1. Pulse Overview

Pulse URL: Inside a New OT/IoT Cyberweapon: IOCONTROL | Claroty - LevelBlue – Open Threat Exchange

Threat Actor: Advanced Persistent Threat (APT) Group

Threat overview: The IOCONTROL cyberweapon is a highly sophisticated attack tool designed to target Operational Technology (OT) and Internet of Things (IoT) environments. It is suspected to be deployed by a nation-state actor to compromise critical infrastructure. This malware has similarities to previous industrial-focused threats, such as Industroyer and TRITON, known for targeting energy grids and safety systems.

2. Indicators of Compromise (IoCs)

Here are the key IoCs identified in the Pulse:

Type	Iocs
IP Address	159.100.6.69
File Hash	366e435a1ea0f597deb6ebe7c0c5acdb6e8b33eb
File Hash	1b39f9b2b96a6586c4a11ab2fdbff8fdf16ba5a0ac7603149023d73f33b84498

3. Analysis:

IP Address: 159.100.6.69

Status: Malicious

Observations:

- The IP 159.100.6.69 has been flagged in multiple threat intelligence databases for potential malicious activity.
- It has been associated with command-and-control (C2) communications, indicating possible involvement in cyberattacks or malware operations.
- The IP has been observed engaging in anomalous network behavior, including repeated connection attempts to industrial control systems (ICS) and IoT devices.
- Some reports link this IP to phishing campaigns and brute-force attacks against remote desktop protocol (RDP) services.

File Hash: 366e435a1ea0f597deb6ebe7c0c5acdb6e8b33eb

Analysis Tool: VirusTotal

Detection Rate: 34/64 security vendors flagged this file as malicious

Details:

- The SHA-1 hash 366e435a1ea0f597deb6ebe7c0c5acdb6e8b33eb corresponds to a sample of the IOCONTROL malware.
- This malware has been linked to Iran-affiliated threat actors and has primarily targeted devices in Israel and the United States.
- The malware exhibits high entropy, which suggests the presence of packed or encrypted payloads. This makes detection difficult for traditional antivirus solutions.
- Executes shell commands such as rm -rf, indicating it can delete system files, disrupt operations, or erase its traces.
- The presence of self-deletion mechanisms suggests an ability to remove evidence after execution.
- Uses MQTT and HTTP/S protocol to communicate with external C2 servers.
- This malware is crafted to interact with PLCs (Programmable Logic Controllers) and SCADA (Supervisory Control and Data Acquisition) systems.

File Hash: 1b39f9b2b96a6586c4a11ab2fdbff8fdf16ba5a0ac7603149023d73f33b84498

Analysis Tool: VirusTotal

Detection Rate: 34/64 security vendors flagged this file as malicious

Details:

- The malware is designed to infiltrate various IoT and OT devices from multiple vendors, such as Baicells, D-Link, Hikvision, Red Lion, Orpak, Phoenix Contact, Teltonika, and Unitronics
- IOCONTROL utilizes the MQTT protocol over port 8883 for secure command-and-control (C2) communications. This choice of protocol allows the malware to blend into legitimate network traffic, making detection more challenging
- The malware can execute any code on the compromised device, granting attackers extensive control.
- It includes mechanisms to remove itself from the infected system, aiding in evasion of forensic analysis.

- The malware establishes persistence by installing itself as a daemon, ensuring it remains active across system reboots. Additionally, it employs DNS over HTTPS (DoH) to conceal its C2 infrastructure

4. **Interpretation of Results**
   Common Patterns:

IOCONTROL has several key characteristics seen in previous cyberattacks on industrial systems:

- **Hides in Normal Traffic**
  - It uses MQTT on ports 8883 and 1883, which are normally used for IoT communication.
  - It also hides its control signals inside encrypted DNS traffic, making it hard to block.
- **Affects Many Different Devices**
  - Unlike most malware that targets a specific system, IOCONTROL can infect devices from multiple companies, including D-Link, Hikvision, Phoenix Contact, and Teltonika.
  - It has the ability to scan networks and run harmful commands on different devices.
- **Designed to Stay Hidden and Persistent**
  - It can delete itself to prevent investigation.
  - It installs itself as a background process, so it stays active even after a system restart.
  - It uses signed files to avoid being flagged as dangerous by security software.
- **Targets Critical Infrastructure**
  - The malware could be used to turn off power grids, disrupt manufacturing, or disable security systems.
  - It has similar traits to past attacks on industrial control systems (ICS), such as Stuxnet or Industroyer.

5. **ICS Relevance**

Threat to Industrial Operations

- If hackers control PLCs (Programmable Logic Controllers) and HMIs (Human-Machine Interfaces), they can manipulate industrial processes,for example, changing how power plants or factory machines work.
- This could lead to equipment failures, production shutdowns, or safety risks.

Hard to Remove

- Once installed, the malware can keep coming back, even if security teams try to remove it.
- It can kill important system processes and stay hidden in the network, making it difficult to fully clean up.

Difficult to Detect

- Many industrial systems do not have strong security software, which makes them easier targets.
- Because the malware uses encrypted communication, traditional firewalls and security tools may not notice the attack.

1. Pulse Overview

Pulse URL: Russian Sandworm hackers targeted 20 critical orgs in Ukraine PART II

Threat Actor: BlackEnergy APT

Threat overview: BlackEnergy is a group of hackers that are believed to be sponsored by the Russian government. They have been involved in cyberattacks for years, and their focus is mainly on critical infrastructure, like power grids and energy systems. In Ukraine, BlackEnergy launched a series of attacks, especially targeting the energy sector. These attacks were carried out using spearphishing techniques, which is a form of cyberattack where malicious emails are sent to specific targets in order to trick them into opening attachments or clicking links that install malware.

2. **Indicators of Compromise (IoCs)**

Here are the key IoCs identified in the Pulse:

Type	Iocs
File Hash	ac2d7f21c826ce0c449481f79138aebd
File Hash	3fa9130c9ec44e36e52142f3688313ff
File Hash	e15b36c2e394d599a8ab352159089dd2

3. Analysis:

File Hash: ac2d7f21c826ce0c449481f79138aebd
Analysis Tool: VirusTotal
Detection Rate: 60/71 security vendors flagged this file as malicious

Details:
Threat Type: The hash is linked to different types of malware, including:

Backdoor: A backdoor allows attackers to secretly access a system without being detected. This means that the malware could give hackers the ability to control the infected system remotely.

Spyware: It can monitor the system, possibly to steal sensitive information like passwords or banking details.

Trojan: This kind of malware pretends to be something safe but actually carries out harmful activities like stealing information or allowing attackers to take control of a system.

Security Companies' Detection: Multiple security companies, like Avira, BitDefender, Avast, and CrowdStrike Falcon, have identified this file as malicious. Some specifically label it as BlackEnergy, which is a known type of malware that has been used in cyberattacks, especially in incidents like disrupting power grids or launching other attacks on critical infrastructure.

Impact: If this malware infects a system, it could:

- Allow attackers to control the system.
- Steal sensitive information.
- Disrupt or damage the system by enabling additional malware or attacks.

File Hash: 3fa9130c9ec44e36e52142f3688313ff
Analysis Tool: VirusTotal
Detection Rate:58/72 security vendors flagged this file as malicious

Details:
Malware Type: The file could represent a virus, backdoor, Trojan, ransomware, or another type of malware. Depending on its behavior, it might allow attackers to control the infected system, steal sensitive information, or disrupt operations.

Security Vendor Detection: The hash might be flagged by multiple cybersecurity companies, each identifying it with different names or categories based on its behavior. For example, if it's part of a broader malware campaign like Emotet, TrickBot, or other known malware families, those names would appear in the detections.

Impact: If infected, the system could experience:

- Unauthorized remote access.
- Data theft, including passwords, banking details, or personal information.
- System compromise, including installing additional malware.

File Hash: e15b36c2e394d599a8ab352159089dd2

Analysis Tool: VirusTotal

Detection Rate: 42/65 security vendors flagged this file as malicious

Details:
Type of Attack: The attack uses a malicious Microsoft Word document that, when opened, asks the user to enable macros. If the user enables macros, the malicious macro embedded in the document gets executed.

Payload Delivery: The macro downloads and executes a dropper file (vba_macro.exe) which installs additional malware.

Persistence: The dropper installs a backdoor file (FONTCACHE.DAT), allowing the attacker to maintain access to the system.

Behavior: The malware facilitates remote access for the attacker, potentially enabling further malicious actions such as data theft or additional malware deployment.

Risk: This method of infection, especially in targeted spearphishing attacks, is highly effective in gaining long-term access to critical systems.

4. **Interpretation of Results**

Common Patterns:

- **Spearphishing**: The attack begins with targeted emails containing malicious Word documents. The emails are crafted to look like legitimate communication, tricking the victim into enabling macros to activate the malware.
- **Remote Access**: The malware installs a backdoor that allows attackers to control the infected system from a distance. This is a common tactic used by advanced persistent threat (APT) groups to maintain long-term access to critical systems.
- **Persistence**: The malware is designed to survive reboots and avoid detection, ensuring that the attackers have ongoing access to the system.

5. **ICS Relevance**

- **Targeting Critical Systems**: This type of malware could be especially harmful in industrial control systems (ICS), where attackers can manipulate the operations of critical infrastructure like power grids, manufacturing systems, or water treatment plants. The backdoor allows attackers to maintain control over systems, potentially causing damage to important industrial operations.

- **Lack of Security**: ICS systems often have weak security and may not be equipped with the latest protection against advanced threats like backdoors. This makes them easy targets for attackers who use techniques like spearphishing.
- **Risk of Long-term Access**: With the ability to maintain persistent access, attackers could cause ongoing disruptions, steal sensitive data, or sabotage industrial processes, putting both the system and the people relying on it at great risk.