Device Threat Intel_

New Threat Campaign Variants Targeting Fortinet and Other Network Devices

March 11, 2026

Executive Summary

The enterprise attack surface has undergone a fundamental shift. Over recent years, threat actors, ranging from sophisticated nation-state APTs to financially motivated ransomware groups, have increased the frequency of systematic exploitation of network infrastructure.

On March 6, 2026, Eclypsium captured new samples of previously undocumented malware strains:

1. **CondiBot (DDoS Botnet Variant):** An evolution of the Mirai-derived Condi DDoS botnet, this new sample was found to be previously unreported on major threat intelligence platforms. It is a multi-architecture binary (written in C) designed to turn compromised Linux devices into nodes for large-scale network attacks.

2. **"Monaco" (SSH Scanner & Crypto Miner):** An active, multi-architecture cryptojacking operation that targets servers, IoT devices, routers, and network devices by brute-forcing weak SSH credentials, harvesting hundreds of SSH servers and sending credentials back to its C2 servers.

Technical Details

CondiBot Variant

CondiBot is a DDoS botnet executor. Its goal is to turn compromised Linux devices into remotely controlled nodes capable of launching large-scale network attacks.

Further analysis concluded it not only attacks Fortinet but impacts other network device vendors as well. It is a generic Linux Botnet agent that tries multiple download methods across multiple filesystems with a variety of architecture payloads for arm, mips and x86. It can work on any vulnerable linux device regardless of the vendor.

Malware Details

Malware Family	CondiBot (Mirai derivate)
Filename	executor
File Hash	- 98e6884ae15a4f6c0142d9e5edd09d596090a7ea5bbcb642da7f1a6536ee0dca executor.arm - 92d8909813dbe7b5471e60fc08f18a1973adcc04b3489ae3b0b667bfbfd7c0e0 executor.arm5 - e40985dfc480b290cd50919c2c7696c908ae84a1443ef5573e700e52b26377c3 executor.arm6 - d8edeb122ec3746e57ddeefc567a9d4994a3ab1d4e4938f82b31cbb67ca6e6bc executor.arm7 - 6bbde22f2319b2498e93ba14570668592d029193a3e48e928d461a001e4e6de1 executor.x86_64 - 7fc6cee89496d01cf39adc90277d5cdad97d3a9d1eeee02015f322715b93a8d5

	executor.x86 - d322ce52f7136d953471ebf5af4179e3b4259845a3ff0c9fdccc3236c8221f52 executor.mpsl - 938b3f1d82282c52480db8887613d3b6a634e4c7e974b66437acbdbf5cae84ce executor.mips
File Type	ELF 64-bit x86_64, statically linked stripped
String artifacts	condi, condibot, CondiBot, condinetwork, condinet, qtxbot
Architectural Variants	arm, arm5. arm6. arm7, mips, x86, x86_64
C2 IP Address	65.222.202.53 (not active)
C2 Port	80 (0x5000)
Listener Port	17664 (0x4500)

Mechanism of Attack

1. **Delivery:** Employs a robust payload drop mechanism that cycles through multiple transfer utilities (wget, curl, tftp, ftpget) to ensure successful download of the multi-architecture binaries.
2. **Execution:** On a compromised device the bot initializes, disables reboot capabilities, connects to a C2 server and kills other botnets
3. **C2 Registration:** Sends a registration packet to the C2 with the bots identifier
4. **Command Receipt:** Waits in select() loop for attack commands from the C2
5. **DDoS Execution:** Dispatches one of the registered attack methods against the specified target
6. **Persistence:** Disables system reboot utilities by setting their permissions to `000`, manipulates the hardware watchdog to ensure the device stays active, and kills competing botnets.

Threat Insights

This variant shows some differences with reported Condi samples originally documented by [Fortinet in 2023].

1. **New Unknown Variant** - The hashes from the samples were not known to threat intelligence and malware analysis platforms such as VirusTotal, ThreatFox, Hybrid Analysis, and ELF Digest
2. **Internal identifier** - A string extracted from the binary reveals “QTXBOT”. This identifier does not appear in previous reports on Condi and may indicate either a forked variant or an internal project name used by the developers.
3. **Expanded Attack Surface** - This sample registers 32 attack handlers, while earlier condi variants documented fewer modules, the additional handlers likely represent new flood techniques or protocol variants. Seen in FUN_004006c0

4. **Competitive Botnet Killing** - This variant contains process-killing logic that references multiple botnet families. This variant has added an additional botnet to its kill list: `/bin/sora`.

"Monaco" SSH Scanner & Crypto Miner

“Monaco” is a SSH Scanner + Crypto Miner written in Go 1.24.0 that brute-forces SSH servers across the internet, compromises them, and deploys Monero cryptocurrency miners with the intention of using compromised devices as free compute to generate crypto revenue.

Malware Details

Malware Family	Cryptominer
Filename	monaco
File Hash	• **MD5:** 3781a533e77c89dfb575d3a94ddf035f • **SHA-1:** 8ac8424de629de2cdc4f76618862d4801c5ff6cc • **SHA-256:** 08e386e9217eac061db97319962523562b292969192bf4505d431a6d087b8057
File Type	ELF 64-bit LSB executable, x86-64, statically linked, stripped
Compiler	Go 1.24.0 (gc), built 2025-02-11
Architectural Variants	Compiled for x86-64, ARM32, ARM64, MIPS big/little-endian — targets servers, IoT devices, routers, and Juniper network equipment
C2 IP Address	8.222.206.6
C2 Port	ports 80 (Apache file hosting), 3333 (mining proxy), 12345 (nice C2), 12346 (monaco C2)
Mining Pool	gulf.moneroocean.stream:20128 (MoneroOcean)
Host indicators	/tmp/monaco or /tmp/nice, chmod 777, XMRig process, MSR writes

Complete listing of hashes for all recovered files from C2:

File	SHA-256
monaco (x86-64)	`08e386e9217eac061db97319962523562b292969192bf4505d431a6d087b8057`
monaco5 (ARM)	`434726214f8a831a52510f611bddf4cb9143f4c5b947159e6d7de57380bfcbb0`

File	SHA-256
monaco7 (ARM, debug)	62c3aa5994ffa7bfda51577085376c1e0ffce35a723fba6f063c06de00f98972
monaco64 (ARM)	ffdb0611d3cb6a09a442408b0276be4d67f962d4787075f5fa86d1703c159f9f
monacomips (MIPS BE)	b361d66e45e40a8375410e270c8f86d181257a9d41b8a7cc1d6994aa1e1dacc7
monacomipsle (MIPS LE)	df0003a9c0b45337edb2a2cfb39bafbec2b102d6343b2fe67fb121e5ee310f1a
nice (x86-64, dynamic)	0e9ba1ce39d7adbc410eef43893cea63e5e5f5cf7ec8f146a92a1c7c3f28baeb
nice7 (ARM)	cdde075f1c1327c058ee934758aa03b11241493757f54326f74f9ba7b48125e6
nice64 (ARM)	9293626cbc04b14269edb7498779e85a3be2162bd96c527bf2b223aad7db7691
nicejunos (MIPS, JunOS)	df840fb6e42675fa5cc6541c3362e200b1f34cfde1bf8710611bfef4d87763a4
nicex (x86-64, static)	bc37d3413c3be056aed298e5a6665543fdb055908e1ae2f50333e9c2e993f64a
nicex2 (x86-64, stripped)	2ccfb8bc5fcb00407b9288b21ab31e965aeca9befd573a7c8f9444d73fb759f2
xmrig (x86-64)	96fc528ca5e7d1c2b3add5e31b8797cb126f704976c8fbeaecdbf0aa4309ad46
xmrigMiner (ARM64)	f17fc5851c26aa07619061e9ef47214a1ee942edc8b21fbd07c3cbaf19955990
xmrigDaemon (ARM64)	e39f3e1e34f807b6f0457f44185f7a63cbafd31dad674f9ea12ea8fdc9e026f6

File	SHA-256
portscan (i386)	`97093a1ef729cb954b2a63d7ccc304b18d0243e2a77d87bbbb94741a0290d762`

Virustotal Share Collection:
https://www.virustotal.com/gui/collection/1d90b71cd437c8d7354ede59b25a4dd27966976a33fb274a87d81c6d9c656288/iocs

Mechanism of Attack

1. **Reconnaissance** - Scans random public IPs for SSH (port 22), excluding private/reserved ranges (~3.6 billion IPs in scope)
2. **Initial Access** - Brute-forces with ~50+ hardcoded passwords (root, admin, ubuntu, postgres, numeric patterns like 123456, India@123)
3. **Payload** - On success it exhibits the following behaviors:
    a. Copies itself to /tmp/monaco,
    b. Kills competing miners
    c. Tunes CPU for mining
    d. Deploys XMRig/XMRigCC for managing the miners
4. **Command & Control** - Reports compromised credentials back to C2 over raw TCP
5. **Persistence** - Utilizes resiliency techniques such as daemonization, forking backup processes, survives SIGTERM/SIGINT via signal handler, and watchdog restarts after stalled scans

Threat Insights

- Most likely a Chinese-speaking threat actor
- Hosted on Alibaba Cloud Singapore (IP 8.222.206.6, AS45102)
- Alibaba Cloud is predominantly Chinese; CNNIC-allocated AS block; cloud IDE workspace ID pattern consistent with Chinese platforms
- Low sophistication — open directory listing on C2, debug builds left on server, default XMRigCC token `mySecret`, password `skema` in plaintext configs

Eclypsium Threat Research Insights

Increasing Trend of Targeting Network Devices

Threat actors are prioritizing network devices as an initial attack vector due to several unique structural advantages they offer:

- **Implicit Trust & "The Visibility Gap":** Most enterprise security stacks (EDR/XDR) are blind to the embedded firmware/software and OS layers of network appliances. Because these devices cannot host traditional security agents, they remain "opaque," allowing attackers to operate undetected for months.
- **Initial Access Without Human Interaction:** Unlike phishing, which requires a user to click a link, network devices are often internet-facing by design. Vulnerabilities in VPNs or Gateways allow for zero-click initial access, enabling attackers to bypass the entire perimeter defense in a single move.
- **High-Level Persistence:** By compromising the firmware of a router or switch, attackers can establish persistence that survives reboots, OS re-imaging, and even hard drive replacements. This "below-the-OS" control allows for long-term espionage and re-infection.
- **Strategic Positioning for Lateral Movement:** A single compromised switch or firewall provides a pivot point to move laterally across VLANs, bridge IT/OT environments, and intercept or redirect sensitive traffic.

Timeline of Network Device Attacks

Eclypsium detects persistent implants, backdoors, in-memory malware and anomalous behavior in network edge and core equipment. Eclypsium detects implants and malware used by both Nation-state APTs and ransomware actors. Threat campaigns which used network devices as initial access vector and persistence (A History of Network Device Threats and What Lies Ahead):

- **Dec 2025** SonicWall SMA1000: Local Privilege Escalation Used in Zero-Day Attacks
- **Oct 2025** F5 Systems Compromised, BIG IP Vulnerabilities Exfiltrated (BRICKSTORM campaign)
- **Sep 2025** Surge in Cisco ASA Scanning Hints At Coming Cyberattacks
- **Sep 2025** RedNovember attacks Cisco ASA / FTD, Ivanti, SonicWALL, PANW GlobalProtect
- **Sep 2025** EOL Devices: Exploits Will Continue Until Security Improves (Cisco, Linksys)
- **Aug 2025** Salt Typhoon targets Cisco and Palo Alto network devices (Cisco, Ivanti, PAN, Fortinet, Sophos)
- **Jul 2025** Vulnerabilities in Netgear Firmware-Based IoT Devices In The Enterprise
- **Jun 2025** The Cisco Vulnerability Salt Typhoon Weaponized Against Canadian Telcos and Viasat
- **Mar 2025** Juniper Network Devices Targeted with Custom Backdoors (J-Magic, TinyShell by UNC3886)
- **Mar 2025** Silk Typhoon Targeting IT Supply Chains and Ivanti Network Devices
- **Mar 2025** Inside Black Basta Ransomware Group

- **Jan 2025** PANdora's Box: Vulnerabilities Found in NGFW
- **Nov 2024** Pacific Rim attacks on Sophos Firewall
- **Oct 2024** The Rise of Chinese APT Campaigns: Volt Typhoon, Salt Typhoon, Flax Typhoon, and Velvet Ant
- **Sept 2024** Velvet Ant attacks Cisco NX-OS and F5 Load Balancers
- **Sept 2024** Flax Typhoon with Raptor Train Botnet compromises Citrix and Zyxel
- **Aug 2024** Fox Kitten Iranian APT Group exploits Citrix Netscaler, Ivanti Pulse VPN, F5, and Palo Alto
- **Apr 2024** Arcane Door with Line Dancer and Line Runner implants in Cisco ASA
- **Apr 2024** PAN-OS Exploitation leads to exfiltration
- **Jan 2024** Volt Typhoon infects KV Botnet on Cisco, ASUS, D-link, Netgear, and Zyxel routers
- **Oct 2023** Citrix attacked by APT41 (Speculoos backdoor), REvil, Maze ransomware
- **Sept 2023** BlackTech APT Group infects Cisco router firmware
- **Apr 2023** Jaguar Tooth malware targets Cisco IOS routers
- **Nov 2022** Pwned Balancers: Commandeering F5 and Citrix for Persistent Access & C2
- **May 2022** F5 BIG-IP exploitation by multiple actors
- **Feb 2022** Cyclops Blink malware targets Watchbox Firebox
- **May 2021** Ivanti Pulse Secure VPN exploitation by APT5, UNC2630, China-nexus actors, REvil
- **Mar 2020** Chinese threat actor APT41 exploits Cisco routers, Citrix, and Zoho
- **Aug 2016** SYNful Knock implants backdoors into Cisco ROMMON

Monitor & Protect Your Network Devices

The traditional perimeter is dissolving, and a reliance on host-based and network-traffic monitoring is no longer sufficient to secure the modern enterprise. To address the documented structural advantages leveraged by threat actors, Enterprises must immediately implement a strategy focused on hardware and device-level integrity.

1. **Eliminate the Visibility Gap:** Leverage security controls to gain deep visibility into the embedded software, firmware and operating system layers of network devices, which are increasingly exploited as initial access vector, for long-term persistence and evasion.

2. **Verify Device Integrity and Trust:** Establish a continuous hardware monitoring program to verify the authenticity and integrity of critical equipment and core components, protecting against embedded software/firmware implants and supply chain threats.

3. **Hardened Security Posture:** Address misconfigurations, critical vulnerabilities, and deploy the latest security patches to reduce risks of exploitation.

YARA Rules

CondiBot Variant

```
None
rule Condi_QTXBOT_Path_Strings
{
    meta:
        author          = "Eclypsium"
        description     = "Detects CondiBot family across all architectures by
co-occurring process-eviction whitelist strings"
        family          = "Condi"

    strings:
        // Verified present as plaintext literals across all 8 architecture
decompilations:
        $s_condi_tmp     = "/tmp/condi"          ascii
        $s_condi_net_tmp = "/tmp/condinetwork"   ascii
        $s_condibot_var  = "/var/condibot"       ascii
        $s_CondiBot_var  = "/var/CondiBot"       ascii
        $s_condinet_var  = "/var/condinet"       ascii
        $s_zxcr_tmp      = "/tmp/zxcr9999"       ascii
        $s_zxcr_var      = "/var/zxcr9999"       ascii

    condition:
        uint32(0) == 0x464C457F and
        5 of them
}
```

```
None
rule Condi_QTXBOT_XOR02_Encoded_Identifiers
{
    meta:
        author          = "Eclypsium"
        description     = "Detects CondiBot variant by XOR-0x02 obfuscated campaign
tag and competitor botnet identifiers"
        family          = "Condi"

    strings:
        // Plaintext strings XOR'd with 0x22
```

```
        // Encoded in binary: "SVZ@MV\""  (53 56 5A 40 4D 56 22) --> QTXBOT
        $xor_qtxbot    = "qtxbot" xor(0x22)

        // Encoded in binary: "JCICK\""   (4A 43 49 43 4B 22) --> HAKAI
        $xor_hakai     = "hakai" xor(0x22)

    condition:
        uint32(0) == 0x464C457F and
        all of them
}
```

```
None
rule Condi_QTXBOT_Payload_Download_Chain
{
    meta:
        author          = "Eclypsium"
        description     = "Detects Condi multi-tool download propagation engine by
exact format string set"
        family          = "Condi"

    strings:
        // All 5 templates verified in all 8 arch decompilations:
        $dl_wget   = "wget http://%s/%s/%s -O %s"                            ascii
        $dl_curl   = "curl -o %s http://%s/%s/%s"                            ascii
        $dl_tftp1  = "tftp %s -c get %s %s"                                  ascii
        $dl_tftp2  = "cd %s && tftp -g -r %s %s"                             ascii
        $dl_ftpget = "ftpget -v -u anonymous -p anonymous -P 21 %s %s %s"    ascii

    condition:
        uint32(0) == 0x464C457F and
        4 of them
}
```