MANUFACTURING CYBER THREATS

SELENA LARSON, DRAGOS INC.

WHO AM I

SELENA LARSON

- Senior Cyber Threat Intelligence Analyst at Dragos.
- Hunting bad people trying to take down critical infrastructure.
- Helping ICS asset owners and operators stay safe and secure.

AGENDA

THREATS TO MANUFACTURING

Cyber risk to the manufacturing sector is increasing, led by disruptive cyberattacks impacting industrial processes, intrusions enabling information gathering and process information theft, and new activity from ICS-targeting adversaries.

THREATS
What are the biggest threats to the manufacturing sector?

OT DIGITAL TRANSFORMATION
What does this mean for cybersecurity?

DEFENSE
How can companies protect themselves?

ACTIVITY GROUPS

TARGETING MANUFACTURING

- Dragos publicly tracks five ICS activity groups targeting or demonstrating interest in targeting manufacturing.

ICS MALWARE

POTENTIAL FOR DISRUPTION

- TRISIS and CRASHOVERRIDE can interact with and disrupt industrial processes.
- It is possible adversaries will target manufacturing companies in the process of developing such malware, even if they are not the ultimate target.
- An adversary could theoretically leverage manufacturing operations as a “testing ground” for disruptive attacks targeting critical infrastructure, like electric utilities, if the same equipment is used.

RANSOMWARE

A SERIOUS THREAT

- EKANS and other ransomware represent a unique and specific risk to industrial operations not previously observed in ransomware operations.
- In 2020, the number of publicly reported ransomware attacks on manufacturing entities has more than tripled compared to 2019, based on data tracked by Dragos.
- Ransomware operators are increasingly incorporating data theft techniques into their campaigns to further ransom demands.

RANSOMWARE

A SERIOUS THREAT

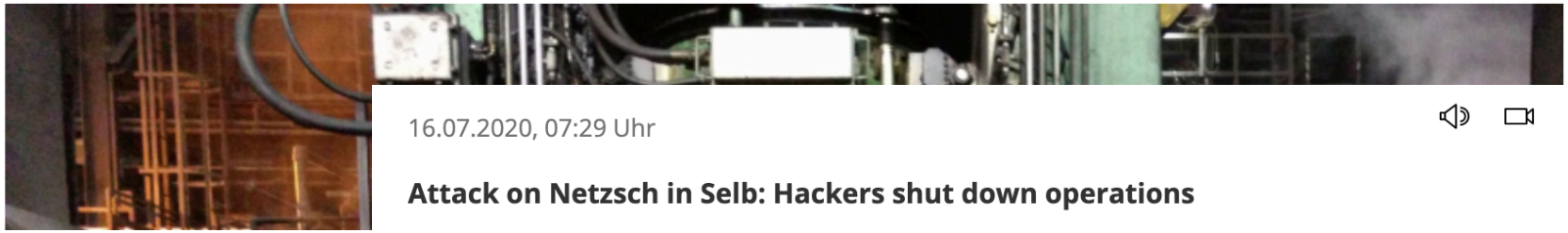
BUSINESS

Affco and meat runs hit by computer snag

Some meat deliveries didn't get through to Auckland and workers' pay was interrupted as freezing company Affco battled sudden IT issues. Jim Kayes reports

Evraz Steel shuts down Regina plant after continent-wide computer hack

Regina / 980 CJME
Evan Radford
Mar 5, 2020 6:25 AM



16.07.2020, 07:29 Uhr

Attack on Netzsch in Selb: Hackers shut down operations

The global mechanical engineering company Netzsch from Selb fell victim to a hacker attack. Large parts of the production stand still for days afterwards. The Central Office for Cybercrime of the Public Prosecutor's Office in Bamberg is investigating.

Hackers infiltrate computer systems at B.C. paper mills

Production has been impacted at 3 Paper Excellence Canada facilities

CBC News · Posted: Feb 24, 2020 2:00 PM PT | Last Updated: February 24

https://www.newsroom.co.nz/2020/05/05/1157253/affco-meat-supply-affected-by-it-issue
https://www.cbc.ca/news/canada/british-columbia/paper-excellence-canada-malware-infection-1.5474274
https://www.br.de/nachrichten/bayern/hacker-angriff-auf-netzsch-in-selb-unbekannte-fordern-loesegeld,S4tTZL4
https://www.cjme.com/2020/03/05/ransom-ware-attack-at-evraz-could-bring-layoffs-to-regina-plant/

INTERNET-EXPOSED ASSETS

USED FOR INITIAL ACCESS

- Industrial and networking assets exposed to the internet are a high risk for manufacturing that can facilitate initial access to a victim environment.

- Last year, 66 percent of IR cases involved adversaries directly accessing the ICS network from the internet, and 100 percent of organizations had routable network connections into their operational environments.

- Adversaries are quick to weaponize and exploit vulnerabilities in internet-facing services including Remote Desktop Protocol (RDP), VPN, and critical network infrastructure services including F5, Palo Alto Networks, Citrix, and Juniper network devices.

INTERNET-EXPOSED ASSETS

USED FOR INITIAL ACCESS

Home › Cyberwarfare

Hackers Knew How to Target PLCs in Israel Water Facility Attacks: Sources

By Eduard Kovacs on April 30, 2020

Sources told *SecurityWeek* that the attackers targeted programmable logic controllers (PLCs) used to control valves. The changes made to the PLC logic were valid, which indicates that the attackers knew exactly what they were doing.

The attack may have been discovered after the compromised PLCs caused suspicious valve changes, but it's unclear if the attackers were trying to cause damage by tampering with valves or if they made an error that led to their discovery.

https://www.securityweek.com/hackers-knew-how-target-plcs-israel-water-facility-attacks-sources

CASE STUDY

In March 2020, Dragos identified an intrusion at a North American entity aligned with PARISITE activity that leveraged a vulnerability in Citrix Netscaler Application Delivery Controller (ADC) for initial access. CVE-2019-19781 was first identified in December 2019. PARISITE is known for quickly incorporating publicly identified vulnerabilities into attack operations and has also exploited vulnerabilities in Virtual Private Network (VPN) services.

ICS VULNERABILITIES

LIKELY LIMITED ADVERSARY USE

- As of October 2020, Dragos researchers assessed and validated 108 advisories containing 262 vulnerabilities impacting industrial equipment found in manufacturing environments.

- Almost half of the advisories described a vulnerability that could cause a loss of view and/or loss of control within a compromised environment.

- Of the vulnerabilities impacting manufacturing industrial equipment, 70 percent require access to the victim network to exploit, 26 percent require an adversary to have access to the vulnerable device itself, and 8 percent require an adversary to be on the local area network to facilitate exploitation.

ICS VULNERABILITIES

LIKELY LIMITED ADVERSARY USE

- ICS vulnerabilities may not be useful to ransomware adversaries that generally would not have the experience to weaponize ICS vulnerabilities.
- Many of them are moot due to insecurity by default in some ICS equipment.
- ICS issues like default credentials, overly permissive fileshares and overly permissive local permissions could be useful to ransomware adversaries.

IP THEFT

OPERATIONAL DATA IS VALUABLE

- IP and theft of trade secrets related to process and automation functions can enable industrial organizations and interested states and governments to fast-track development.

- It can also support state sponsored espionage activities for political or national security efforts.

- Obtaining material specifications for products is likely not enough to replicate them. Adversaries may want to steal the algorithms, engineering designs, and programming specifications to replicate the entire production process, not just the material goods and services output.

CORONAVIRUS IMPACTS

Malicious Activity Targeting COVID-19 Research, Vaccine Development

Original release date: July 16, 2020

Print | Tweet | Send | Share

In response to malicious activity targeting COVID-19 research and vaccine development in the United States, United Kingdom (UK), and Canada, the Cybersecurity and Infrastructure Security Agency (CISA), UK's National Cyber Security Centre (NCSC), Canada's Communications Security Establishment (CSE), and the National Security Agency (NSA) released a Joint Cybersecurity Advisory to expose the threat. A malicious cyber actor is using a variety of tools and techniques to target organizations involved in COVID-19 research and vaccine development. Tools include SOREFANG, WELLMESS, and WELLMAIL malware

https://us-cert.cisa.gov/ncas/current-activity/2020/07/16/malicious-activity-targeting-covid-19-research-vaccine-development

https://www.bbc.com/news/technology-54642870

Tech

Dr Reddy's: Covid vaccine-maker suffers cyber-attack

By Joe Tidy
Cyber reporter

22 October

Coronavirus pandemic

THIRD-PARTY/SUPPLY CHAIN

LEVERAGING TRUSTED CONNECTIONS

- Contractors, vendors, etc. can have direct access to operational environments for activities like updates, inspections, or new equipment installations.

- Enterprise Resource Planning (ERP) providers are potential infection vectors that could bridge the IT and OT gap if proper segmentation and security are not in place. ERP services require access to operations assets like data historians to monitor and store information relating to production, supply chain, inventory, and safety.

THIRD-PARTY/SUPPLY CHAIN

LEVERAGING TRUSTED CONNECTIONS

- Manufacturing entities are part of a global supply chain supporting multiple other industries, making them a target for adversaries targeting industries like electric utility or pharmaceutical. Some manufacturing companies' activities stretch into multiple industrial verticals.

AUTOS MARCH 12, 2020 / 10:54 AM / UPDATED 8 MONTHS AGO

Volkswagen plans to tap electric car batteries to compete with power firms

By Reuters Staff 2 MIN READ

https://www.reuters.com/article/us-volkswagen-electric-energy/volkswagen-plans-to-tap-electric-car-batteries-to-compete-with-power-firms-idUSKBN20Z2D5

NETWORK SEGMENTATION

FLAT NETWORKS COMMON

- Major issues include: Interconnections between IT and OT via poor network segmentation, maintenance interconnections between environments, and a lack of access restrictions.

- If segmentation exists between enterprise and operations leveraging jump hosts and access restrictions, manufacturing facilities often leverage the same Wide Area Network (WAN) connection across all manufacturing plants.

WI-FI CONNECTIONS

"SMART" FACTORIES AND OTHER RISKS

- Operators are adopting Wi-Fi enabled machine tools and diagnostic equipment that enable workers to move around plants and factories without tripping over power cords.
- Internet connected tools connect to historian databases for quality assurance, regulatory, and logistics purposes, among others.
- Tools may be connected to enterprise or operations resources and used as network access points or targeted in an attack meant to disrupt operations.

WI-FI CONNECTIONS

"SMART" FACTORIES AND OTHER RISKS

- Logistics applications and services enable moving parts of manufacturing assets – such as vehicles, drivers, and goods – to communicate and interact with static assets like warehouses or human resources.

- Employees and contractors use mobile and desktop hardware with Wi-Fi connections to use applications and services, regularly access enterprise, and in some cases, access operations networks.

LACK OF VISIBILITY

BUILDING A HOUSE WITHOUT A FOUNDATION

- Connections are increasing, but a lack of visibility into processes, assets, and communications remain.
- 81 percent of organizations Dragos worked with had extremely limited or no visibility into the ICS/OT network.
- Observations from IR engagements found no instances of security and process data aggregation for incident analysis requiring manual retrieval of logs and distributed analysis.

DEFENSIVE RECOMMENDATIONS

MITRE ATT&CK FOR ICS

- Look for threat behaviors and known Tactics, Techniques, and Procedures (TTPs) that adversaries targeting manufacturing use, like those mapped to ATT&CK for ICS.

Initial Access	Execution	Persistence	Evasion	Discovery	Lateral Movement	Collection	Command and Control	Inhibit Response Function	Impair Process Control	Impact
Data Historian Compromise	Change Program State	Hooking	Exploitation for Evasion	Control Device Identification	Default Credentials	Automated Collection	Commonly Used Port	Activate Firmware Update Mode	Brute Force I/O	Damage to Property
Drive-by Compromise	Command-Line Interface	Module Firmware	Indicator Removal on Host	I/O Module Discovery	Exploitation of Remote Services	Data from Information Repositories	Connection Proxy	Alarm Suppression	Change Program State	Denial of Control
Engineering Workstation Compromise	Execution through API	Program Download	Masquerading	Network Connection Enumeration	External Remote Services	Detect Operating Mode	Standard Application Layer Protocol	Block Command Message	Masquerading	Denial of View
Exploit Public-Facing Application	Graphical User Interface	Project File Infection	Rogue Master Device	Network Service Scanning	Program Organization Units	Detect Program State		Block Reporting Message	Modify Control Logic	Loss of Availability
External Remote Services	Man in the Middle	System Firmware	Rootkit	Network Sniffing	Remote File Copy	I/O Image		Block Serial COM	Modify Parameter	Loss of Control
Internet Accessible Device	Program Organization Units	Valid Accounts	Spoof Reporting Message	Remote System Discovery	Valid Accounts	Location Identification		Data Destruction	Module Firmware	Loss of Productivity and Revenue
Replication Through Removable Media	Project File Infection		Utilize/Change Operating Mode	Serial Connection Enumeration		Monitor Process State		Denial of Service	Program Download	Loss of Safety
Spearphishing Attachment	Scripting					Point & Tag Identification		Device Restart/Shutdown	Rogue Master Device	Loss of View
Supply Chain Compromise	User Execution					Program Upload		Manipulate I/O Image	Service Stop	Manipulation of Control
Wireless Compromise						Role Identification		Modify Alarm Settings	Spoof Reporting Message	Manipulation of View
						Screen Capture		Modify Control Logic	Unauthorized Command Message	Theft of Operational Information
								Program Download		
								Rootkit		
								System Firmware		
								Utilize/Change Operating Mode		

DEFENSIVE RECOMMENDATIONS

BUILDING RESILIENCE

- Ensure an understanding of network interdependencies and conduct crown jewel analysis to identify potential weaknesses that could disrupt business continuity.

- Ensure networks are segmented to the greatest extent possible. Ensure emergency response plans are well-documented to detail segmentation efforts in case of emergency. For example, implement firewall rules to segment critical ICS components from the network that can be activated and deactivated depending on the safety and security of the environment, and any potential malicious activity.

DEFENSIVE RECOMMENDATIONS

BUILDING RESILIENCE

- Services and equipment that are not needed for real-time communications or direct access to operations should be virtualized. This can improve vulnerability management and enable improved security for interdependencies.

- Isolate equipment and services used for Building Access Control (BAC) and Heating, Ventilation, and Air Conditioning (HVAC). These services can be considered secondary or support systems that are critical to maintaining safe, reliable manufacturing operations and considered potential targets for adversaries seeking to disrupt manufacturing production.

THANK YOU

info@dragos.com

DRAGOS