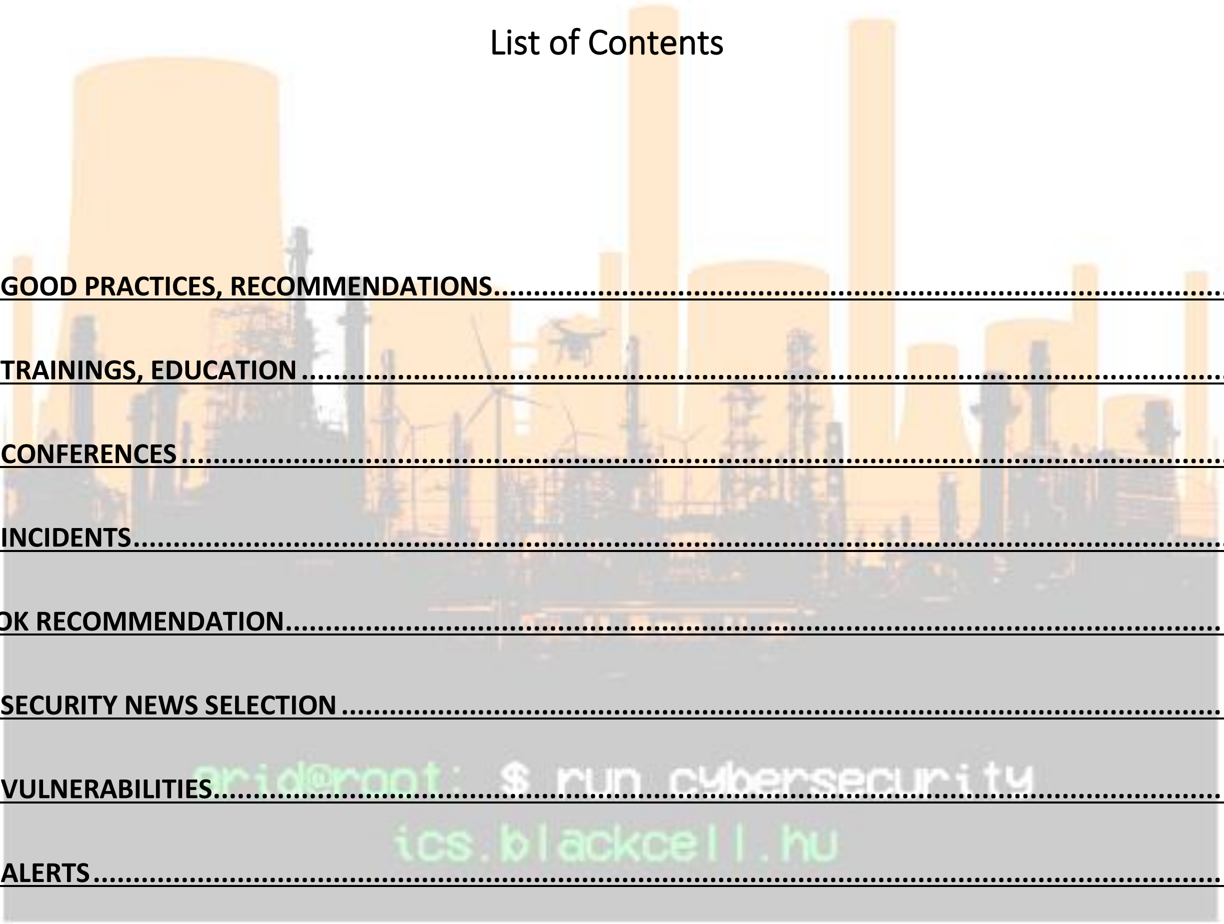
BLACK CELL
Információs értékei védelmében

2022 August, Industrial Control Systems security feed

Black Cell is committed for the security of Industrial Control Systems (ICS) and Critical Infrastructure, therefore we are publishing a monthly security feed. This document gives useful information and good practices to the ICS and critical infrastructure operators and provides information on vulnerabilities, trainings, conferences, books, and incidents on the subject of ICS security. Black Cell provides recommendations and solutions to establish a resilient and robust ICS security system in the organization. If you're interested in ICS security, feel free to contact our experts at info@blackcell.io.

List of Contents



ICS good practices, recommendations

Cybersecurity Best Practices for the Manufacturing Industry

Cloud Security Alliance New Jersey Chapter published a best practice document about the Cybersecurity Best Practices for the Manufacturing Industry.

The best practice gives some brief background, from Industry 1.0 to 4.0, presents current Industry 4.0 Technology Advances and the existing US cyber risk management frameworks for the specific manufacturing sector, define cybersecurity challenges to legacy manufacturing organizations.

The following topics are also part of the best practice: practical top 10 list of items to quickly address with Industry 1.0-4.0 technology vulnerabilities, aligning manufacturing cybersecurity efforts with the business, looking past Industry 4.0 into the future of cloud.

The practical top 10 list are as follows:

1. Categorization of critical assets and data by business priority inclusive of physical and safety priorities

2. Segmentation of the information technology (IT) and operational technology (OT) networks, and further segmentation of the OT network per the Purdue model architecture with consideration of implementing zones and conduits (CheckPoint Software Technology Limited, 2021)

3. Restriction of remote access to only allowed parties at allowed times with availability of Audit trails

4. Application of least privilege access and privileged access management principles

5. Enforcing of access control, on-boarding and off-boarding policies

6. Implementation of a vulnerability management system and patching cadence as per risk determination (where risk = Likelihood * Impact) and informed threat intelligence with robust security threat detection and logging capabilities on systems and endpoints where applicable

7. System installation with hardened security baselines inclusive of application whitelisting and strict change management guidelines

8. Development and testing of cybersecurity incident response plans

9. Using a mature resiliency approach for business continuity and disaster recovery capabilities

10. Provides cyber security awareness training for OT staff

root: $ run cybersecurity
ics.blackcell.hu

Source and more information available on the following link (if you register, you can download it for free):

https://cloudsecurityalliance.org/artifacts/manufacturing-industry-cybersecurity-challenges/

ICS trainings, education

Without aiming to provide an exhaustive list, the following trainings are available in September 2022:

Periodic online courses:

The Coursera (https://www.coursera.org/) website provides an opportunity to take advantage of online trainings regarding ICS security. The trainings provide video instructions, and the candidates could demonstrate their knowledge in the field of ICS and IoT and the related cloud security. After the course, the University of Colorado, Boulder issues a certificate to the graduates. The following courses are available:

- Developing Industrial Internet of Things Specialization
- Development of Secure Embedded Systems Specialization
- Industrial IoT Markets and Security

More details can be found on the following website:

https://www.coursera.org/search?query=-%09Developing%20Industrial%20Internet%20of%20Things%20Specialization&

ICS CERT offers the following courses:

- Introduction to Control Systems Cybersecurity
- Intermediate Cybersecurity for Industrial Control Systems (201), (202)
- ICS Cybersecurity
- ICS Evaluation

More details can be found on the following website:

https://www.us-cert.gov/ics/Training-Available-Through-ICS-CERT

ICS-CERT Virtual Learning Portal (VLP) provides the following short courses:

- Operational Security (OPSEC) for Control Systems (100W) - 1 hour
- Differences in Deployments of ICS (210W-1) – 1.5 hours
- Influence of Common IT Components on ICS (210W-2) – 1.5 hours
- Common ICS Components (210W-3) – 1.5 hours
- Cybersecurity within IT & ICS Domains (210W-4) – 1.5 hours
- Cybersecurity Risk (210W-5) – 1.5 hours
- Current Trends (Threat) (210W-6) – 1.5 hours
- Current Trends (Vulnerabilities) (210W-7) – 1.5 hours
- Determining the Impacts of a Cybersecurity Incident (210W-8) – 1.5 hours
- Attack Methodologies in IT & ICS (210W-9) – 1.5 hours
- Mapping IT Defense-in-Depth Security Solutions to ICS - Part 1 (210W-10) – 1.5 hours
- Mapping IT Defense-in-Depth Security Solutions to ICS - Part 2 (210W-11) – 1.5 hours
- Industrial Control Systems Cybersecurity Landscape for Managers (FRE2115) - 1 hour

VLP courses are available on the same website, like the other ICS-CERT courses.

SANS online courses in the field of ICS security:

- ICS410: ICS/SCADA Security Essentials
- ICS515: ICS Active Defense and Incident Response

More details can be found on the following websites:

https://www.sans.org/cyber-security-courses/ics-scada-cyber-security-essentials/#training-and-pricing
https://www.sans.org/cyber-security-courses/ics-visibility-detection-response/#training-and-pricing

Udemy provides online courses in ICS and SCADA security. From the basics of ICS and SCADA security principles to the technological solutions and governance questions, the below course could help to understand the essence of the ICS/SCADA security.

- ICS/SCADA Cyber Security
- Learn SCADA from Scratch to Hero (Indusoft & TIA portal)
- Fundamentals of OT Cybersecurity (ICS/SCADA)
- An Introduction to the DNP3 SCADA Communications Protocol
- Learn SCADA from Scratch - Design, Program and Interface

More details can be found on the following website:

https://www.udemy.com/ics-scada-cyber-security/

The **Department of Homeland Security's** two days training is useful for the ICS/SCADA operators:

- SCADA security training

grid@root: $ run cybersecurity
ics.blackcell.hu

The courses are available live online.

More details can be found on the following website:

https://www.tonex.com/training-courses/scada-security-training/

The **SCADAhacker.com** website provides ICS security online courses:

- Fundamentals of Industrial Control System Cyber Security

The training takes 40-120 hours, and 8 modules can help to understand the ICS cybersecurity issues. The training focuses on the „Blue teaming" activities, for ICS and SCADA systems.

If you have a certificate, like CISSP or CEH, the course can help to add some ICS and SCADA specific knowledge.

Ethical Hacking for Industrial Control Systems

This exciting new and very advanced course supplies an environment to learn and apply offensive cyber operational (OCO) skills to a range of operational technology architectures. It introduces tactics, techniques, and procedures (TTP) to a range of real-world architectures, components, devices, and protocols that leverage both traditional software vulnerabilities and other more subtle, hard-to-find yet equally or more powerful human vulnerabilities that arise from typical system configuration and usage.

More details can be found on the following website:

https://scadahacker.com/training.html

INFOSEC-Flex SCADA/ICS Security Training Boot Camp gives the possibility for ICS/SCADA operators to get ready for external and internal threats.

The 4 days course guarantees the "Certified SCADA Security Architect" certification for the candidates (93% exam pass rate).

The basics of the ICS/SCADA security, governance, security controls, penetration testing and other topics can help the participants to become an ICS/SCADA security expert.

More details can be found on the following website:

https://www.infosecinstitute.com/courses/scada-security-boot-camp/

Industrial Control System (ICS) & SCADA Cyber Security Training

This is a three day course, what is designed for:

- IT and ICS cybersecurity personnel
- Field support personnel and security operators
- Auditors, vendors and team leaders
- Electric utility engineers
- System personnel & System operators
- Independent system operator personnel
- Electric utility personnel involved with ICS security.
- Technicians, operators, and maintenance personnel
- Investors and contractors in the electric industry
- Managers, accountants, and executives of electric industry

More details can be found on the following website:

https://www.tonex.com/training-courses/industrial-control-system-scada-cybersecurity-training/

Bsigroup: Certified Lead SCADA Security Professional training course

This five-day training course will enable you to develop the expertise to plan, design and implement an effective programme to protect SCADA systems. You'll gain an understanding of common Industrial Control Systems (ICS) threats, vulnerabilities, and risks, and how they can be managed.

By attending this course you'll gain the knowledge and skills to advise on or manage risks related to SCADA environments and systems as a qualified professional. On successful completion of the PECB exam that takes place on the final day of this course, you'll gain Certified Lead SCADA Security Professional status.

Duration: 5 days, anytime at your office

More details can be found on the following website:

https://www.bsigroup.com/en-GB/our-services/digital-trust/cybersecurity-information-resilience/Training/certified-lead-scada-security-professional/

ICS/SCADA security training seminar

The courses are derived from 28 years of first-hand technology experience and industry best practices. The classes are customized to your team's requirements and taught at your offices, classrooms and online live by world-class instructors with publications, patents, awards/honors, and a passion to share knowledge.

More details can be found on the following website:

https://www.enoinstitute.com/scada-ics-security-training-seminar/

NEW in this security feed:

grid@root: $ run cybersecurity
ics.blackcell.hu

The Industrial Cyber Security Certification Course

This ICS Cybersecurity certification covers all aspects of Industrial Cyber security including a special advanced module on Understanding IEC 62443-2-4 that is very useful for not only automation system vendors and system integrators, but also to owners/operators to know what to expect from the vendor that supplies, installs, commissions and maintains the Industrial Control System.

When you complete the requirements of this course, you earn the title of CICP- Certified Industrial Cybersecurity Professional. (CICP)

More details can be found on the following website:

https://prettygoodcourses.com/courses/industrial-cybersecurity-professional/

ICS conferences

In September 2022, the following ICS/SCADA security conferences and workshops will be organized (not comprehensive):

Cyber Security for Industrial Control Systems

The threat of cyber-attacks on industrial control systems is a reality that no organisation can ignore.

These attacks not only have the potential to cause massive financial damages and loss of production downtime but can have dangerous implications for the whole industry. Cyber Security for Industrial Control Systems addresses the key challenges as identified by experts working in industrial control and SCADA systems.

You will learn to implement resilient and sustainable cybersecurity strategies, hear about the latest technology-based solutions and gain advice to mitigate the ever-increasing risks facing critical systems today.

London, UK; September 8th – 9th 2022

More details can be found on the following website:

https://cyberics.theiet.org/

9th Cyber & SCADA Security for Power and Utilities 2022

The 9th Cyber & SCADA Security conference for IT/OT security professionals specifically from Power & Utilities companies. The event offers the chance to meet decision-makers from leading European Energy companies, tackling the latest issues through recent case studies and holds the opportunity to participate in open-floor dialogue and discussion. The topics that will be addressed are the following:

- Stronger cyber resiliency through verification, visibility & velocity
- Consolidating OT Cyber Security capabilities in a global company
- Integrated SOC: system integration and upgrade
- Zero Trust Use Cases
- Military Grade Cyber-AI for OT
- Proposal for organisation, processes and validation in context with cyber-secure architecture

Virtual Conference; September 20th – 21st 2022

More details can be found on the following website:

https://www.ee-isac.eu/9th-cyber-scada-security-for-power-and-utilities-2022/

Cyber Security for Critical Assets European Summit

The CS4CA Europe Summit gives cyber security experts a platform to discuss the problems affecting the region’s critical infrastructure community, and most importantly, how to solve them.

With rising geopolitical tensions in Europe, threats to critical infrastructure are on the rise. State-backed threat actors are now more armed and determined than ever to take down OT networks and even cause physical damage to critical infrastructure, economies and societies. This adds to the threats already posed by cybercriminal groups responsible for the rise of ransomware. In such a threatening environment, we will require all the skills, processes and people available to us to keep our societies running and our population safe.

London, UK; September 20th – 21st 2022

More details can be found on the following website:

https://europe.cs4ca.com/

9th annual Control Systems Cybersecurity USA Conference

From geopolitical cyber risk to ransomware, cascading supply chain vulnerabilities to insecure sensors and devices proliferating across blind spots in asset inventories, the urgency to manage operational technology risk, faster – has never been so crucial.

Yet whilst balancing these exponential threats to smart infrastructure, our common goal as a community must be to educate, inform and facilitate the design and governance of a secure digital transformation across the enterprise to ensure the resilience and sustainability of the business as a whole.

Florida, Kenzies, USA; 29th – 30th 2022

More details can be found on the following website:

https://www.cybersenate.com/control-systems-cybersecurity-usa/

ICS incidents

European Energy Company Hit by Ransomware in Luxembourg

Creos, an electricity network and natural gas pipelines operator (Energy supplier) company in Luxembourg hit by a ransomware, named Black Cat.

The attackers encrypted many valuable files and presumably stole sensitive files (attackers said that the stolen files volume is 180,000, or roughly 150 Gb of information, including contracts, passports, bills, and emails). Creos parent company Encevo said gas and electricity supply has not been impacted by the attack.

The attackers also published screenshots but didn't publish compromised files until the promised time. Nonetheless the parent company (Encevo) published, that they recommended the customers to update their login details as soon as possible.

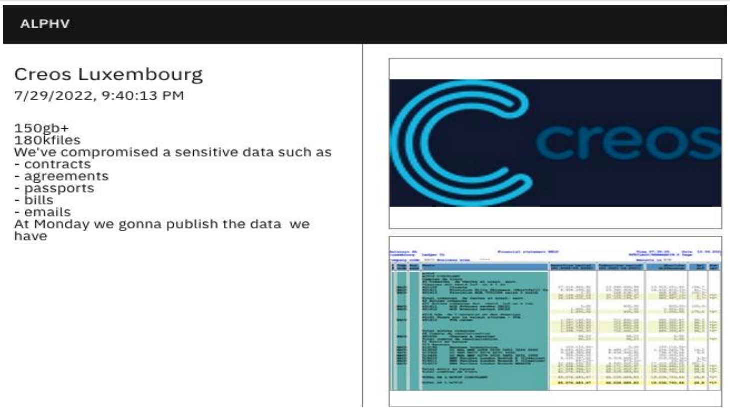
Encevo published the following statement:

"Following the announcement of Monday, July 25 and in accordance with our legal information obligations, we confirm that the various entities of the Encevo Group have been the victim of a Cyber-attack. During this attack, a number of data were exfiltrated from computer systems or made inaccessible by hackers.

The group is currently making every effort to analyze the hacked data. For the moment, the Encevo Group does not yet have all the information necessary to personally inform each person concerned. Encevo registered a complaint with the Police of the Grand Duchy and of course notified the CNPD (National Commission for Data Protection), the ILR (Luxembourg Institute of Regulation) and the competent ministries."

The sources and more information are available on the following links:

https://www.darkreading.com/risk/european-energy-supplier-encevo-breached-in-attack
https://www.securityweek.com/luxembourg-energy-company-hit-ransomware
https://www.encevo.eu/en/encevo-cyberattack/



Creos Luxembourg
7/29/2022, 9:40:13 PM

150gb+
180kfiles
We've compromised a sensitive data such as
- contracts
- agreements
- passports
- bills
- emails
At Monday we gonna publish the data we have

Source: https://www.securityweek.com/luxembourg-energy-company-hit-ransomware

Book recommendation

Practical Industrial Cybersecurity: ICS, Industry 4.0, and IIoT

In Practical Industrial Cybersecurity: ICS, Industry 4.0, and IIoT, veteran electronics and computer security author Charles J. Brooks and electrical grid cybersecurity expert Philip Craig deliver an authoritative and robust discussion of how to meet modern industrial cybersecurity challenges. The book outlines the tools and techniques used by practitioners in the industry today, as well as the foundations of the professional cybersecurity skillset required to succeed on the SANS Global Industrial Cyber Security Professional (GICSP) exam.

Full of hands-on explanations and practical guidance, this book also includes:

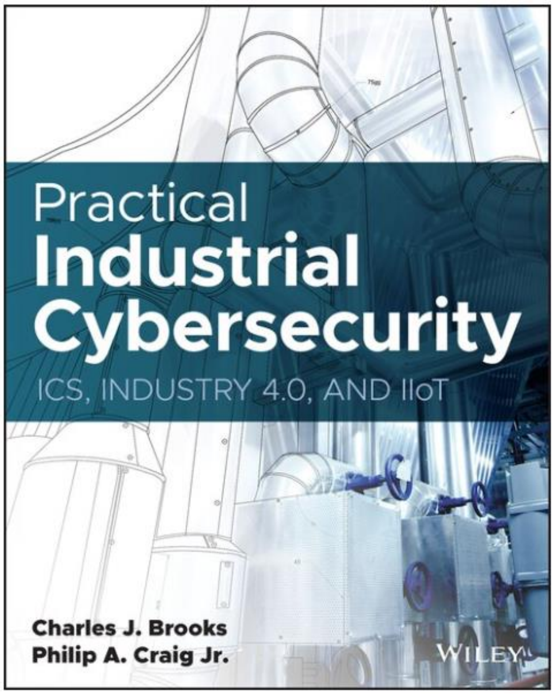
Comprehensive coverage consistent with the National Institute of Standards and Technology guidelines for establishing secure industrial control systems (ICS).
Rigorous explorations of ICS architecture, module and element hardening, security assessment, security governance, risk management, and more.

Authors/Editors: Philip A. Craig, Charles J. Brooks

Year of issue: 2022

The book is available at the following link:

https://www.chapters.indigo.ca/en-ca/books/practical-industrial-cybersecurity/9781119883029-item.html



ICS security news selection

Two Big OT Security Concerns Related to People: Human Error and Staff Shortages

A survey of 3,500 security experts from around the world shows that a lot of the cybersecurity problems related to operational technology (OT) involve people, specifically human error and a significant shortage of staff.

The survey, conducted by IoT and OT security firm SCADAfence, found that more than 75% of experts believe their OT security risk level is high or severe for the company’s overall risk profile. …

Source and more information:

https://www.securityweek.com/two-big-ot-security-concerns-related-people-human-error-and-staff-shortages

Securing Smart Cities from the Ground Up

Smart technology continues to change how people live and interact with the cities around them. While the full value of a connected city evolves – one that leverages innovations powered by artificial intelligence and machine learning – cybersecurity stands as one of its greatest challenges. …

Source and more information:

https://www.securityweek.com/securing-smart-cities-ground

Tainted password-cracking software for industrial systems used to spread P2P Sality bot

During a routine vulnerability assessment, Dragos researchers discovered a campaign targeting industrial engineers and operators with Sality malware.

grid@root: $ run cybersecurity
ics.blackcell.hu

Threat actors behind the campaign used multiple accounts across several social media platforms to advertise password-cracking software for Programmable Logic Controller (PLC), Human-Machine Interface (HMI), and project files. …

Source and more information:

https://securityaffairs.co/wordpress/133281/malware/sality-malware-industrial-systems.html

Number of Ransomware Attacks on Industrial Orgs Drops Following Conti Shutdown

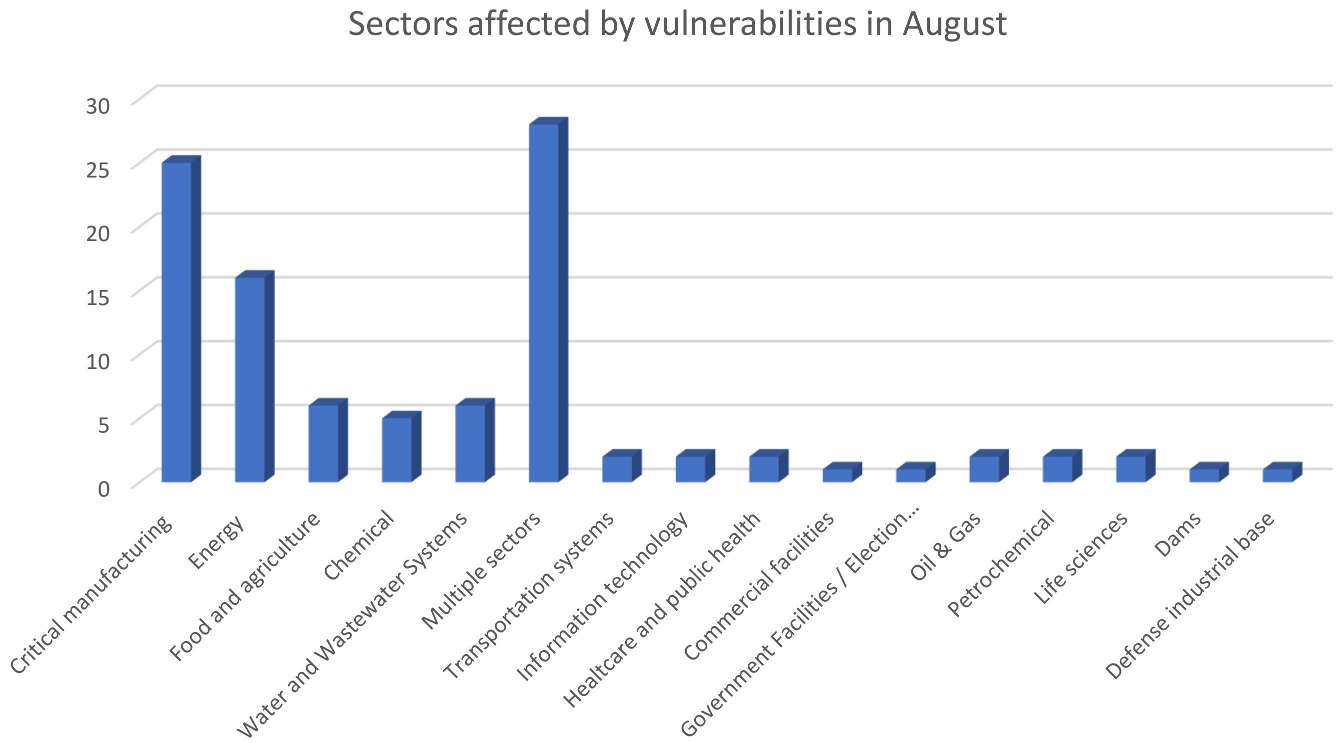
The number of ransomware attacks on industrial organizations decreased from 158 in the first quarter of 2022 to 125 in the second quarter, and it may be — at least partially — a result of the Conti operation shutting down.

According to data collected by industrial cybersecurity firm Dragos, Conti accounted for a significant chunk of the ransomware attacks on industrial organizations and infrastructure in the previous quarters and the threat actor's decision to pull the plug on the operation in May could have led to the drop in the number of attacks in the second quarter. …

Source and more information:
https://www.securityweek.com/number-ransomware-attacks-industrial-orgs-drops-following-conti-shutdown

ICS vulnerabilities

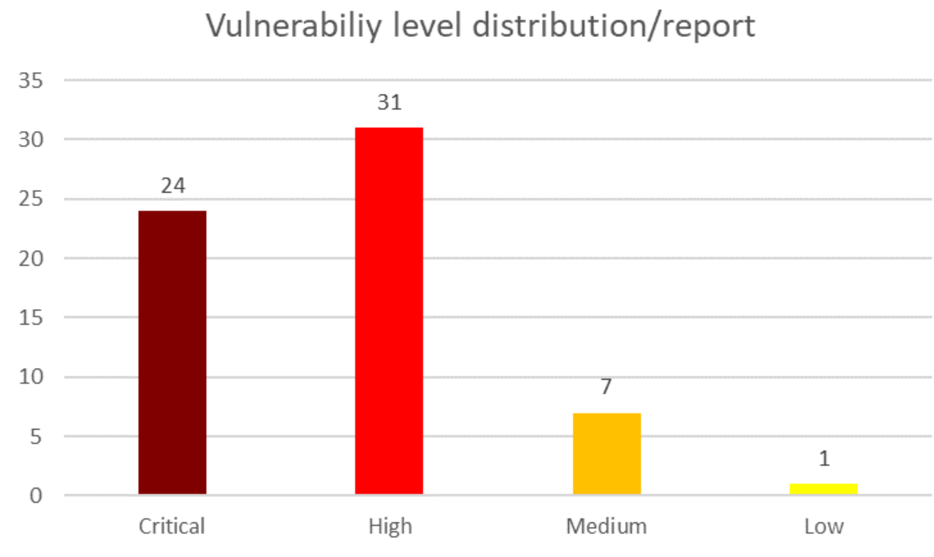
In August 2022, the following vulnerabilities were reported by the National Cybersecurity and Communications Integration Center, Industrial Control Systems (ICS) Computer Emergency Response Teams (CERTs) – ICS-CERT:


Sectors affected by vulnerabilities in August

Average number of vulnerabilities per vulnerability report in August: **1,76**

The most common vulnerabilities in August:

Vulnerability	CWE number	Piece
Heap-based Buffer Overflow	CWE-122	5
Infinite Loop	CWE-835	5
Cleartext Transmission of Sensitive Information	CWE-319	5
Command injection	CWE-77	4
Out-of-bounds Read	CWE-125	4
Stack-based Buffer Overflow	CWE-121	4



ICSA-22-242-01: **Hitachi Energy FACTS Control Platform (FCP) Product**

High level vulnerability: Reliance on Uncontrolled Component.

https://www.cisa.gov/uscert/ics/advisories/icsa-22-242-01

ICSA-22-242-02: **Hitachi Energy Gateway Station (GWS) Product**

High level vulnerability: Reliance on Uncontrolled Component.

https://www.cisa.gov/uscert/ics/advisories/icsa-22-242-02

ICSA-22-242-03: **Hitachi Energy MSM Product**

High level vulnerability: Reliance on Uncontrolled Component.

https://www.cisa.gov/uscert/ics/advisories/icsa-22-242-03

ICSA-22-242-04: **Hitachi Energy RTU500 series**

High level vulnerability: Improper Input Validation.

https://www.cisa.gov/uscert/ics/advisories/icsa-22-242-04

ICSA-22-242-05: **Fuji Electric D300win**

High level vulnerabilities: Out-of-bounds Read, Write-what-where Condition.

https://www.cisa.gov/uscert/ics/advisories/icsa-22-242-05

ICSA-22-242-06: **Honeywell ControlEdge**

Critical level vulnerability: Missing Authentication for Critical Function.

https://www.cisa.gov/uscert/ics/advisories/icsa-22-242-06

ICSA-22-242-07: **Honeywell Experion LX**

Critical level vulnerability: Missing Authentication for Critical Function.

https://www.cisa.gov/uscert/ics/advisories/icsa-22-242-07

ICSA-22-242-08: **Honeywell Trend Controls Inter-Controller Protocol**

High level vulnerability: Cleartext Transmission of Sensitive Information.

https://www.cisa.gov/uscert/ics/advisories/icsa-22-242-08

ICSA-22-242-09: Omron CX-Programmer

High level vulnerability: Use After Free.

https://www.cisa.gov/uscert/ics/advisories/icsa-22-242-09

ICSA-22-242-10: PTC Kepware KEPServerEX

Critical level vulnerabilities: Heap-based Buffer Overflow, Stack-based Buffer Overflow.

https://www.cisa.gov/uscert/ics/advisories/icsa-22-242-10

ICSA-22-242-11: Sensormatic Electronics iSTAR

Critical level vulnerability: Command Injection.

https://www.cisa.gov/uscert/ics/advisories/icsa-22-242-11

ICSA-22-221-01: Mitsubishi Electric Multiple Factory Automation Products (Update B)

Critical level vulnerabilities: Infinite Loop, OS Command Injection.

https://www.cisa.gov/uscert/ics/advisories/icsa-22-221-01

ICSA-22-237-01: FATEK Automation FvDesigner

High level vulnerability: Out-of-bounds Write.

https://www.cisa.gov/uscert/ics/advisories/icsa-22-237-01

ICSA-22-235-01: ARC Informatique PcVue

Medium level vulnerability: Cleartext Storage of Sensitive Information.

https://www.cisa.gov/uscert/ics/advisories/icsa-22-235-01-0

ICSA-22-235-02: Delta Industrial Automation DIALink

Critical level vulnerability: Use of Hard-coded Cryptographic Key.

https://www.cisa.gov/uscert/ics/advisories/icsa-22-235-02

ICSA-22-235-03: mySCADA myPRO

Critical level vulnerability: Command Injection.

https://www.cisa.gov/uscert/ics/advisories/icsa-22-235-03

ICSA-22-235-05: Measuresoft ScadaPro Server

High level vulnerability: Out-of-bounds Write.

https://www.cisa.gov/uscert/ics/advisories/icsa-22-235-05

ICSA-22-235-06: Measuresoft ScadaPro Server and Client

High level vulnerabilities: Untrusted Pointer Dereference, Stack-based Buffer Overflow, Use After Free, Link Following.

https://www.cisa.gov/uscert/ics/advisories/icsa-22-235-06

ICSA-22-235-07: Hitachi Energy RTU500

High level vulnerability: Stack-based Buffer Overflow.

https://www.cisa.gov/uscert/ics/advisories/icsa-22-235-07

ICSA-22-153-02: Illumina Local Run Manager (Update A)

Critical level vulnerabilities: Path Traversal, Unrestricted Upload of File with Dangerous Type, Improper Access Control, Cleartext Transmission of Sensitive Information.
https://www.cisa.gov/uscert/ics/advisories/icsa-22-153-02

ICSA-22-172-01: Mitsubishi Electric MELSEC iQ-R, Q, L Series and MELIPC Series (Update A)

High level vulnerability: Improper Resource Locking.
https://www.cisa.gov/uscert/ics/advisories/icsa-22-172-01

ICSA-22-221-01: Mitsubishi Electric Multiple Factory Automation Products (Update A)

Critical level vulnerabilities: Infinite Loop, OS Command Injection.
https://www.cisa.gov/uscert/ics/advisories/icsa-22-221-01

ICSA-22-167-14: Siemens OpenSSL Affected Industrial Products (Update B)

High level vulnerability: Infinite Loop.
https://www.cisa.gov/uscert/ics/advisories/icsa-22-167-14

ICSA-21-194-07: Siemens Industrial Products LLDP (Update D)

Critical level vulnerabilities: Classic Buffer Overflow, Uncontrolled Resource Consumption.
https://www.cisa.gov/uscert/ics/advisories/icsa-21-194-07

ICSA-21-131-03: Siemens Linux-based Products (Update J)

High level vulnerability: Use of Insufficiently Random Values.
https://www.cisa.gov/uscert/ics/advisories/icsa-21-131-03

ICSA-22-228-01: Yokogawa CENTUM Controller FCS

Medium level vulnerability: Denial of Service.
https://www.cisa.gov/uscert/ics/advisories/icsa-22-228-01

ICSA-22-228-02: LS ELECTRIC PLC and XG5000

Medium level vulnerability: Inadequate Encryption Strength.
https://www.cisa.gov/uscert/ics/advisories/icsa-22-228-02

ICSA-22-228-04: Softing Secure Integration Server

High level vulnerabilities: Out-of-bounds Read, Uncontrolled Search Path Element, Improper Authentication, Relative Path Traversal, Cleartext Transmission of Sensitive Information, NULL Pointer Dereference, Integer Underflow.
https://www.cisa.gov/uscert/ics/advisories/icsa-22-228-04

ICSA-22-228-03: Delta Industrial Automation DRAS

Medium level vulnerability: Improper Restriction of XML External Entity Reference.
https://www.cisa.gov/uscert/ics/advisories/icsa-22-228-03

ICSA-22-228-05: B&R Industrial Automation Automation Studio 4

High level vulnerability: Unrestricted Upload of File with Dangerous Type.
https://www.cisa.gov/uscert/ics/advisories/icsa-22-228-05

ICSA-22-228-06: **Emerson Proficy Machine Edition**

Critical level vulnerabilities: Missing Support for Integrity Check, Improper Access Control, Unrestricted Upload of File with Dangerous Type, Improper Verification of Cryptographic Signature, Insufficient Verification of Data Authenticity, Path Traversal: '\..\filename'.
https://www.cisa.gov/uscert/ics/advisories/icsa-22-228-06

ICSA-22-228-07: **Sequi PortBloque S**

Critical level vulnerabilities: Improper Authentication, Improper Authorization.
https://www.cisa.gov/uscert/ics/advisories/icsa-22-228-07

ICSA-22-132-08: **Siemens Industrial Products with OPC UA** (Update B)

Medium level vulnerability: Null Pointer Dereference.
https://www.cisa.gov/uscert/ics/advisories/icsa-22-132-08

ICSA-22-223-01: **Siemens Simcenter STAR-CCM+**

Medium level vulnerability: Exposure of Sensitive Information to an Unauthorized Actor.
https://www.cisa.gov/uscert/ics/advisories/icsa-22-223-01

ICSA-22-223-02: **Siemens Teamcenter**

High level vulnerabilities: Command Injection, Infinite Loop.
https://www.cisa.gov/uscert/ics/advisories/icsa-22-223-02

ICSA-22-223-03: **Schneider Electric EcoStruxure, EcoStruxure Process Expert, SCADAPack RemoteConnect for x70**

Critical level vulnerabilities: Heap-based Buffer Overflow, Wrap or Wraparound, Classic Buffer Overflow, Out-of-bounds Write.
https://www.cisa.gov/uscert/ics/advisories/icsa-22-223-03

ICSA-22-223-04: **Emerson ROC800, ROC800L and DL8000**

Medium level vulnerability: Insufficient Verification of Data Authenticity.
https://www.cisa.gov/uscert/ics/advisories/icsa-22-223-04

grid@root: $ run cybersecurity
www.blackcell.hu

ICSA-22-223-05: **Siemens SICAM A8000 Web Server Module**

Low level vulnerability: Improper Access Control.
https://www.cisa.gov/uscert/ics/advisories/icsa-22-223-05

ICSA-22-223-06: **Siemens SICAM TOOLBOX II**

Critical level vulnerability: Use of Hard-coded Credentials.
https://www.cisa.gov/uscert/ics/advisories/icsa-22-223-06

ICSA-22-223-07: **Siemens SCALANCE**

Critical level vulnerabilities: Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection'), Allocation of Resources Without Limits or Throttling, Basic Cross Site Scripting.
https://www.cisa.gov/uscert/ics/advisories/icsa-22-223-07

ICSA-22-104-12: Siemens SIMATIC S7-400 (Update A)

High level vulnerability: Improper Restriction of Operations within the Bounds of a Memory Buffer.

https://www.cisa.gov/uscert/ics/advisories/icsa-22-104-12

ICSA-21-222-05: Siemens Industrial Products Intel CPUs (Update E)

High level vulnerability: Missing Encryption of Sensitive Data.

https://www.cisa.gov/uscert/ics/advisories/icsa-21-222-05

ICSA-21-194-07: Siemens Industrial Products LLDP (Update C)

Critical level vulnerabilities: Classic Buffer Overflow, Uncontrolled Resource Consumption.

https://www.cisa.gov/uscert/ics/advisories/icsa-21-194-07

ICSA-21-131-03: Siemens Linux-based Products (Update I)

High level vulnerability: Use of Insufficiently Random Values.

https://www.cisa.gov/uscert/ics/advisories/icsa-21-131-03

ICSA-22-195-07: Siemens Datalogics File Parsing Vulnerability (Update A)

High level vulnerability: Heap-based buffer Overflow.

https://www.cisa.gov/uscert/ics/advisories/icsa-22-195-07

ICSMA-20-170-04: Baxter Sigma Spectrum Infusion Pumps (Update B)

High level vulnerabilities: Use of Hard-coded Password, Cleartext Transmission of Sensitive Data, Incorrect Permission Assignment for Critical Resource, Operation on a Resource After Expiration or Release.

https://www.cisa.gov/uscert/ics/advisories/icsma-20-170-04

ICSA-19-099-03: Siemens Industrial Products with OPC UA (Update H)

High level vulnerability: Uncaught Exception.

https://www.cisa.gov/uscert/ics/advisories/ICSA-19-099-03

ICSA-20-014-05: Siemens TIA Portal (Update F)

High level vulnerability: Path Traversal.

https://www.cisa.gov/uscert/ics/advisories/icsa-20-014-05

ICSA-22-167-13: Siemens Teamcenter (Update A)

Critical level vulnerability: Use of Hard-coded Credentials.

https://www.cisa.gov/uscert/ics/advisories/icsa-22-167-13

ICSA-22-132-16: Siemens Teamcenter (Update B)

High level vulnerabilities: Stack-based Buffer Overflow, Improper Restriction of XML External Entity Reference.

https://www.cisa.gov/uscert/ics/advisories/icsa-22-132-16

ICSA-22-132-12: Siemens Industrial Products (Update B)

High level vulnerability: Improper Restriction of Operations within the Bounds of a Memory Buffer.

https://www.cisa.gov/uscert/ics/advisories/icsa-22-132-12

ICSA-22-195-18: Siemens RUGGEDCOM ROS (Update A)

High level vulnerability: Improper Control of Generation of Code.

https://www.cisa.gov/uscert/ics/advisories/icsa-22-195-18

ICSA-22-195-09: Simcenter Femap and Parasolid (Update A)

High level vulnerability: Out-of-bounds Read.

https://www.cisa.gov/uscert/ics/advisories/icsa-22-195-09

ICSA-22-195-12: Siemens SRCS VPN Feature in SIMATIC CP Devices (Update A)

Critical level vulnerabilities: Heap-based Buffer Overflow, Command Injection, Code Injection.

https://www.cisa.gov/uscert/ics/advisories/icsa-22-195-12

ICSA-22-221-01: Mitsubishi Electric GT SoftGOT2000

Critical level vulnerabilities: Infinite Loop, OS Command Injection.

https://www.cisa.gov/uscert/ics/advisories/icsa-22-221-01

ICSA-22-221-02: Emerson ControlWave

Critical level vulnerability: Insufficient Verification of Data Authenticity.

https://www.cisa.gov/uscert/ics/advisories/icsa-22-221-02

ICSA-22-221-03: Emerson OpenBSI

Critical level vulnerabilities: Use of Broken or Risky Cryptographic Algorithm, Use of Hard-coded Cryptographic Key.

https://www.cisa.gov/uscert/ics/advisories/icsa-22-221-03

ICSA-22-216-01: Digi ConnectPort X2D

Critical level vulnerability: Execution with Unnecessary Privileges.

https://www.cisa.gov/uscert/ics/advisories/icsa-22-216-01

ICSA-22-207-01: Inductive Automation Ignition (Update A)

High level vulnerability: Improper Restriction of XML External Entity Reference.

https://www.cisa.gov/uscert/ics/advisories/icsa-22-207-01

ICSA-21-238-03: Delta Electronics DIAEnergie (Update C)

Critical level vulnerabilities: Use of Password Hash with Insufficient Computational Effort, Authentication Bypass Using an Alternate Path or Channel, Unrestricted Upload of File with Dangerous Type, SQL Injection, Cross-site Request Forgery, Cross-site Scripting, Cleartext Transmission of Sensitive Information.

https://www.cisa.gov/uscert/ics/advisories/icsa-21-238-03

ICSA-22-081-01: Delta Electronics DIAEnergie (Update C)

Critical level vulnerabilities: Path Traversal, Incorrect Default Permissions, SQL Injection, Uncontrolled Search Path Element.

https://www.cisa.gov/uscert/ics/advisories/icsa-22-081-01

ICSA-21-049-02: Mitsubishi Electric FA Engineering Software Products (Update F)

High level vulnerabilities: Heap-based Buffer Overflow, Improper Handling of Length Parameter Inconsistency.

https://www.cisa.gov/uscert/ics/advisories/icsa-21-049-02

ICSA-20-212-04: Mitsubishi Electric Factory Automation Engineering Products (Update H)

High level vulnerability: Unquoted Search Path or Element.

https://www.cisa.gov/uscert/ics/advisories/icsa-20-212-04

The vulnerability reports contain more detailed information, which can be found on the following website:

https://ics-cert.us-cert.gov/advisories

Continuous monitoring of vulnerabilities is recommended, because relevant information on how to address vulnerabilities, patch vulnerabilities and mitigate risks are also included in the detailed descriptions.

ICS alerts

In August 2022, ICS-CERT has published an alert:

2021 Top Malware Strains

This joint Cybersecurity Advisory (CSA) was coauthored by the Cybersecurity and Infrastructure Security Agency (CISA) and the Australian Cyber Security Centre (ACSC). This advisory provides details on the top malware strains observed in 2021. Malware, short for “malicious software,” can compromise a system by performing an unauthorized function or process. Malicious cyber actors often use malware to covertly compromise and then gain access to a computer or mobile device.

In 2021, the top malware strains included remote access Trojans (RATs), banking Trojans, information stealers, and ransomware. Most of the top malware strains have been in use for more than five years with their respective code bases evolving into multiple variations. The most prolific malware users are cyber criminals, who use malware to deliver ransomware or facilitate theft of personal and financial information.

Key Findings

The top malware strains of 2021 are: Agent Tesla, AZORult, Formbook, Ursnif, LokiBot, MOUSEISLAND, NanoCore, Qakbot, Remcos, TrickBot and GootLoader.

Malicious cyber actors have used Agent Tesla, AZORult, Formbook, LokiBot, NanoCore, Remcos, and TrickBot for at least five years.
Malicious cyber actors have used Qakbot and Ursnif for more than a decade.

Mitigations

- Update software, including operating systems, applications, and firmware, on IT network assets.
- Enforce MFA.
- If you use RDP and/or other potentially risky services, secure and monitor them closely.
- Maintain offline (i.e., physically disconnected) backups of data.
- Provide end-user awareness and training.

grid@root: $ run cybersecurity
ics.blackcell.hu

Source and more details can be found on the following website:

https://www.cisa.gov/uscert/ncas/alerts/aa22-216a