IOControl Malware: What's New, What's Not?

By By Michael Freeman Head of Threat Intelligence

Archived: 2026-04-05 20:47:11 UTC

IOControl malware is a sophisticated Linux backdoor, initially identified as OrpraCab and QueueCat in 2023. It re-emerges in 2024 as IOControl, targeting ARM-based IoT and Linux systems. Despite recent media mischaracterization as OT-specific malware, IOControl operates primarily as a Linux backdoor with advanced techniques for persistence, obfuscation, and C2 (Command and Control) communication.

Key Takeaways:

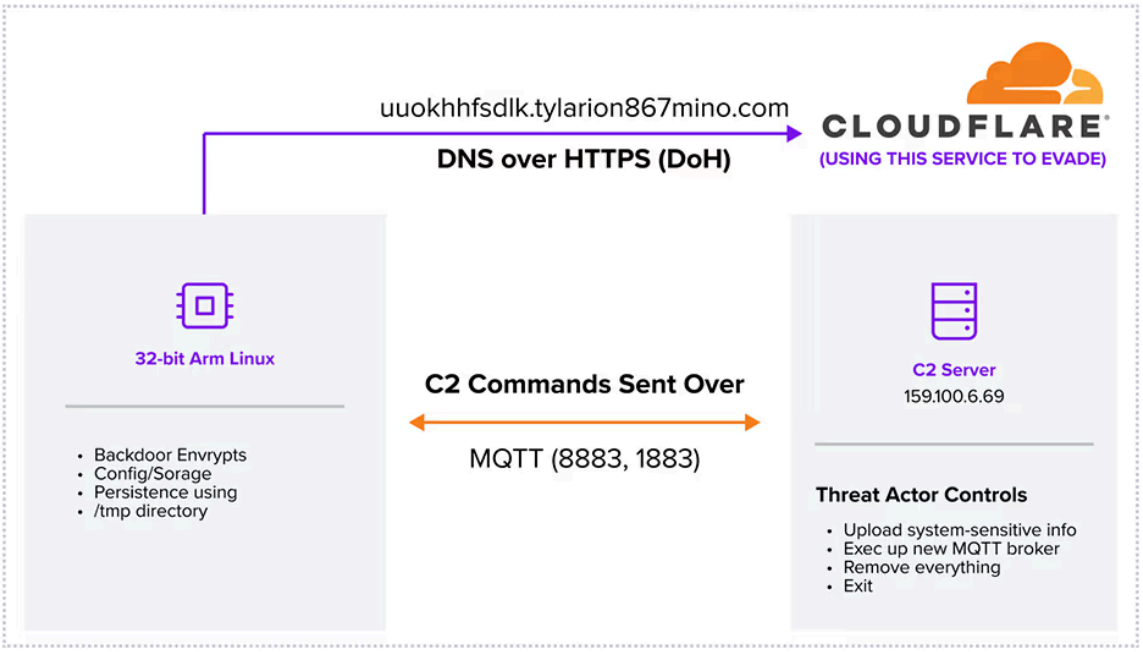
- **This malware is not new**. It was first seen using other names over a year ago, at the end of 2023.
- **This is not OT-specific device malware** but behaves more like a Linux backdoor compiled for 32-bit ARM devices.
- **Armis helps by providing Indicators Of Compromise (IOCs) and behaviors** that can be used to identify the presence of this malware in your organization.

Background and How it Works

IOControl has been attributed to CyberAv3ngers, an Iranian-linked hacking group associated with the country's state-sponsored cyber efforts, including the Islamic Revolutionary Guard Corps (IRGC). This malware has been deployed in campaigns against systems in Israel and the United States, impacting devices like routers, programmable logic controllers (PLCs), firewalls, and Supervisory Control and Data Acquisition (SCADA) systems.

The malware deploys a backdoor that's automatically executed every time an affected device restarts. It leverages the widely used MQTT (Message Queuing Telemetry Transport) protocol to disguise malicious traffic.

MQTT, introduced initially to streamline SCADA monitoring in oil pipeline operations, has since become a favored protocol for IoT communication due to its lightweight nature and scalability. This malware's use of MQTT on ports 8883 and 1883, in combination with suspicious domains and the presence of stealthy filesystem artifacts, highlights a deliberate attempt to blend into IoT environments while maintaining persistence and operational security. Other malware families that use MQTT are Chrysaor, MQsTTang, and WailingCrab.



By leveraging MQTT over TLS, the adversary's C2 traffic blends effortlessly with legitimate IoT network noise, providing both encryption and a lower likelihood of raising immediate suspicion. Passing messages via an MQTT broker offers the attacker an additional layer of indirection, complicating attribution and enhancing their operational security.

Detection – Indicators Of Compromise

Below are some concrete Indicators of Compromise (IOCs) and detection strategies derived from the scripts and code snippets presented. Security professionals can use these IOCs and behaviors to identify the presence of this malware in their environments.

Process and Behavior IOCs:

- **PID Files:**
  The presence of `/var/run/iocontrol.pid` associated with a non-standard or unknown process is a red flag.MD5: c92e2655d115368f92e7b7de5803b7bc, Magic: ELF 32-bit MSB executable, ARM, version 1, statically linked, Size: 16208,Version: 1.0.5, Packer: upx
- **Environment Variables:**

Env Variable	Value	Purpose
0_0	22e70a3056aa209e90dc5a354edda2c1	AES KEY
0_1	1c3b88f1e4720dc6	AES IV

1	1.0.5	Version
3	5958ce	MQTT User
4	3-4953-8c18-3f9625	MQTT Pass

- **Infinite Loop Persistence Mechanism:**
  A script continuously checks for the `iocontrol` process using `pidof "iocontrol"` and restarting it if it's not found. This watchdog-like behavior is not typical for legitimate software.

Domain and Networking IOCs:

- **C2 Domain:** `uwochhfsdltk.tylarion867mino.com`
  Any outbound connections to this domain, especially over unusual ports, should be flagged.
- **Port Usage:** `Port 8883` and `1883` are used for outbound connections. This port is less commonly used for regular web traffic and could indicate suspicious MQTT-like or encrypted command and control channels.
- IP: 159.100.6.69 for the broker
- **DoH Queries:** DNS-over-HTTPS lookups via Cloudflare's resolver:
  - Queries to `1.1.1.1:443/dns-query?name=` with suspicious parameters or unknown hostnames.
  - Look for unusual patterns of DoH usage that are not common for normal system DNS resolution.

File and Path IOCs:

- **MD5 :** c92e2655d115368f92e7b7de5803b7bc
- **Suspicious Binary:**
  A binary named `iocontrol` present in `/usr/bin/` (or any directory) that is not part of a known software package or repository.
- **Malicious Directories and Logs:**
  - `/tmp/iocontrol/` directory and `/tmp/iocontrol.log` file. Legitimate software rarely stores persistent logs or binaries in `/tmp`.
- **Startup/Persistence Scripts:**
  - `/etc/rc3.d/S93InitSystemd.sh` is suspicious. This script may be masquerading as a standard init script but contains malicious content.
  - Any shell script in `/etc/rc*.d/` directories that references `iocontrol`.
- The threat actor used a script named "mr_soul_controller" and a module "oblivator" to wipe Linux device files.

Suspicious Commands

- **Environment Queries:**
  The script uses commands like `whoami, hostname, current_user, timezone,`

and Techniques:	`uname -r, device_model`, and `firmware_version` to harvest system information. While these commands are legitimate, security teams should look for aggregated usage from unknown scripts or binaries. • **Strings, UID and tokens to look for:** ◦ Strings like `X8XR7tHHD1CqmhNS, XXFrxHMDI1CqmIN5`, `855958ce-6483-4953-8c18-3f9625d88c27`, `sCgcVpkXixEUTgEJqY708N5w2c42DssIEutp7ZIeNgt17G78iy`, and `cS9cYpXiX1EtUEBdjQ7O8N5wC42DssIEutp7ZtNEtg17G78iy` within scripts or binaries may indicate embedded credentials, keys, or tokens used for C2 authentication. • **Redirection and Obfuscation:** Frequent use of `2>&1`, `>/dev/null`, and `/dev/urandom` indicate attempts to hide output and possibly generate keys for obfuscation.

APT Group Biographical Intelligence Package

The biographical intelligence package below outlines the expertise, operations, and evolving strategies of this Iranian-linked APT (Advanced Persistent Threat) group, providing actionable insights to enhance defenses against their campaigns.

Name(s)	• OilRig (APT34): The most commonly used name attributed by cybersecurity firms. • HELIX KITTEN: CrowdStrike designation. • Magic Hound: Used for campaigns targeting specific sectors like energy and telecommunications. • Cobalt Gypsy: Focus on espionage and disruptive operations.
Nation-State Attribution	• Country: Iran • Sponsor: Likely linked to Iran’s Ministry of Intelligence and Security (MOIS) and Iranian military organizations.
Core Objectives	• Cyber-Espionage: Stealing sensitive data from organizations in sectors like energy, telecommunications, finance, and government. • Operational Disruption: Targeting infrastructure and operational technology (OT) systems to disrupt services or gain leverage. • Surveillance: Monitoring and manipulating communications and critical data for geopolitical gain.
Core Expertise	• Network Penetration

	• Highly skilled in exploiting public-facing vulnerabilities in enterprise software, IoT/OT devices, and supply chain ecosystems. • Development and use of custom malware like IOControl, OrpraCab, and QueueCat.
Operational Security (OpSec)	• Extensive use of encryption, AES for configuration and storage, and & TLS for command-and-control (C2) communications. • DNS-over-HTTPS (DoH) using Cloud Flare and domain fronting to evade detection and attribution. • Lightweight IoT and MQTT protocols to blend malicious traffic into legitimate IoT network noise.
Custom Toolkit(s)	• Use of modular frameworks that allow easy adaptation to new targets. • Proficiency in crafting specialized backdoors, like IOControl, optimized for IoT and Linux ARM devices. • Examples: Karkoff, Stonedrill, Shamoon, DNSpionage, and DownPaper.
Target Profiling	• Capable of deep reconnaissance, gathering system details (e.g., kernel versions, device models, geolocation) to tailor attacks. • Use social engineering tactics, spear-phishing campaigns, and watering-hole attacks for initial access.
Command and Control (C2)	• Primary Communication Protocols: MQTT over TLS (port 8883/1883): This protocol disguises C2 traffic as legitimate IoT messaging. • DNS-over-HTTPS (DoH): Used with services like Cloudflare to encrypt and obfuscate DNS queries.
Access Channels	• Spear-Phishing: Custom-crafted emails targeting specific individuals within an organization. Example: Using geopolitical or industry-relevant lures to gain trust and encourage malicious file downloads. • Exploitation of Vulnerabilities: focus on unpatched enterprise software (e.g., VPNs, web servers, and email platforms). • Ease of IoT/OT device exploitation, leveraging lightweight protocols like MQTT. • Supply Chain Attacks: Compromising software supply chains to distribute malware under the guise of legitimate updates.

Exfiltration Methods	• Encryption of stolen data before transmission. • Use of legitimate cloud services to exfiltrate data (e.g., Google Drive, Dropbox). • Splitting data into smaller chunks to evade detection.
Tools, Techniques, and Procedures (TTPs)	Tactics: • Multi-stage attacks involving reconnaissance, exploitation, lateral movement, and exfiltration. • Reliance on stealthy malware and backdoors to maintain persistence. • Extensive use of living-off-the-land techniques to blend into normal network activity. Key Techniques: • Phishing Campaigns: Heavily customized to the target's industry and region. • Credential Harvesting: Deployment of keyloggers and credential stealers. Use of phishing to obtain VPN and enterprise credentials. • Exploitation of Known Vulnerabilities: Common CVEs targeted include VPN vulnerabilities (e.g., CVE-2019-11510) and flaws in IoT firmware. • Lateral Movement: Deployment of tools like PowerShell scripts and Mimikatz for network traversal and privilege escalation. Known Malware Families: • Stonedrill: Designed for data destruction. • Shamoon: Wiper malware used for disruptive campaigns. • DownPaper: A custom backdoor for espionage. • IOControl: Focused on IoT and Linux ARM devices. • DNSpionage: A tool for DNS tunneling and exfiltration. Techniques for Persistence: • Use of startup scripts (`/etc/rc*.d/`) and PID monitoring to maintain malware presence. • Frequent updates to malware binaries and configurations.
Potential Partnerships and Affiliations	• Iranian Government Agencies: Likely collaboration with MOIS for intelligence-gathering operations. • Military Units: Coordination with cyber-military units for operational support and deployment. External Affiliations:

<table>
<tr><td></td><td>

Other State-Sponsored Groups: Sharing infrastructure and tactics with groups like Charming Kitten (APT35).
Regional Alliances: Possible cooperation with proxy groups operating in the Middle East.

Third-Party Operators:

Contracting freelance hackers or groups with specialized skills in IoT exploitation and advanced obfuscation techniques.

</td></tr>
<tr><td>Historical Campaigns</td><td>
2018: Shamoon 3

Disrupted critical infrastructure in the Middle East.
Employed data-wiping malware to cripple operations.

2020: DNSpionage Campaign

Targeted government and telecommunications entities in the Middle East.
Used DNS tunneling to exfiltrate data.

2023–2024: IOControl Campaign

Focused on IoT devices and Linux ARM systems.
Exploited MQTT and DNS-over-HTTPS for stealthy C2 operations.

</td></tr>
<tr><td>Current Priorities and Strategic Goals</td><td>

Expanding IoT/OT Targeting: Leveraging lightweight protocols and exploiting poorly secured devices.
Global Espionage: Gathering intelligence on energy production, telecommunications, and military activities.
Disruption Campaigns: Targeting critical infrastructure as leverage in geopolitical disputes.

</td></tr>
<tr><td>Key Indicators of Group Activity</td><td>
<table>
<tr><th>Category</th><th>Indicators</th></tr>
<tr><td>Infrastructure</td><td>Dynamic domains like `tylarion867mino.com`</td></tr>
<tr><td>C2 Traffic</td><td>MQTT (ports 8883/1883)</td></tr>
<tr><td>Techniques</td><td>DNS-over-HTTPS (DoH)</td></tr>
<tr><td>Persistence</td><td>Startup scripts and PID monitoring</td></tr>
<tr><td>Reconnaissance</td><td>Use of commands like `whoami`, `uname -r`|</td></tr>
<tr><td>Malware</td><td>IOControl, Shamoon, DNSpionage</td></tr>
</table>
</td></tr>
</table>

Recommendations for Defense

Understanding the operational tactics of IOControl malware helps organizations to implement a robust defense against similar threats. By correlating these indicators—unfamiliar binaries and scripts, suspicious domains and ports, hidden persistence mechanisms, and system reconnaissance commands—security professionals can detect, investigate, and mitigate this malware before it causes further harm.

1. **Threat Intelligence Integration**
    - Incorporate these TTPs and IOCs into your SIEM/SOAR platforms and threat feeds.
2. **IoT Security**
    - Implement segmentation and restrict MQTT usage to trusted brokers. Here's how Armis helps.
3. **Proactive Patch Management:**
    - Prioritize vulnerabilities exploited by this group. Here's how Armis helps.
4. **Monitoring C2 Channels:**
    - Identify DNS-over-HTTPS usage and non-standard domain patterns. Here's how Armis helps.

About Armis Labs

Armis Labs, a division of Armis, is a team of seasoned security professionals dedicated to staying ahead of the ever-evolving cybersecurity landscape With a deep understanding of emerging threats and cutting-edge methodologies, Armis Labs empowers organizations with unparalleled visibility and expertise to protect against the evolving threats that matter most, including IOControl.

Armis Labs security practitioners are utilizing cutting edge technology that include dynamic honeypots, incident forensics, reverse engineering, dark web monitoring, and human intelligence to proactively identify and mitigate threats before they manifest. Leveraging advanced AI/ML technologies, Armis Labs' proactive threat detection capabilities enable organizations to stay one step ahead of cyber adversaries, minimizing the risk of potential breaches while stopping potential damage before it occurs.

Contact us to discuss how we can help improve your defensive security posture by ensuring your entire attack surface is defended and managed in real-time.
