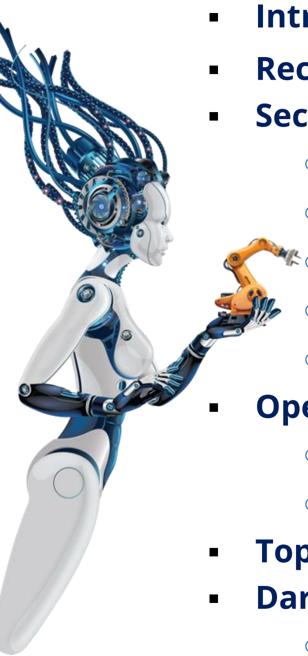
CYBLE

Operational Technology (OT)/ Industrial Control System (ICS) Sensor Intelligence Report

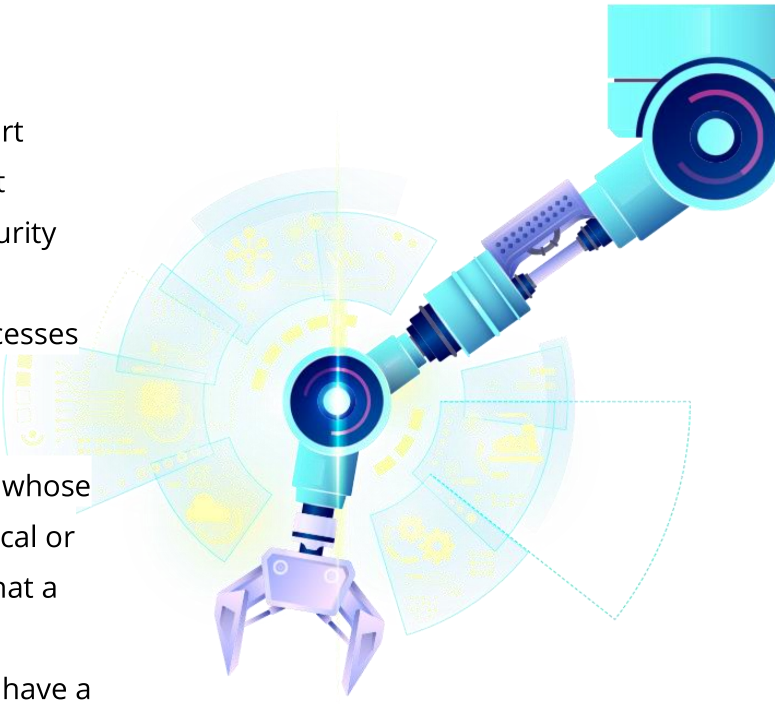
October 12, 2023

CONTENT



- **Introduction** 3
- **Recent Spotlight** 5
- **Sectoral Attack Distribution** 7
  - Attacks on Manufacturing Sector 8
  - Attacks on the Oil & Gas Sector 10
  - Attacks on Energy Sector 11
  - Attacks on Building Automation System 14
  - Attacks on Healthcare & Public Health Sector 15
- **Operation Technology (OT) Vulnerabilities** 16
  - Operation Technology (OT) Advisory Overview 17
  - Vulnerability Severity Overview 17
- **Top 10 Industry-Wise Ransomware Attacks** 18
- **Darkweb & Cyber Crime Activities** 19
  - Data Breaches & Leaks 19
  - Distribution of Access 19
- **Overall Insights** 20
  - Attacker IP 20
  - Top 10 ASN 20
  - Top ICS components targeted 22
  - Attacks observed by Country 22
  - Attacker Source IP Reputation 23
- **Next Steps** 25
- **Disclaimer** 25
- **Indicators of Compromise (IOC)** 25
- **Recommendation** 26

Introduction



Cyble’s Quarterly OT Sensor Intelligence Report provides insights into threat actors and threat vectors that Operational Technology (OT) Security teams should consider while designing and implementing their security controls and processes to safeguard critical infrastructure.

Critical Infrastructure sectors comprise those whose assets, systems, and networks, whether physical or virtual, are considered so vital to the nation that a successful cyber-attack on the infrastructure, resulting in breakdown or destruction, would have a debilitating effect on security, national economic security, national public health or safety, etc.

Cyble's Threat Hunting service employs a suite of tools to capture real-time attack data on various Industrial Control System (ICS) equipment using honeypot sensors. The equipment simulated is deployed in the Critical Information Sector.

The targeted attacks on Industrial Control Systems using malicious programs such as **Stuxnet, Triton, BlackEnergy3, Industroyer2, CrashOverider, Pipedream** etc, show that Threat Actors (TAs) are well equipped with specific strains of malware that can chain multiple vulnerabilities within IT and OT environment to target a specific ICS component. With the right amount of resources and skillsets, APT groups and State sponsored attackers continuously develop ICS specific malwares to increase their scope of impact.

At the same time, due to the geopolitical instability among various regions, **Hacktivist groups and the Anonymous collective were also observed actively targeting internet-exposed ICS assets**. Public exploits, open-source tools, documentations and the lacking security posture of organizations dealing in critical infrastructure sector have made it convenient for malicious attackers to penetrate and exploit ICS environments.

The role of Initial access brokers, leaked sensitive documents and leaked credentials have **increased the risk of ransomware attacks on CI sector**, One such notable and high-impact incident was the Colonial Pipeline ransomware attack, which was carried out by suspected Russian Ransomware Gang Darkside in May last year. This led to the shutdown of the pipeline and a substantial multi-million dollar ransomware payout to restore operations. A single compromised password - likely leaked on the dark web - was responsible for the attack.

In later sections, this report gives insights into top targeted countries, port details, source IP addresses of the attack, along with network operator details. This report offers a list of the next steps that could be taken as recommendations to secure networks and a list of Indicators of Compromise. This report covers our findings for Q3 2023.

Recent Spotlight

1 **July 2023,** In collaboration with the U.S. government, Rockwell Automation analyzed a newly identified exploit capability associated with Advanced Persistent Threat (APT) actors. This capability targets specific communication modules by Rockwell Automation within particular models of ControlLogix EtherNet/IP (ENIP) communication modules.

2 **July 2023,** Lockbit 3.0 targeted Japan's largest port. The incident forced the port to stop handling shipping containers that came to the terminal by trailer.

3 **July 2023,** The Cybersecurity and Infrastructure Security Agency (CISA) alerted organizations about threat actors exploiting CVE-2023-3519, an unauthenticated remote code execution (RCE) vulnerability affecting NetScaler (formerly Citrix) Application Delivery Controller (ADC) and NetScaler Gateway.

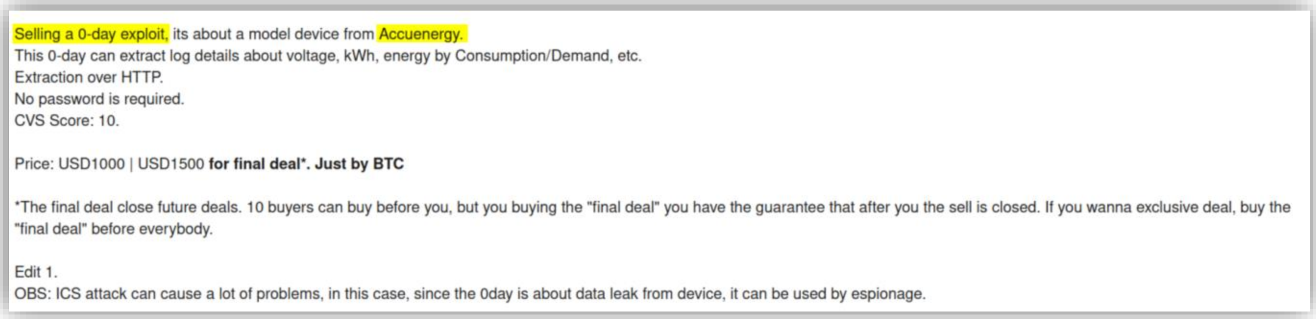
4 **August 2023,** Energy One, an Australian company that provides software products and services to the energy sector, was hit by a cyberattack.

5 **August 2023,** GhostSec claimed to have breached the FANAP Behnama software, which the Iranian government apparently uses to surveil and monitor its citizens.

6 **September 2023,** Canadian authorities raised an alert for a "Distributed Denial of Service campaign targeting multiple Canadian sectors".

7

September 2023, Cyble observed that the Threat Actor claimed to sell a zero-day exploit related to a model device from Accuenergy, as shown below.



Selling a 0-day exploit, its about a model device from Accuenergy.
This 0-day can extract log details about voltage, kWh, energy by Consumption/Demand, etc.
Extraction over HTTP.
No password is required.
CVS Score: 10.

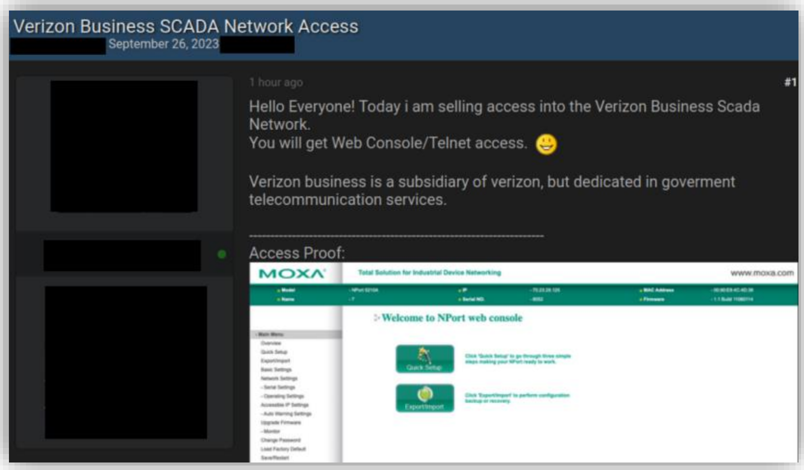
Price: USD1000 | USD1500 **for final deal*. Just by BTC**

*The final deal close future deals. 10 buyers can buy before you, but you buying the "final deal" you have the guarantee that after you the sell is closed. If you wanna exclusive deal, buy the "final deal" before everybody.

Edit 1.
OBS: ICS attack can cause a lot of problems, in this case, since the 0day is about data leak from device, it can be used by espionage.

8

September 2023, Cyble observed that a Threat Actor claiming to sell "Verizon Business SCADA Network Access" via which attackers can get Web Console and Telnet Access. As per the Access Proof shared by TA, the access being sold was **MOXA Nport**.



Verizon Business SCADA Network Access
[redacted] September 26, 2023 [redacted]

[redacted]

[redacted]

[redacted]

1 hour ago #1

Hello Everyone! Today i am selling access into the Verizon Business Scada Network.
You will get Web Console/Telnet access. 😃

Verizon business is a subsidiary of verizon, but dedicated in goverment telecommunication services.

Access Proof:

Cyble Research and Intelligence Labs (CRIL) has previously published a blog covering details on Serial to Ethernet devices such as Moxa and the impact of cyber attacks on these devices.

Sectoral Attack Distribution

The findings below are based on Industrial Control System (ICS) equipment, Protocols, and other assets used within the specific critical infrastructure sectors.

Note: On April 13, 2022 Cybersecurity and Infrastructure Security Agency (CISA) published an advisory stating, *"The APT actors have developed custom-made tools for targeting ICS/SCADA devices. The tools enable them to scan for, compromise, and control affected devices once they have established initial access to the operational technology (OT) network."*
This incident indicates that Advanced Persistence Threat (APT) exhibits the capability to gain full system access to multiple industrial control system (ICS)/Supervisory Control and Data Acquisition (SCADA) devices, including:

- Schneider Electric programmable logic controllers (PLCs),
- OMRON Sysmac NEX PLCs, and
- Open Platform Communications Unified Architecture (OPC UA) servers.

The ICS components stated above rely on the protocols mentioned in the Manufacturing Sector.

Attacks on the Manufacturing sector

The Manufacturing Sector comprises establishments engaged in the mechanical, physical, or chemical transformation of materials, substances, or components into new products.

Establishments in Manufacturing sectors are typically plants, factories, or mills, and they usually employ heavy machinery, power-driven machines, and material-handling equipment.

Port 102

S7 communication is a proprietary network protocol for S7 series PLCs developed and maintained by Siemens. It is used to program PLCs with Siemens Step7 software tools, exchange data between PLCs, and access PLCs from SCADA systems for data requests and diagnostic purposes. The image below represents the attacks observed on port 102 by the Cyble Global Sensor Intelligence Network.

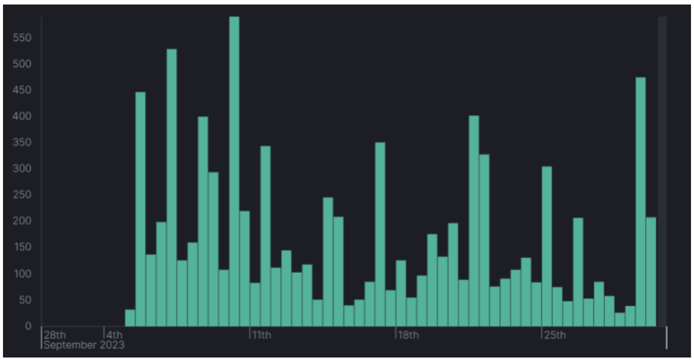


Figure 1- Attacks observed on Port 102

Port 502

The Modbus protocol was developed for industrial automation systems and Modicon programmable controllers. It is the most common ICS protocol mainly because it is simple and robust. The image below represents the attacks observed on port 502 by the Cyble Global Sensor Intelligence Network.

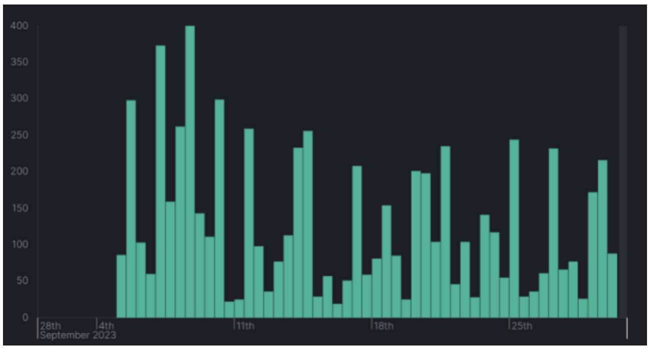


Figure 2- Attacks observed on Port 502

Port 44818

EtherNet/IP is one of the popular ICS protocols. Rockwell/Allen-Bradley and OMRON devices widely use EtherNet/IP. This protocol was found running on TCP and UDP ports 44818. Ethernet/IP uses the Ethernet infrastructure to manage the connection between various automation devices such as robots, PLCs, sensors, and other industrial machines. The image below represents the attacks observed on port 44818 by the Cyble Global Sensor Intelligence Network.

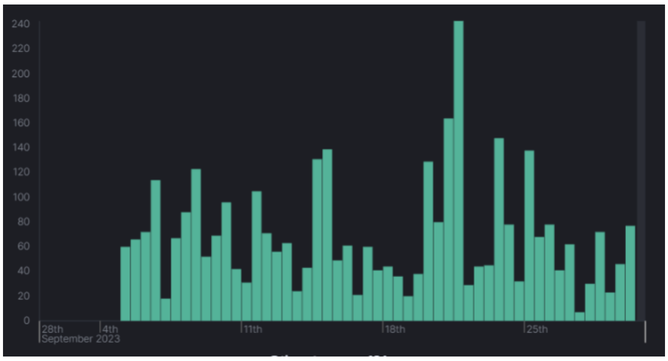


Figure 3- Attacks observed on Port 44818

Attacks on Oil and Gas Sector

The Oil and Gas industry is one of the largest sectors in the world in terms of dollar value, generating a trillion dollars in revenue. Oil is crucial to the global economic framework, impacting everything from transportation to heating and electricity to industrial production and manufacturing, as well as defense.

Port 10001

Automated Tank Gauges (ATGs) are used to monitor fuel tank inventory levels, track deliveries, raise alarms that indicate problems with the tank or gauge (such as a fuel spill), and perform leak tests in accordance with environmental regulatory compliance. The most common configuration is to map these to TCP port 10001. The image below represents the attacks observed on port 10001 by the Cyble Global Sensor Intelligence Network.

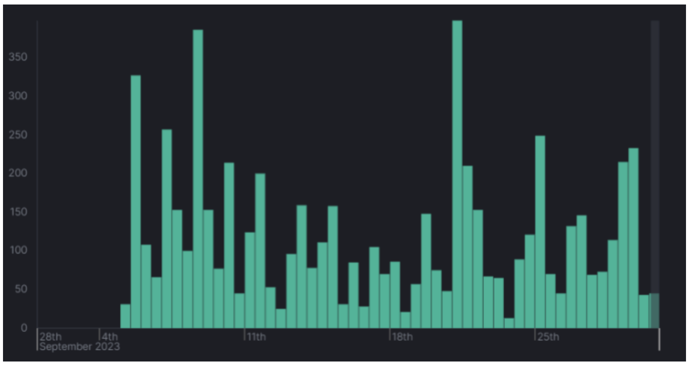


Figure 4- Attacks observed on Port 10001

Attacks on the Energy Sector

The electric power industry covers organizations and assets involved in the generation, transmission, distribution, and sale of electric power to the public and industries within the nation.

Note: The Russian–Ukraine conflict uncovered a new piece of malware named INDUSTROYER2. The notification for malware was provided by UA-CERT on April 12, 2022, stating -

"*Cyber-attack of the Sandworm group on energy facilities of Ukraine using malware INDUSTROYER2 and CADDYWIPER.*"

INDUSTROYER2 is written in C++ and implements the IEC-104 protocol to modify the state of remote terminal units (RTUs) over TCP. The malware crafts configurable IEC-104 Application Service Data Unit (ASDU) messages to change the state of a remote station's Information Object Addresses (IOAs) to ON or OFF. IOAs identify a specific data element on a device and may correspond to power line switches or circuit breakers in an RTU or relay configuration.

This incident points out that while targeting a particular sector, Threat Groups are developing malware that targets a particular device or protocol being used within that sector.

Port 2404

IEC 60870-5-104 protocol (aka IEC 104) is a part of IEC Telecontrol Equipment and Systems. IEC 60870-5 provides a communication profile for sending basic telecontrol messages between two systems in electrical engineering and power system automation. Telecontrol means transmitting supervisory data and data acquisition requests for controlling power transmission grids.

IEC 104 provides network access to IEC 60870-5-101 (aka IEC 101) using standard transport profiles. In simple terms, it delivers IEC 101 messages as application data (L7) over TCP, port 2404.

IEC 104 enables communication between the control station and a substation via a standard TCP/IP network. The communication is based on the client-server model. The image below represents the attacks observed on port 2404 by the Cyble Global Sensor Intelligence Network.

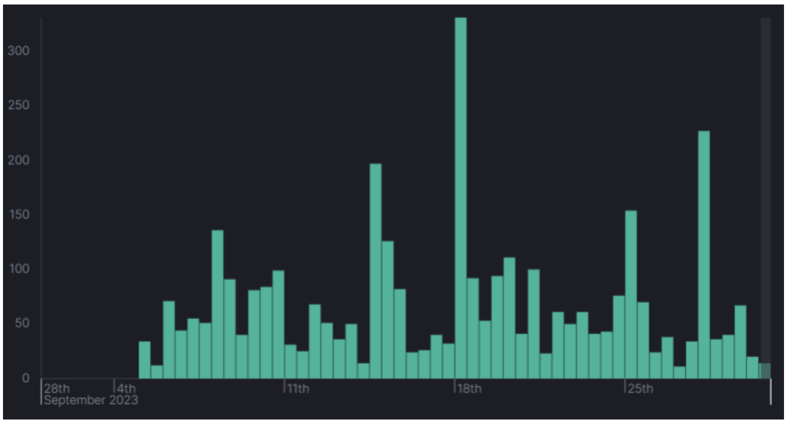


Figure 5- Attacks observed on Port 2404

Port 1025

Port 1025 is being used to simulate Smart Meter Kamstrup. Kamstrup 382, which is a one-, two-, or three-phase direct meter for domestic customers. It can register the consumption in one or two tariffs. Port number 50100 is being used to simulate the **Kamstrup Management protocol**. The image below represents the attacks observed on ports 1025 and 50100 by the Cyble Global Sensor Intelligence Network.

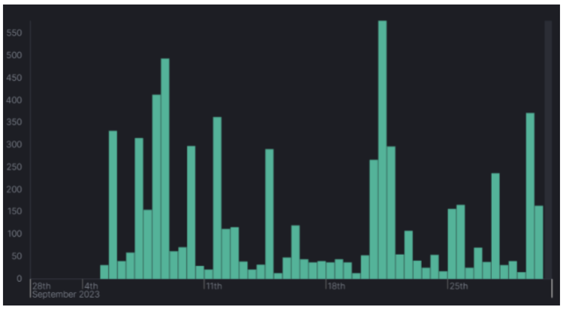


Figure 6 - Attacks observed on Port 1025

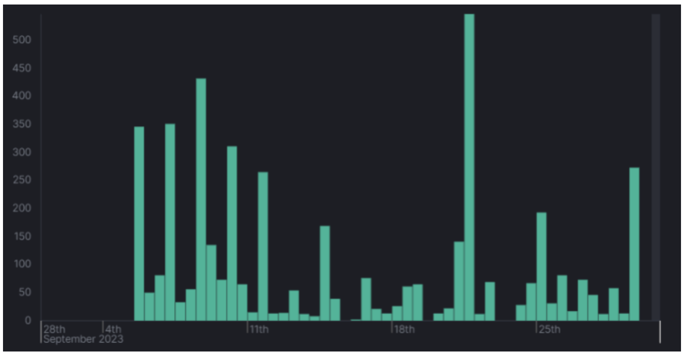


Figure 7 - Attacks observed on Port 50100

Attacks on Building Automation Systems (BAS)

A Building Automation System (BAS) is a network designed to connect and automate certain functions inside a building. The nation's buildings are increasingly relying on building control systems with embedded communications technology, and many are enabled via the Internet. These systems provide critical services that allow a building to meet the functional and operational needs of building occupants but might be easy targets for hackers and people with malicious intent.

Note: "A Chinese-speaking Advanced Persistent Threat (APT) was seen exploiting the **ProxyLogon** Microsoft Exchange vulnerability to deploy the **ShadowPad malware**, researchers said, with the end goal of taking over Building-Automation Systems (BAS) and moving deeper into networks."

Port 47808

BACnet was designed to allow communication of building automation and control systems for applications such as heating, ventilating, and air-conditioning control (HVAC), lighting control, access control, and fire detection systems and their associated equipment. The BACnet protocol provides mechanisms for computerized building automation devices to exchange information, regardless of the building service they perform. The image below represents the attacks observed on port 47808 by the Cyble Global Sensor Intelligence Network.

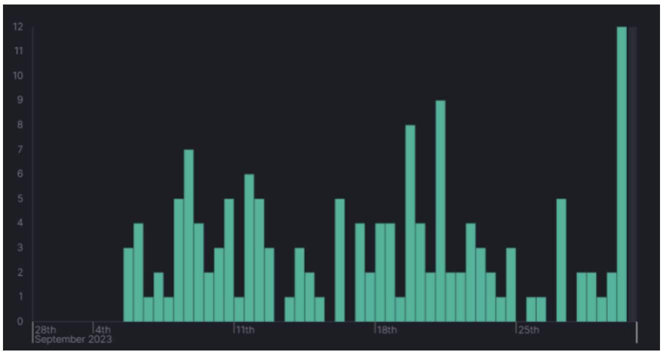


Figure 8- Attacks observed on Port 47808

Attacks on the Healthcare and Public Health Sectors

Attacks on the Healthcare and Public Health sectors have increased drastically in the last few months. Cyble has observed numerous data leaks, ransomware attacks, and social engineering attacks on entities within this sector.

HL7 is a set of international standards for healthcare providers transferring clinical and administrative data between software applications. Fast Healthcare Interoperability Resources (FHIR) is a standard describing data formats and elements and an Application Programming Interface (API) for exchanging electronic health records (EHR). The standard was created by the Health Level Seven International (HL7) healthcare standards organization.
These standards are frequently implemented so that healthcare organizations can make sure their systems are interoperable and their documentation and clinical transactions are consistent with other hospitals.

Port 2575

Port 2575 is registered at IANA for HL7. The image below represents the attacks observed on port 2575 by the Cyble Global Sensor Intelligence Network.

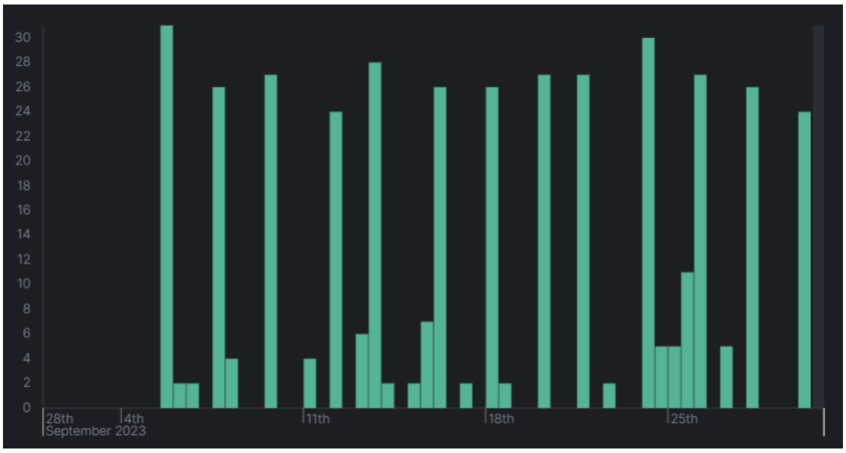


Figure 9- Attacks observed on Port 2575

Operation Technology (OT) Vulnerabilities

The rapid advancements in technology and the convergence of IT and OT have expanded the scope for malicious attackers, thus increasing the scope for vulnerabilities that an attacker can exploit to launch a targeted attack on the critical infrastructure sector.
In today's environment, it is imperative to provide business context to cyber risk to facilitate sound decisions and tailored approaches for risk mitigation.

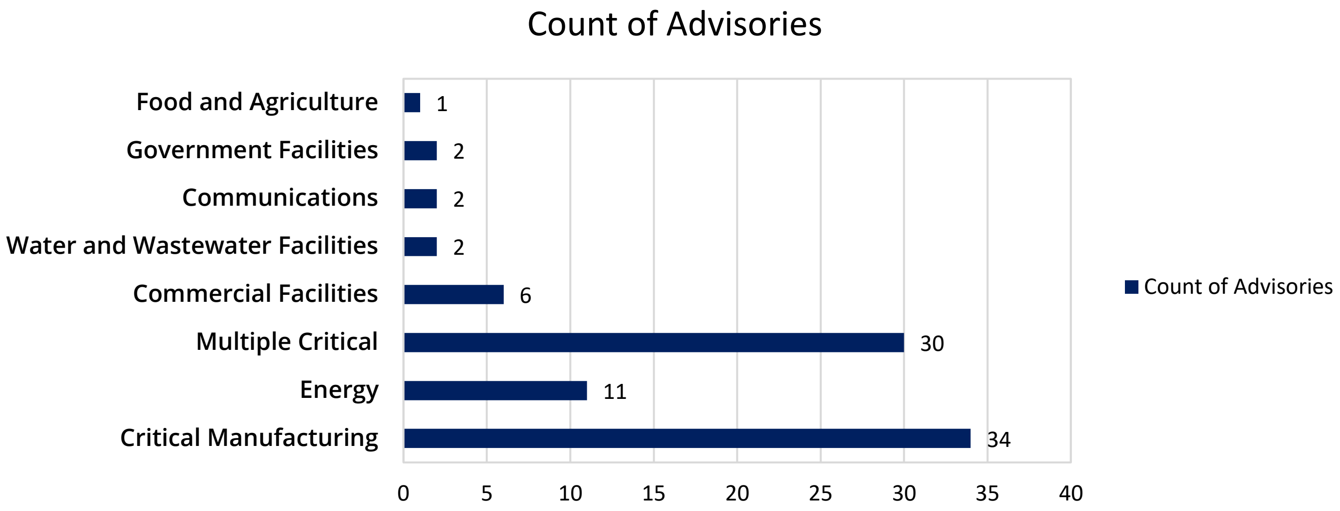
Organizations must focus on protecting the assets within their environment, which add more value to a business and are critical for operational purposes than the ones that add little. Hence, organizations dealing within the OT sector should prioritize safeguarding Cyber Crown Jewel.

Organizations dealing with the Critical Infrastructure (CI) sector should consider utilizing Software Bill of Materials (SBOM) while remediating vulnerabilities within their environment, as TAs are actively scanning for assets through which they can perform lateral movement within the IT or OT environment to target a specific asset like Programmable Logic Controller (PLC), workstation used to develop ladder logic for PLCs, Internet of Things (IoT) devices, etc.

The landscape of vulnerabilities in the OT sector can be seen with the collaboration of State and Private organizations coming together in detecting, reporting, and notifying vulnerabilities in various Industrial Control System (ICS) components. CISA releases regular advisories and alerts for various vendors within this sector to alert organizations about potential flaws within their environment that can be exploited. Also, these advisories help researchers and plant operators to understand and predict which critical infrastructure sectors and what Industrial Control System (ICS) components might pose a risk to the organization.

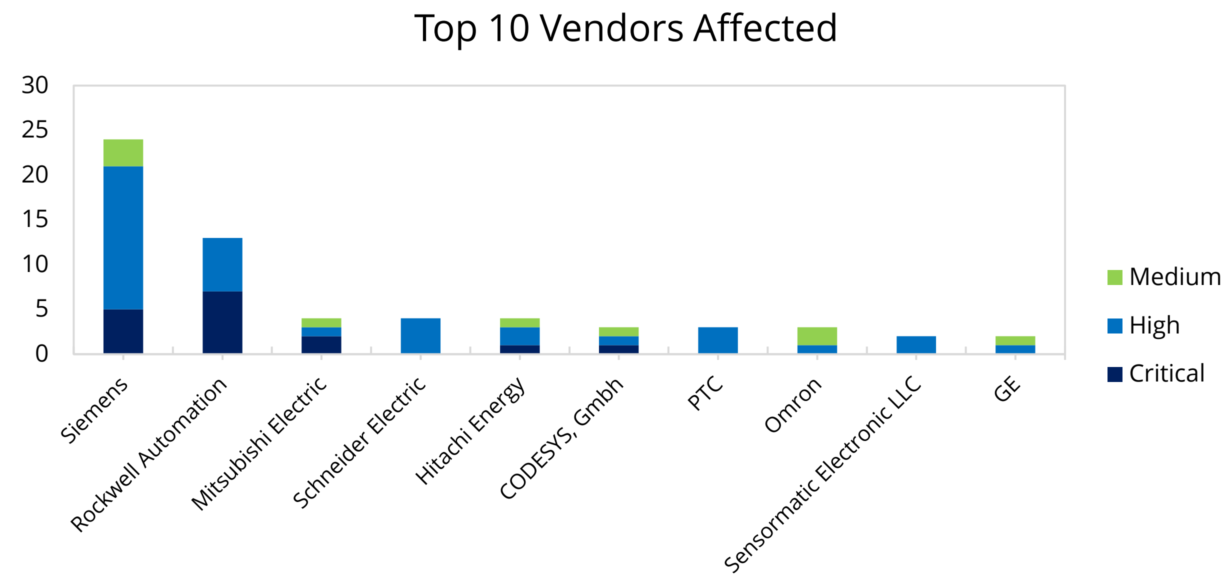
Operation Technology (OT) Advisory Overview

The figure below shows represents the advisories released by the Cybersecurity and Infrastructure Security Agency (CISA) for critical infrastructure sectors for Q3 2023. OEM vendors providing OT assets to Critical Manufacturing and Multiple Critical Infrastructure sectors reported several vulnerabilities.



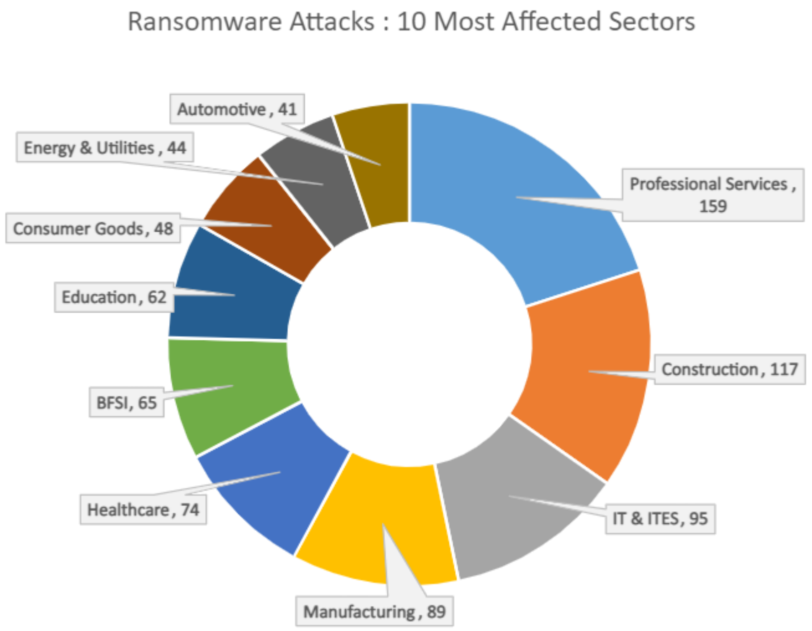
Vulnerability Severity Overview

The below figure represents the severity of vulnerabilities affecting various ICS components used within critical infrastructure sectors issued by the top 10 vendors for Q3 2023. Multiple vulnerabilities were disclosed in products by Siemens and Rockwell Automation.



Top 10 Industry-Wise Ransomware Attacks

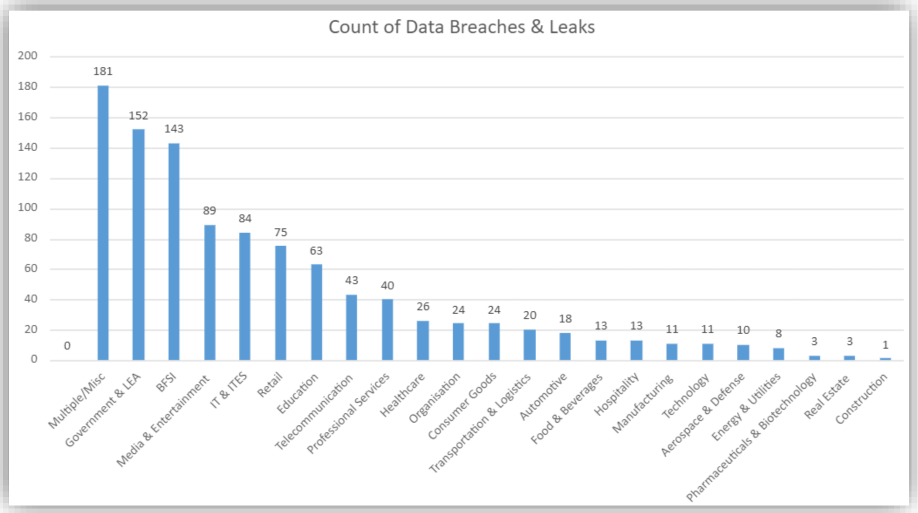
The below figure depicts the top 10 industries attacked by different ransomware groups in Q3, 2023. Professional Services and construction along IT & ITES remained the top targeted Industry.



Dark Web and Cybercrime Activities

Data breaches and Leaks

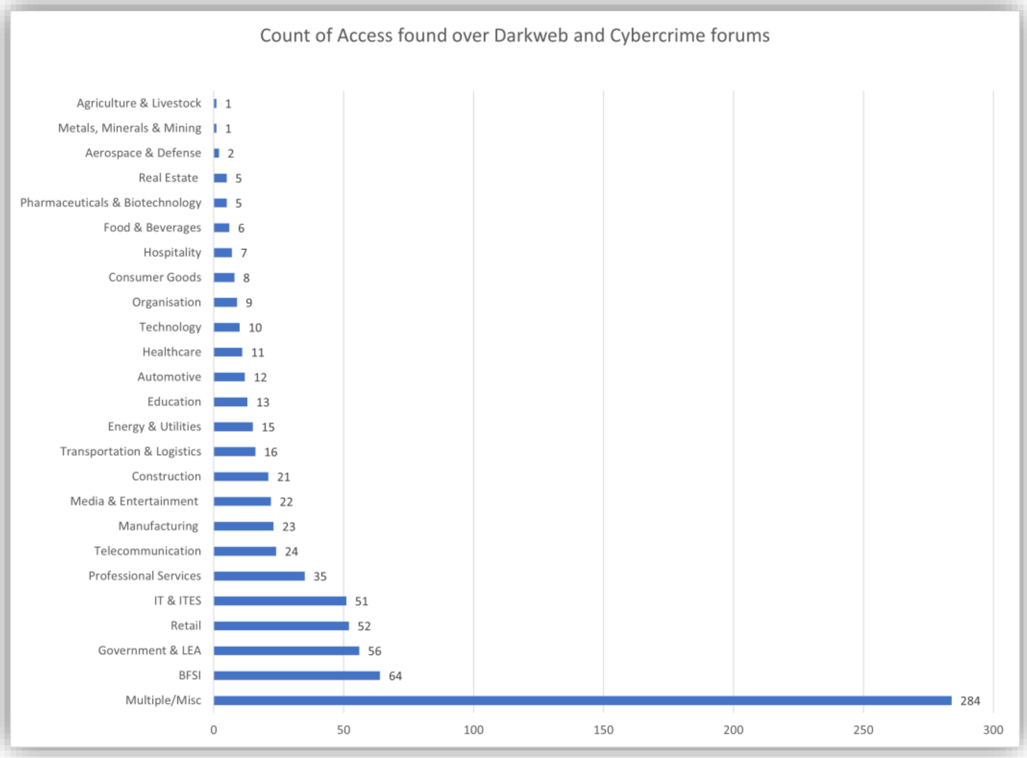
The figure below shows the data breaches and leaks associated with various organizations dealing in the critical infrastructure sector. Government & LEA were most impacted by data breaches that were observed in Q3, 2023



Distribution of Access

A successful cyber-attack by any of the ransomware, data extortion, Advanced Persistent Threat (APT) groups, and other sophisticated cybercriminals is typically preceded by an initial compromise into the victim's enterprise network. The massive rise in ransomware attacks and organized cybercrime activities suggests that initial access being sold over underground forums is widely being utilized by cybercriminals.

Cybercriminals have been improving their tactics and acquiring sophisticated cybercrime tools and techniques to remain ahead of the LEA and cybersecurity community. We have observed IABs playing a notorious role in the organized cybercrime ecosystem. Cybercriminals, including ransomware groups, have created this convenient arrangement to monetize their efforts, thereby reducing their risks and adding further layers of anonymity. The figure below depicts the count of access found over the Darkweb and Cybercrime forums.



Overall Insights

Attacker IP

The following is a list of the top 10 Source IP addresses with the respective attack count.

Source IP	Count
121.196.55.134	7,810
137.184.73.94	281
54.70.100.133	273
34.79.162.186	249
34.76.96.55	246
89.33.44.152	225
54.37.79.75	194
139.144.52.241	188
152.32.234.194	185
152.32.234.194	184

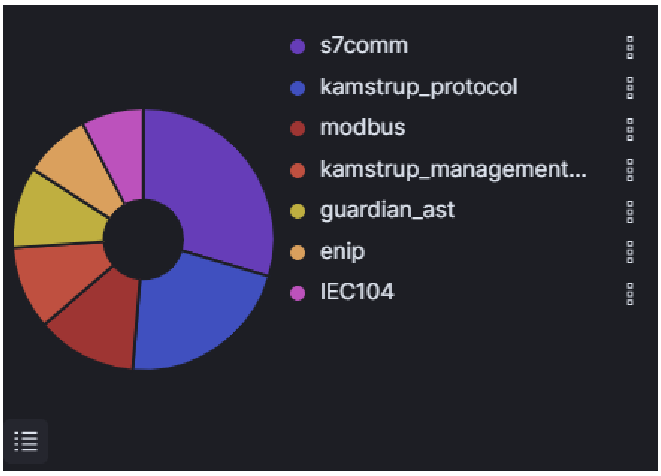
Top 10 ASN

Below is a list of the top 10 ASNs (network operators) with their respective attack counts. In Q3, 2023, we noticed a high volume of attacks from Hangzhou Alibaba Advertising Co., Ltd.

AS	ASN	Count
37963	Hangzhou Alibaba Advertising Co., Ltd.	7,811
396982	GOOGLE-CLOUD-PLATFORM	1,526
14061	DIGITALOCEAN-ASN	1,173
63949	Akamai Connected Cloud	850
6939	HURRICANE	476
16276	OVH SAS	451
135377	UCLOUD INFORMATION TECHNOLOGY HK LIMITED	404
398324	CENSYS-ARIN-01	391
16509	AMAZON-02	315
400161	HAWAIIRESEARCH	225

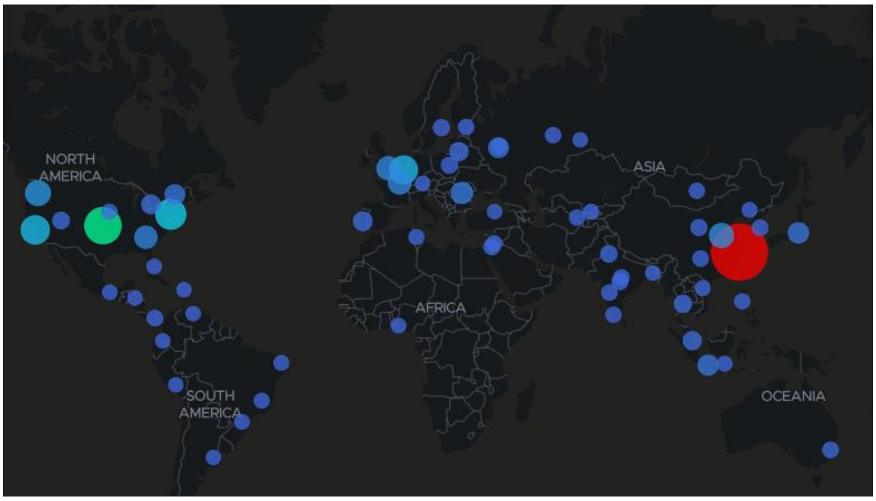
Top ICS components targeted

The below figure represents the various ICS components and protocols targeted for Q3 2023. S7comm (30%), Kamstrup (22%), and Modbus (12%) protocols were among the highest-targeted protocols by attackers

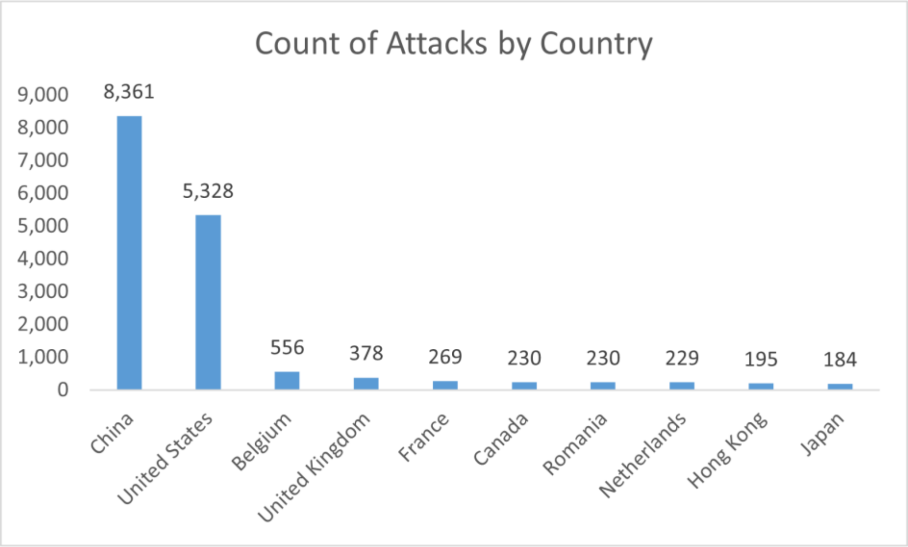


Attacks Observed by Country

The geographical representation of attacks observed by Cyble OT/ICS sensors is shown below.

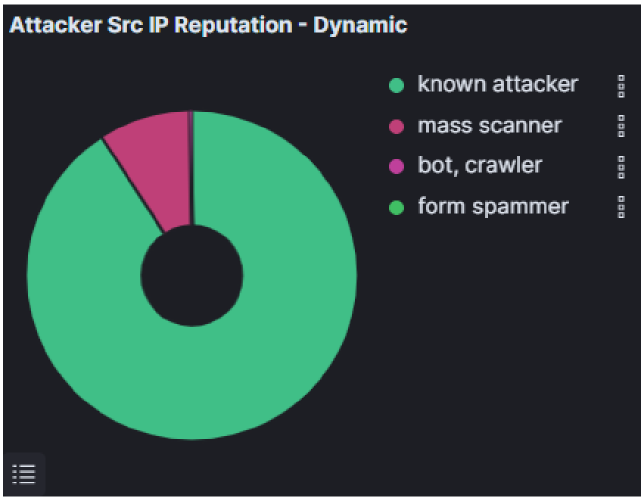


The top 10 countries by attacks are shown below.



Attacker Source IP Reputation

It was observed that the majority of attacks originated from known attackers (91%), and mass scanning attempts were (9%), as shown in the image below.



A surge in ransomware attacks on organizations dealing in the production of Operational Technology (OT) and Industrial Internet of Things (IIoT) was observed in Q3, 2023.

Hacktivist groups actively launched Distributed Denial of Service (DDoS) attacks on multiple organizations globally, which is a significant concern for organizations. DDoS attacks can compromise an organization's ability to access mission-critical applications and deliver vital digital services, which can cost an organization time and money and may impose reputational costs while resources and services are inaccessible.

Researchers at Cyble also observed that Threat Actors (TAs) over cybercrime forums are now selling access to specific Operational Technology components. These components hold a critical role in the Industrial Control System (ICS) environment, and any unauthorized manipulation might significantly impact operations within that organization.

Exposing critical assets such as Human Machine Interface, Supervisory Control and Data Acquisition (SCADA) systems, Programmable Logic Controllers, Remote desktop control applications, etc, due to improper network segmentation allows attackers to easily perform recon and exploitation activities. Hence, organizations dealing in the Critical Infrastructure sector should have proper asset visibility.

NEXT STEPS

- We recommend blocking or monitoring the listed IPs on your security systems shared in the IOC list below.
- We recommend the immediate patching of all vulnerabilities within the IT/OT environment and the routine monitoring of the top Suricata alerts in the internal networks, along with the logs generated from ICS components.
- We recommend that organizations emphasize proper network segmentation to prevent lateral movements of TA and to prevent exposing critical assets over the internet.
- We suggest our clients constantly check for Attackers' ASNs and IPs in the real-time attack table.
- We recommend resetting default usernames and passwords immediately to mitigate brute-force attacks and enforce periodic password changes.
- It is advised to enforce proper access controls within the ICS environment, which is crucial to stop TAs from exploiting operations within the IT/OT environment.
- Securing physical access controls is extremely important for organizations dealing in critical infra sectors.

DISCLAIMER

The information and opinions contained in this document are provided "as is" and without any warranties or guarantees. Reference herein to any specific commercial products, process, or service by trade name, trademark, manufacturer, or otherwise does not necessarily constitute or imply its endorsement, recommendation, or favoring by Cyble Inc. The views and opinions of authors expressed herein do not necessarily state or reflect those of Cyble Inc. and shall not be used for advertising or product endorsement purposes.

INDICATORS OF COMPROMISE (IOCs)

IOC data for each sector identified are shared in a separate spreadsheet by industry.

Recommendations

- Make sure physical access controls and network perimeter security placed by the organization are adequate.

- Implement proper network segmentation to prevent attackers from performing lateral movement and minimize exposure of critical assets over the internet.

- Keep critical assets behind properly configured and updated firewalls.

- Utilize Software Bill of Materials (SBOM) to gain more visibility into assets.

- Keeping software, firmware, and applications updated with the recent patches and mitigations released by the official vendor is necessary to prevent attackers from exploiting vulnerabilities.

- Implementing proper access controls and a zero-trust policy within the IT/OT environment.

- Organizations should follow a strong password policy at all times.

- Regular Audits, Vulnerability, and Pentesting exercises are key in finding security loopholes that an attacker may exploit.

- Continuous monitoring and logging can help in detecting network anomalies early.

- Implement Multi-Factor Authentication wherever possible.

- Keep track of advisories and alerts issued by vendors and state authorities.

- Cyber security awareness training programs for employees within the organization.

- Enhance Risk Mitigation strategies throughout the organization.

- Implement secure backup, archiving, and recovery processes.

About Us

Cyble is a global threat intelligence SaaS provider that helps enterprises protect themselves from cybercrimes and exposure in the Darkweb. Its prime focus is to provide organisations with real-time visibility to their digital risk footprint. Backed by Y combinator as part of the 2021 winter cohort, Cyble has also been recognized by Forbes as one of the top 20 Best Cybersecurity Start-ups to watch in 2020. Headquartered in Alpharetta, Georgia, and with offices in Australia, Singapore, Dubai and India, Cyble has a global presence. To learn more about Cyble, Visit www.cyble.com