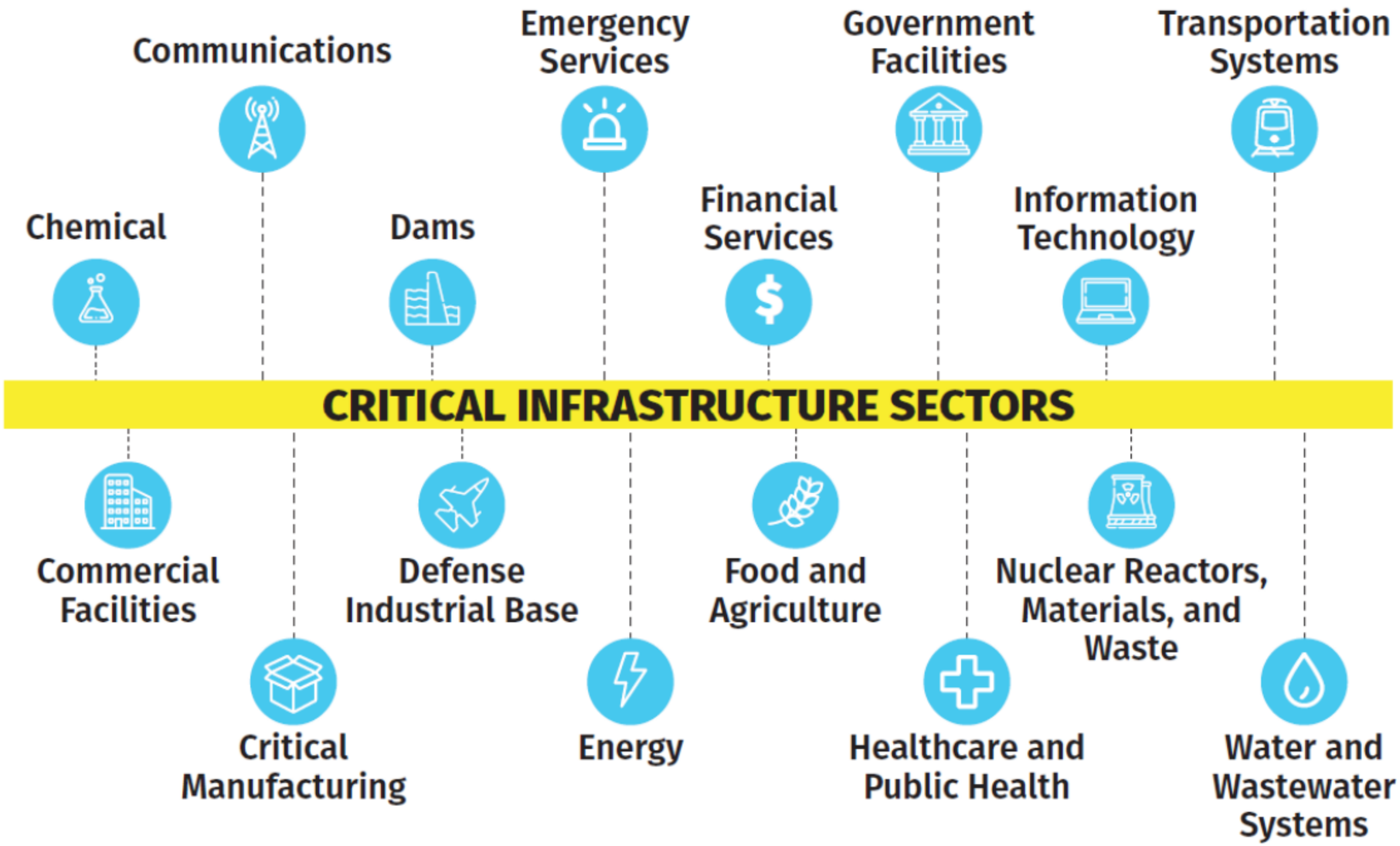
Lecture Outline

- Critical Infrastructures
- Industrial Control Systems
- Vulnerabilities in Industrial Control Systems
- Cyber Kill Chain of Industrial Control Systems
- Cyber War
  - Stuxnet
  - Sandworm' s Attacks
    - Ukraine Power Grid Attacks
    - NoPetya Attacks
  - Russian invasion of Ukraine (2022 -present)

What is a critical infrastructure?

- National Infrastructure are those facilities, systems, sites, information, people, networks and processes, necessary for a country to function and upon which daily life depends.
- It also includes some functions, sites and organizations which are not critical to the maintenance of essential services, but which need protection due to the potential danger to the public (civil nuclear and chemical sites for example)

Examples of critical infrastructure sectors



What is really critical?

Those critical elements of infrastructure (namely assets, facilities, systems, networks or processes and the essential workers that operate and facilitate them), the loss or compromise of which could result in:

a) Major detrimental impact on the availability, integrity or delivery of essential services – including those services whose integrity, if compromised, could result in significant loss of life or casualties – taking into account significant economic or social impacts; and/or

b) Significant impact on national security, national defence, or the functioning of the state.

Critical infrastructures and Industrial Control Systems

Many Critical infrastructures are controlled and monitored by Industrial Control Systems (ICS)

- Electricity generation plants
- Transportation systems
- Manufacturing facilities

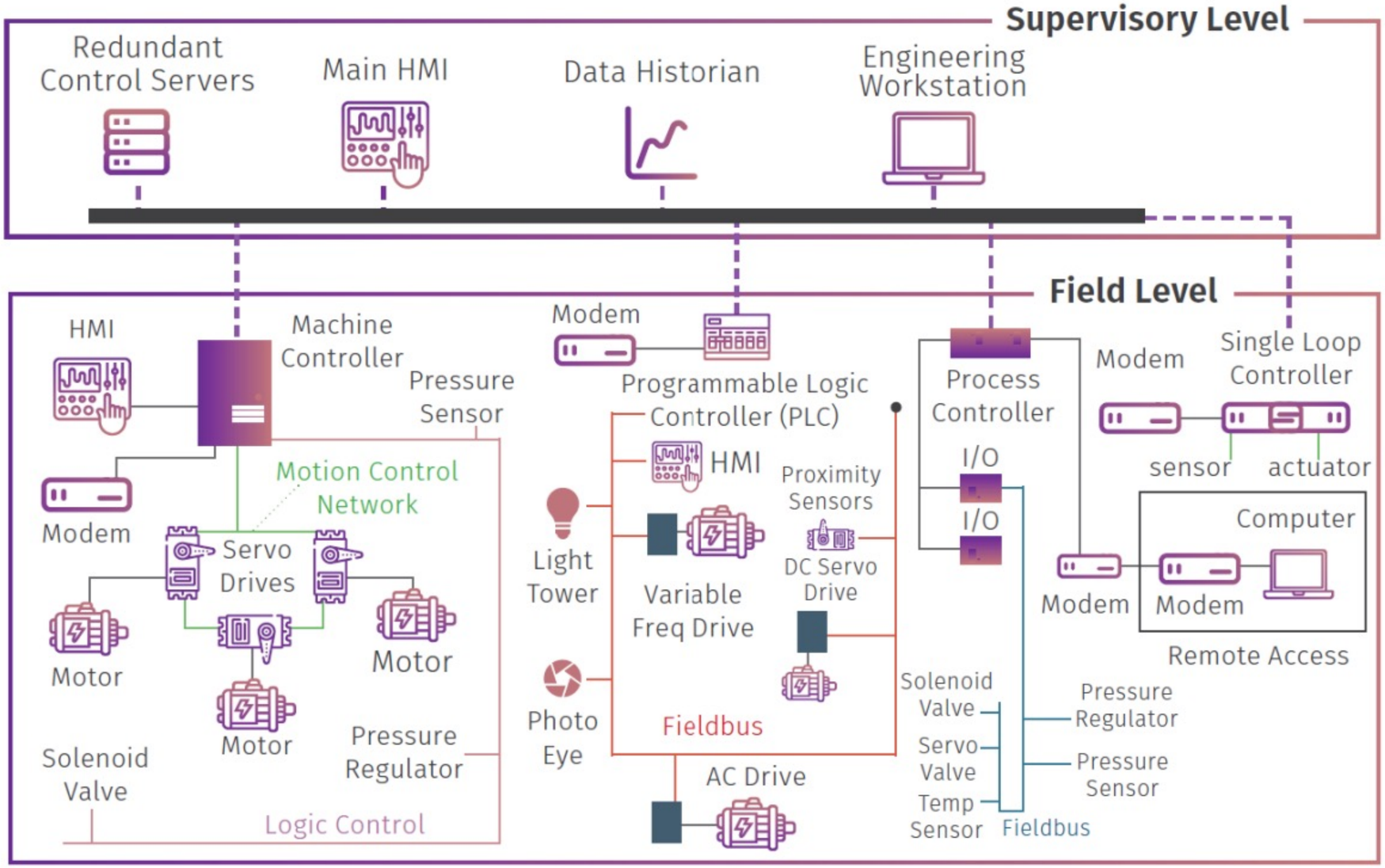
• ICS control our critical infrastructures, safety-critical processes and most production processes. ICS are now everywhere around us, often hiding in everyday functionality.”

Good Morning with ICS

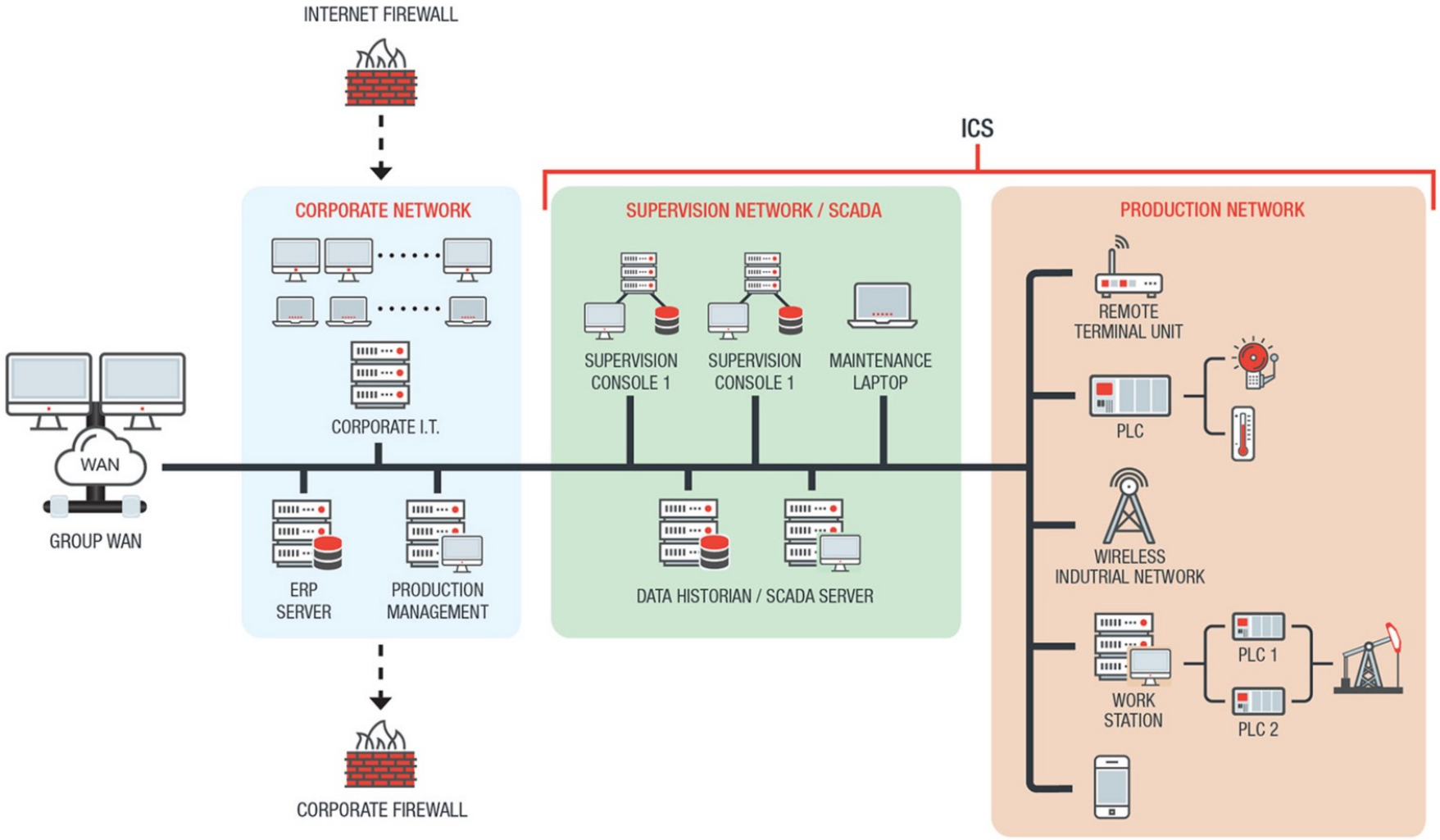
What ICS controlled functions did you use this morning before you arrived at your desk? None? Then, we ask you to re-trace your steps.

Your alarm clock awoke you. You turned on the bedside light. **The required extra Watts were generated, transported and distributed under ICS control.** While you took a shower, **ICS adjusted the drinking water production process and maintained the pressure in the pipelines to your home.** Heating of your home and cooking breakfast required the production, transport and distribution of gas. All these processes are controlled by ICS. The cup of milk you used required **automatic milking, strict temperature control of the intermediate storage tanks, and processing and packaging at the milk factory, all under ICS control.** You either took the **train (ICS-controlled signalling, points, power and traction), or road transport (ICS controlled traffic lights, safety systems in tunnels and traffic control of lanes).** Arriving at the office, you passed the **ICS-operated barrier to the parking lot** and the **ICS-controlled security barrier or doors to enter the premises.** The air conditioning, fire protection and evacuation systems of your organization are all operated by ICS 24/7, as well as the elevator you took to your office at the top floor. The (critical) large coffee/tea/chocolate/soup machine has embedded ICS and is connected to the Internet …

Industrial Control Systems Key Components



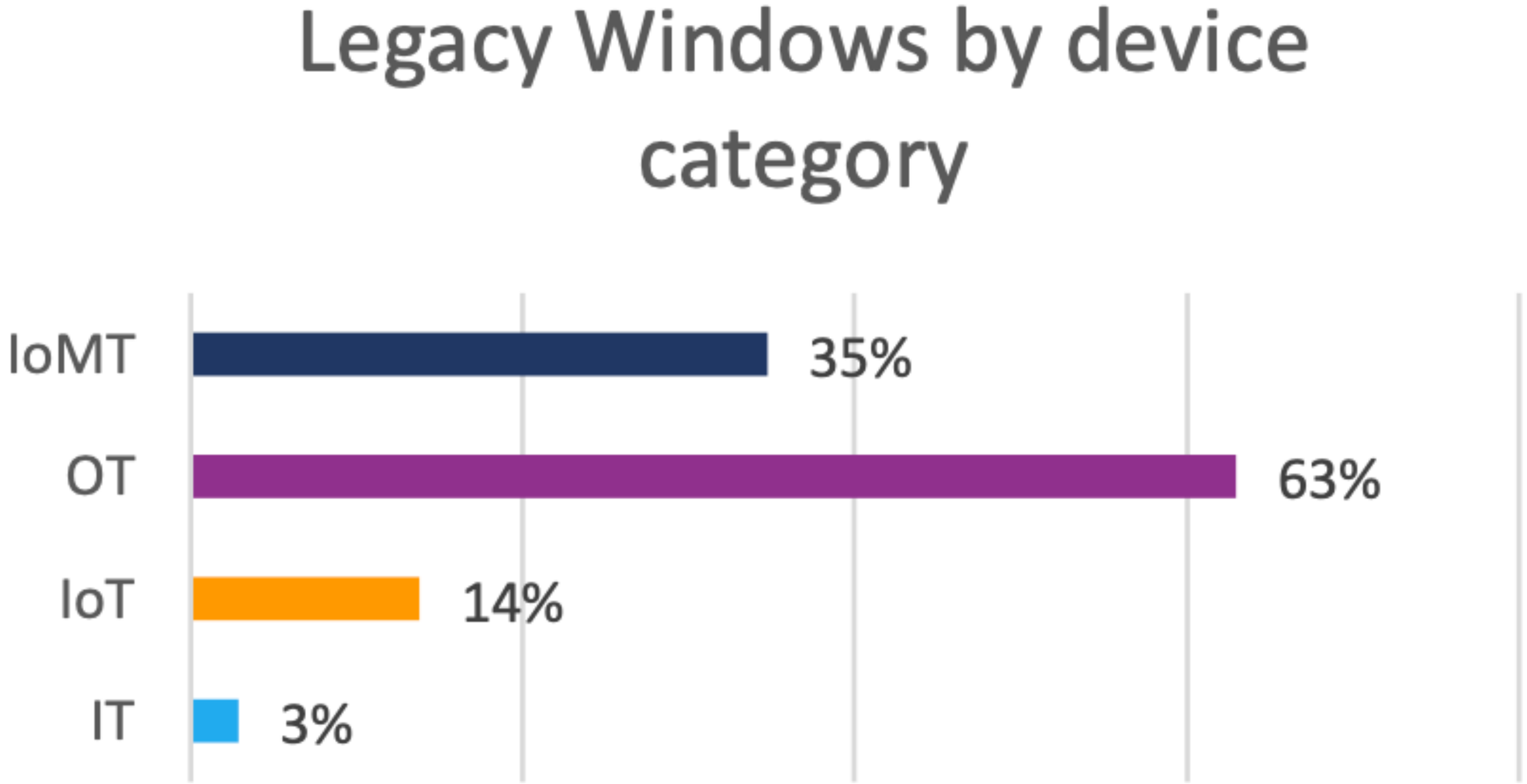
SCADA


INTERNET FIREWALL
ICS
CORPORATE NETWORK
SUPERVISION NETWORK / SCADA
PRODUCTION NETWORK
REMOTE TERMINAL UNIT
SUPERVISION CONSOLE 1
SUPERVISION CONSOLE 1
MAINTENANCE LAPTOP
CORPORATE I.T.
PLC
WAN
GROUP WAN
WIRELESS INDUTRIAL NETWORK
ERP SERVER
PRODUCTION MANAGEMENT
DATA HISTORIAN / SCADA SERVER
PLC 1
WORK STATION
PLC 2
CORPORATE FIREWALL

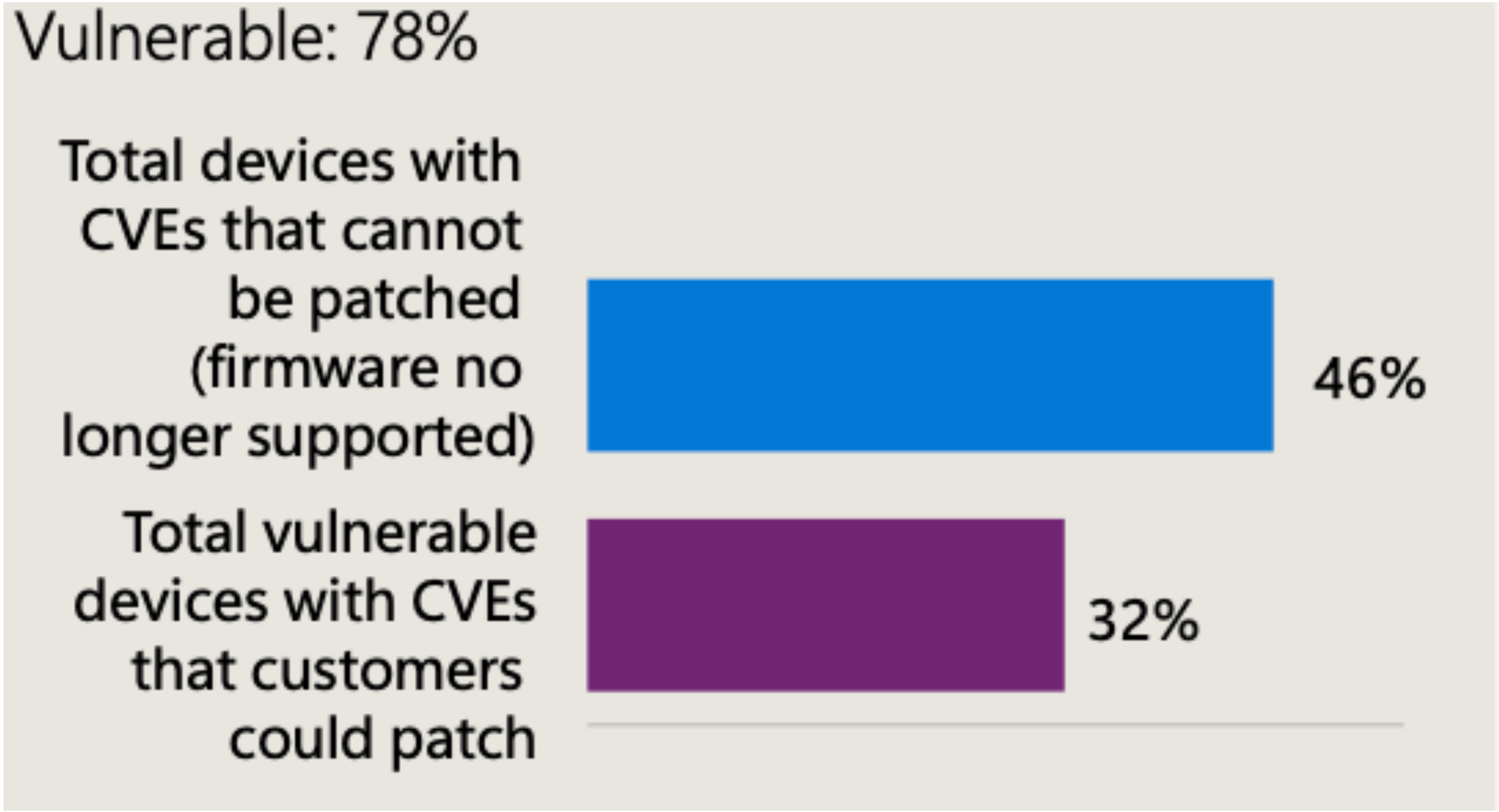
Most Vulnerable Devices

IoT Devices	OT Devices	IOMT Devices
Network Attached Storage (NAS)	Uninterruptible power supply (UPS)	Healthcare Workstation
Printer	Programmable Logic Controller (PLC)	Imaging
IP Camera	Engineering Workstation	Nuclear Medicine Systems
Out of Band Management	Building Automation	Blood Glucose Monitor
VoiP	Remote Terminal Unit	Patient Monitor

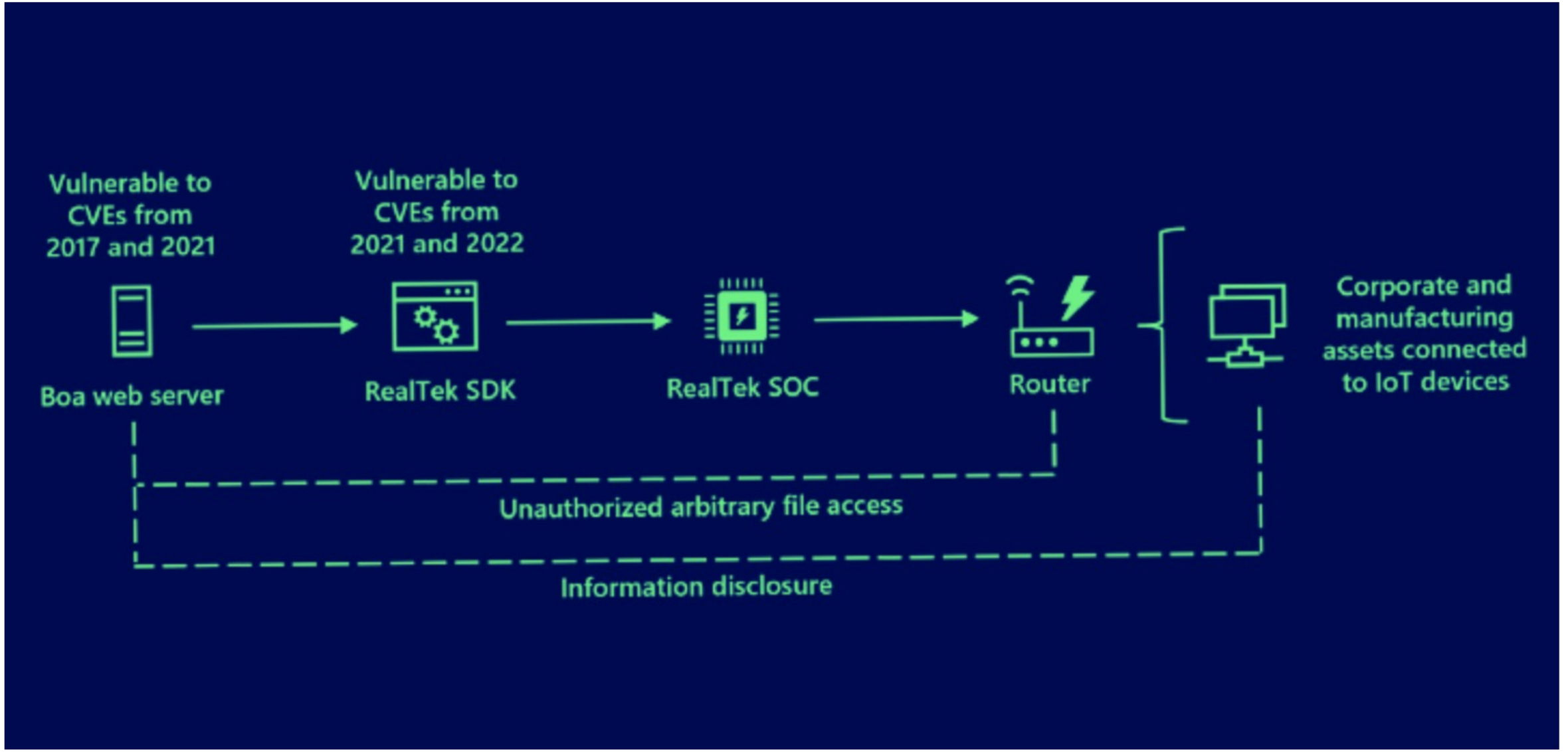
Legacy Operating Systems



Unpatched devices



Vulnerable Embedded Software: Boa web server



Vulnerable Embedded Software: CODESYS Vulnerabilities

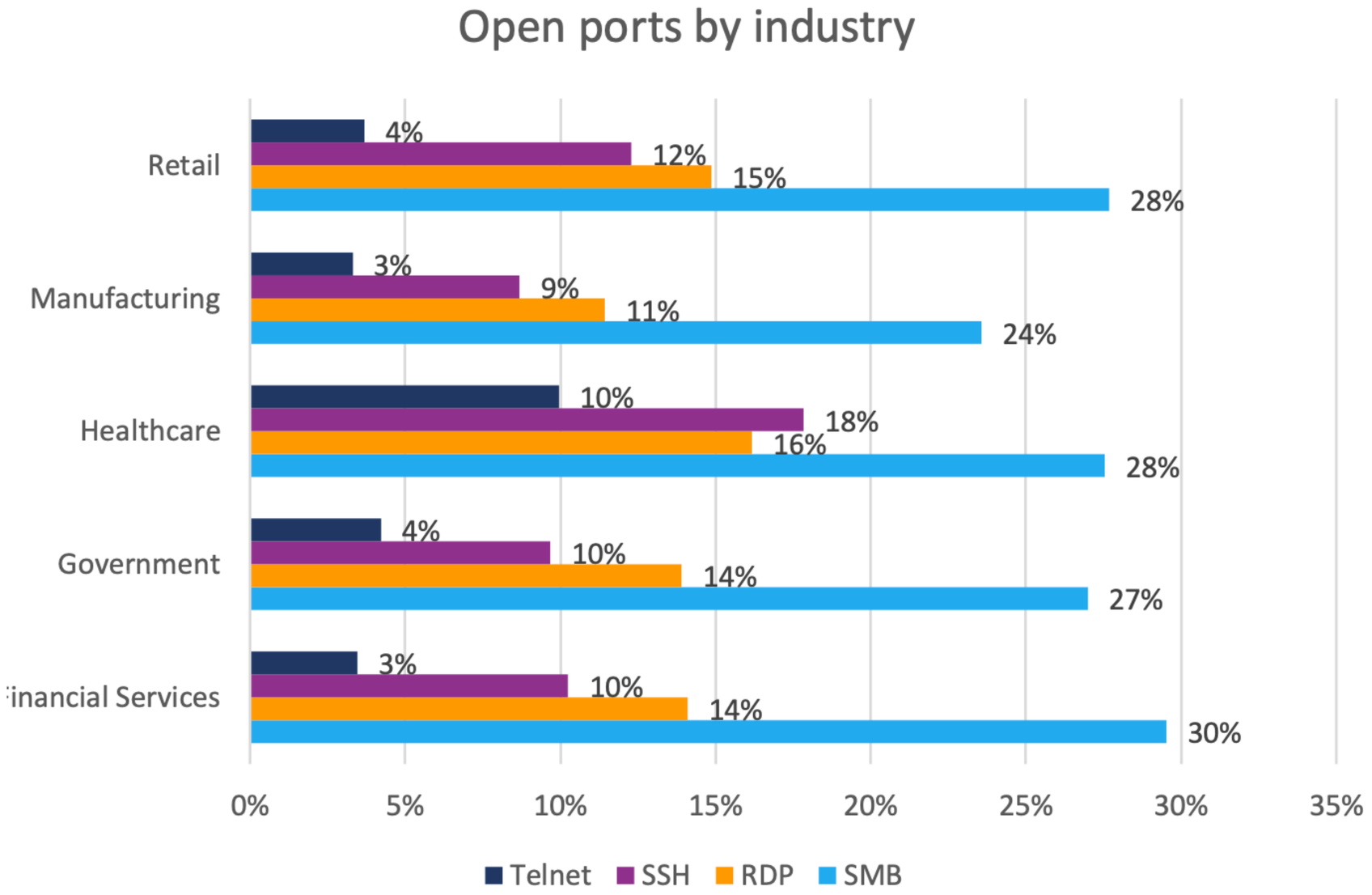
Research Threat intelligence Microsoft Defender for IoT Vulnerabilities and exploits ·

10 min read

Multiple high severity vulnerabilities in CODESYS V3 SDK could lead to RCE or DoS

By Microsoft Threat Intelligence

Open Ports

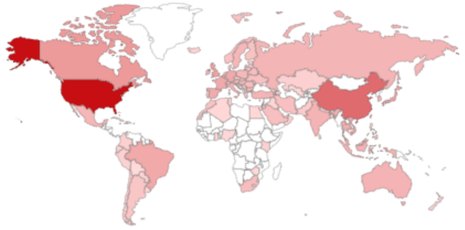

Open ports by industry
Retail
4%
12%
15%
28%
Manufacturing
3%
9%
11%
24%
Healthcare
10%
18%
16%
28%
Government
4%
10%
14%
27%
inancial Services
3%
10%
14%
30%
0%
5%
10%
15%
20%
25%
30%
35%
Telnet
SSH
RDP
SMB

Internet exposure

TOTAL RESULTS

472,905

TOP COUNTRIES



United States	**399,012**
China	**31,745**
Canada	**4,144**
United Kingdom	**2,643**
Japan	**2,458**

More...

TOP ORGANIZATIONS

Google LLC	**360,691**

View Report | Download Results | Historical Trend | Browse Images | View on Map

Access Granted: Want to get more out of your existing Shodan account? Check out **everything you have access to.**

165.85.147.58

2023-11-06T10:10:57.386034

Palo Alto Networks, Inc

United States, Santa Clara

```
No data returned
```

34.43.8.115

2023-11-06T10:10:50.945113

115.8.43.34.bc.googleusercontent.com

Google LLC

United States, Mountain View

```
No data returned
```

34.107.175.20

2023-11-06T10:10:48.765118

20.175.107.34.bc.googleusercontent.com

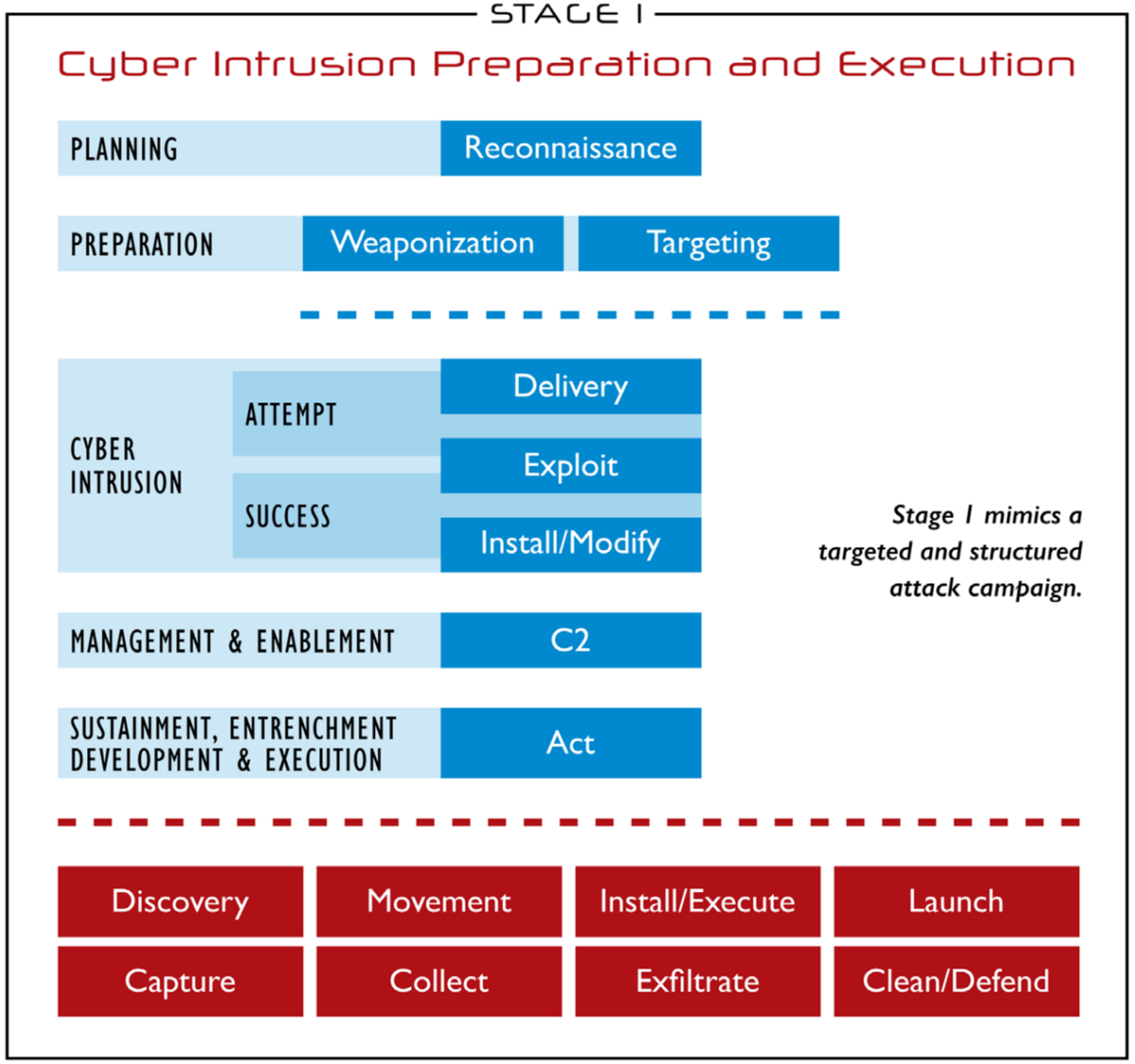
Google LLC

United States, Kansas City

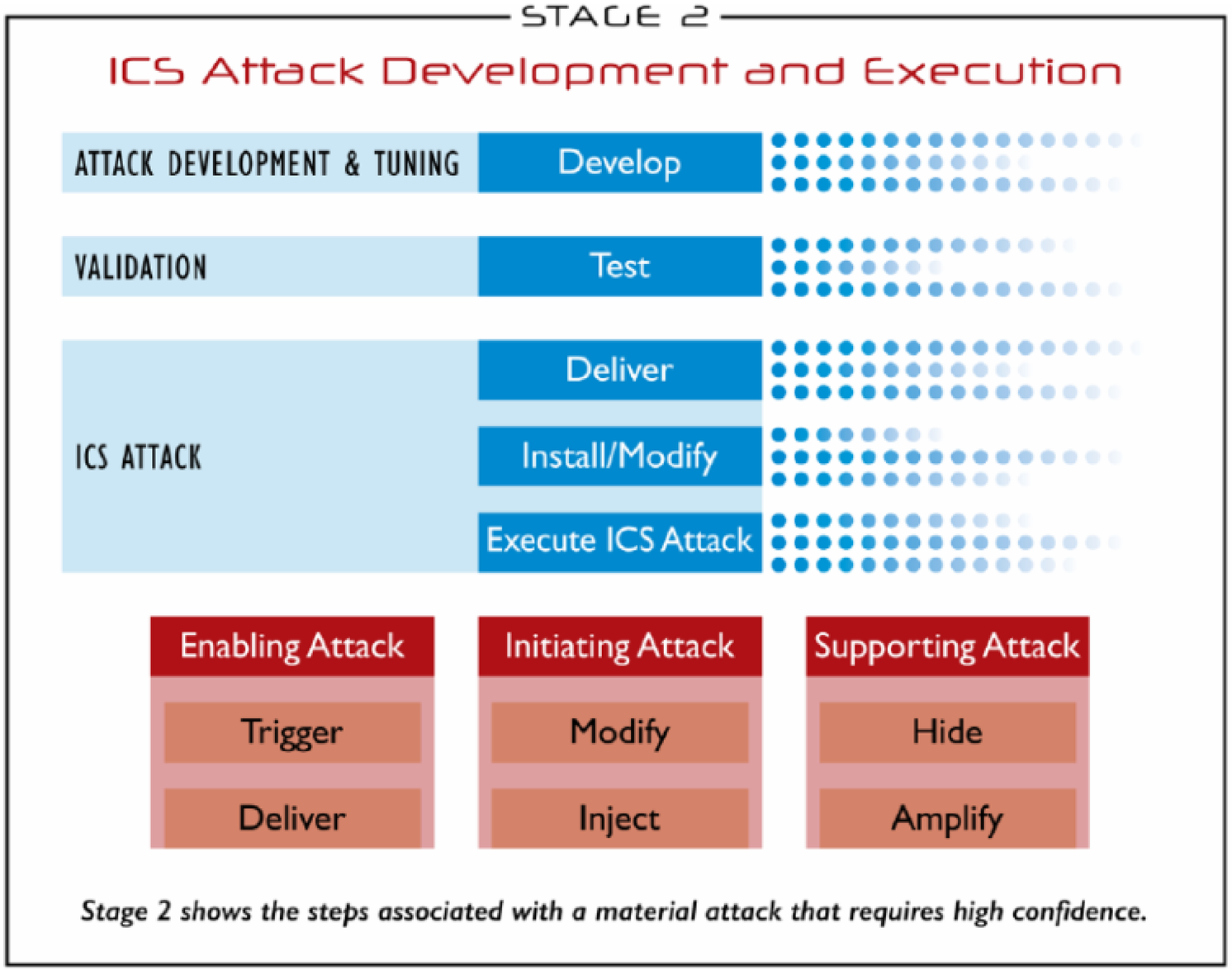
```
No data returned
```

cloud

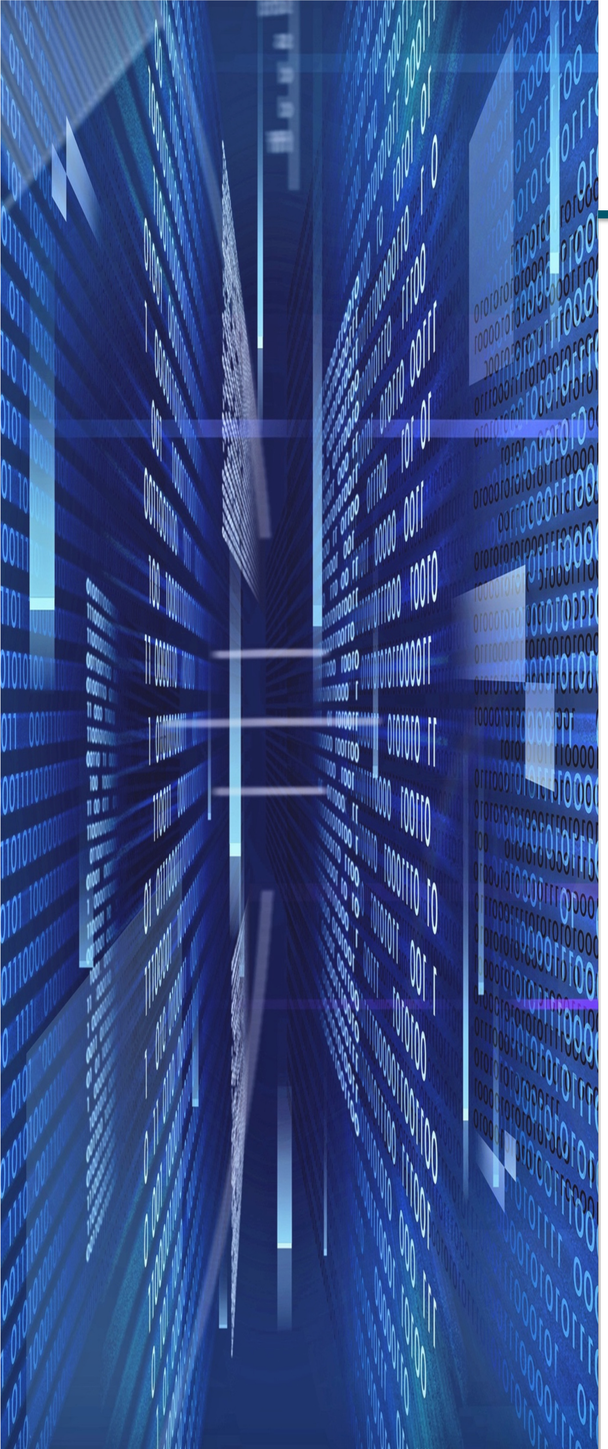
ICS Cyber Kill Chain



ICS Cyber Kill Chain



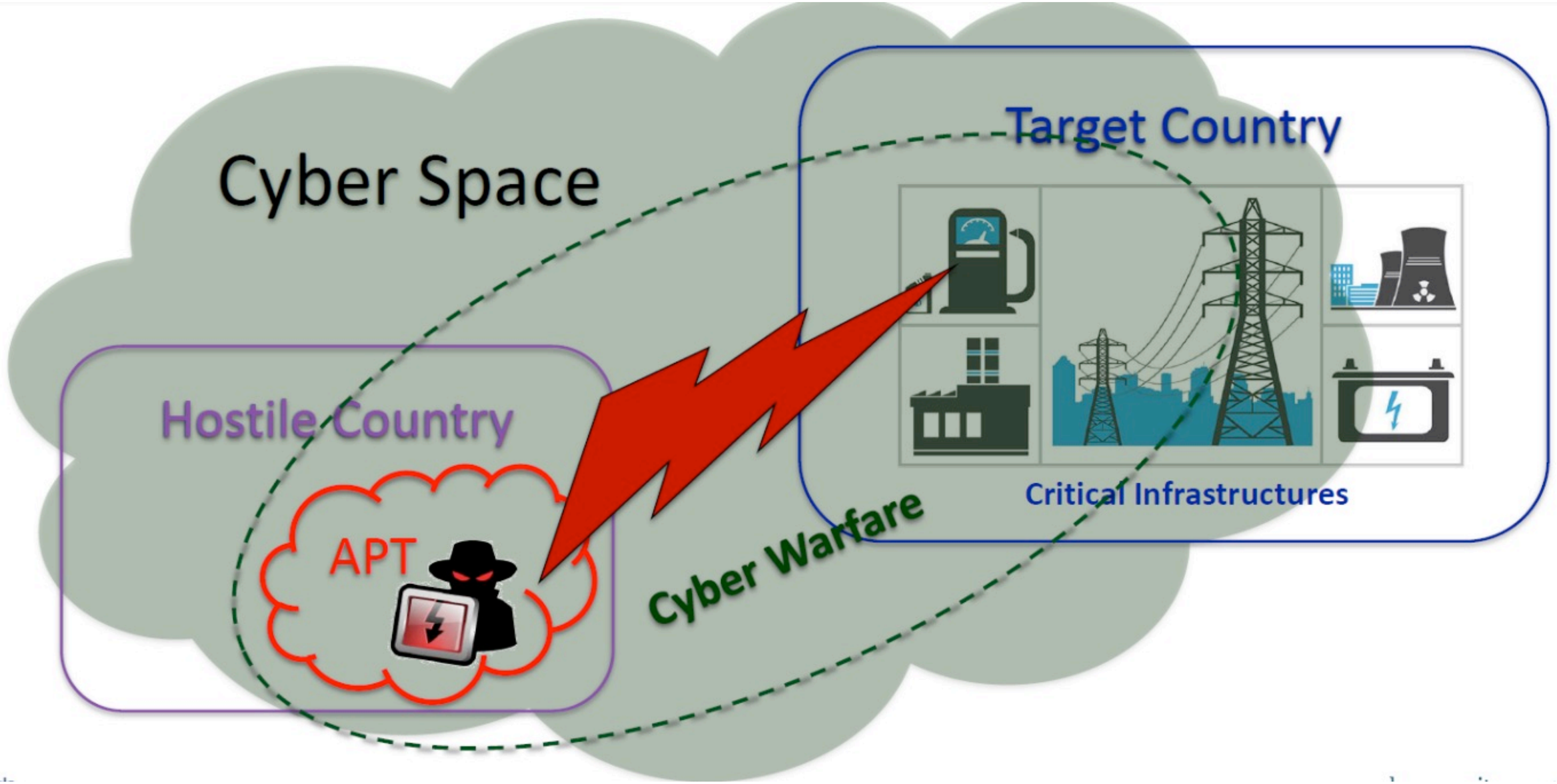
Stage 2 shows the steps associated with a material attack that requires high confidence.



Cyber war

Prof. Federica Paci

Cyberwar


Cyber Space
Target Country
Hostile Country
APT
Cyber Warfare
Critical Infrastructures

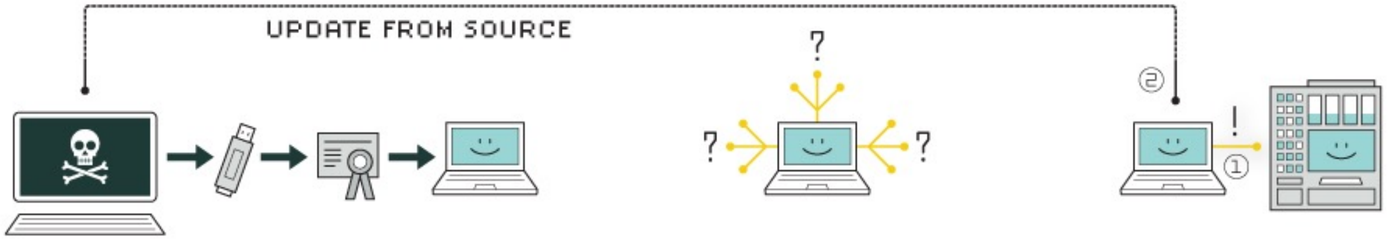
Types of Cyberwarfare Attacks

Stuxnet

- First cyber weapon
- Targeted
  - PLCs used to control and monitor centrifuges to enrich uranium
  - 70% of the infection target nuclear plants in Iran
- First detected in June 2010
- Extremely sophisticated malware
  - > 10.000 line of codes
  - 4 zero-day vulnerabilities
  - 2 rootkits
- Creators
  - the U.S. National Security Agency, the CIA, and Israeli intelligence

Stuxnet

HOW STUXNET WORKED



1. infection
Stuxnet enters a system via a USB stick and proceeds to infect all machines running Microsoft Windows. By brandishing a digital certificate that seems to show that it comes from a reliable company, the worm is able to evade automated-detection systems.

2. search
Stuxnet then checks whether a given machine is part of the targeted industrial control system made by Siemens. Such systems are deployed in Iran to run high-speed centrifuges that help to enrich nuclear fuel.

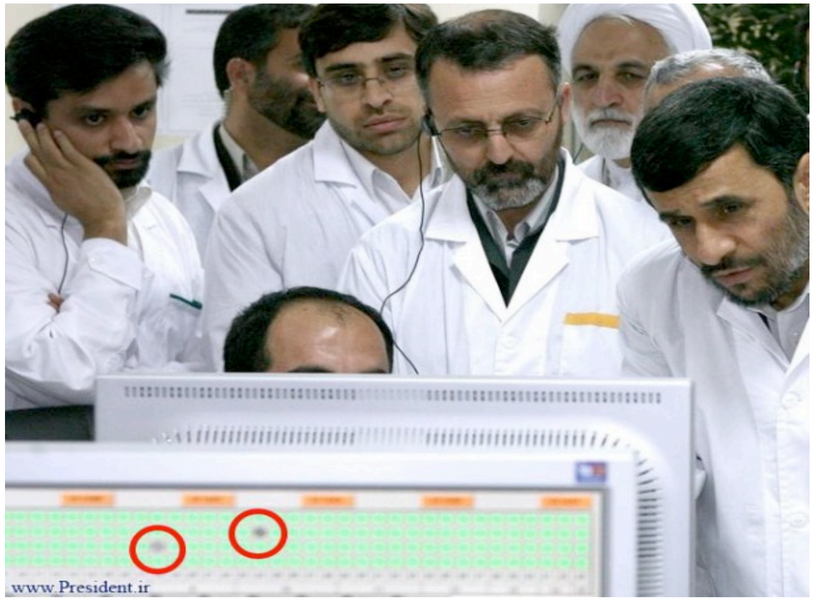
3. update
If the system isn't a target, Stuxnet does nothing; if it is, the worm attempts to access the Internet and download a more recent version of itself.

4. compromise
The worm then compromises the target system's logic controllers, exploiting "zero day" vulnerabilities-software weaknesses that haven't been identified by security experts.

5. control
In the beginning, Stuxnet spies on the operations of the targeted system. Then it uses the information it has gathered to take control of the centrifuges, making them spin themselves to failure.

6. deceive and destroy
Meanwhile, it provides false feedback to outside controllers, ensuring that they won't know what's going wrong until it's too late to do anything about it.

Reconnaissance

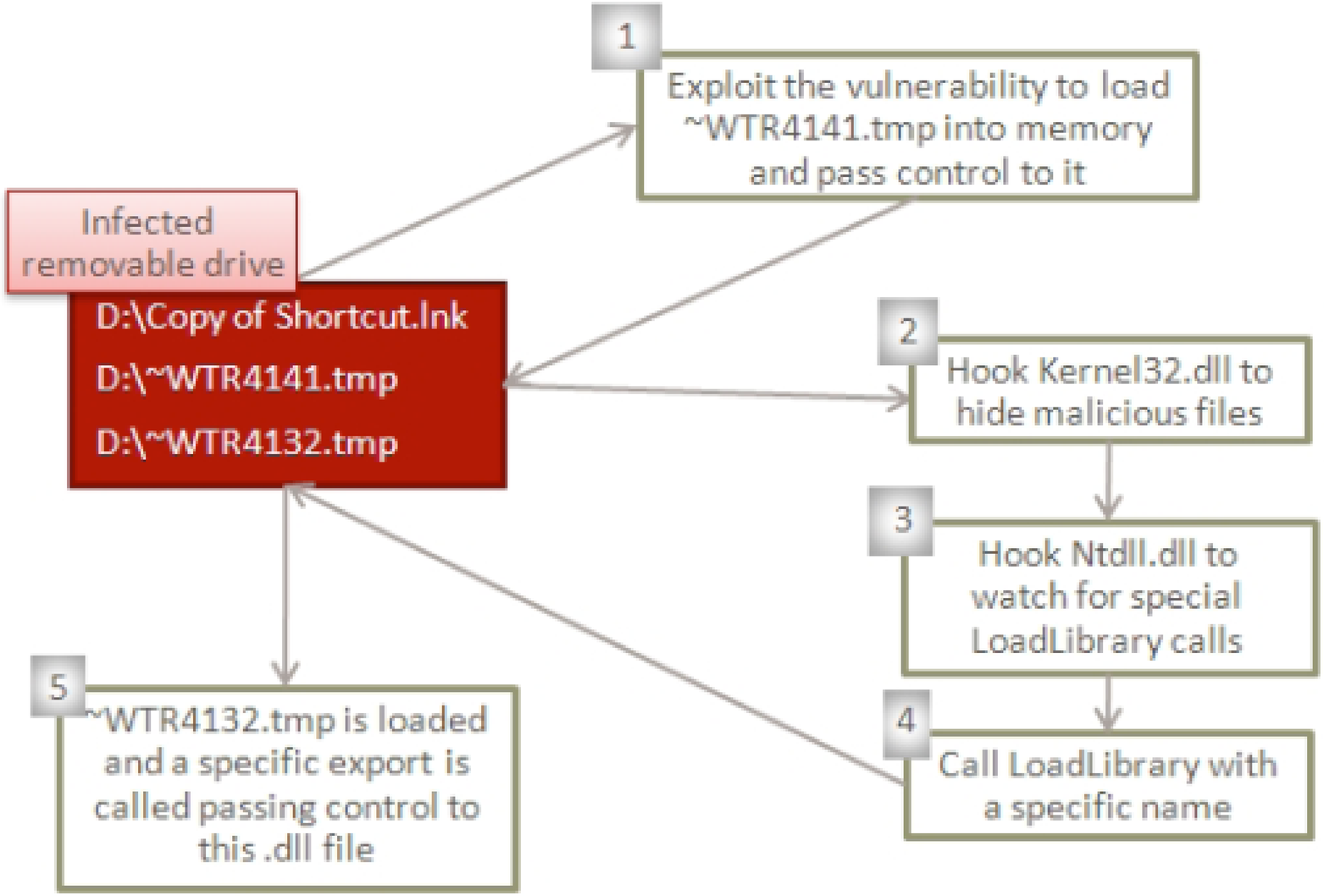


Spreading Techniques

Stuxnet uses different propagation techniques:

- Network propagation techniques
  - Infecting WinCC machines via a hardcoded database server password
  - Propagating through the MS10-061 Print Spooler Zero-Day Vulnerability
  - Propagating through the MS08-067 Windows Server Service Vulnerability
- Removable drive propagation
  - LNK Vulnerability (CVE-2010-2568)
  - Autorun.inf

LNK Vulnerability



Autorun.inf

```
00000000: 4D5A9000 03000000 04000000 FFFF0000  MZ▌.........ÿÿ..
00000010: B8000000 00000000 40000000 00000000  ¸.......@.......
00000020: 00000000 00000000 00000000 00000000  ................
00000030: 00000000 00000000 00000000 E0000000  ............à...
00000040: 0E1FBA0E 00B409CD 21B8014C CD215468  ..º..´.Í!¸.LÍ!Th
00000050: 69732070 726F6772 616D2063 616E6E6F  is program canno
00000060: 74206265 2072756E 20696E20 444F5320  t be run in DOS
00000070: 6D6F6465 2E0D0D0A 24000000 00000000  mode....$.......
00000080: CF7A777C 8B1B192F 8B1B192F 8B1B192F  Ïzw|▌../▌../▌../
00000090: ACDD642F 9D1B192F ACDD622F 9C1B192F  ¬Ýd/▌../¬Ýb/▌../
000000A0: 8B1B182F 6D1B192F ACDD6B2F DA1B192F  ▌../m../¬Ýk/Ú../
```

```
00041000: 0D0A5B61 75746F72 756E5D0D 0A6F626A  ..[autorun]..obj
00041010: 65637444 65736372 6970746F 723D7B42  ectDescriptor={B
00041020: 33313535 33372D36 3341422D 39353132  315537-63AB-9512
00041030: 2D393941 392D3246 34363737 32333541  -99A9-2F4677235A
00041040: 34347D0D 0A                          44}..
00041050: 636F6D6D 616E643D 2E5C4155 544F5255  command=.\AUTORU
00041060: 4E2E494E 460D0A                5C4D656E  N.INF..    \Men
00041070: 753D4025 77696E64 6972255C 73797374  u=@%windir%\syst
00041080: 656D3332 5C736865 6C6C3332 2E646C6C  em32\shell32.dll
00041090: 2C2D3834 39360D0A                    ,-8496..
000410A0:     0D0A 55736541 75746F50 4C41593D      ..UseAutoPLAY=
000410B0: 300D0A                               0..
```

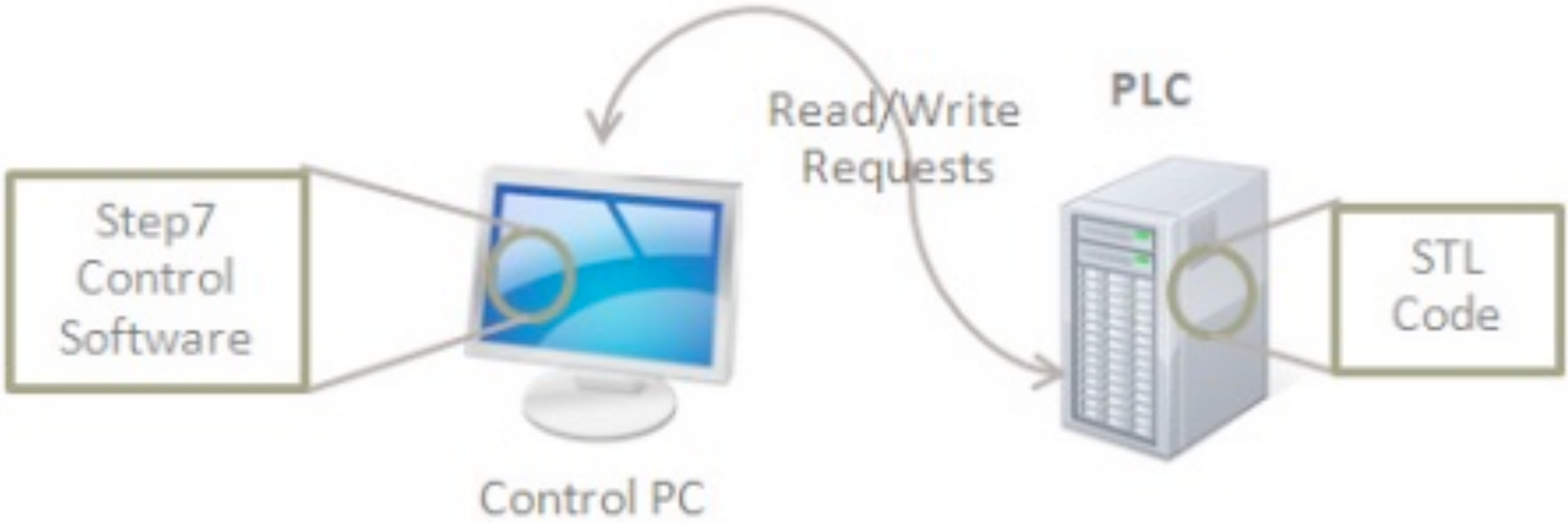
Command and Control (C2)

- After installation Stuxnet contacts the command and control server on port 80 and sends some basic information about the compromised computer to the attacker via HTTP.

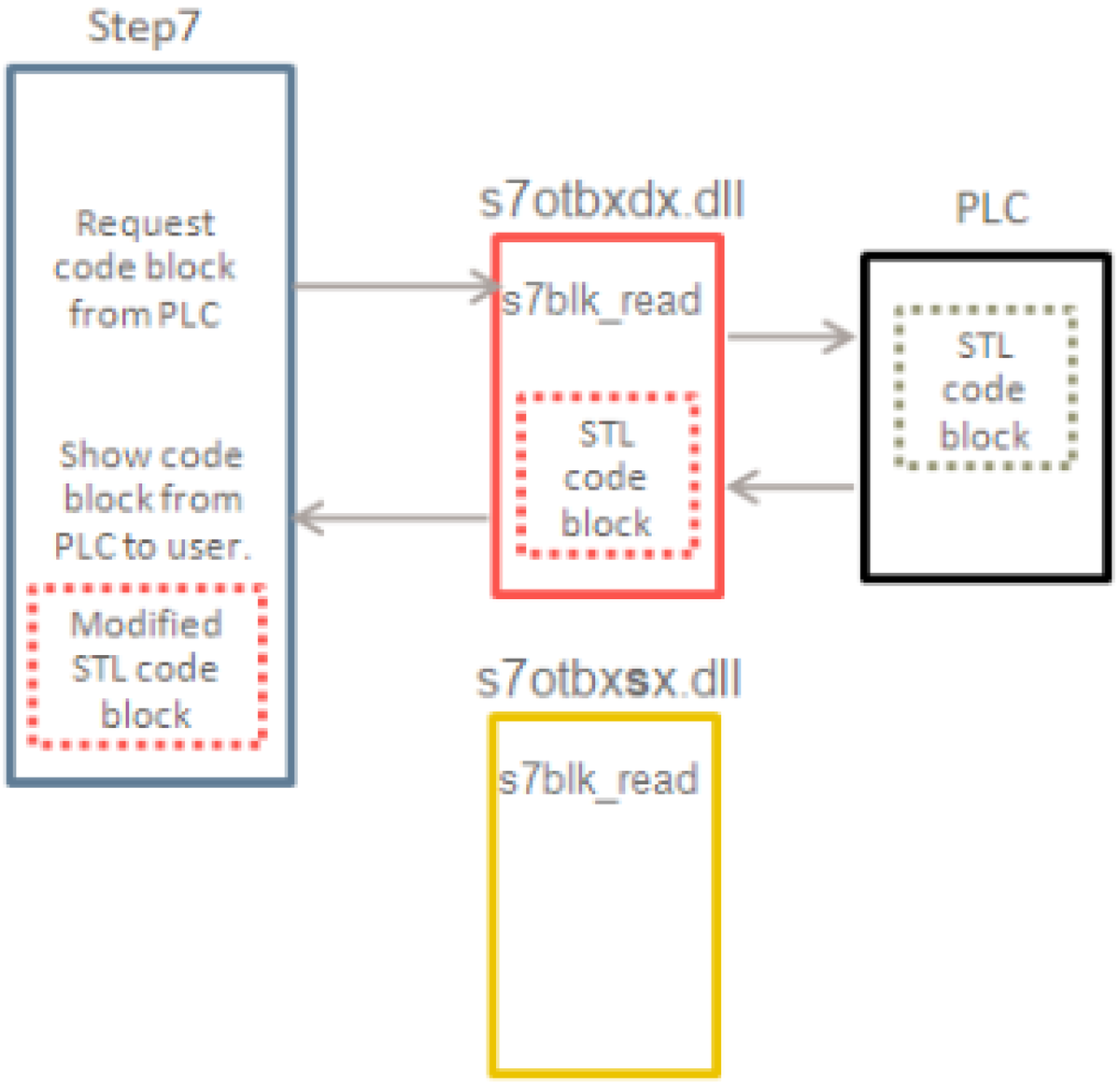
- Two command and control servers have been used in known samples:
  - mypremierfutbol[.]com
  - www[.]todaysfutbol[.]com

- Stuxnet can download additional files e.g backdoor or an updated version of Stuxnet

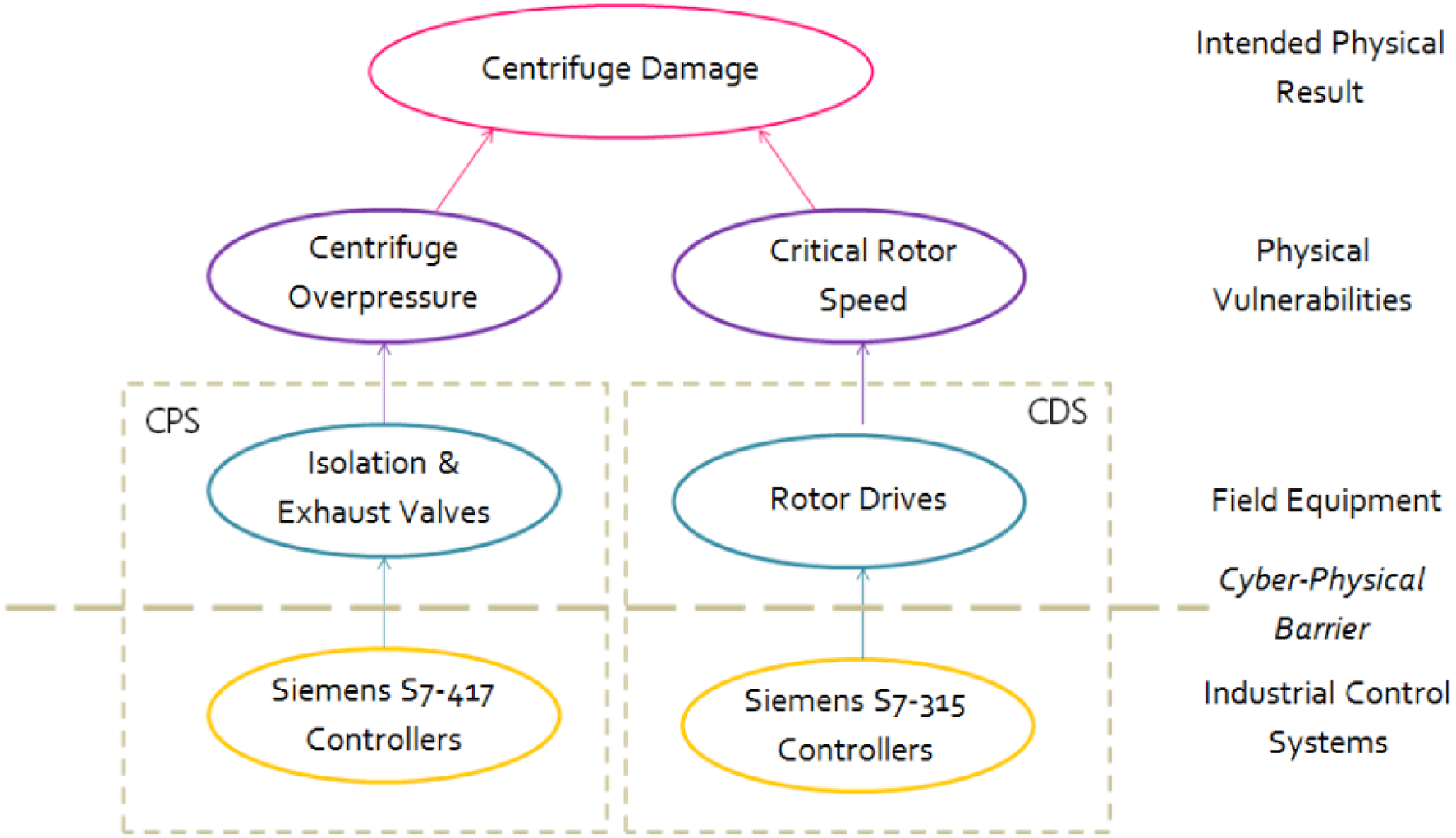
Modifying PLC Code



Modifying PLC Code



PLC Attack Code



Sandworm's Attacks

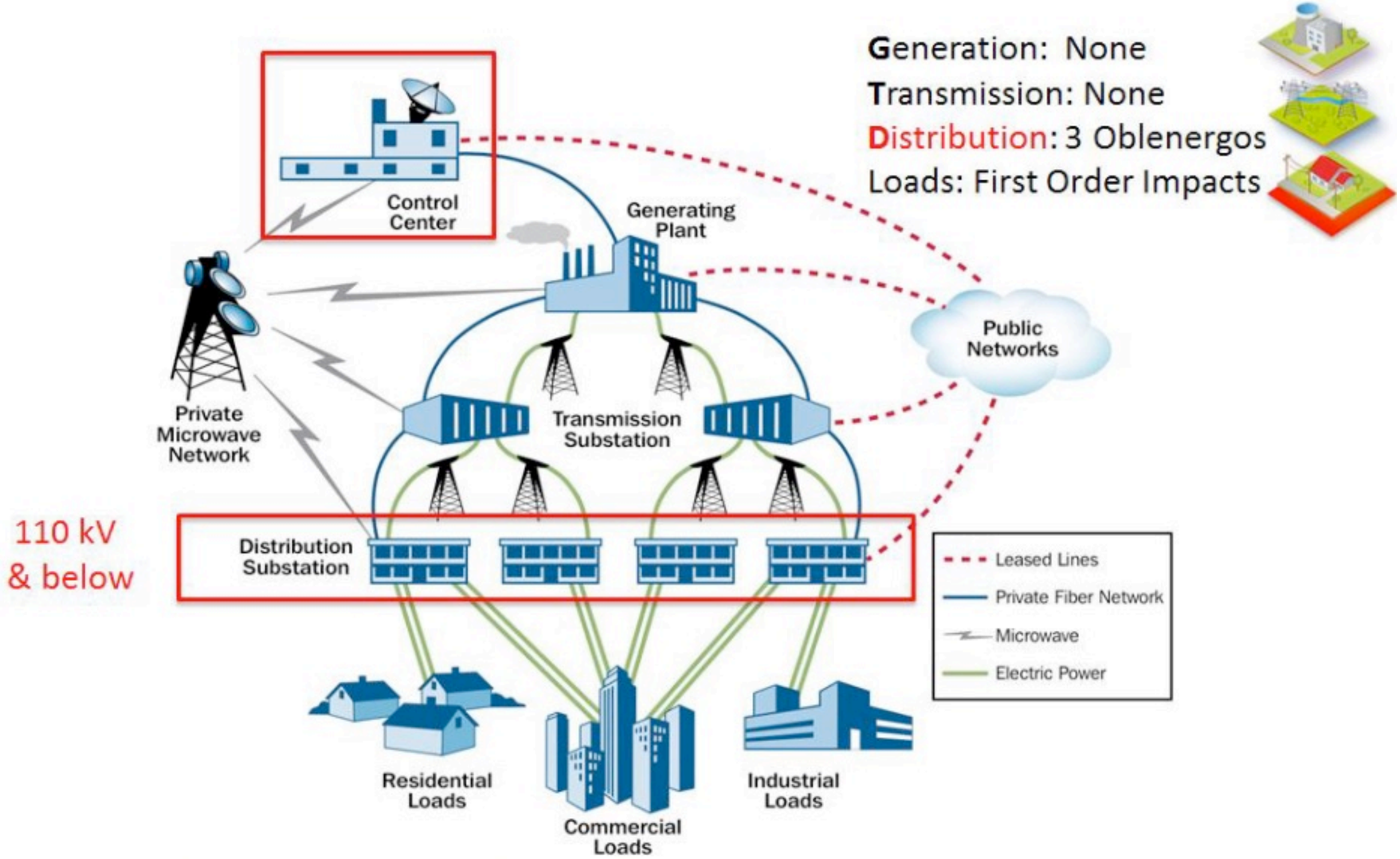
Sandworm's attacks

- 2015 – 2016 Ukrainian Government & Critical Infrastructure
- 2017 – Spearphishing campaign targeting French President Macron's "La République En Marche!" ("En Marche!") political party
- June 2017 - NotPetya Outbreak
- 2017 – Spearphishing campaign against PyeongChang Winter Olympics Hosts, Participants, Partners, and Attendees
- 2017 - PyeongChang Winter Olympics IT Systems (Olympic Destroyer)
- 2018 - Novick Poisoning Investigations
- 2018 – 2019 Georgian Companies and Government Entities

December 23 2015 attack to Ukrainian power grid

- Three electricity distribution companies in Ukraine were the target of a cyber attack that resulted in power outages
- The attackers opened breakers at 30 distribution substations in the capital city Kiev and western Ivano-Frankivsk region
- 225,000 customers were left without electricity from 1 to 6 hours
- The companies were able to restore service quickly

Electric System Overview



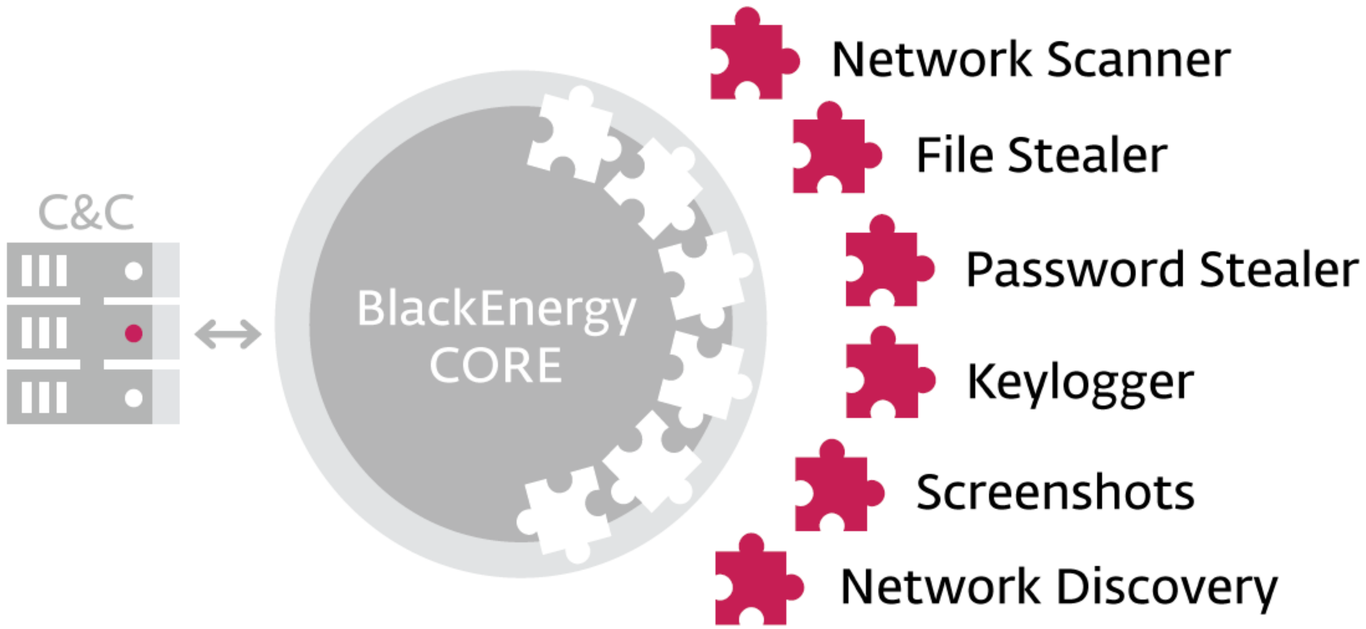
Source: Modification to the DHS Energy Sector-Specific Plan 2010

Attack Techniques

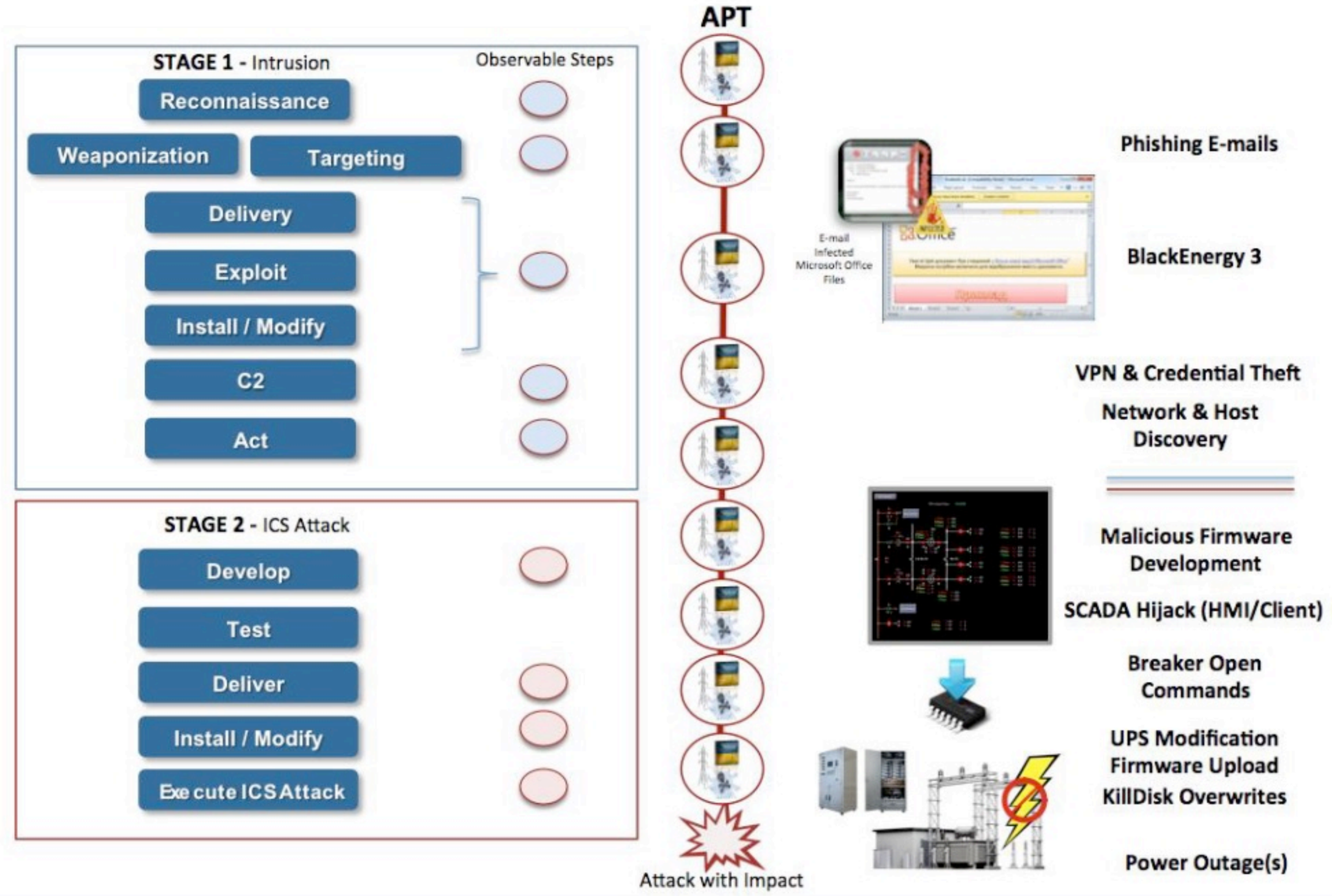
The Attack Methodology

- Emails sent to personnel in the administrative or IT network of the electricity companies
- When they open the attached documents the users were requested to enable macros in the document
- The result was to install Black Energy 3 on the victim machines
- **BlackEnergy 3 malware** connected to command and control (C2) IP addresses to enable communication by the adversary with the malware and the infected systems
- Installing malicious software identified as a modified or customized **KillDisk** across the environment
- KillDisk made the Windows systems inoperable by **manipulating or deleting the master boot record**, but on other systems it just deleted logs and system events
- They also leveraged a remote telephonic DoS on the energy company's call center with thousands of calls to ensure that impacted customers could not report outages

BlackEnergy3



The Attack Cyber Kill Chain



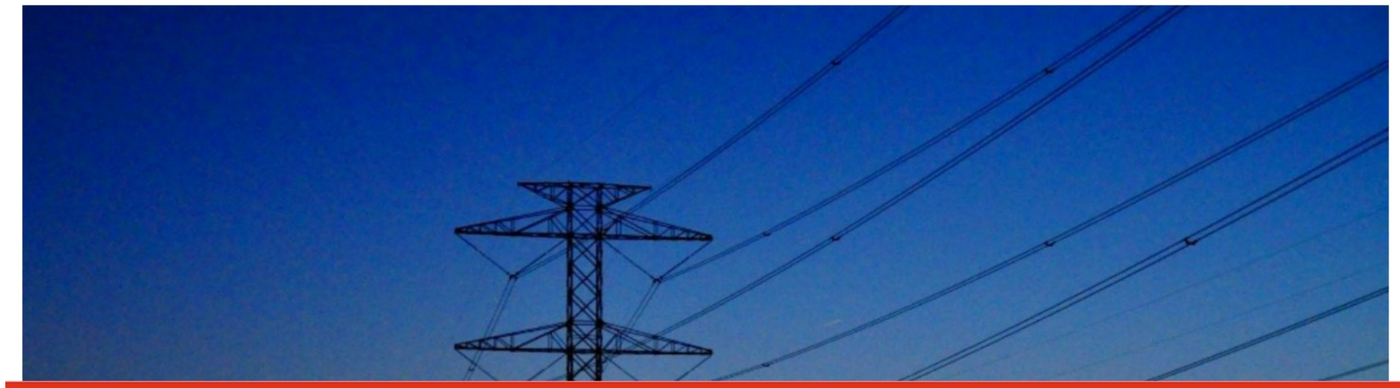
The second attack

The Ukrainian Power Grid Was Hacked Again

KZ

KIM ZETTER

Jan 10 2017, 3:07pm



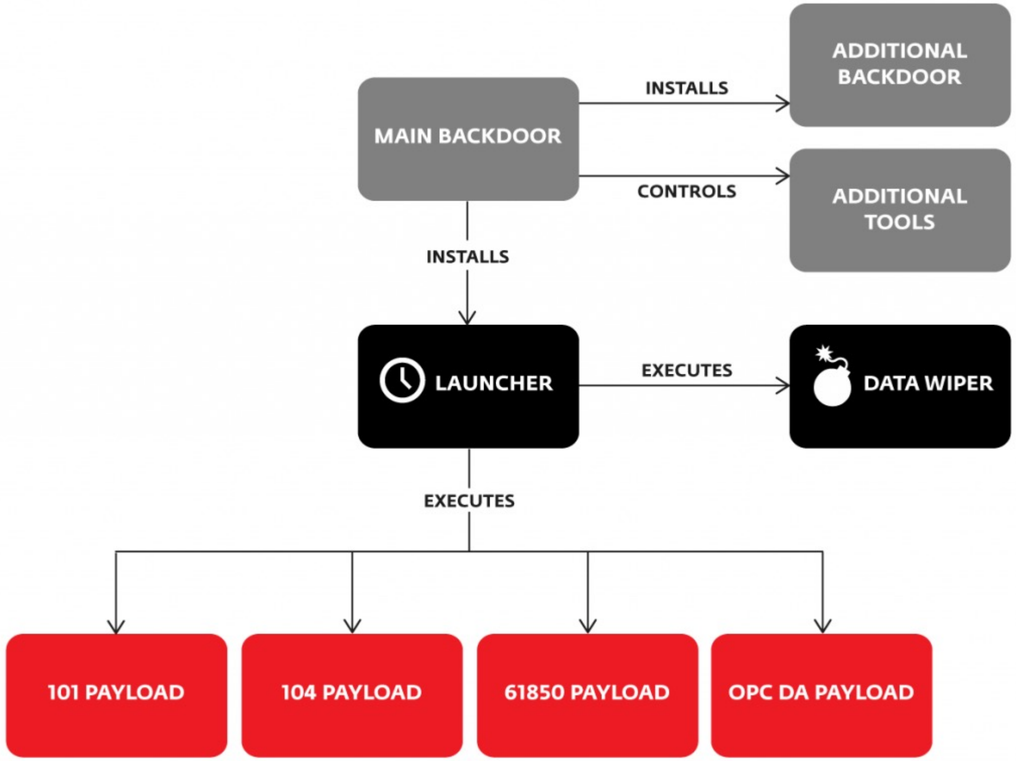
December 17th 2016 Attack

- A single transmission substation in northern Kiev lost power
- The blackout lasted just 1 hour
- It started with the spearphishing campaign in the summer of July 2016
- Sandworm was able to automate the control of the circuit breakers without compromising operators workstations
- The malware used was more sophisticated and targeted for ICS

Industroyer

- Sophisticated piece of malware designed to disrupt the working processes of industrial control systems (ICS), specifically industrial control systems used in electrical substations
- Implements the following communication protocols commonly used in ICS
  - IEC 60870-5-101 (aka IEC 101)
  - IEC 60870-5-104 (aka IEC 104)
  - IEC 61850
  - OLE for Process Control Data Access (OPC DA)
- Implements DDOS against protection relays, specifically the *Siemens SIPROTEC* range

Industroyer structure and functionalities



NotPetya

On June 27th 2017 a major ransomware attack affected different organizations around the world

- Ukraine's central bank, state telecom, municipal metro, and Kiev's Boryspil Airport
- Danish shipping company Maersk
- US pharmaceutical company Merck, a Pittsburgh-area hospital, and the US offices of law firm DLA Piper

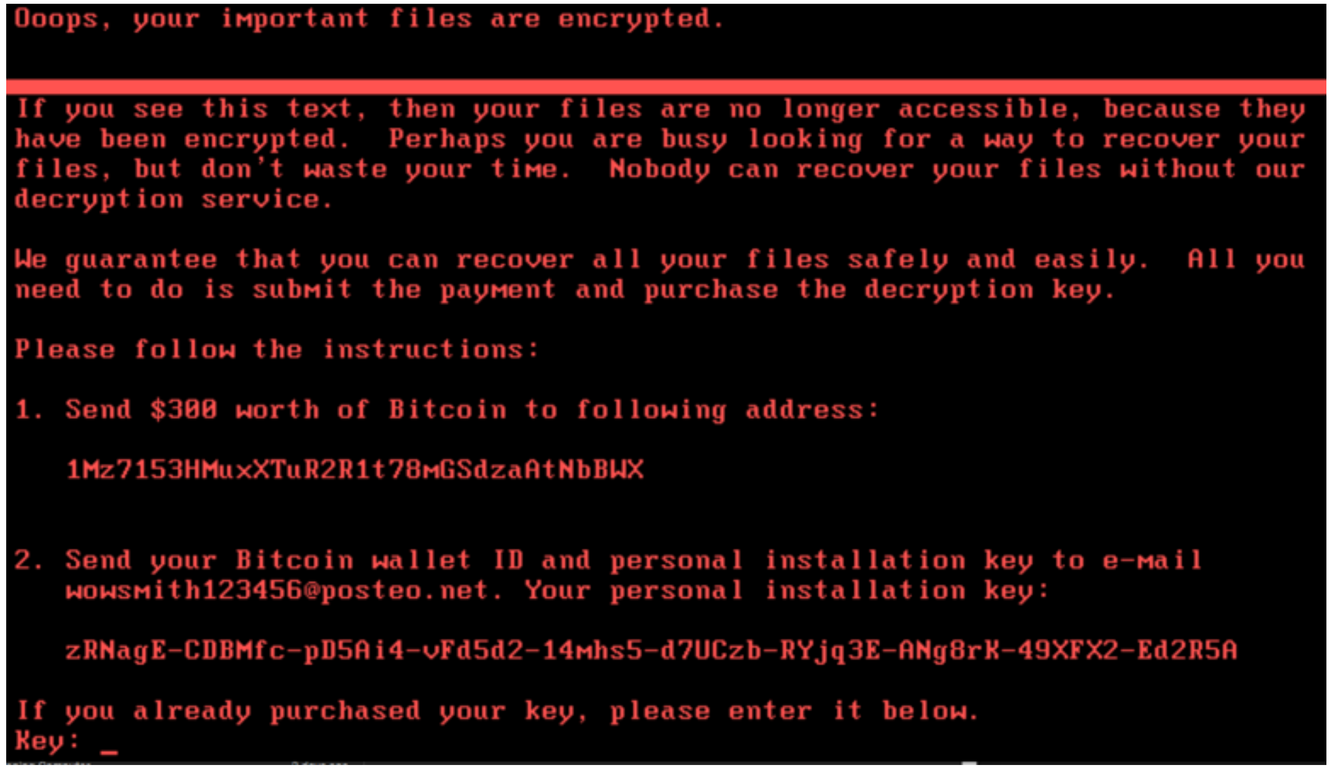
Not Petya key functionalities

- Delivered as a M.E.Doc tax account software update
  - Reroute traffic from the computers updating M.E.Doc from the Update Server to another server locate in France which delivered the malware
- Once downloaded on a machine it search for other hosts on the local network to infect
  - To spread uses EternalBlue and EternalRomance exploits
- Encrypts files and drives with AES 128
- Publish ransom note asking for $300 in bitcoins
  - Use same bitcoin address for all infections
  - Asked to send email to confirm the payment
- Compromise most hosts on local network in 2 hours

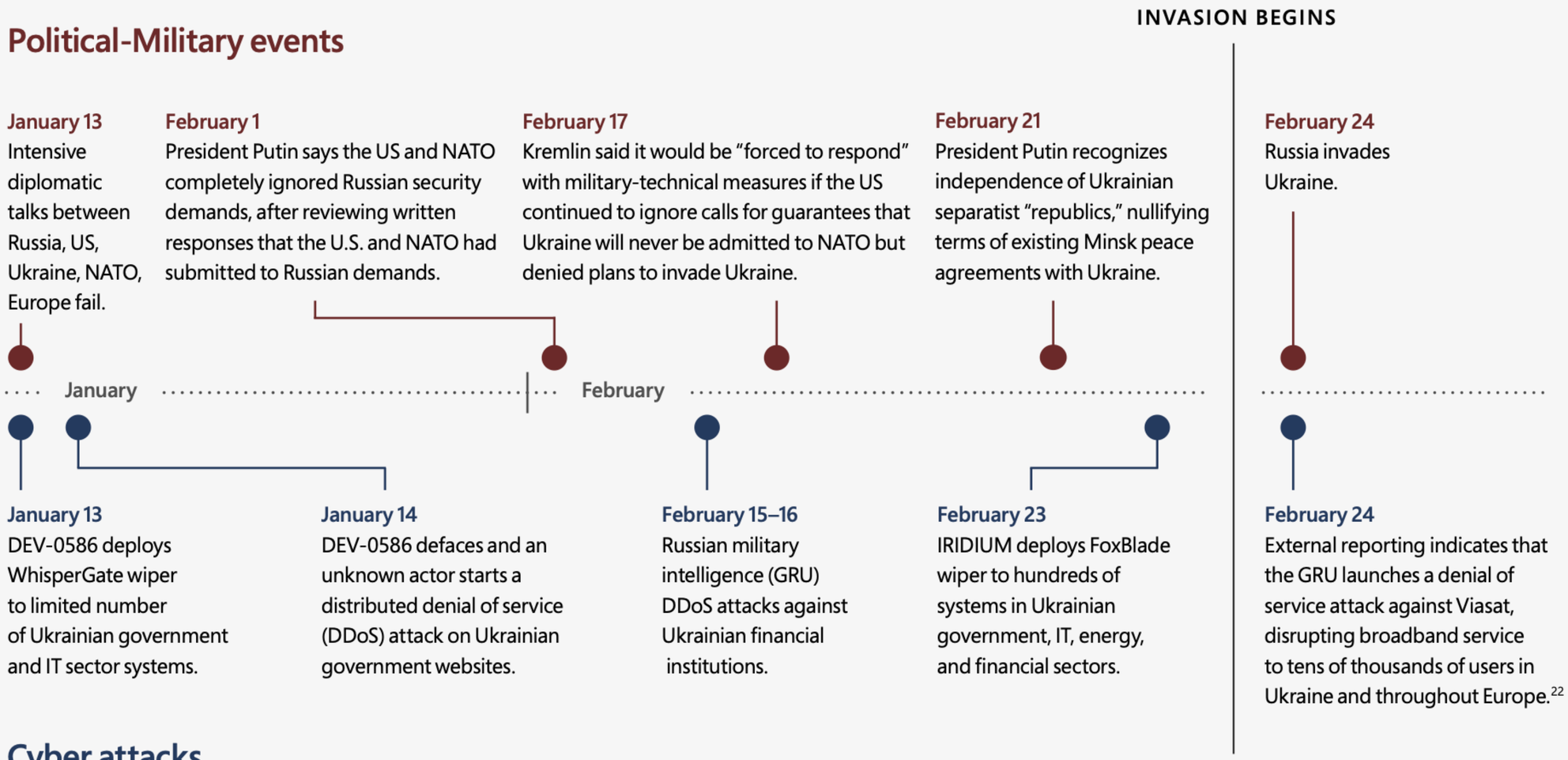
Sabotage vs Ransom

File Encryption

- Random Key pair per drive
- Victim ID
  - Random string
- No method for communicating key



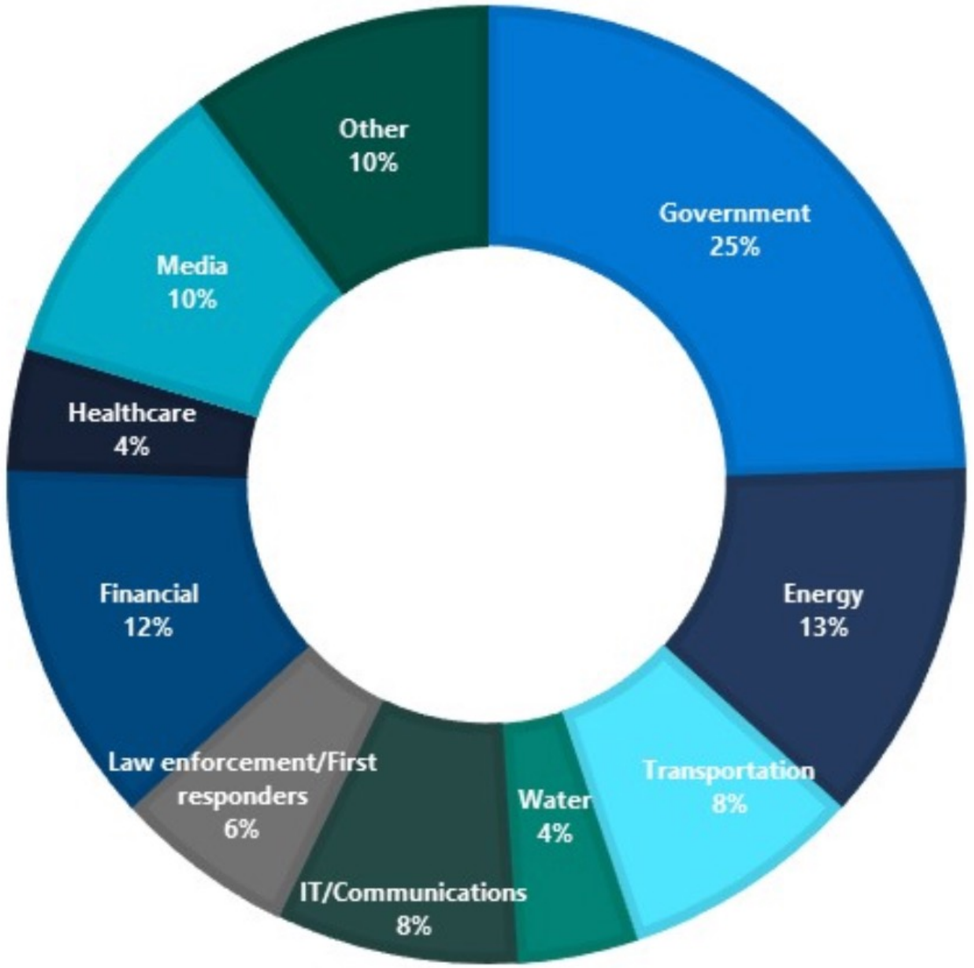
Timeline of Attacks before the Invasion of Ukraine



Destructive Attacks against Ukraine After the Invasion

Week 1 (February 23-March 2)	Destructive Malware: **FoxBlade, Lasainraw (IsaacWiper), DesertBlade, malicious use of SecureDelete utility** Number of Destructive Incidents: **22**
Week 2 (March 3-9)	Distructive Malware: **none** Number of Destructive Incidents: **0**
Week 3 (March 10-16)	Destructive Malware: **FoxBlade, malicious use of SecureDelete utility** Number of Destructive Incidents: **4**
Week 4 (March 17-23)	Destructive Malware: **DesertBlade, FiberLake, SonicVote, malicious use of SecureDelete utility** Number of Destructive Incidents: **6**
Week 5 (March 24-30)	Destructive Malware: **FoxBlade, SonicVote, malicious use of SecureDelete utility** Number of Destructive Incidents: **3**
Week 6 and beyond (March 31 – April 8)	Destructive Malware: **CaddyWiper, Industroyer 2.0** Number of Destructive Incidents **2**

Targets of Destructive Attacks



Viasat Attack

Russian military behind hack of satellite communication devices in Ukraine at war's outset, U.S. officials say

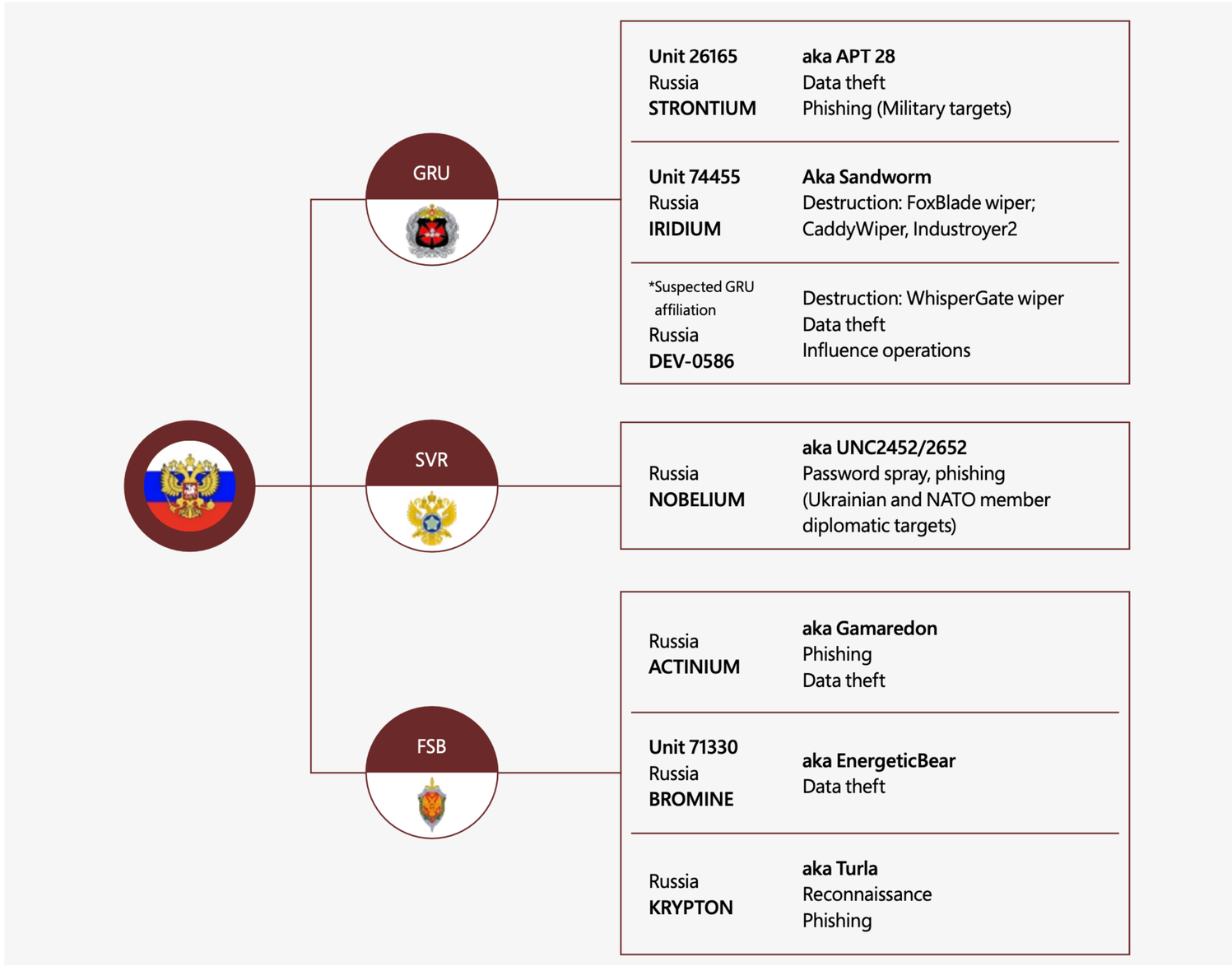
By Ellen Nakashima

March 24, 2022 at 10:25 p.m. EDT

MOST READ NATIONAL SECURITY >

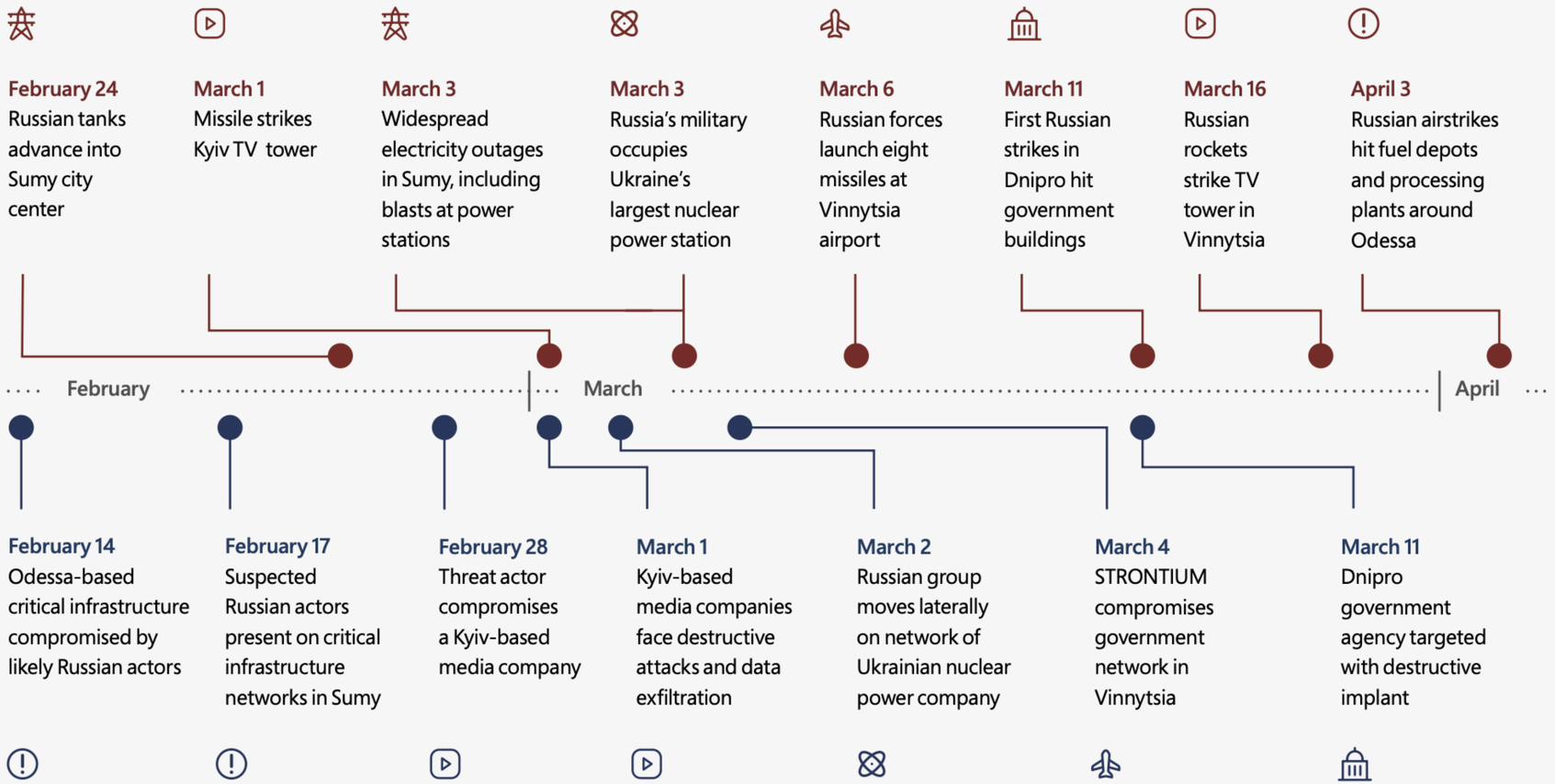
1 A novel defense in Trump's Georgia case: The 2020 election

Actors Involved



Post-invasion attacks

Military strikes



Cyber intrusions or attacks

Legend:

- Critical Infrastructure
- Electrical Infrastructure
- Nuclear Energy
- Transportation
- Media
- Government

Influence Operations against Ukraine

Dmytro Kuleba
@DmytroKuleba
Ukraine government official

The manic obsession with which various Russian officials fantasize about non-existent biological or chemical weapons or hazards in Ukraine is deeply troubling and may actually point at Russia preparing another horrific false flag operation. This tweet is for the record.

4:35 PM · Mar 10, 2022 · Twitter for iPhone

9,082 Retweets **461** Quote Tweets **27.8K** Likes

Ukraine destroys five bot farms that were spreading 'panic' among citizens

Over 100,000 fake accounts were allegedly used to spread misinformation about Russia's invasion.

Written by **Charlie Osborne,** Contributing Writer

March 29, 2022 at 4:09 a.m. PT

Influence Operations against Ukraine citizens

Наше урядове капітал-шоу у світлі останніх подій остаточно наплювало на совість та мораль. Марно балакаючих лицемірних пик, як Арестович, слухати вже не можливо. Та в цих блядських російських свинях більше порядності, ніж в наших придворних блазнях. Вони думають, що ми тут у Маріуполі красуємося перед камерами, підбираючи охуенні ракурси? Покидьки, блять! Ці "патріоти" нас просто залишили в цьому пеклі щоб ми здохли! Я пишаюсь, що ми с побратимами готові віддати свої життя за ради нашої мети. Нас таких не одна сотня, і ми готові змішати з гівном солодкуватих покидьків цієї клоунської зграї, поки самі не станемо двохсотими, бо їх зраду може змити тільки їх загибель. І нехай хоч хтось наважиться нам перешкодити, влаштуємо їм зустріч з чортами.

Зараз, я звертаюся особисто до Вас, [redacted]. Якщо у вашій душі є хоч крапля українського патріотизму, Ви зобов'язані не дозволити нашій спільній мрії розчинитися у брехні та пропаганді цих лицемірних блазнів. Я закликаю Вас виконати національний обов'язок, відстояти право називатися українським народом і покінчити з цією зграєю безхребетних тварин. Разом Ми-Сила! Слава Нації! Смерть ворогам! Слава Україні! Україна по над усе!

the light of recent events, our government capital has finally spat on conscience and morality. . . If there is even a drop of Ukrainian patriotism in your soul, you are obliged not to allow our common dream to dissolve into lies and propaganda of these hypocritical clowns. I urge you to fulfill your national duty, to defend the right to be called the Ukrainian people and to put an end to this pack of invertebrates.

Influence Operations against other NATO members

With the help of the Greens: The USA is planning to destroy the German economy

The fact that the USA wants to destroy the German economy is considered a conspiracy theory and Russian propaganda, but it is obvious. Now a very interesting document confirms this.

Resources

- E. Luiijf, B. J. Paske, “Cyber Security of Industrial Control Systems”, 2015
- K. Stouffer, J. Falco, K. Kent, K. “Guide to Industrial Control Systems (ICS) Security Recommendations of the National Institute of Standards and Technology”, NIST Special Publication, vol. 800, 2008
- J. Andress, S. Winterfield, “Cyber Warfare: Techniques, Tactics and Tools for Security Practitioners”, 2014
- Michael J. Assante and Robert M. Lee. The Industrial Control Systems Cyber Kill Chain, 2015.

Resources

- Symantec, W32.Stuxnet Dossier, February 2011.
- Ralph Langner, To Kill a Centrifuge.
- SANS ICS, Analysis of the Cyber Attack on the Ukrainian Power Grid.
- BlackEnergy APT Attacks in Ukraine employ spearphishing with Word documents: https://securelist.com/blackenergy-apt-attacks-in-ukraine-employ-spearphishing- with-word-documents/73440/
- ESET report, WIN32/INDUSTROYER -A new threat for industrial control systems
- **A new ransomware attack is infecting airlines, banks, and utilities across Europe**

  https://www.theverge.com/2017/6/27/15879480/petrwrap-virus-ukraine-ransomware-attack-europe-wannacry

- Microsoft. An overview of Russia’s cyberattack activity in Ukraine.