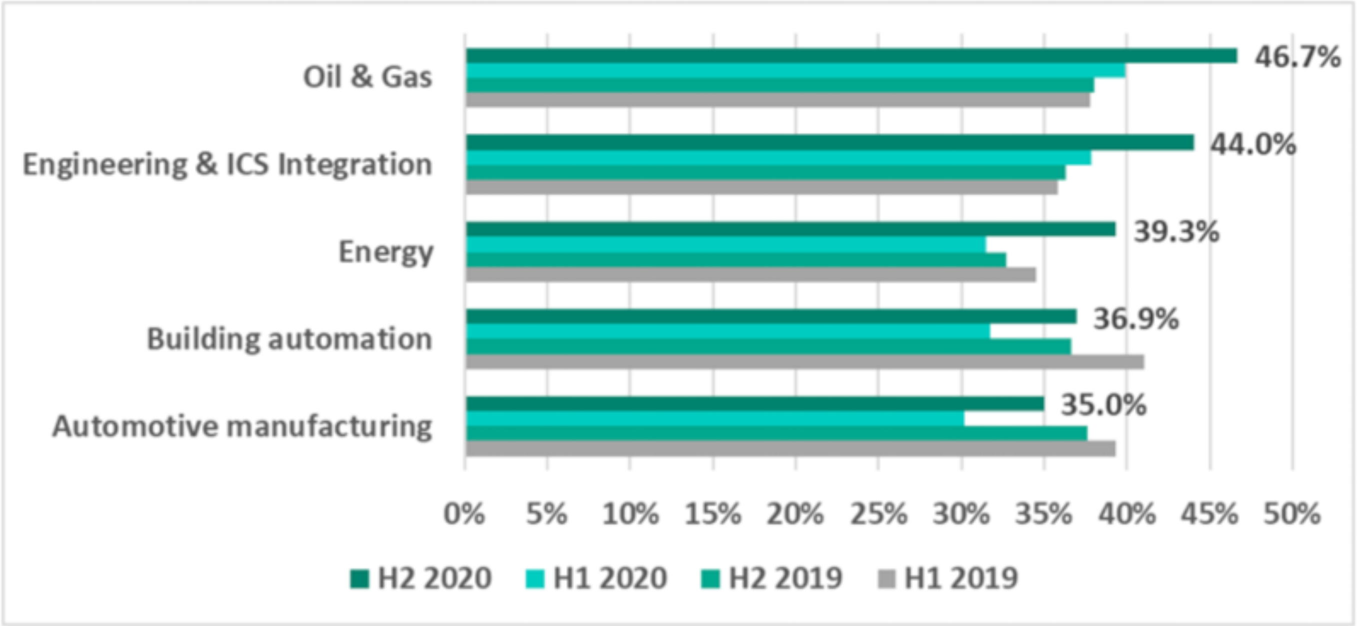
OT Threats

Threat Sources (US-Cert, CISA)

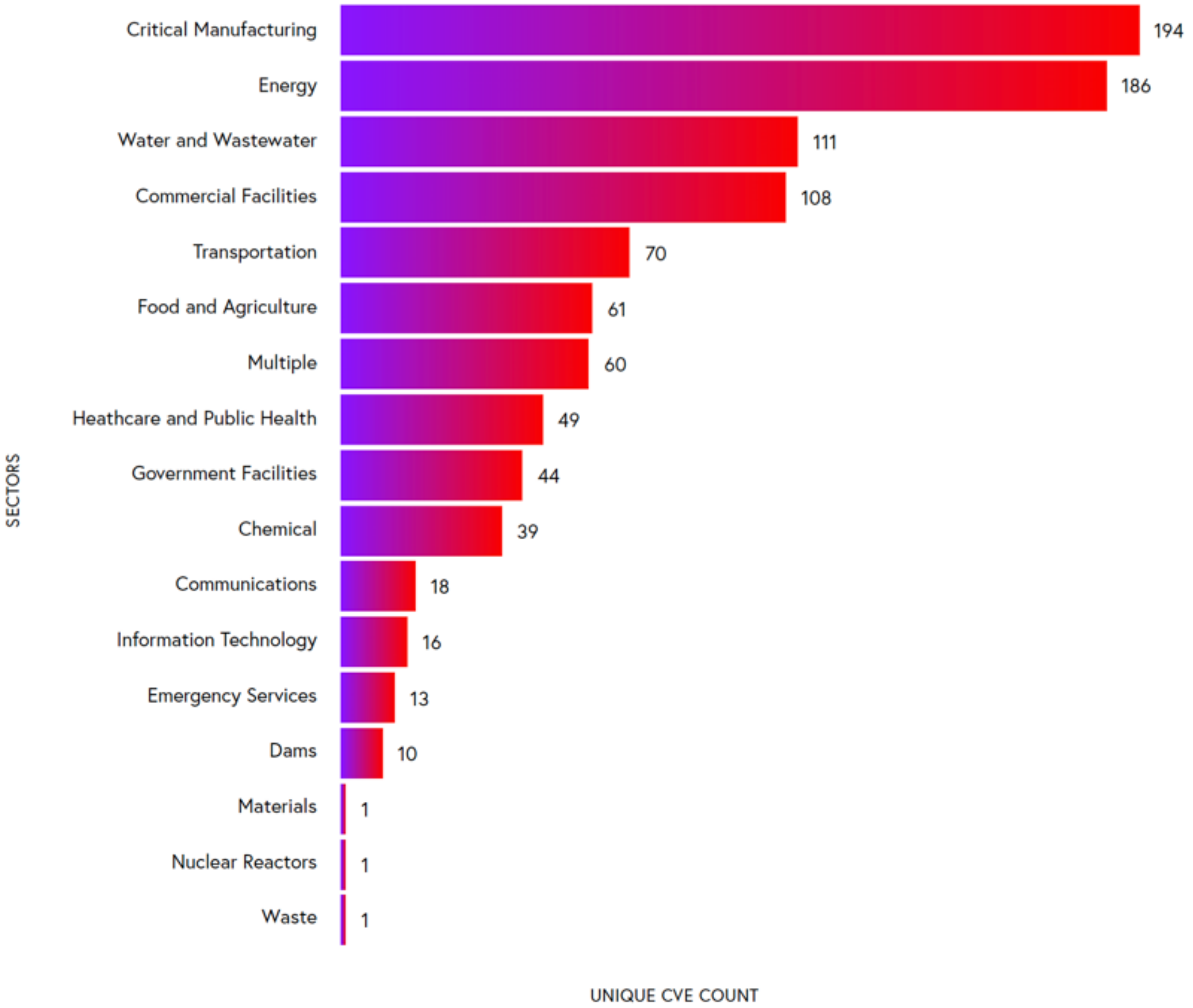
- National Governments
- Terrorists
- Industrial Spies and Organized Crime Groups
- Hacktivists
- Hackers

Increasing Level of Threats



Percentage of ICS computers on which malicious objects were blocked in selected industries

Kaspersky (2021)



Vulnerabilities per Sector

Claroty (2021, p19)

History of ICS Incidents (Hamsley & Fisher, 2018, p2-3)

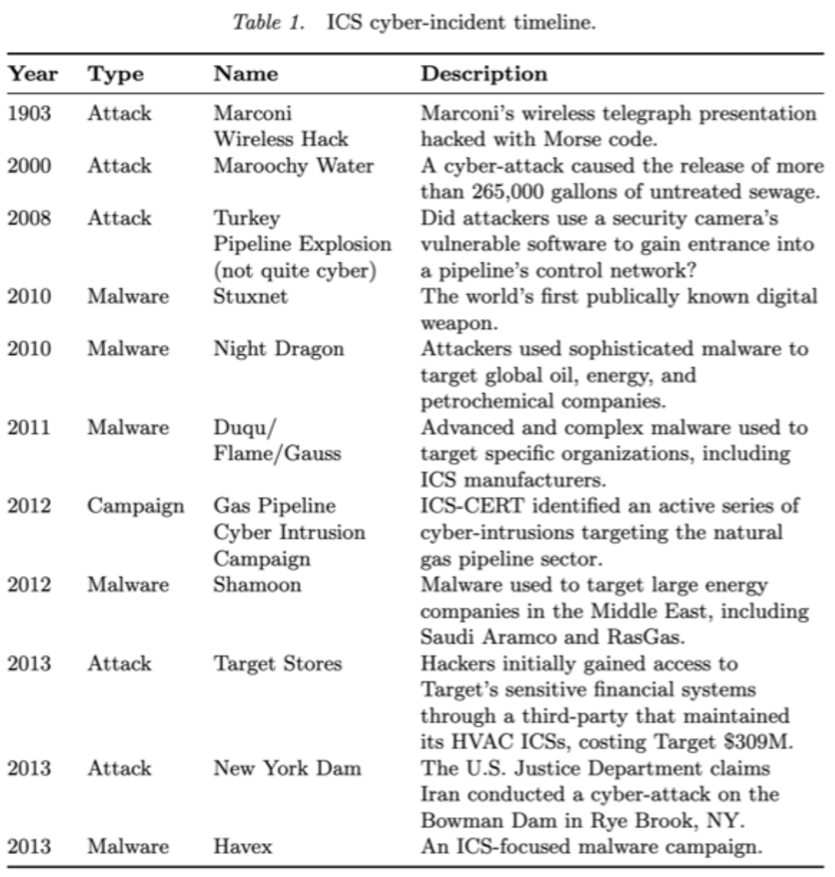


Table 1. ICS cyber-incident timeline.

Year	Type	Name	Description
1903	Attack	Marconi Wireless Hack	Marconi's wireless telegraph presentation hacked with Morse code.
2000	Attack	Maroochy Water	A cyber-attack caused the release of more than 265,000 gallons of untreated sewage.
2008	Attack	Turkey Pipeline Explosion (not quite cyber)	Did attackers use a security camera's vulnerable software to gain entrance into a pipeline's control network?
2010	Malware	Stuxnet	The world's first publically known digital weapon.
2010	Malware	Night Dragon	Attackers used sophisticated malware to target global oil, energy, and petrochemical companies.
2011	Malware	Duqu/ Flame/Gauss	Advanced and complex malware used to target specific organizations, including ICS manufacturers.
2012	Campaign	Gas Pipeline Cyber Intrusion Campaign	ICS-CERT identified an active series of cyber-intrusions targeting the natural gas pipeline sector.
2012	Malware	Shamoon	Malware used to target large energy companies in the Middle East, including Saudi Aramco and RasGas.
2013	Attack	Target Stores	Hackers initially gained access to Target's sensitive financial systems through a third-party that maintained its HVAC ICSs, costing Target $309M.
2013	Attack	New York Dam	The U.S. Justice Department claims Iran conducted a cyber-attack on the Bowman Dam in Rye Brook, NY.
2013	Malware	Havex	An ICS-focused malware campaign.

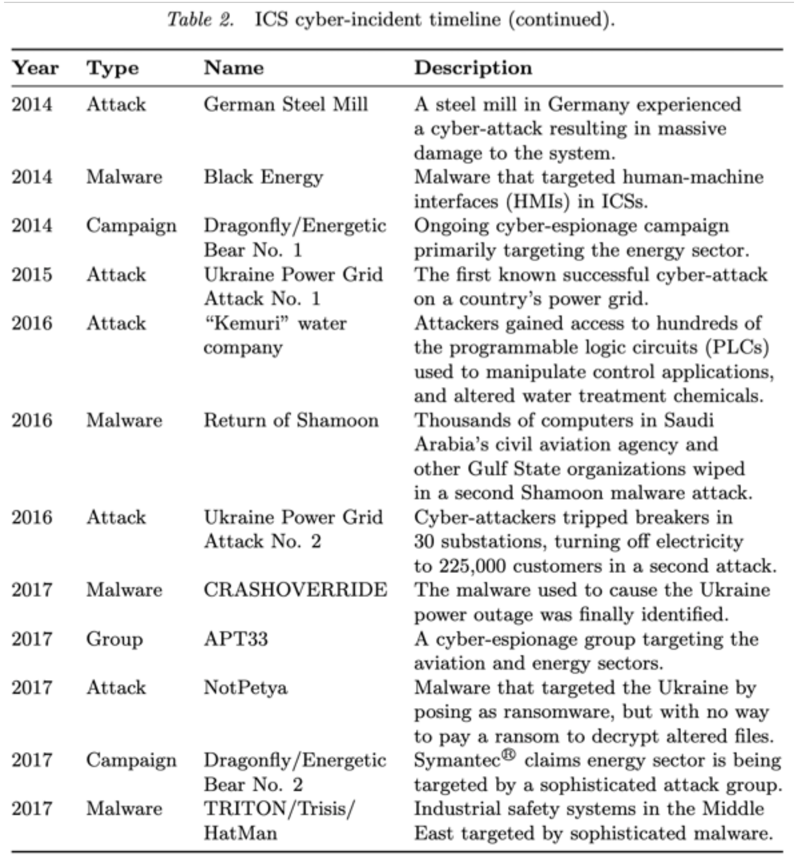
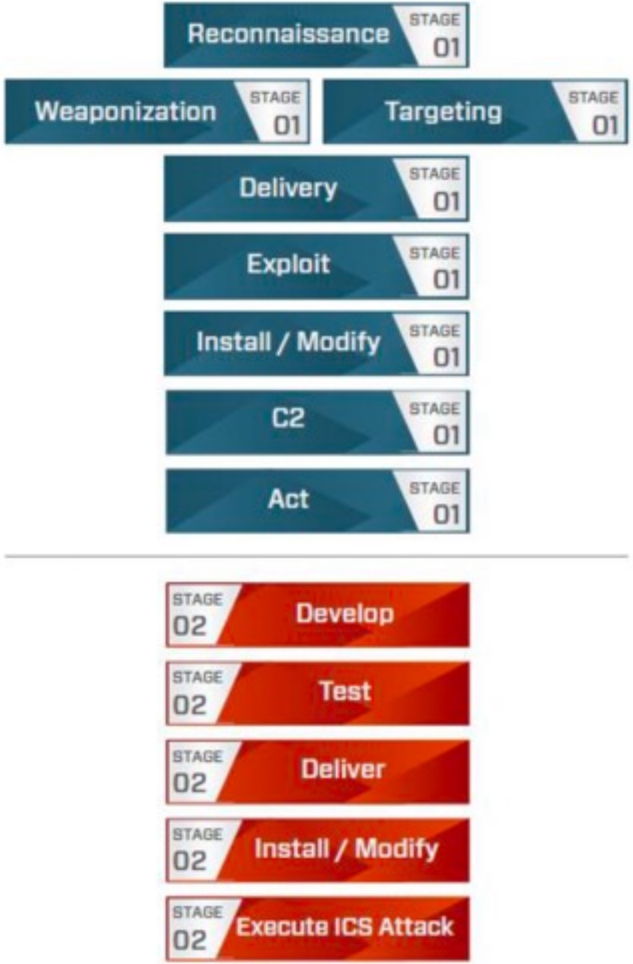


Table 2. ICS cyber-incident timeline (continued).

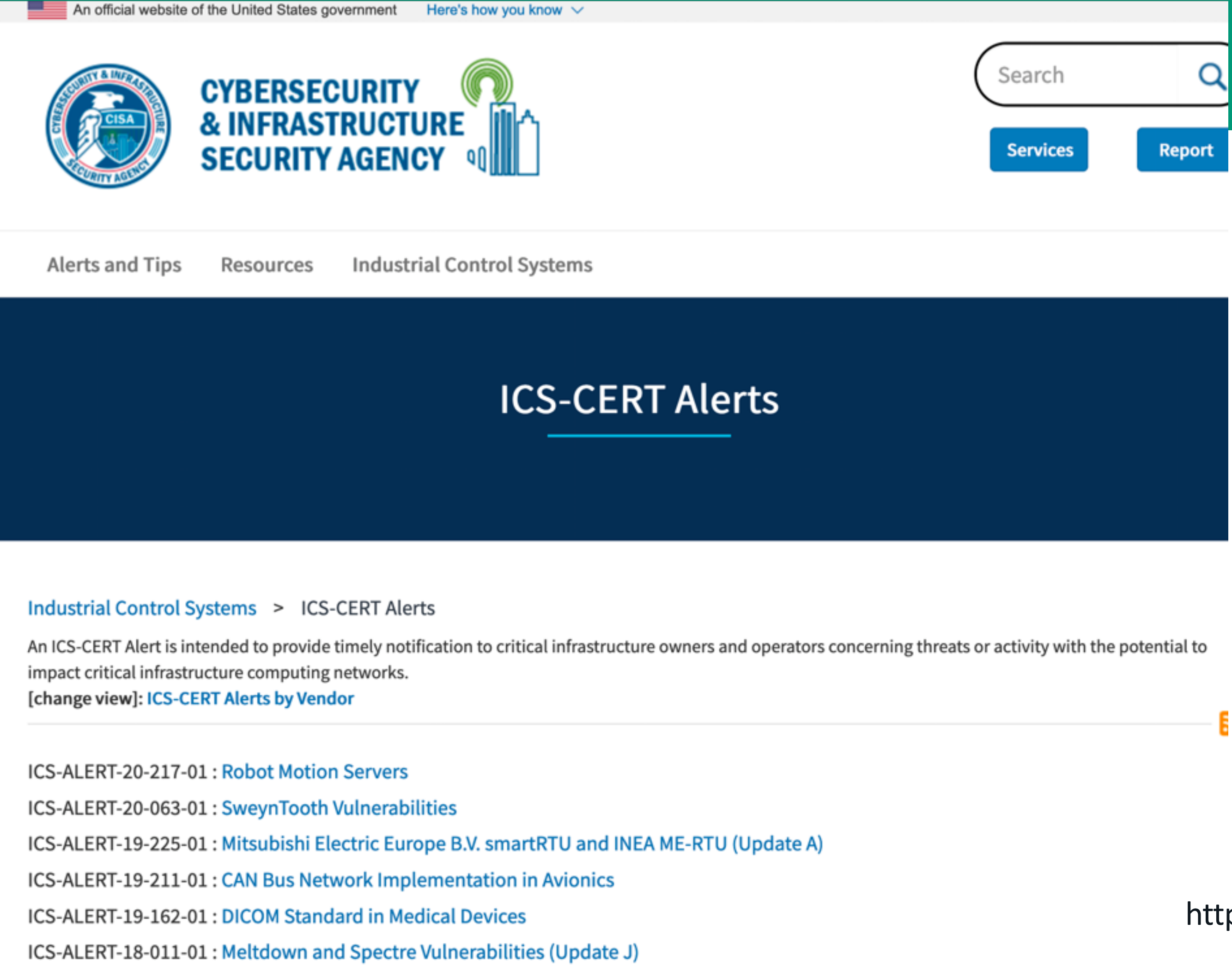
Year	Type	Name	Description
2014	Attack	German Steel Mill	A steel mill in Germany experienced a cyber-attack resulting in massive damage to the system.
2014	Malware	Black Energy	Malware that targeted human-machine interfaces (HMIs) in ICSs.
2014	Campaign	Dragonfly/Energetic Bear No. 1	Ongoing cyber-espionage campaign primarily targeting the energy sector.
2015	Attack	Ukraine Power Grid Attack No. 1	The first known successful cyber-attack on a country's power grid.
2016	Attack	"Kemuri" water company	Attackers gained access to hundreds of the programmable logic circuits (PLCs) used to manipulate control applications, and altered water treatment chemicals.
2016	Malware	Return of Shamoon	Thousands of computers in Saudi Arabia's civil aviation agency and other Gulf State organizations wiped in a second Shamoon malware attack.
2016	Attack	Ukraine Power Grid Attack No. 2	Cyber-attackers tripped breakers in 30 substations, turning off electricity to 225,000 customers in a second attack.
2017	Malware	CRASHOVERRIDE	The malware used to cause the Ukraine power outage was finally identified.
2017	Group	APT33	A cyber-espionage group targeting the aviation and energy sectors.
2017	Attack	NotPetya	Malware that targeted the Ukraine by posing as ransomware, but with no way to pay a ransom to decrypt altered files.
2017	Campaign	Dragonfly/Energetic Bear No. 2	Symantec® claims energy sector is being targeted by a sophisticated attack group.
2017	Malware	TRITON/Trisis/ HatMan	Industrial safety systems in the Middle East targeted by sophisticated malware.

ICS Cyber Kill Chain

Firgure 2: ICS Cyber Kill Chain



Slowik, (2019, p2)


An official website of the United States government
Here's how you know
CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY
Search
Services
Report
Alerts and Tips
Resources
Industrial Control Systems

ICS-CERT Alerts

Industrial Control Systems > ICS-CERT Alerts

An ICS-CERT Alert is intended to provide timely notification to critical infrastructure owners and operators concerning threats or activity with the potential to impact critical infrastructure computing networks.

[change view]: **ICS-CERT Alerts by Vendor**

ICS-ALERT-20-217-01 : Robot Motion Servers

ICS-ALERT-20-063-01 : SweynTooth Vulnerabilities

ICS-ALERT-19-225-01 : Mitsubishi Electric Europe B.V. smartRTU and INEA ME-RTU (Update A)

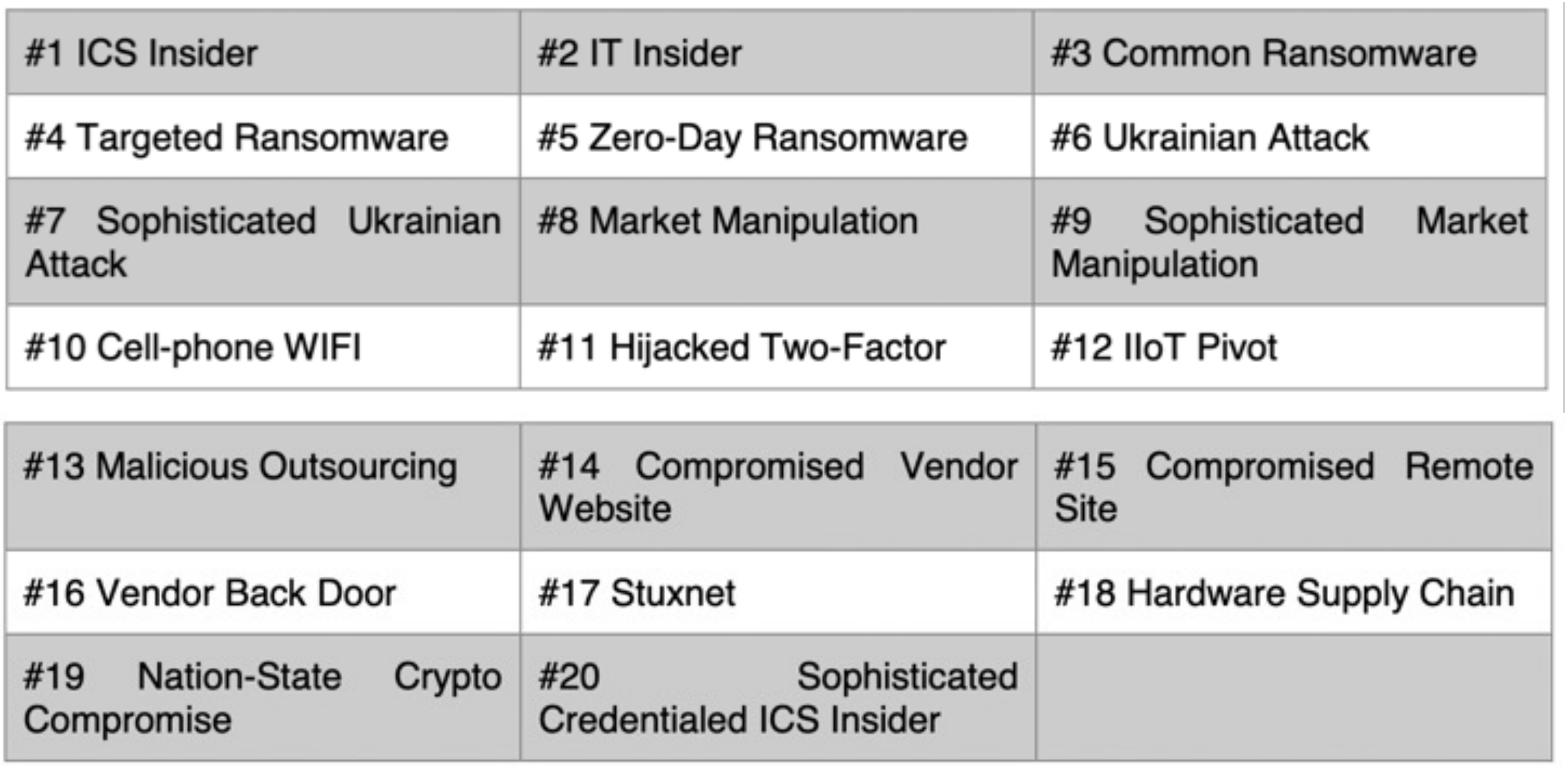
ICS-ALERT-19-211-01 : CAN Bus Network Implementation in Avionics

ICS-ALERT-19-162-01 : DICOM Standard in Medical Devices

ICS-ALERT-18-011-01 : Meltdown and Spectre Vulnerabilities (Update J)

https://us-cert.cisa.gov/ics/alerts

Top 20 ICS Cyber Attacks (Ginter, 2018)



#1 ICS Insider	#2 IT Insider	#3 Common Ransomware
#4 Targeted Ransomware	#5 Zero-Day Ransomware	#6 Ukrainian Attack
#7 Sophisticated Ukrainian Attack	#8 Market Manipulation	#9 Sophisticated Market Manipulation
#10 Cell-phone WIFI	#11 Hijacked Two-Factor	#12 IIoT Pivot
#13 Malicious Outsourcing	#14 Compromised Vendor Website	#15 Compromised Remote Site
#16 Vendor Back Door	#17 Stuxnet	#18 Hardware Supply Chain
#19 Nation-State Crypto Compromise	#20 Sophisticated Credentialed ICS Insider	