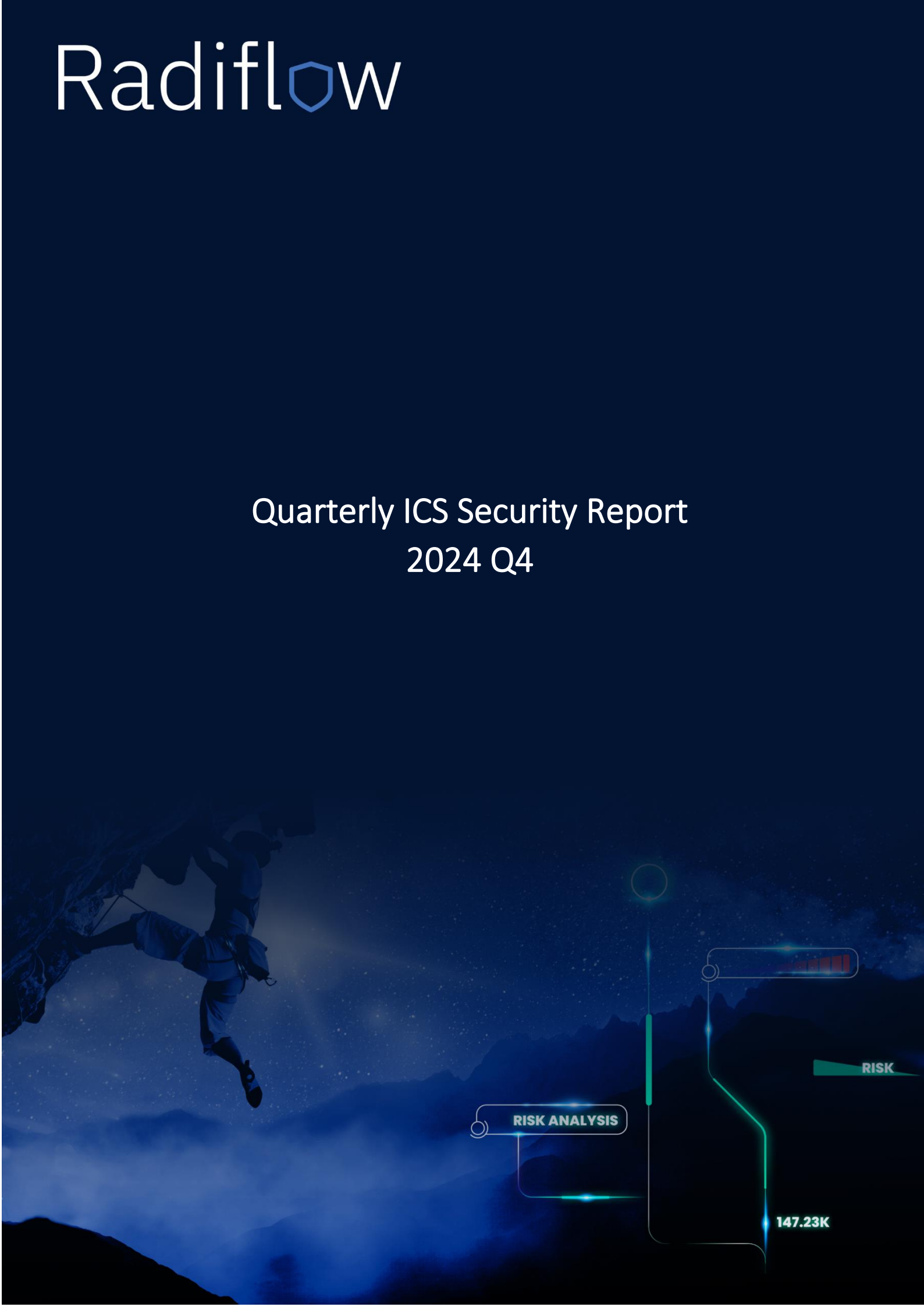
Radiflow

Quarterly ICS Security Report
2024 Q4



Radiflow

Contents

Radiflow

Executive Summary

This report offers a detailed analysis of key ICS cybersecurity developments during Q4 2024, highlighting significant incidents, newly identified vulnerabilities, and evolving threat trends. Key findings include ransomware attacks on OT operators across critical sectors, the emergence of sophisticated malware targeting OT and IoT environments, and important insights from recent CISA ICS advisories.

The report also examines vulnerabilities in industrial automation systems from major vendors, providing actionable recommendations to address associated risks. Additionally, Radiflow has enhanced the CIARA Threat Intelligence database with updates on advanced threat groups and new techniques, equipping customers with the tools to strengthen their OT defenses.

Radiflow strongly encourages customers and partners to review the findings, apply necessary security updates, and adopt best practices to reduce exposure to emerging threats.

ICS Cybersecurity Incidents

Energy

On December 9, 2024, the Lynx ransomware gang targeted Electrica Group, a leading Romanian energy supplier serving over 3.8 million customers. Electrica announced that the Group's critical systems, including SCADA, remained unaffected; however, disruptions occurred due to proactive measures implemented to contain the incident.

On October 29, 2024, Newpark Resources, a Texas-based oilfield services provider, detected a ransomware attack by an unknown actor. The incident disrupted business applications, including financial and operational reporting systems. However, the company's manufacturing and field operations continued in all material respects, utilizing established downtime procedures to ensure minimal disruption to essential activities.

Water and Wastewater

On October 3, 2024, American Water, the largest publicly traded U.S. water and wastewater utility, detected unauthorized activity within its computer networks, identifying it as a cybersecurity incident. In response, the company disconnected certain systems, including its customer billing platform, to protect data and prevent further harm. Despite these measures, water and wastewater operations remained unaffected.

Manufacturing

In November 2024, Schneider Electric experienced a cyberattack by the Hellcat ransomware group. The attackers claimed to have accessed the company's Atlassian Jira system, exfiltrating approximately 40GB of compressed data, including project details and over 400,000 rows of user information. Schneider Electric confirmed the unauthorized access to an internal project tracking platform but stated that their products and services remained unaffected. This incident marks the company's third cyber breach in less than two years, following previous attacks by the Cactus ransomware group in February 2024 and the Cl0p ransomware group in 2023.

Communications

In December 2024, BT Group, a UK-based telecommunications company, was hit by a Black Basta ransomware attack. The company promptly isolated the affected servers, ensuring services remained fully operational. Black Basta claimed responsibility, alleging the theft of 500GB of sensitive data, including financial records, user data, and confidential documents

New Malware

A new malware, IOCONTROL, has been identified targeting Operational Technology (OT) and Internet of Things (IoT) environments. Developed by the advanced threat actor group Cyber Avengers, IOCONTROL was discovered during an attack on Orpak and Gasboy fuel management systems. The malware is specifically designed to compromise OT and IoT environments, featuring capabilities such as evading detection mechanisms and manipulating operational configurations to disrupt normal system processes.

Radiflow

ICS Vulnerabilities

In this section of the cyber update, we offer an aggregated overview and statistics of cyber vulnerabilities and notable ICS vulnerabilities published in Q4 of 2024.
Total new vulnerabilities in Q4: **11,064**
ICS vulnerabilities published in Q4: **334**

severity	CVEs
Critical	**49**
High	**191**
Medium	**84**
Low	**10**

Total new CISA KEVs (Known Exploited Vulnerabilities) in Q4 of 2024: **55**
ICS Vulnerabilities Within CISA KEV: **3**

CVE	CVSS	Vendor	Product	Affected ICS
CVE-2024-0012	10.0	Palo Alto Networks	PAN-OS	Siemens RUGGEDCOM APE1808
CVE-2024-9474	6.9	Palo Alto Networks	PAN-OS	
CVE-2023-44487	7.5	IETF	HTTP/2	Siemens SINC INS

CISA ICS Advisories

Total new CISA ICS advisories in Q4 of 2024: **115**.
Notable ICS Vulnerabilities:

SIEMENS

Product	CVE	CVSS	details	Mitigation
SINEC Security Monitor	CVE-2024-47553	9.9	Improper input validation vulnerability	Update to V4.9.0
SINEC Security Monitor	CVE-2024-47562	9.3	command injection vulnerability	Update to V4.9.0
HiMed Cockpit	CVE-2023-52952	9.3	A restricted desktop environment escape vulnerability	Update to V11.6.2
PSS SINCAL	CVE-2024-45181	9.3	A vulnerability in a third party component used by PSS SINCAL - WibuKey	update WibuKey Runtime for Windows to V6.70
SINEC INS	CVE-2023-32002	9.8	A vulnerability in Node.js allows bypass of the policy mechanism, exposing sensitive data	Update to SINEC INS V1.0 SP2 Update 3
SINEC INS	CVE-2023-39332	9.8	An improper input validation vulnerability in a third-party component - Node.js	Update to SINEC INS V1.0 SP2 Update 3
SINEC INS	CVE-2023-47100	9.8	An improper input validation vulnerability in a third-party component -	Update to SINEC INS V1.0 SP2 Update 3

			Perl	
SINEC INS	CVE-2023-52389	9.8	A buffer overflow vulnerability in a third-party component - UTF32Encoding.cpp	Update to SINEC INS V1.0 SP2 Update 3
SINEC INS	CVE-2024-46888	9.9	A path traversal vulnerability leading to code execution	Update to SINEC INS V1.0 SP2 Update 3
SINEC INS	CVE-2024-46890	9.1	An improper input validation vulnerability in the web API	Update to SINEC INS V1.0 SP2 Update 3
SINEC INS	CVE-2023-44487	7.5	a vulnerability in the HTTP/2 protocol used by the product allows rapidly creating and canceling requests, causing denial of service. NOTE: **This vulnerability is exploited in the wild.**	Update to SINEC INS V1.0 SP2 Update 3
TeleControl Server	CVE-2024-44102	10.0	Insecure deserialization vulnerability enabling remote code execution	Update to V3.1.2.1
RUGGEDCOM APE1808	CVE-2024-0012	10.0	An authentication bypass vulnerability in a third-party component - Palo Alto Networks PAN-OS NOTE: **This vulnerability is exploited in the wild.**	Siemens has released a patch and recommends limiting access to the management interface to trusted internal IP addresses
RUGGEDCOM APE1809	CVE-2024-9474	6.9	An OS command injection vulnerability in a third-party component - Palo Alto Networks PAN-OS, allows privilege escalation with root privileges. NOTE: **This vulnerability is exploited in the wild.**	Siemens has released a patch and recommends limiting access to the management interface to trusted internal IP addresses
SIMATIC PCS neo V5.0 and SINEC NMS	CVE-2024-49775	9.8	A heap-based buffer overflow vulnerability in the integrated UMC component	SIMATIC PCS neo V5.0: Update to V5.0 Update 1 Update SINEC NMS to V3.0 SP2 and UMC to V2.15 Siemens has provided additional workarounds: 1. Filter the Ports 4002 and 4004 to only accept connections to/from the IP addresses of machines that run UMC 2.If no RT server machines are used, Port 4004 can be blocked

Schneider Electric

Product	CVE	CVSS	details	Mitigation
Modicon M340 CPU and Modicon MC80	CVE-2024-8937	9.2	a vulnerability tampering with memory area involved in the authentication process	Update to Version SV3.65, Schneider also provided workaround mitigations
Modicon M340 CPU and Modicon MC81	CVE-2024-8938	9.2	a vulnerability tampering with memory area involved in memory size computation	Update to Version SV3.65, Schneider also provided workaround mitigations
EcoStruxure IT Gateway versions 1.21.0.6, 1.22.0.3, 1.22.1.5, and 1.23.0.4	CVE-2024-10575	10.0	A missing authorization vulnerability	Update to EcoStruxure IT Gateway version 1.23.1.10
PowerLogic PM5560, PM5561, PM5562, PM5563, and PM8ECC	CVE-2021-22763	9.2	A weak password recovery mechanism which may allow an attacker to gain unauthorized access	PM5560, PM5563, and PM 5580 update to version 2.8.3 PM5561 update to version 10.7.3 PM5562 update to version 4.3.5
Modicon M241/M251 /M258/LMC058	CVE-2024-11737	9.8	An improper input validation vulnerability leads to a denial of service and a loss of confidentiality and integrity	The vendor is actively developing a remediation for the controllers and, in the interim, advises adhering to industry-standard cybersecurity best practices to mitigate potential risks.

Rockwell Automation

Product	CVE	CVSS	details	Mitigation
DataMosaix Private Cloud: Versions 7.07	CVE-2019-17543	9.3	buffer overflow vulnerability	Update to version v7.09
DataMosaix Private Cloud: Versions 7.07	CVE-2019-18276	9.3	A privilege escalation vulnerability leading to remote code execution	Update to version v7.10
DataMosaix Private Cloud: Versions 7.07	CVE-2019-9893	9.8	A privilege escalation vulnerability leading to remote code execution	Update to version v7.11

ThinManager	CVE-2024-10386	9.8	Missing authentication for critical function	apply vendor fix, and Limit communications to TCP port 2031 exclusively to devices that require a connection to ThinManager
FactoryTalk Updater	CVE-2024-10943	9.1	An authentication bypass vulnerability	Update to V4.20.00
PM1k	CVE-2024-12371	9.8	A device takeover vulnerability allowing access to the Policyholder user (high privilege)	Update to firmware revision 4.020
PM1k	CVE-2024-12372	9.8	A heap buffer overflow causing denial-of-service	Update to firmware revision 4.020
PM1k	CVE-2024-12373	9.8	A buffer overflow causing denial-of-service	Update to firmware revision 4.020

mySCADA

Product	CVE	CVSS	details	Mitigation
myPRO Manager and myPRO Runtime	CVE-2024-47407	10.0	Improper input validation vulnerability	Update mySCADA PRO Manager to version 1.3 Update mySCADA PRO Runtime to version 9.2.1
myPRO Manager and myPRO Runtime	CVE-2024-52034	10.0	operating system command injection vulnerability	Update mySCADA PRO Manager to version 1.3 Update mySCADA PRO Runtime to version 9.2.2
myPRO Manager and myPRO Runtime	CVE-2024-45369	9.2	weak authentication process	Update mySCADA PRO Manager to version 1.3 Update mySCADA PRO Runtime to version 9.2.3
myPRO Manager and myPRO Runtime	CVE-2024-47138	9.8	no authentication for the administrative interface	Update mySCADA PRO Manager to version 1.3 Update mySCADA PRO Runtime to version 9.2.4

Kieback&Peter

Product	CVE	CVSS	details	Mitigation
DDC4000 series	CVE-2024-41717	9.8	a path traversal vulnerability	update firmware to v1.21.0
DDC4000 series	CVE-2024-43698	9.8	weak credentials	update firmware to v1.21.0

Radiflow

DELTA

Product	CVE	CVSS	details	Mitigation
DIAEnergie Versions v1.10.01.008 and prior	CVE-2024-43699	9.8	SQL injection vulnerability allowing data exfiltration	update to DIAEnergie v1.10.01.009
InfraSuite Device Master: Versions 1.0.12 and prior	CVE-2024-10456	9.8	A deserialization vulnerability resulting in remote code execution	update to version 1.0.13

elvaco

Product	CVE	CVSS	details	Mitigation
CMe3100: Version 1.12. 1	CVE-2024-49397	9.2	affected product is vulnerable to cross-site scripting	update to version 1.13.3
CMe3100: Version 1.12. 1	CVE-2024-49398	9.1	affected product is vulnerable to unrestricted file uploads	update to version 1.13.3

Automated Logic

Product	CVE	CVSS	details	Mitigation
Automated Logic WebCTRL® Server version 7.0	CVE-2024-8525	10	No authentication for file upload allowing remote execution	The vendor released a patch, however, version 7.0 is End-of-Life (EOL), and it is recommended to update to the latest version

Hitachi Energy

Product	CVE	CVSS	details	Mitigation
MicroSCADA Pro/X SYS600 versions 10.0 - 10.5	CVE-2024-4872	9.9	A vulnerability in the query validation allowing code injection	Update to Version 10.6
MicroSCADA Pro/X SYS600: Versions 9.4 FP2 HF1 - 9.4 FP2 HF5	CVE-2024-4872	9.9	A vulnerability in the query validation allowing code injection	Apply Patch 9.4 FP2 HF6

CIARA Threat Intelligence Updates

MITRE has released version 16 of ATT&CK, introducing new techniques and groups while refining those for existing ones. This update includes 11 new groups, updates to techniques for 27 existing groups, 19 new techniques, and one new ICS software entry - Fuxnet.

In addition, we have enhanced our Threat Intelligence knowledge by incorporating three new cyber threat groups into CIARA and updating details on **53** existing groups. These enhancements, primarily based on Radiflow's threat intelligence research, extend beyond the updates provided by MITRE. The update has been fully integrated into the CIARA signatures file.

Threat groups added

Black Basta

We added Black Basta to our Threat Intelligence (TI) due to its role as a ransomware-as-a-service (RaaS) group, compromising over 500 organizations globally since 2022. Their tactics include phishing, exploiting vulnerabilities, and a double-extortion model. Black Basta notably targets critical sectors like healthcare, manufacturing, and energy.

Snatch

We added Snatch to our Threat Intelligence (TI) following its inclusion in a joint CISA and FBI Cybersecurity Advisory under project #StopRansomware. Advisory AA23-263A highlights Snatch's ransomware activities targeting critical infrastructure, using tactics such as data exfiltration, encryption, and the "double extortion" method.

Sandman

We added Sandman to our Threat Intelligence (TI) due to recent research identifying this APT group targeting telecommunications providers. Their use of a LuaJIT-based toolkit demonstrates advanced espionage capabilities and a focus on stealth.

Major threat groups updated

Velvet Ant

We updated our Threat Intelligence (TI) group "Velvet Ant" based on their identified cyber espionage activities targeting critical infrastructure, as detailed in recent research. Velvet Ant, a China-nexus threat group, is known for exploiting zero-day vulnerabilities, including a Cisco IOS XE flaw, and deploying advanced malware to exfiltrate sensitive data.

Sandworm

We updated Sandworm in our Threat Intelligence (TI) to include the group's new techniques to target Industrial Control Systems (ICS).

APT28

We updated our Threat Intelligence (TI) on APT28 following recent reports highlighting their continued cyber espionage and information warfare activities. Leveraging advanced phishing, malware campaigns, and exploitation of vulnerabilities, APT28 remains a significant threat globally.

Ember Bear

We updated our Threat Intelligence (TI) to reflect the latest tactics and operations of Russian GRU cyber actors from Unit 29155, also known as Ember Bear, as detailed in CISA Advisory AA24-249A. This unit has targeted critical infrastructure globally, using advanced malware and sophisticated techniques for espionage, and sabotage.

Common Hacktivists

We updated our Threat Intelligence (TI) group "Common Hacktivists" to include recent pro-Russia hacktivist activities targeting Operational Technology (OT) environments, as highlighted in joint research by CISA, FBI, NSA, and others. These groups exploit vulnerabilities and deploy DDoS attacks to disrupt critical infrastructure, underscoring the escalating threat from politically motivated actors.

Threat Group	Techniques	Industry	Country	Region	Aliases
agrius	V	V	V	V	V
APT1	V	X	X	X	V
APT17	V	X	X	X	V
APT27	V	X	X	X	V
APT28	V	V	X	X	V
APT29	V	X	X	X	V
APT33	V	X	X	X	V
APT39	V	X	V	V	V
APT41	V	X	X	X	V
Cleaver	V	X	X	X	V
Cobalt Group	V	X	X	X	X
Common Hacktivists	V	X	X	X	X
CopyKittens	V	V	X	X	V
Cyber Avengers	V	X	X	X	X
Daggerfly	V	V	V	V	V
DarkHotel	V	X	X	X	V
DarkHydrus	V	X	X	X	V
Dragonfly	V	X	X	X	V
DragonOK	V	X	V	X	V
Ember Bear	V	X	X	X	V
Equation Group	V	X	X	X	V
Fox Kitten	V	X	X	X	V
Gamaredon Group	V	X	X	X	V
INC Ransom	V	V	V	V	X
Inception	V	X	X	X	V
Ke3chang	V	X	X	X	X
Kimsuky	V	X	X	X	V
LOCKBIT	V	X	X	X	X
Lotus Blossom	V	X	V	V	V
Magic Hound	V	X	X	X	X
Molerats	V	X	X	X	V
Moonstone Sleet	V	V	X	X	V
MuddyWater	V	X	X	X	V
Mustang Panda	X	X	X	X	V

NEODYMIUM	**V**	X	X	X	X
OilRig	**V**	X	X	X	**V**
Play	**V**	**V**	**V**	**V**	**V**
PROMETHIUM	**V**	X	X	X	**V**
RansomHub	**V**	X	X	X	**V**
RedCurl	**V**	**V**	**V**	**V**	**V**
Saint Bear	**V**	**V**	**V**	**V**	**V**
Sandworm	**V**	X	X	X	**V**
SideWinder	**V**	X	X	X	**V**
Star Blizzard	**V**	**V**	**V**	**V**	**V**
TA505	**V**	X	X	X	**V**
TA577	**V**	X	X	X	**V**
TEMP.Veles	**V**	X	X	X	**V**
Tonto	**V**	X	X	X	**V**
Turla	**V**	**V**	**V**	**V**	**V**
Velvet Ant	**V**	X	X	X	X
Volt Typhoon	**V**	X	X	X	**V**
Winnti Group	**V**	**V**	**V**	**V**	**V**
Winter Vivern	**V**	**V**	**V**	**V**	**V**

Radiflow's best practice recommendations

Radiflow's recommended best practices are derived from the vulnerabilities, incidents, and threat intelligence detailed in this report. These guidelines aim to mitigate identified risks and enhance the resilience of OT environments.

- Properly segment the ICS/SCADA networks and ensure they are disconnected from the internet.
- Audit remote connections to supervisory/operations/basic control zones based on approved protocols and workstations.
- Implement robust access control measures:
  - Enforce role-based access control (RBAC) to limit access to sensitive systems based on job responsibilities.
  - Regularly review and update access permissions, especially for privileged accounts and after personnel changes.
  - Limit administrative access to essential personnel and systems.
- Ensure basic cyber-hygiene practices:
  - Enforce multi-factor authentication for remote access to ICS networks and devices
  - Regularly change all passwords of ICS/SCADA devices and systems, especially default passwords, to strong per-device passwords.
  - Regularly back up devices.

Ongoing Support

Thank you for trusting Radiflow to reduce risks in your OT environment. We are committed to providing you with the latest insights and product improvements to defend against evolving threats.https://attack.mitre.org/resources/updates/

If you suspect malicious ICS network activity, or to obtain the CIARA update files, please contact our team at support@radiflow.com or visit our official website at Radiflow.com.

Additional Info

https://www.cisa.gov/news-events/ics-advisories/icsa-24-326-01
https://www.cisa.gov/news-events/ics-advisories/icsa-24-277-03

https://www.cisa.gov/news-events/ics-advisories/icsa-24-303-03

https://www.cisa.gov/news-events/ics-advisories/icsa-24-291-01

https://www.cisa.gov/news-events/ics-advisories/icsa-24-331-04

https://www.cisa.gov/news-events/ics-advisories/icsa-24-291-05

https://www.cisa.gov/news-events/ics-advisories/icsa-24-326-07

https://www.cisa.gov/news-events/ics-advisories/icsa-24-284-16

https://www.cisa.gov/news-events/ics-advisories/icsa-24-305-01

https://www.cisa.gov/news-events/ics-advisories/icsa-24-319-14

https://www.cisa.gov/news-events/ics-advisories/icsa-24-352-03

https://www.cisa.gov/news-events/ics-advisories/icsa-24-326-04

https://www.cisa.gov/news-events/ics-advisories/icsa-24-326-05

https://www.cisa.gov/news-events/ics-advisories/icsa-24-331-01

https://www.cisa.gov/news-events/ics-advisories/icsa-24-352-04

https://www.cisa.gov/news-events/ics-advisories/icsa-24-284-06

https://www.cisa.gov/news-events/ics-advisories/icsa-24-284-08

https://www.cisa.gov/news-events/ics-advisories/icsa-24-284-09

https://www.cisa.gov/news-events/ics-advisories/icsa-24-319-08

https://www.cisa.gov/news-events/ics-advisories/icsa-24-319-10

https://www.cisa.gov/news-events/ics-advisories/icsa-24-338-02

https://www.cisa.gov/news-events/ics-advisories/icsa-24-354-04
https://attack.mitre.org/resources/updates/

https://www.radiflow.com/radiflow-labs/ukrainian-blackjack-apt-attack-on-moscow-ot-infrastructure-fuxnet/

https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-249a

https://www.cisa.gov/resources-tools/resources/defending-ot-operations-against-ongoing-pro-russia-hacktivist-activity