INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-05-07 06:36 UTC

Hardware Supply Chain Backdoors: Hidden Radios, Covert Drivers, and Nation-State Persistence in Critical Infrastructure

THREAT CAMPAIGN | **CRITICAL** | CVSS 7.5

SCC Item ID	SCC-CAM-2026-0282
Type	Threat Campaign
Severity	CRITICAL
CVSS Base Score	7.5
Affected Products	Solar inverters (U.S. highway infrastructure), consumer drones, 3D printers, networked IoT devices (overseas manufacturers), macOS systems at cryptocurrency firms
Published	2026-05-06T13:00:29+00:00
Discovery Source	Rss:T1 Threatintel

Executive Summary

SentinelLabs researchers presented three converging supply chain threats at LabsCon25: undocumented cellular radio modules found in Chinese-manufactured solar inverters deployed across U.S. highway infrastructure, a kernel-level sabotage framework assessed as active since 2005, and a North Korean campaign targeting macOS systems at cryptocurrency firms. The unifying risk is component-level opacity: organizations cannot verify what embedded hardware transmits or what kernel drivers execute, making detection with standard security tooling unreliable. Critical infrastructure operators, financial sector firms, and any organization sourcing hardware from affected manufacturers face persistent, hard-to-detect compromise with potential for operational disruption, data exfiltration, and long-dwell espionage.

Technical Analysis

Three distinct threat vectors were documented. (1) Hardware backdoor: Undocumented cellular radio modules embedded in Chinese-manufactured solar inverters deployed in U.S. highway infrastructure enable covert out-of-band communication, corroborated by Reuters reporting (May 2025). No firmware CVE is assigned; the backdoor is physical/hardware layer (CWE-506: Embedded Malicious Code, CWE-912: Hidden Functionality). MITRE mapping: T1195.003 (Compromise Hardware Supply Chain), T1071 (Application Layer Protocol). (2) Kernel sabotage framework: A high-precision driver-level sabotage capability, referenced in ShadowBrokers material, assessed as operational since approximately 2005, making it contemporaneous with or predating Stuxnet discovery (2010). Operates at kernel level, evading most userland detection. CWE mappings: CWE-693

(Protection Mechanism Failure), CWE-494 (Download of Code Without Integrity Check). MITRE: T1542 (Pre-OS Boot), T1542.003 (Bootkit), T1542.001 (System Firmware), T1601 (Modify System Image). Attribution: nation-state suspected, unattributed. (3) BlueNoroff/Hidden Risk (DPRK, Lazarus subcluster): Targets macOS systems at cryptocurrency and Web3 firms. Initial access via spearphishing with fake crypto news lures (T1566.001, T1566.002). Delivers novel macOS persistence mechanisms (T1547). Uses masquerading (T1036.005) and web services for C2 (T1102). No patch is available for hardware-layer backdoors; kernel sabotage remediation requires hardware/firmware attestation and re-imaging from verified media. BlueNoroff macOS indicators and IOCs are documented in the SentinelLabs report. No CVE assigned to any of the three vectors.

Action Checklist

1. Step 1: Containment, Identify all solar inverters and grid-connected hardware sourced from Chinese manufacturers in your environment. Isolate units from internet-facing network segments. For cryptocurrency and Web3 firms, isolate macOS endpoints that may have received crypto-news-themed email attachments in the past 90 days. Demand vendors provide hardware bill-of-materials and RF emission disclosures or cease procurement; escalate to procurement leadership if vendors refuse.
2. Step 2: Detection, For hardware backdoors: conduct RF spectrum analysis near solar inverter installations to identify unexpected cellular transmissions. For kernel sabotage: review kernel driver load events, unsigned or anomalously timestamped drivers, and boot integrity logs (Windows: Event ID 7045 and Get-SecureBootPolicy PowerShell cmdlet; Linux: kernel module load logs and dmesg). For BlueNoroff/Hidden Risk: search macOS endpoints for persistence entries documented in the SentinelLabs BlueNoroff report (LaunchAgents, LaunchDaemons, login items added post-phishing); review email gateway logs for crypto-news-themed lures with document or application attachments.
3. Step 3: Eradication, Hardware backdoors: no firmware patch exists; physical removal or replacement of affected inverter units is the only confirmed remediation. For kernel-level sabotage: re-image affected systems from official, signed OS media (Windows LTSC from Microsoft, Ubuntu LTS from Canonical) with cryptographic hashes verified against the vendor's official distribution channel using PowerShell or GPG signatures. Validate boot chain integrity via TPM/Secure Boot attestation before returning to production. For BlueNoroff macOS: remove identified persistence mechanisms per SentinelLabs IOC guidance, revoke and rotate any credentials or wallet keys accessible from compromised endpoints.
4. Step 4: Recovery, Validate boot integrity on re-imaged systems before reconnecting to production networks. For solar inverter replacements, require hardware attestation documentation and RF certification from vendors before deployment. Monitor reinstated macOS endpoints for re-infection indicators (anomalous outbound connections to domains flagged in SentinelLabs Hidden Risk report, see sources) for a minimum of 30 days post-remediation. Refer to SentinelLabs Hidden Risk report for complete IOC list including domains, IPs, and file hashes.
5. Step 5: Post-Incident, This campaign exposes three control gaps: absence of hardware bill-of-materials (HBOM) requirements in procurement, lack of kernel driver integrity verification in operational baselines, and insufficient email security controls for targeted spearphishing at crypto-sector firms. Incorporate HBOM requirements into vendor contracts per NIST SP 800-161r1 (C-SCRM). Enforce UEFI Secure Boot and kernel driver signing policies. Apply CISA supply chain risk management guidance for critical infrastructure hardware procurement.

IR / Forensic Enrichment

Triage Priority	IMMEDIATE
Escalation Criteria	Escalate immediately to CISA ICS-CERT and senior leadership if RF transmissions are confirmed from solar inverters deployed in U.S. highway or grid infrastructure, if kernel-level unsigned drivers are found on OT-adjacent systems, or if BlueNoroff persistence is confirmed on macOS endpoints with access to cryptocurrency wallets or private keys — any of these conditions represents active nation-state implant presence in critical infrastructure or financial systems requiring regulatory notification and potential law enforcement referral.
Recovery Notes	Re-imaged systems must pass TPM/Secure Boot attestation and kernel driver integrity baseline checks before reconnecting to any OT or production network segment. Replacement solar inverter hardware must be accompanied by FCC Equipment Authorization documentation confirming all RF-capable components before physical installation. Monitor all reinstated macOS endpoints and OT network segments for a minimum of 30 days using the SentinelLabs BlueNoroff IOC list and RF spectrum baselines as detection references, given BlueNoroff's demonstrated capability to re-establish persistence through credential reuse or secondary phishing waves targeting the same crypto-sector personnel.
Forensic Artifacts	RTL-SDR IQ captures (.sigmf or .wav format) from 700–2100 MHz LTE band recorded during active solar inverter operation — evidence of undocumented cellular modem transmissions from hardware with no FCC-authorized radio components | Windows System Event Log entries for Event ID 7045 (Service Installed) and Sysinternals sigcheck output for C:\Windows\System32\drivers\ — evidence of kernel-level unsigned or anomalously timestamped drivers consistent with the kernel sabotage framework assessed active since 2005 | macOS LaunchAgent and LaunchDaemon plist files created within the 90-day phishing window at ~/Library/LaunchAgents/, /Library/LaunchAgents/, and /Library/LaunchDaemons/ — persistence artifacts deposited by BlueNoroff Hidden Risk campaign following crypto-news-themed lure delivery | Full forensic disk image (SHA-256 verified) of kernel-sabotaged systems acquired before re-imaging — preserves driver file creation timestamps, binary artifacts, and any rootkit-level modifications that would survive standard log collection | Email gateway logs (MTA, O365 Unified Audit Log, or Proofpoint/Mimecast export) documenting delivery of crypto-news-themed attachments (.dmg, .app bundles, PDFs) to macOS endpoints at cryptocurrency firms during the 90-day spearphishing window attributed to BlueNoroff/Hidden Risk

Per-Action IR Details

Step 1: Containment — Identify all solar inverters and grid-connected hardware sourced from Chinese manufacturers in your environment. Isolate units from internet-facing network segments. For cryptocurrency and Web3 firms, isolate macOS endpoints that may have received crypto-news-themed email attachments in the past 90 days. Contact vendors for hardware bill-of-materials and RF emission disclosures.

NIST Phase: Containment

Reference: NIST 800-61r3 §3.3 — Containment Strategy

Controls: NIST IR-4 (Incident Handling), NIST SA-12 (Supply Chain Protection), NIST SC-7 (Boundary Protection), CIS 1.1 (Establish and Maintain Detailed Enterprise Asset Inventory), CIS 4.4 (Implement and Manage a Firewall on Servers)

Compensating: Run 'nmap -sn ' or query your DHCP server's lease table to enumerate all OT/IoT endpoints by MAC OUI prefix — cross-reference Chinese inverter manufacturer OUIs (e.g., Huawei: 00:18:82, Growatt: varies) against IEEE OUI registry (standards-oui.ieee.org). For macOS isolation, use 'networksetup -setairportpower en0 off' and

'networksetup -setv4off Ethernet' to cut network access without physical intervention. Request HBOM and FCC RF certification documentation from vendors; absence of FCC ID on cellular-capable hardware is itself a red flag.

Evidence: Before isolating solar inverter units, capture PCAP using Wireshark or tcpdump on the network segment for at least 15 minutes to record all outbound connections from inverter management IPs — specifically flag any traffic to non-vendor IP ranges, unexpected cellular APN hostnames, or DNS queries to .cn TLDs. For macOS endpoints, capture a full directory listing of ~/Library/LaunchAgents/, /Library/LaunchAgents/, /Library/LaunchDaemons/, and ~/Library/Application Support/ before any remediation, and preserve email gateway logs showing crypto-news-themed attachment delivery events from the past 90 days (MTA logs, O365 Unified Audit Log, or Proofpoint/Mimecast export).

Step 2: Detection — For hardware backdoors: conduct RF spectrum analysis near solar inverter installations to identify unexpected cellular transmissions. For kernel sabotage: review kernel driver load events, unsigned or anomalously timestamped drivers, and boot integrity logs (Windows: Event ID 7045, Linux: kernel module load logs). For BlueNoroff/Hidden Risk: search macOS endpoints for persistence entries documented in the SentinelLabs BlueNoroff report (LaunchAgents, LaunchDaemons, login items added post-phishing); review email gateway logs for crypto-news-themed lures with document or application attachments.

NIST Phase: Detection Analysis

Reference: NIST 800-61r3 §3.2 — Detection and Analysis

Controls: NIST SI-4 (System Monitoring), NIST AU-2 (Event Logging), NIST AU-6 (Audit Record Review, Analysis, and Reporting), NIST IR-5 (Incident Monitoring), CIS 8.2 (Collect Audit Logs), CIS 7.1 (Establish and Maintain a Vulnerability Management Process)

Compensating: RF detection: Use a $25 RTL-SDR dongle with GQRX or SDR# software to scan the 700–2100 MHz LTE band near inverter installations — unexpected narrowband transmissions in LTE Band 12/17 (700 MHz, common for US rural cellular) from hardware that should be WiFi-only or wired-only is a confirmed indicator. Kernel driver detection (Windows): Run 'Get-WinEvent -LogName System | Where-Object {$_.Id -eq 7045}' in PowerShell to list all service/driver installs; pipe to 'Select-Object TimeCreated, Message' and flag entries with timestamps predating the system's known build date or lacking a valid Authenticode signature (verify with 'Get-AuthenticodeSignature '). Linux kernel modules: 'cat /proc/modules' and cross-reference with 'modinfo ' — flag modules with no signing key or a self-signed key. macOS BlueNoroff persistence: Run 'find /Library/LaunchAgents /Library/LaunchDaemons ~/Library/LaunchAgents -name "*.plist" -newer /var/log/install.log' to identify plist files created after the phishing window; use 'osquery' with 'SELECT * FROM launchd WHERE path NOT LIKE "/System/%";' to enumerate non-Apple launch items.

Evidence: For the kernel sabotage framework (assessed active since 2005), preserve Windows System Event Log exports filtered to Event ID 7045 (Service Installed) and Event ID 219 (kernel driver load warning) from all OT-adjacent Windows hosts; capture 'sigcheck -vr -u -e C:\Windows\System32\drivers\' output (Sysinternals sigcheck) to identify unsigned drivers before any remediation. For RF backdoor confirmation, record RTL-SDR spectrum captures as IQ files (.wav or .sigmf format) timestamped during active inverter operation — these constitute forensic evidence of undocumented RF emissions. For BlueNoroff/Hidden Risk macOS: capture 'sudo log show --predicate "eventMessage contains \"LaunchAgent\"" --last 90d' output and preserve the full plist content of any non-Apple launch items, along with 'sudo log show --predicate "processImagePath contains \"crypto\"" --last 90d' for any process execution tied to phishing lure filenames.

Step 3: Eradication — Hardware backdoors: no firmware patch exists; physical removal or replacement of affected inverter units is the only confirmed remediation. For kernel-level sabotage: re-image affected systems from cryptographically verified media; validate boot chain integrity via TPM/Secure Boot attestation before returning to production. For BlueNoroff macOS: remove identified persistence mechanisms per SentinelLabs IOC guidance, revoke and rotate any credentials or wallet keys accessible from compromised endpoints.

NIST Phase: Eradication

Reference: NIST 800-61r3 §3.4 — Eradication

Controls: NIST IR-4 (Incident Handling), NIST SI-2 (Flaw Remediation), NIST SI-7 (Software, Firmware, and Information Integrity), NIST CM-3 (Configuration Change Control), CIS 2.2 (Ensure Authorized Software is Currently

Supported), CIS 4.6 (Securely Manage Enterprise Assets and Software)

Compensating: Hardware eradication: Document inverter serial numbers, firmware versions, and physical location before removal — photograph the PCB interior if units are opened, looking for undocumented daughter boards or cellular modem chips (SIM slots, antenna connectors, or LTE module markings such as SIM7600 or EC25). Kernel sabotage re-image: Verify installation media integrity with 'Get-FileHash -Algorithm SHA256 ' (Windows) or 'sha256sum ' (Linux) against vendor-published checksums before imaging; after re-image, run 'tpm2_pcrread' (Linux tpm2-tools) or 'Confirm-SecureBootUEFI' (Windows PowerShell) to attest boot chain integrity. BlueNoroff macOS credential rotation: use 'security delete-generic-password' and 'security delete-internet-password' CLI commands to purge keychain entries accessible to compromised processes; revoke all cryptocurrency wallet private keys stored in macOS Keychain or browser extensions on affected endpoints and generate new keys on a clean, air-gapped device.

Evidence: Before re-imaging kernel-sabotaged systems, acquire a full forensic disk image using 'dc3dd if=/dev/sda hash=sha256 hof=evidence.img.sha256 of=evidence.img' (Linux) or FTK Imager (Windows) — the kernel sabotage framework's assessed 2005 origin means artifacts may include legacy driver files with creation timestamps inconsistent with the OS install date, which will be lost without prior imaging. For BlueNoroff macOS eradication, preserve copies of all identified LaunchAgent/LaunchDaemon plist files, the associated binary payloads they reference, and the output of 'sudo eslogger exec' or 'sudo log show --last 90d' covering the phishing delivery window before removing any persistence mechanisms. Retain the SentinelLabs IOC list as the authoritative reference for comparing identified binaries.

Step 4: Recovery — Validate boot integrity on re-imaged systems before reconnecting to production networks. For solar inverter replacements, require hardware attestation documentation and RF certification from vendors before deployment. Monitor reinstated macOS endpoints for re-infection indicators (anomalous outbound connections to domains flagged in SentinelLabs report) for a minimum of 30 days post-remediation.

NIST Phase: Recovery

Reference: NIST 800-61r3 §3.5 — Recovery

Controls: NIST IR-4 (Incident Handling), NIST SI-7 (Software, Firmware, and Information Integrity), NIST CP-10 (System Recovery and Reconstitution), NIST SA-12 (Supply Chain Protection), CIS 7.3 (Perform Automated Operating System Patch Management), CIS 4.2 (Establish and Maintain a Secure Configuration Process for Network Infrastructure)

Compensating: Boot integrity validation: On re-imaged Windows hosts, run 'msinfo32' and verify 'Secure Boot State: On' and 'BIOS Mode: UEFI' before domain-joining; on Linux, 'mokutil --sb-state' confirms Secure Boot enforcement. For replacement solar inverters, require vendors to provide FCC Equipment Authorization records (searchable at fccid.io by device model) confirming all radio transmitters are documented — reject any unit where embedded radio modules are not listed in the FCC grant. macOS re-infection monitoring: Deploy osquery with the query 'SELECT name, path, keep_alive FROM launchd WHERE path NOT LIKE "/System/%" AND path NOT LIKE "/usr/%";' on a 5-minute schedule via a cron job, and use 'lsof -i' piped through 'grep -v LISTEN' to catch anomalous outbound connections; compare outbound DNS queries against the BlueNoroff C2 domain list from the SentinelLabs report using '/etc/hosts' blocking or a local Pi-hole instance.

Evidence: Before reconnecting re-imaged systems to production, capture a clean baseline using 'Get-FileHash -Recurse C:\Windows\System32\drivers\' (Windows) and store SHA-256 hashes for all kernel drivers — this establishes an integrity baseline to detect re-infection by the kernel sabotage framework if it re-enters via a different vector. For reinstated macOS endpoints, run 'sudo fs_usage -f filesys' for 10 minutes during first production use to capture any new file writes to persistence directories (~Library/LaunchAgents, /tmp, ~/Library/Application Support) that would indicate Hidden Risk re-infection from a missed persistence mechanism or credential-based re-access by BlueNoroff operators.

Step 5: Post-Incident — This campaign exposes three control gaps: absence of hardware bill-of-materials (HBOM) requirements in procurement, lack of kernel driver integrity verification in operational baselines, and insufficient email security controls for targeted spearphishing at crypto-sector firms. Incorporate HBOM requirements into vendor contracts per NIST SP 800-161r1 (C-SCRM). Enforce UEFI Secure Boot and kernel driver signing policies. Apply CISA supply chain risk management guidance for critical infrastructure

hardware procurement.

NIST Phase: Post Incident

Reference: NIST 800-61r3 §4 — Post-Incident Activity

Controls: NIST IR-4 (Incident Handling), NIST IR-8 (Incident Response Plan), NIST SA-12 (Supply Chain Protection), NIST SI-2 (Flaw Remediation), NIST SI-7 (Software, Firmware, and Information Integrity), NIST AU-6 (Audit Record Review, Analysis, and Reporting), CIS 7.1 (Establish and Maintain a Vulnerability Management Process), CIS 7.2 (Establish and Maintain a Remediation Process), CIS 2.1 (Establish and Maintain a Software Inventory)

Compensating: HBOM operationalization for resource-constrained teams: Create a vendor attestation form requiring manufacturers to list all integrated circuits, wireless modules, and firmware components with version numbers — cross-reference any cellular chipsets against the FCC Authorization database before accepting delivery. Kernel driver signing enforcement: Use Group Policy (Computer Configuration > Windows Settings > Security Settings > Local Policies > Security Options > 'Driver Signing: Block') on Windows and configure '/etc/modprobe.d/' with 'install /bin/false' on Linux for known-unsigned modules identified during the incident. Email security for BlueNoroff-style spearphishing targeting crypto firms: Deploy DMARC (p=reject), DKIM, and SPF using free tools (mxtoolbox.com for validation); configure mail gateway rules to sandbox or quarantine any macOS .app bundle, .dmg, or PDF attachment arriving from external senders with crypto or financial keywords in subject lines.

Evidence: For the lessons-learned record, preserve the full RF spectrum captures from inverter installations, all kernel driver sigcheck outputs, and the complete inventory of BlueNoroff LaunchAgent artifacts as structured evidence supporting each identified control gap — these artifacts directly demonstrate the absence of HBOM controls (undocumented radio module), kernel driver signing enforcement (unsigned/anomalously timestamped drivers), and email gateway effectiveness (successful delivery of phishing lures). This evidence package should be formatted per NIST IR-6 (Incident Reporting) requirements and shared with CISA via their ICS-CERT reporting portal given the critical infrastructure (highway solar) component of this campaign.

Detection Guidance

Hardware RF backdoor: Deploy RF spectrum analyzers near solar inverter installations; flag any cellular-band transmissions not attributable to authorized devices. Review inverter network traffic for unexpected outbound connections, particularly to cellular gateway IPs. Kernel sabotage framework: Query SIEM for kernel module or driver load events with anomalous timestamps, unsigned signatures, or names inconsistent with installed software baselines. On Linux, review /proc/modules and dmesg for unexpected entries. On Windows, audit Event ID 7045 (new service installed) and compare against approved driver inventory. Use integrity monitoring tools to detect changes to boot sectors or firmware. BlueNoroff/Hidden Risk macOS: Search for LaunchAgent and LaunchDaemon plist files created outside of software installation windows; review Login Items for unfamiliar entries. Hunt for outbound connections to domains and IPs published in the SentinelLabs Hidden Risk report. Inspect email gateway logs for messages containing fake cryptocurrency news headlines with .dmg, .pkg, or document attachments. Behavioral indicator: macOS processes spawning unexpected child processes after document or application execution. Caveat: BlueNoroff persistence mechanisms have historically evaded standard macOS EDR detection; manual review and memory forensics may be required to confirm compromise.

Indicators of Compromise

Type	Value	Context	Confidence
URL	`https://www.sentinelone.com/labs/bluenoroff-hidden-risk-threat-actor-targets-macs-with-fake-crypto-news-and-novel-persistence/`	SentinelLabs BlueNoroff/Hidden Risk report — contains macOS IOCs including domains, hashes, and persistence mechanism details. Search-retrieved URL; validate before use.	HIGH
URL	`https://www.sentinelone.com/labs/labscon25-replay-please-connect-to-the-foreign-entity-to-enhance-your-user-experience/`	SentinelLabs LabsCon25 hardware supply chain presentation — solar inverter cellular radio module findings. Search-retrieved URL; validate before use.	HIGH
URL	`https://www.sentinelone.com/labs/fast16-mystery-shadowbrokers-reference-reveals-high-precision-software-sabotage-5-years-before-stuxnet/`	SentinelLabs kernel sabotage framework analysis — driver-level persistence IOCs and ShadowBrokers reference material. Search-retrieved URL; validate before use.	HIGH

Framework Mappings

MITRE-ATTACK

- **T1195** — Supply Chain Compromise
- **T1587.001** — Malware
- **T1071** — Application Layer Protocol
- **T1071.001** — Web Protocols
- **T1566.001** — Spearphishing Attachment
- **T1542.003** — Bootkit
- **T1195.003** — Compromise Hardware Supply Chain
- **T1036.005** — Match Legitimate Resource Name or Location
- **T1601** — Modify System Image
- **T1542** — Pre-OS Boot
- **T1091** — Replication Through Removable Media
- **T1547** — Boot or Logon Autostart Execution
- **T1059** — Command and Scripting Interpreter
- **T1566.002** — Spearphishing Link
- **T1102** — Web Service
- **T1082** — System Information Discovery
- **T1542.001** — System Firmware

NIST-800-53R5

- **SA-9** — External System Services
- **SR-2** — Supply Chain Risk Management Plan

- **SR-3** — Supply Chain Controls and Processes
- **SI-7** — Software, Firmware, and Information Integrity
- **CA-7** — Continuous Monitoring
- **SC-7** — Boundary Protection
- **SI-4** — System Monitoring
- **AT-2** — Literacy Training and Awareness
- **SI-3** — Malicious Code Protection
- **SI-8** — Spam Protection
- **CM-7** — Least Functionality
- **CM-3** — Configuration Change Control

OWASP-TOP10-2021

- **A08:2021** — Software and Data Integrity Failures

CIS-V8

- **2.5** — Allowlist Authorized Software
- **2.6** — Allowlist Authorized Libraries
- **15.1** — Establish and Maintain an Inventory of Service Providers

NIST-CSF-2

- **GV.SC-01** — Cybersecurity supply chain risk management program

ISO-27001-2022

- **A.5.21** — Managing information security in the ICT supply chain

SOC2-TSC

- **CC9.2** — Manages risks associated with vendors and business partners

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1195	Supply Chain Compromise	Initial-Access
T1587.001	Malware	Resource-Development
T1071	Application Layer Protocol	Command-And-Control
T1071.001	Web Protocols	Command-And-Control
T1566.001	Spearphishing Attachment	Initial-Access
T1542.003	Bootkit	Persistence
T1195.003	Compromise Hardware Supply Chain	Initial-Access

Technique ID	Technique Name	Tactic
T1036.005	Match Legitimate Resource Name or Location	Defense-Evasion
T1601	Modify System Image	Defense-Evasion
T1542	Pre-OS Boot	Defense-Evasion
T1091	Replication Through Removable Media	Lateral-Movement
T1547	Boot or Logon Autostart Execution	Persistence
T1059	Command and Scripting Interpreter	Execution
T1566.002	Spearphishing Link	Initial-Access
T1102	Web Service	Command-And-Control
T1082	System Information Discovery	Discovery
T1542.001	System Firmware	Persistence

Sources

Source	URL	Tier
SentinelLabs - We are hunters, reversers, exploit developers, and tinkerers shedding light on the world of malware, exploits, APTs, and cybercrime across all platforms.	https://www.sentinelone.com/labs/labscon25-replay-please-connect-to...	T3
	https://www.sentinelone.com/labs/labscon25-replay-please-connect-to...	T3
	https://www.sentinelone.com/labs/fast16-mystery-shadowbrokers-refer...	T3
	https://www.sentinelone.com/labs/bluenoroff-hidden-risk-threat-acto...	T3
Rogue communication devices found in Chinese solar power inverters	https://www.reuters.com/sustainability/climate-energy/ghost-machine...	T2

Generated 2026-05-07 06:36 UTC by TJS Security Command Center