Dec 05 2023

NETMANAGEIT

Intelligence Report

IRGC-Affiliated Cyber Actors Exploit PLCs in Multiple Sectors, Including U.S. Water and Wastewater Systems Facilities

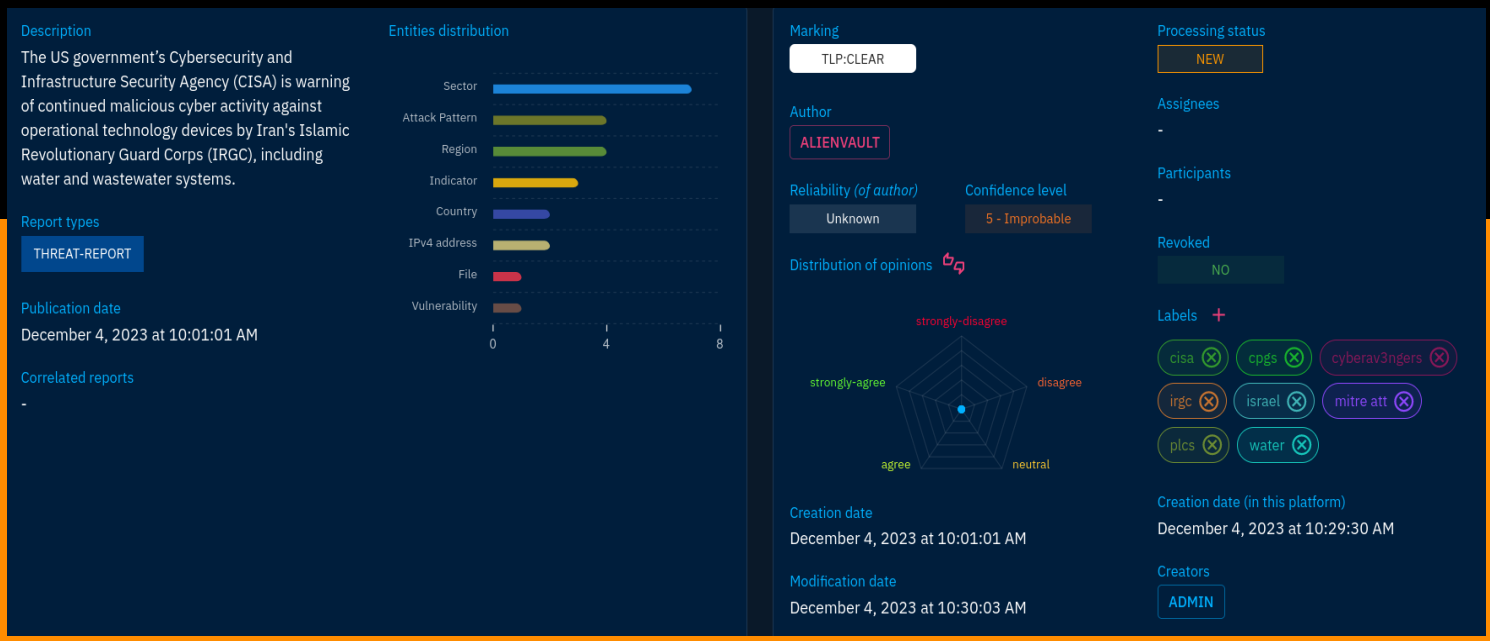

Table of contents

Overview

- Description 4
- Confidence 4
- Content 5

Entities

- Attack-Pattern 6
- Sector 9
- Indicator 11
- Country 14
- Region 15
- Vulnerability 16

Observables

- StixFile 17

- IPv4-Addr 18

External References

- External References 19

Overview

Description

The US government’s Cybersecurity and Infrastructure Security Agency (CISA) is warning of continued malicious cyber activity against operational technology devices by Iran's Islamic Revolutionary Guard Corps (IRGC), including water and wastewater systems.

Confidence

This value represents the confidence in the correctness of the data contained within this report.

15 / 100

Content

N/A

Attack-Pattern

Name

Process Discovery

ID

T1057

Description

Adversaries may attempt to get information about running processes on a system. Information obtained could be used to gain an understanding of common software/applications running on systems within the network. Adversaries may use the information from [Process Discovery](https://attack.mitre.org/techniques/T1057) during automated discovery to shape follow-on behaviors, including whether or not the adversary fully infects the target and/or attempts specific actions. In Windows environments, adversaries could obtain details on running processes using the [Tasklist](https://attack.mitre.org/software/S0057) utility via [cmd](https://attack.mitre.org/software/S0106) or `Get-Process` via [PowerShell](https://attack.mitre.org/techniques/T1059/001). Information about processes can also be extracted from the output of [Native API](https://attack.mitre.org/techniques/T1106) calls such as `CreateToolhelp32Snapshot`. In Mac and Linux, this is accomplished with the `ps` command. Adversaries may also opt to enumerate processes via /proc. On network devices, [Network Device CLI](https://attack.mitre.org/techniques/T1059/008) commands such as `show processes` can be used to display current running processes.(Citation: US-CERT-TA18-106A)(Citation: show_processes_cisco_cmd)

Name

Brute Force

ID

T1110

Description

Adversaries may use brute force techniques to gain access to accounts when passwords are unknown or when password hashes are obtained. Without knowledge of the password for an account or set of accounts, an adversary may systematically guess the password using a repetitive or iterative mechanism. Brute forcing passwords can take place via interaction with a service that will check the validity of those credentials or offline against previously acquired credential data, such as password hashes. Brute forcing credentials may take place at various points during a breach. For example, adversaries may attempt to brute force access to [Valid Accounts](https://attack.mitre.org/techniques/T1078) within a victim environment leveraging knowledge gathered from other post-compromise behaviors such as [OS Credential Dumping](https://attack.mitre.org/techniques/T1003), [Account Discovery](https://attack.mitre.org/techniques/T1087), or [Password Policy Discovery](https://attack.mitre.org/techniques/T1201). Adversaries may also combine brute forcing activity with behaviors such as [External Remote Services](https://attack.mitre.org/techniques/T1133) as part of Initial Access.

Name

Video Capture

ID

T1125

Description

An adversary can leverage a computer's peripheral devices (e.g., integrated cameras or webcams) or applications (e.g., video call services) to capture video recordings for the purpose of gathering information. Images may also be captured from devices or applications, potentially in specified intervals, in lieu of video files. Malware or scripts may be used to interact with the devices through an available API provided by the operating system or an application to capture video or images. Video or image files may be written to disk and exfiltrated later. This technique differs from [Screen Capture](https://attack.mitre.org/techniques/T1113) due to use of specific devices or applications for video

recording rather than capturing the victim's screen. In macOS, there are a few different malware samples that record the user's webcam such as FruitFly and Proton. (Citation: objective-see 2017 review)

Name

Account Access Removal

ID

T1531

Description

Adversaries may interrupt availability of system and network resources by inhibiting access to accounts utilized by legitimate users. Accounts may be deleted, locked, or manipulated (ex: changed credentials) to remove access to accounts. Adversaries may also subsequently log off and/or perform a [System Shutdown/Reboot](https://attack.mitre.org/techniques/T1529) to set malicious changes into place.(Citation: CarbonBlack LockerGoga 2019)(Citation: Unit42 LockerGoga 2019) In Windows, [Net](https://attack.mitre.org/software/S0039) utility, `Set-LocalUser` and `Set-ADAccountPassword` [PowerShell](https://attack.mitre.org/techniques/T1059/001) cmdlets may be used by adversaries to modify user accounts. In Linux, the `passwd` utility may be used to change passwords. Accounts could also be disabled by Group Policy. Adversaries who use ransomware or similar attacks may first perform this and other Impact behaviors, such as [Data Destruction](https://attack.mitre.org/techniques/T1485) and [Defacement](https://attack.mitre.org/techniques/T1491), in order to impede incident response/recovery before completing the [Data Encrypted for Impact](https://attack.mitre.org/techniques/T1486) objective.

Sector

Name
Heavy industries
Description
Private entities working to transform raw materials into manufactured products (Chemicals, metal etc.).
Name
Energy
Description
Public and private entities operating to extract, store, transport and process fuel, entities managing energy plants and energy storage and distribution and entities managing fuel waste.
Name
Food and drinks businesses
Description
Businesses preparing and serving food and drinks to customers in exchange for money.

Name
Manufacturing
Description
Private entities transforming and selling goods, products and equipment which are not included in other activity sectors.
Name
Health
Description
Public and private entities involved in research, services and manufacturing activities related to public health.
Name
Transport
Description
All entities involved in the movement of people or goods from one place to another.
Name
Hospitality
Description
Private entities offering to customersâ€™ leisure activities and experiences.

Indicator

Name
178.162.227.180
Description
CC=DE ASN=AS28753 Leaseweb Deutschland GmbH
Pattern Type
stix
Pattern
[ipv4-addr:value = '178.162.227.180']
Name
440b5385d3838e3f6bc21220caa83b65cd5f3618daea676f271c3671650ce9a3
Pattern Type
stix
Pattern

[file:hashes.'SHA-256' = '440b5385d3838e3f6bc21220caa83b65cd5f3618daea676f271c3671650ce9a3']

Name

185.162.235.206

Description

ISP: WorldStream B.V. **OS:** Linux ---------- Hostnames: ---------- Domains: ---------- Services: **22:** ``` SSH-2.0-OpenSSH_8.2p1 Debian-4 Key type: ssh-rsa Key: AAAAB3NzaC1yc2EAAAADAQABAAABgQCejB4stKiQ2JLwTiXiEuApEfzBgOFzVgM5yZ8z2IAKseND UafW8oYmPE9gUb4FcN4iEetfzuMhofowiwa+R4+cG6tGmICjQPj0RlFHxN1vqe6th77S+eLJW7VW +6R0u0/OihsFEZN4FVxwdP96hv5It68HCqw6/wzIOv6uWJAeC1LCHlpO0nxOcKUncG34wmFjl3UV HPpHl9aQY5xDWnL+lM1oiNmOlmmBzm20TlfB1IoY9wBiiY84PFv5kphJzP0wDNY/f1ttm3i5M7nZ T4863jNp8PrDVK/sVo9BTgaWGiESLvoAxvJzoYIuIAqDDf6bcI9US5FVKR6voaXL/kRNwa/m/2dx wjIpv0BkmujMleZgIc3cL2Zeh3vxqmUhIdsy88aTIuA84EG/J563LnMTCqWZOj/UmiZwgsFDsigH 2KkJ6lYhBSbqC+qrqFrZ45oVh/nQdCIDG9iJmPR0Ry9CQdft2OVSB73HLB23ohCSD3b0dJP+Zshg vKUDatyLyu8= Fingerprint: 5b:d7:51:cd:f9:76:bb:85:45:8c:3d:fd:7f:be:86:6b Kex Algorithms: curve25519-sha256 curve25519-sha256@libssh.org ecdh-sha2-nistp256 ecdh-sha2-nistp384 ecdh-sha2-nistp521 diffie-hellman-group-exchange-sha256 diffie-hellman-group16-sha512 diffie-hellman-group18-sha512 diffie-hellman-group14-sha256 Server Host Key Algorithms: rsa-sha2-512 rsa-sha2-256 ssh-rsa Encryption Algorithms: chacha20-poly1305@openssh.com aes128-ctr aes192-ctr aes256-ctr aes128-gcm@openssh.com aes256-gcm@openssh.com MAC Algorithms: umac-64-etm@openssh.com umac-128-etm@openssh.com hmac-sha2-256-etm@openssh.com hmac-sha2-512-etm@openssh.com hmac-sha1-etm@openssh.com umac-64@openssh.com umac-128@openssh.com hmac-sha2-256 hmac-sha2-512 hmac-sha1 Compression Algorithms: none zlib@openssh.com ``` ---------- **139:** ``` \x83\x00\x00\x01\x8f ``` ---------- **445:** ``` SMB Status: Authentication: enabled SMB Version: 2 Capabilities: raw-mode ``` ---------- **3389:** ``` Remote Desktop Protocol \x03\x00\x00\x13\x0e\xd0\x00\x00\x124\x00\x02\x1f\x08\x00\x02\x00\x00\x00 Remote Desktop Protocol NTLM Info: OS: Windows 10 (version 1809)/Windows Server 2019 (version 1809) OS Build: 10.0.17763 Target Name: WIN-09GQ5U5MILS NetBIOS Domain Name: WIN-09GQ5U5MILS NetBIOS Computer Name: WIN-09GQ5U5MILS DNS Domain Name: WIN-09GQ5U5MILS FQDN: WIN-09GQ5U5MILS ``` ---------- **5985:** ``` HTTP/1.1 404 Not Found Content-Type: text/html; charset=us-ascii Server: Microsoft-HTTPAPI/2.0 Date: Tue, 14 Nov 2023 12:55:13 GMT Connection: close Content-Length: 315 WinRM NTLM Info: OS: Windows Server 2019 (version 1809) OS Build: 10.0.17763 Target Name: WIN-09GQ5U5MILS

NetBIOS Domain Name: WIN-09GQ5U5MILS NetBIOS Computer Name: WIN-09GQ5U5MILS DNS Domain Name: WIN-09GQ5U5MILS FQDN: WIN-09GQ5U5MILS ``` ----------

Pattern Type

stix

Pattern

[ipv4-addr:value = '185.162.235.206']

Country

Name
Israel

Name
United States

Region

Name
Asia
Name
Northern America
Name
Middle East
Name
Americas

Vulnerability

Name
CVE-2023-22515

Description
Atlassian Confluence Data Center and Server contains a broken access control vulnerability that allows an attacker to create unauthorized Confluence administrator accounts and access Confluence.

StixFile

Value
440b5385d3838e3f6bc21220caa83b65cd5f3618daea676f271c3671650ce9a3

IPv4-Addr

Value
185.162.235.206
178.162.227.180

External References

- https://otx.alienvault.com/pulse/656de9ae8d88a6c091f68c3c
- https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-335a