DRAGOS

Threat Perspective

# Data Center Operations

info@dragos.com | www.dragos.com

# Table of Contents

# Executive Summary

The modern data center provides critical data processing, communications, storage, backup, and other essential services to the 16 critical infrastructure verticals. With increased cloud technology adoption in critical industrial infrastructure, cloud technology acts as a force multiplier for innovation, efficiency, and reliability within critical infrastructure. Successful operation of cloud resources relies on the complex coordination of industrial control systems (ICS) and operational technology (OT) typically localized in a single facility – a data center (DC).

Dragos assesses with high confidence that the ICS/OT systems within data centers are often connected with technologies that increase the attack surface of traditionally segmented OT networks. Dragos has observed various adversaries deliberately targeting and creating tooling with functionality specific to Data Center Infrastructure Management (DCIM) devices for assessed offensive cyber purposes. DCIMs provide a converged point of management for data center information technology (IT) and OT systems. Cyber activity targeting DCIMs poses a significant risk to the operation of OT systems within data centers and the availability of services critical infrastructure asset owners rely on.

Considering this risk and related threats to data centers, Dragos recommends the implementation of five critical controls for world-class OT cybersecurity identified by the SANS Institute - which presents a framework for implementing a world-class OT cybersecurity program to defend against adversary activity directed against OT networks, be it intellectual property theft, ransomware, or targeted cyber-physical effects.

# Key Findings

- DC operations are critically dependent on a varied ecosystem of OT equipment such as power management systems; heating, ventilation, and cooling (HVAC); fire and life safety systems; water treatment systems; building automation systems (BAS); physical security systems, etc.
- Management of data center OT systems is often carried out by a diverse portfolio of vendors, integrators, and leased data center management – all with varying levels of security capabilities and governance of the third-party and trusted relationship.
- Security researchers identified an adversary campaign targeting cloud service providers (CSP), managed service providers (MSP), and internet service providers (ISP), which utilized stolen data center IT staff credentials to enable unauthorized access to data center management devices with OT capability.[1]
- Dragos observed communications between DCIM devices and a known extortion group (Karakurt Data Extortion Group), indicating that data center operations are a high-value target for extortion and ransomware operations.
- Dragos observed malware samples associated with the WASSONITE Threat Group, which included functionality targeting specific configuration management databases (CMDB) software often used within data center environments. Based on the functionality the adversary included in the malware variant, Dragos assesses with moderate confidence that WASSONITE used the tooling for information gathering and asset

[1] Cyber Attacks On Data Center Organizations – Resecurity

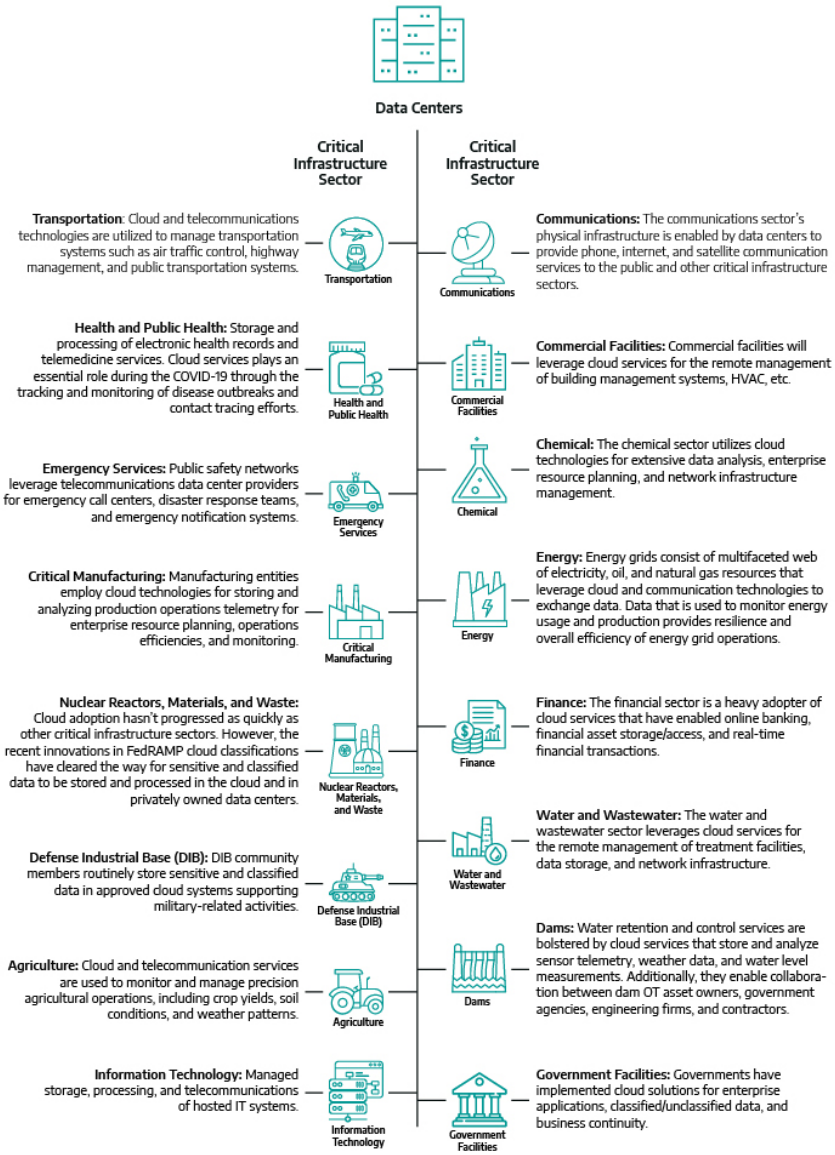
enumeration. Given that asset owners are increasingly using CMDB to manage OT systems, this adversary interest and targeting represents an area of potential risk.

- Adversaries have historically targeted data centers where they have an interest in the data that is being processed/hosted inside the facility.

# Industry Overview

Modern data centers service all 16 critical infrastructure verticals with varying levels of integration. Data center cloud services are used to store, process, and analyze vast amounts of data generated by the 16 sectors. Asset owners are motivated to adopt cloud technologies that enable competitive advantages, operations efficiencies, and resiliency. Cloud adoption varies by industry, but cloud services are used to fulfill several functions across industrial verticals:

FIGURE 1: DATA CENTERS IN CRITICAL INFRASTRUCTURE



***Analyst Note:*** *Dragos is aware of different regional critical infrastructure and key resource sector designations. This report utilizes the 16 critical infrastructure sector definitions as defined by the United States Cybersecurity and Infrastructure Security Agency (CISA) for general purposes.*[2]

# Cyber Threats Targeting Data Center Operations – Industry Focus

## Building Automation/Management Controls Threats

Building automation/management systems (BMS) consist of software, hardware, and communications protocols that integrate multiple building operations systems to optimize building performance, energy management, and facility management. Data center BMS are tasked with managing HVAC operation for people and IT equipment. The real-time management of HVAC in DCs is a differentiating/competitive factor that directly affects available computing power. A compromise of the BMS in a data center could impact (at a minimum) the ambient temperature, humidity, and air particulates.

Data centers manage HVAC operations in real-time through complex control systems which rely on data from facility air handling units (AHU) and computer room air conditioner (CRAC) units. These AHUs/CRAC units leverage communication protocols such as BACnet over wired or wireless mediums to BMS servers that can make on-the-spot HVAC adjustments to direct digital controllers (DDC).

### Dragos Professional Services BAS Findings

Dragos Professional Services engagements have found several commonalities in BAS and Building Management Systems (BMS) configurations that provide possible avenues for adversaries to impact dependent OT/IT processes Table 1 shows examples of Dragos research findings aligned with the relevant MITRE ATT&CK Protocols that adversaries could use to take advantage of vulnerable BAS/BMS systems.

TABLE 1 BAS/BMS COMMON FINDINGS

| BAS/BMS Finding | ATT&CK Function |
|---|---|
| Dual-Homed Asset | TA0109 Lateral Movement<br>T0818 Engineering Workstation Compromise |
| Lack of IT/OT Demilitarized Zone | T0843 Program Download<br>T0880 Loss of Safety |
| BACnet Input Value Manipulation | T0836 Modify Parameter<br>T0879 Damage to Property<br>T0831Manipulation of Control<br>T0832 Manipulation of View |

[2] A Guide to a Critical Infrastructure Security and Resilience - November 2019 - CISA

**APT Uses ShadowPad Backdoor and MS Exchange Vulnerability to Attack BAS**

Adversaries routinely gain initial access into systems by exploiting vulnerable, public-facing assets such as those CISA catalogs.[3] Organizations that do not segment their BAS from public facing IT and OT assets increase their attack surface and risk additional attack vectors, such as lateral movement or ransomware. On 27 June 2022, the Kaspersky ICS CERT team reported an attack against at least three different organizations in telecommunications, manufacturing, and transportation using the ShadowPad backdoor against the victim's BAS infrastructure. Kaspersky ICS CERT assesses the likely objectives of the BAS intrusion are focused on information gathering. As described above, adversary access to a BAS can enable severe impacts to the operation of critical DC OT systems, with potential implications for DC stability and operations.

During the intrusion, the Kaspersky ICS CERT team observed the threat actor successfully compromise at least one engineering computer in Building Automation Systems belonging to a telecommunications company in Pakistan. The threat actor exploited a known Microsoft Exchange Server Remote Code Execution Vulnerability (CVE-2021-26855) for a means of initial access throughout this operation. According to the Kaspersky ICS CERT team, the threat actor routinely executed a series of commands via the command line interface (T0807 Command-Line Interface) for T0846 Remote System Discovery. Additionally, the threat actor sent malicious cmd.exe scripts over the local network using the "net use" service. A complete list of the MITRE ATT&CK tactics, techniques, and procedures (TTP) used in this intrusion can be found in the Kaspersky ICS CERT Report, Attacks on industrial control systems using ShadowPad.[4]

## Fire and Life Safety Systems Threats

Fire and life safety systems are tasked with executing the automated and manual safety protections for data center building occupants and equipment. Sensors, controllers, and various computing technologies synchronize to carry out the life and equipment-protection functions. A life safety system is exclusively designed to prevent the loss of life, and fire safety systems are designed for multiple functions, such as: protecting the the property from fire damage, fire/smoke detection, and fire/smoke mitigation. Fire and life safety systems are implemented in various architectures of passive or active systems. Dragos is unaware of any pervasive threats to passive fire and life safety systems as they are typically non-networked systems whose process depends on physical hazard detection rather than computing. Active fire and life safety systems monitor various physical parameters such as temperature, smoke, carbon monoxide, etc. Fire and life safety systems are then actuated depending on the logic of the designed systems. Standard process outputs from fire and life safety systems include fire suppression systems, HVAC changes, building lighting, and building access changes (locking and unlocking of doors).

In cases where third-party vendors leverage remote access solutions to manage the fire and life safety systems, there is a risk of a third-party compromise that may impact the control system. This is generally seen when a data center is in a multi-tenant building. Adversaries often scan the internet hunting for vulnerable remote access technologies that are exposed on the public internet. This opens the door for opportunistic exploitation of those vulnerable remote technologies that the fire and life safety management vendor can leverage. The OT impact of an intrusion into fire and life safety systems is primarily architecture dependent, but at a minimum, the access could be used for lateral movement, information gathering, or the deliberate activation of fire suppression systems. Dragos assesses that it is unlikely that a fire and life safety system process can be entirely denied or disrupted due to the physical fail-safe and override mechanisms in place for these systems.

[3] CISA Known Exploited Vulnerabilities Catalog - CISA
[4] Attacks on Industrial Control Systems Using ShadowPad – Kaspersky ICS CERT

## Data Center Infrastructure Management Threats

Data Center Infrastructure Management (DCIM) systems manage and optimize a data center's physical infrastructure while enabling data center management through integration with Enterprise Resource Management (ERP) technologies. DCIMs are a collection of tools and applications that provide these asset owners with real-time data on servers, storage devices, power management systems, and HVAC systems. OT systems within data centers will send real-time telemetry to the DCIM via protocols such as simple network management protocol (SNMP), Modbus, BACnet, hypertext transfer protocol (HTTP/S), and most commonly, Open Platform Communications (OPC). DCIMs offer adversaries large attack surfaces with common protocols and heavily connected architectures with multiple OT systems within reach.

### Targeting of DCIM Technologies

Adversaries operating within data center environments have targeted DCIM technologies since at least March 2020. Since that time, Dragos has identified malware variants linked with the WASSONITE threat group that have multiple features that allow it to communicate with DCIM technologies including CMDB devices. Most modern DCIM technologies have a built-in CMDB or connection to a CMDB associated with an ERP system. This malware also exhibited enumeration features, which allowed the adversaries to effectively reconnoiter a victim's OT environment.

In addition to the WASSONITE-linked malware samples, Dragos also observed activity between November 2022 and February 2023 suggesting DCIM technology in the European Union may have been attacked by the Karakurt Data Extortion Group. In fact, in late 2022, the Infinitum IT CTI team attributed the IP address in question (Table 2) to the Karakurt Data Extortion Group through their research into Conti ransomware operations.[5] Dragos observed this communication occur via a secure shell over port 22. Dragos is unaware of an OT impact to the DC operations that hosted the DCIM, however, the DCIM device was removed after March 2023. Dragos is also unaware of any possible Conti ransomware impact to DCIM technologies during this period. CISA assesses that Karakurt primarily obtains access to victim devices by purchasing stolen credentials via third-party intrusion broker networks.[6]

TABLE 2 ADVERSARY INFRASTRUCTURE USED IN DCIM TARGETING, NOV22-FEB23

| Adversary Controlled IP Address | Observed Communication Ports |
|---|---|
| 45.141.84[.]126 | 22 – Secure Shell |

### Stolen Credentials from Data Center IT Staff

The marketplaces for stolen credentials have recently included cloud service providers and managed service providers of data centers. Between September 2021 and January 2023, Resecurity researchers identified a campaign targeting cloud service providers (CSP), managed service providers (MSP), and internet service providers (ISP) that utilized stolen data center IT staff credentials to facilitate unauthorized access to data center management devices with OT capability.[7] Data center IT staff credentials were included in the data set from the following organizations:

[5] Attacks on industrial control systems using ShadowPad – Kaspersky
[6] Karakurt Data Extortion Group – CISA
[7] Cyber Attacks On Data Center Organizations – Resecurity

TABLE 3 ADVERTISED IT STAFF CREDENTIALS FOR DC-RELATED ORGANIZATIONS

| Organization Name | Organization Type |
|---|---|
| China Telecom Americas | Cloud and Data Center Services |
| China Telecom Global | Cloud and Data Center Services |
| Cyxtera | Data Center Operations |
| CenturyLink | Internet Service Provider and Telecommunications |
| Nutanix | Cloud Service/Technology Provider |
| GDS Holdings | Data Center Operations |
| Idemia | Identity Management |

## Power Management Systems Threats

Data centers use various power management systems to ensure uninterrupted power supplies (UPS), power quality, and efficient energy distribution (and, in some cases, generation). These systems include OT devices such as UPS, power distribution units (PDU), automatic transfer switches (ATS), power monitoring systems, and connections to renewable energy assets. The attack surface of the power management system within a data center can vary greatly depending on the power system architecture and whether there are onsite power generation capabilities. UPS and renewable energy assets are often managed by third parties that leverage remote access solutions for real-time monitoring and sometimes control of the OT assets. The management interfaces utilized by managed service providers also offer an intrusion vector for adversaries to achieve direct access into the power management system. In March 2022, CISA published reporting on cyber attacks against UPS devices. CISA assesses that adversaries are gaining access to a variety of internet-connected UPS devices through default credentials.[8]

This threat activity highlights two important threat modeling factors:

1. Internet-connected OT devices will continue to be reconnoitered and opportunistically/deliberately exploited
2. Adversaries are aware of the remote access capabilities baked into many UPS systems and are actively looking for them

Even if a UPS system is not directly connected to the internet, the path of least resistance for an adversary to gain access to the DC power management systems will likely be through the management interfaces.

## Water Management Systems Threats

Data centers will often utilize an on-site water treatment capability to ensure the proper functioning of water-cooling systems to prevent damage to equipment caused by impurities and contaminants in the water. Water treatment in a data center is a managed industrial process that combines sensor inputs from field devices to anticipate water scaling, corrosion, and microbiological problems with a real-time capability to adjust water chemistry. Water management vendors will require routine access to site-specific water telemetry to develop water treatment analytics. This data will leave the data center through a remote access solution, cloud connection, or mobile vendor equipment (laptops, meter reading devices, etc.).

Dragos is unaware of any pervasive threats targeting the water management systems of data centers. The water management system's threat environment is largely architecturally dependent on how the vendor maintains access.

[8] Mitigating Attacks Against Uninterruptible Power Supply Devices – CISA

Water management vendors pose a significant third-party vendor risk due to their pervasive access into multiple data center water management systems. A single compromise of a water management vendor could impact the water treatment process for multiple data centers.

## Physical Security Systems

Physical security systems are designed/implemented to protect the data center facility, equipment, and personnel from physical threats. Physical threats include unauthorized access, theft, and damage. Data center physical security systems will typically consist of access control, surveillance, and perimeter security systems. Physical security systems are physically distributed around the data center to ensure their sensor coverage is representative of the data center's physical footprint. This distribution will often require the use of wireless communication mediums such as Wi-Fi, Bluetooth, etc. Wireless interdiction technologies such as jamming, interception, or masquerading threaten the wireless signals of physical control systems even though proper configuration of the wireless communications media will mitigate these wireless threats. Additionally, data centers routinely implement cameras with sensor technology that can perform functions such as heat monitoring. This additional telemetry is often communicated to DCIM servers through protocols such as MQTT.

Surveillance systems with internet-connected cameras are a target of choice for botnet developers and operators. Dragos assesses with moderate confidence that multiple threat groups target IP cameras in support of initial access and information-gathering operations. This threat activity highlights that known OT impact threat groups have the intention and capability to develop and maintain botnets that leverage IoT devices. If a data center is leveraging internet-connected cameras as a part of its physical security system, then engagement with IoT botnet activity should be anticipated.

## Supply Chain Considerations

DC operations employ a complex and regionally varying supply chain of mission-critical equipment. OT-specific equipment can face supply constraints that may impact the recovery time. Data center asset owners should be aware of the following threats to their supply chains:

**Counterfeit Hardware:** Counterfeit server hardware has been sold through ad hoc equipment retailers that have modified and masked counterfeit equipment to appear legitimate. In 2022, a U.S.-based person was charged with the widespread sale of counterfeit Cisco Systems network equipment. [9] This incident represents a concerted effort between retailers and China-based counterfeiters to supply counterfeit/substandard industrial networking equipment that is often used in data center environments.

**Malicious and Unwanted Software/Firmware:** The 2020 SolarWinds supply chain incident was a sophisticated event where malicious software was deployed through a legitimate software update from trusted vendors. SolarWinds estimates that 18,000 were infected with the tampered SolarWinds Orion software, giving the adversary unprecedented access into the affected organizations.[10] Additionally, there are regional regulations regarding the use of specific manufacturer's equipment in DC environments. The U.S. Federal Communication Commission has banned the sale and import of new Huawei and ZTE telecommunications devices. The reason for the regulation cites national security and concerns over data confidentiality that is processed with Huawei/ZTE equipment. Several other nations, such as Canada, England, and Australia, have implemented similar regulations citing the same national security concerns[11].

[9] Florida man charged with selling $1bn worth of fake Cisco networking equipment - Data Center Dynamics
[10] A 'Worst Nightmare' Cyberattack: The Untold Story Of The SolarWinds Hack – NPR
[11] FCC bans U.S. sales of Huawei and ZTE equipment over national security concerns – Axios

**Equipment Transportation/Storage Theft:** Data center equipment is particularly vulnerable to physical theft during the equipment transportation and storage phases of construction. The National Equipment Register (NER) and National Insurance Crime Bureau (NIB) assess that equipment theft is highest during the construction phases and most often occurs off-premise.[12] From transportation to delivery, DC equipment is likely to be stored in locations with varying levels of physical security.

# Cyber Threats Targeting Data Center Operations – Regional Assessment

Dragos does not perform attribution on threats. However, when other third-parties perform attribution, especially government entities, we document this for others if it is of interest. It is our position that this style of attribution is not valuable from a network defense perspective and thus Dragos does not spend resources on performing this action internally.

## North America

Data centers in North America service highly sensitive client data such as the Defense Industrial Base (DIB) and federal government. Recent adversary activity targeting U.S-based data center IT staff represents a threat landscape focus on the operations of the data center. Adversaries have demonstrated an understanding of the data center operators and leaser relationship and will likely continue to exploit data centers through the supply chain and management channels.

## Europe

Data centers in Europe have been targeted to strategically impact the data owners whose data is perceived to have been processed at the facility. Russia has caused at least $1.79B worth of damage to Ukraine's telecommunication infrastructure since the start of its invasion of Ukraine.[13] The Office of the Director of National Intelligence (ODNI) assesses that Russia will likely continue and improve its ability to target critical infrastructure and telecommunications in the region,[14] and that the geopolitical climate in the EU will continue the threaten the security of regionally specific data centers.

## The Middle East and North Africa (MENA)

The MENA data center market is anticipated to grow at a compound annual growth rate of 20.4% between 2022-2028, according to RationalStat's analysis.[15] This rapid growth and quick implementation of large data center projects create an expanding risk to the supply chain of MENA data centers. OT threat groups such as HEXANE have been observed targeting telecommunication entities with custom C++ backdoors and credential-stealing PowerShell scripts as recently as August 2022 in the MENA region. Additionally, Sentinel Labs published research on a threat actor dubbed "Metador" that has achieved pervasive access into the telecommunications and internet service provider (ISP) infrastructure in the MENA region. Sentinel Labs assesses that this advanced threat actor is focused on

[12] 2016 Equipment Theft Report - National Equipment Register, National Insurance Crime Bureau
[13] Russia caused at least $1.79 billion worth of damage to Ukraine's telecoms infrastructure – Data Center Dynamics
[14] 2023 ODNI Threat Assessment– Office of the Director of National Intelligence
[15] Middle East Data Center Market - Industry Outlook & Forecast 2022-2027- Research and Markets

widespread data collection operations and long-term, reliable access into MENA ISPs/telecommunications infrastructure.[16] Asia-Pacific (APAC).

Data center service providers in the APAC were the most heavily targeted in the IT staff credential campaign uncovered by Resecurity's research.[17] Dragos has observed the WASSONITE threat group creating tooling to target data center-specific technologies, highlighting that TGs have the capability and intention of targeting data centers in the APAC region with tailored malware and possible impacts to the data center OT systems.

### South America

Brazil currently hosts the majority of data centers in South America. Crowdstrike assesses that China-Nexus adversaries primarily target the telecommunications and technology sectors within South America .[18] Increased investments from CSP giants such as AWS, Microsoft, Google, Oracle, Huawei, etc., further increase the data center targeting incentive for cybercrime groups that also aid espionage activities for host nation competitive intelligence.

## Defensive Recommendations

Considering this risk and related threats to data centers, Dragos recommends the "5 Critical Controls for World-Class OT Cybersecurity" identified by the SANS Institute[19] - which presents a framework for implementing a world-class OT cybersecurity program to defend against adversary activity directed against OT networks, be it Intellectual Property theft, ransomware, or targeted cyber-physical effects.

A first step in implementing these controls is achieving executive alignment on the role and importance of OT cybersecurity and the specific risks an OT cybersecurity program is meant to defend against, if not well understood. One possible way to achieve this organizational alignment is to tie the effort back to real-world scenarios. The information in the documents detailed above clearly outlines the capabilities developed by adversaries and their intended impacts. This detail can be instrumental in understanding how the capabilities might impact a given network, the potential operational and business implications, and the steps necessary to defend against and remediate the potential effects.

Translating cyber risks into the impact on an organization's operations and functions can help executive stakeholders engage on the topic of OT cybersecurity. Once an organization can achieve executive and board-level alignment on the importance of investing in OT cybersecurity, the foundation is in place for the implementation of the five critical controls shown below:

1. **ICS INCIDENT RESPONSE**
   Operations-informed incident response (IR) plan with focused system integrity and recovery capabilities during an attack exercise designed to reinforce risk scenarios and use cases tailored to the ICS environment. OT's incident and response plan is distinct from IT's because:
   - OT involves different device types, communication protocols, and different types of tactics, techniques, and procedures (TTPs) specific to the industrial threat groups.
   - Investigation requires a different set of tools and languages.

[16] The Mystery of Matador An Unattributed Threat Hiding in Telcos Isps and Universities – Sentinel One
[17] Cyber Attacks On Data Center Organizations – Resecurity
[18] 2023 Global Threat Report – CrowdStrike
[19] The Five ICS Cybersecurity Critical Controls – SANS Institute

- Managing the potential impact of an incident is different for WWS compared to pipelines, electrical grids, and manufacturing plants.

**2. DEFENSIBLE ARCHITECTURE**

Architectures that support visibility, log collection, asset identification, segmentation, industrial DMZs (Demilitarized Zones), and process-communication enforcement. OT security strategies often start with hardening the environment - removing extraneous OT network access points, maintaining strong policy control at IT/OT interface points, and mitigating high-risk vulnerabilities.

- Perhaps even more important than secure architecture are the people and processes to maintain it.
- The resources and technical skills required to adapt to new vulnerabilities and threats should not be underestimated.
- Ransomware is one of your top threats and network segmentation of IT/OT systems is critical to containing the spread.

**3. ICS NETWORK VISIBILITY MONITORING**

Continuous network security monitoring of the ICS environment with protocol-aware toolsets and system of systems interaction analysis capabilities used to inform operations of potential risks to control. You can't protect what you can't see.

- A successful OT security posture maintains an inventory of assets, maps vulnerabilities against those assets (and mitigation plans), and actively monitors traffic for potential threats.
- The visibility gained from monitoring your industrial assets validates the security controls implemented in a defensible architecture.
- Threat detection from monitoring allows for scaling and automation for large and complex networks.
- Additionally, monitoring can also easily identify vulnerabilities for action.
- CHERNOVITE's PIPEDREAM can only be detected by monitoring East-West communications with ICS-aware protocols - you won't be able to identify your most dangerous threats – the ones with physical impacts, without a complete view of activity across your OT network.

**4. SECURE REMOTE ACCESS**

Identify and inventory all remote access points and allowed destination environments, on-demand access, and multi-factor authentication (MFA), where possible, jump host environments to provide control and monitor points within the secure segment. Secure remote access is critical to OT environments.

- One key method, multi-factor authentication (MFA), is a rare case of a classic IT control that can be appropriately applied to OT.
- Implement MFA across your systems of systems to add an extra layer of security for a relatively small investment.
- Where MFA is not possible, consider alternate controls such as jump hosts with focused monitoring.
- The focus should be placed on connections in and out of the OT network, not connections inside the network.

**5. RISK-BASED VULNERABILITY MANAGEMENT**

Understanding the cyber digital controls in place and device operating conditions that aid in risk-based vulnerability management. This includes decisions to patch for the vulnerability, mitigate the impact, or monitor for possible exploitation. Knowing your vulnerabilities and having a plan to manage them is critical to a defensible architecture.

- While patching an IT system like a worker's laptop is relatively easy, shutting down a plant has enormous costs.

- An effective OT vulnerability management program requires timely awareness of key vulnerabilities that apply to the environment, with correct information and risk ratings, and alternative mitigation strategies to minimize exposure while continuing to operate.

**Data Center vendor/leaser technical guidance:** should, at a minimum, cover the following topics in accordance with the data center's security governance and policies:

- Vendor-owned and managed laptops/transient devices
- Removeable media
- Collaboration tools
- Vendor/Leaser wireless networks

# Dragos Threat Groups

## CHERNOVITE


CHERNOVITE has the capability to disrupt, degrade, and potentially destroy industrial environments and physical processes in industrial environments. Through normal business, independent research, and collaboration with various partners in early 2022, Dragos identified and analyzed the capabilities of a new industrial control systems (ICS)-tailored malware PIPEDREAM. PIPEDREAM is the seventh known ICS-specific malware following STUXNET, HAVEX, BLACKENERGY2, CRASHOVERRIDE, and TRISIS.

The PIPEDREAM malware framework module MOUSEHOLE utilizes an open platform communication unified architecture (OPC UA) client that contains functionality found in legitimate applications.[20] The ubiquity of OPC UA within Data Center environments makes them susceptible to OT impacts via the MOUSEHOLE module of the PIPEDREAM malware framework, which includes a range of functionality targeting this protocol.

## HEXANE


HEXANE targets oil and gas and telecommunications in Africa, the Middle East, and Southwest Asia. Dragos identified the group in May of 2019. HEXANE operations rely on malicious document files to drop malware on victim machines, from which HEXANE can then proceed to further actions and objectives on the target network.[21]

HEXANE has been observed targeting telecommunications entities with custom C++ backdoors and credential-stealing PowerShell scripts as recently as August 2022. Telecommunications are a critical component of data center cloud services to distributed customers – with some data centers functioning entirely as telecommunications points.

*Associated Groups:* CHRYSENE, OilRig, Lyceum

[20] Analysis of MOUSEHOLE and Open-Source OPC UA Library - Dragos
[21] HEXANE - Dragos

## WASSONITE


WASSONITE targets entities in nuclear energy, electric, oil and gas, aerospace, data center, and advanced manufacturing industries, predominately in South Asia and East Asia, with some additional entities targeted in North America. This TG targets electric generation, nuclear energy, manufacturing, and research entities in India and likely South Korea and Japan. The group's operations rely on the Appleseed and DTrack malware families, credential capture tools, and system tools for lateral movement. WASSONITE has operated since at least 2018.

Dragos observed WASSONITE utilizing data center native technologies (Configuration Management Databases) to further advance their cyber operations and information gathering objectives.

*Associated Groups:* Lazarus Group

# In Conclusion

Data centers are a crucial component of the critical infrastructure ecosystem, enabling the processing, storage, and management of OT-related data for all industrial sectors. Additionally, data center operations often rely on the complex operations of site-hosted OT systems that are at risk from their increasing attack surface. Numerous adversaries have demonstrated the intent and capability to disrupt data center operations through direct targeting and indirectly through supply chain attacks. In addition, advanced adversaries and threat groups have attacked data centers for espionage and information-gathering purposes while leveraging persistent access to telecommunication and internet service provider's infrastructure.


# ABOUT DRAGOS, INC.

Dragos, Inc. has a global mission to safeguard civilization from those trying to disrupt the industrial infrastructure we depend on every day. Dragos is privately held and headquartered in the Washington, DC area with regional presence around the world, including Canada, Australia, New Zealand, Europe, and the Middle East.

**To learn more about a Dragos Threat Intelligence subscription, contact us for a demonstration.**

Request a Demo



This report was prepared for and shared with Dragos Threat Intelligence customers in June 2023. The threat intelligence contained in this report is still relevant and applicable.

info@dragos.com @DragosInc @Dragos, Inc.