INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-03-29 18:39 UTC

EU Adds Teeth to Cyber Accountability: Sanctions Target Flax Typhoon, i-Soon, and Iranian Influence Operators

THREAT CAMPAIGN | **HIGH** | CVSS 5.0

SCC Item ID	SCC-CAM-2026-0051
Type	Threat Campaign
Severity	HIGH
CVSS Base Score	5.0
Affected Products	EU member state critical infrastructure, Swedish SMS services, Charlie Hebdo subscriber systems, approximately 65,000 devices across six EU member states
Published	2026-03-21

Executive Summary

The European Union has imposed targeted sanctions on three state-affiliated cyber contractors, China's Integrity Technology Group (Flax Typhoon) and i-Soon, and Iran's Emennet Pasargad, for operations that compromised approximately 65,000 SOHO and edge devices across six EU member states, disrupted Swedish SMS infrastructure, and exposed Charlie Hebdo subscriber data. These sanctions mirror 2025 U.S. Treasury OFAC designations against the same Chinese entities, signaling coordinated Western cost-imposition. Organizations operating critical infrastructure in the EU, particularly those with SOHO router exposure or public-facing systems, face elevated risk from contractor-model threat actors who sell persistent access to state customers.

Technical Analysis

Three threat actor clusters are implicated across distinct operational profiles. Flax Typhoon (Integrity Technology Group / Ethereal Panda / RedJuliett) built botnet infrastructure by compromising SOHO routers using living-off-the-land techniques including command scripting (T1059), external remote services (T1133), and valid accounts (T1078), leveraging compromised VPS infrastructure (T1583.003) and botnet routing (T1584.005) to maintain persistence across approximately 65,000 devices in six EU states. i-Soon (Anxun Information Technology) operated as an offensive contractor-for-hire providing exploitation services (T1190), exfiltration via web services (T1567), and command-and-control over application-layer protocols (T1071.001) to Chinese state customers. Emennet Pasargad conducted hack-and-leak influence operations including spearphishing (T1598), data theft, and doxing of Charlie Hebdo subscribers, alongside SMS-based influence

operations targeting Swedish infrastructure (T1650). Underlying weaknesses include missing authentication for critical functions (CWE-306), hardcoded credentials in SOHO devices (CWE-798), and improper authentication controls (CWE-287). No CVEs are attributed in the item data. No patches are applicable to the sanctions action itself; remediation focuses on infrastructure hardening and exposure reduction.

Action Checklist

1. Step 1, Immediate: Cross-reference your organization's vendor and third-party lists against sanctioned entities (Integrity Technology Group, Anxun Information Technology / i-Soon, Emennet Pasargad) and their known aliases; any active contracts or data flows may carry legal and compliance obligations under EU and U.S. sanctions regimes.
2. Step 2, Detection: Hunt for SOHO router compromise indicators in your environment, review firewall and DHCP logs for unexpected outbound connections from edge routers, check for unauthorized VPN or remote access sessions (T1133), and query authentication logs for valid account use outside business hours or from anomalous source IPs (T1078).
3. Step 3, Assessment: Inventory all internet-exposed SOHO routers, edge devices, and remote access endpoints; identify devices running end-of-life firmware or using default/hardcoded credentials (CWE-798, CWE-306); prioritize remediation for devices in OT-adjacent or critical infrastructure network segments.
4. Step 4, Communication: Brief legal and compliance teams on sanctions designations; if your organization operates in EU member states or transacts with entities in the affected sectors, coordinate with counsel on obligations under EU restrictive measures; notify relevant sector-specific regulators if a compromise is identified.
5. Step 5, Long-term: Implement SOHO and edge device hardening aligned to CIS Benchmarks for network devices; enforce credential rotation policies that eliminate default and shared credentials; establish recurring threat intelligence reviews mapping Flax Typhoon, i-Soon, and Emennet Pasargad TTPs (per MITRE ATT&CK entries above) to your detection rule set and control gaps.

IR / Forensic Enrichment

Triage Priority	IMMEDIATE
Escalation Criteria	Escalate to incident response firm and external counsel immediately if: (1) any sanctioned entity is identified in your vendor or data flow inventory, (2) unauthorized SOHO router access or outbound command-and-control traffic is confirmed, (3) your organization operates critical infrastructure in an EU member state, or (4) regulatory notification obligation is triggered (72-hour window).
Recovery Notes	Post-containment: verify all patched/replaced SOHO routers pass hardened baseline compliance check (CIS Benchmark) before returning to production. Conduct forensic analysis of any compromised routers (preserve full device logs, configs, and firmware image for investigation). Re-run detection hunt (Step 2) against the 30-day window post-recovery to confirm no lateral movement or persistence mechanisms remain. Document timeline of remediation actions, regulatory notifications, and lessons learned in incident report per NIST 800-61 §3.4.3.

Forensic Artifacts	Firewall/UTM egress logs and NetFlow records (30-day minimum) for anomalous outbound connections from edge router IP ranges | Router device logs and syslog exports (SSH, telnet, web login attempts, configuration changes, reboot events) | DHCP lease history and current leases showing device MAC addresses, assigned IPs, and lease duration anomalies | Windows Event Log 4624/4625 and 4688 (logon, logoff, process creation) for lateral movement from compromised edge devices | Linux /var/log/auth.log, /var/log/syslog, and SSH host keys (ssh-rsa, ssh-ed25519) for unauthorized access patterns and persistence indicators

Per-Action IR Details

Step 1 — Immediate: Cross-reference your organization's vendor and third-party lists against sanctioned entities (Integrity Technology Group, Anxun Information Technology / i-Soon, Emennet Pasargad) and their known aliases; any active contracts or data flows may carry legal and compliance obligations under EU and U.S. sanctions regimes.

NIST Phase: Preparation

Reference: NIST 800-61r3 §2.1 (preparation phase — establish tools, procedures, and knowledge base)

Controls: NIST 800-53 PM-9 (supply chain risk management), NIST 800-53 SA-3 (system development life cycle), CIS 6.5 (third-party software security)

Compensating: Export your vendor list (procurement database, contracts folder) to CSV. Use grep or ctrl+F to search for exact entity names: 'Integrity Technology Group', 'i-Soon', 'Anxun Information Technology', 'Emennet Pasargad', and known aliases from public sanctions lists (EU Council Registry, OFAC SDN list). Cross-reference against your firewall egress rules, VPN provider lists, and SaaS subscriptions. Document matches in a spreadsheet with contract end date and data classification. No tool required.

Evidence: Capture before action: procurement database exports (vendor names, contract dates, data classifications), current firewall rules and VPN configurations, SaaS subscription lists, any signed MSAs or data processing agreements referencing the sanctioned entities. This establishes baseline to detect unauthorized relationships or data flows post-discovery.

Step 2 — Detection: Hunt for SOHO router compromise indicators in your environment — review firewall and DHCP logs for unexpected outbound connections from edge routers, check for unauthorized VPN or remote access sessions (T1133), and query authentication logs for valid account use outside business hours or from anomalous source IPs (T1078).

NIST Phase: Detection Analysis

Reference: NIST 800-61r3 §3.2.1 (detection and analysis — monitor and investigate)

Controls: NIST 800-53 SI-4 (information system monitoring), NIST 800-53 AU-6 (audit review, analysis, and reporting), CIS 8.2 (collect audit logs)

Compensating: Query firewall logs manually (via SSH or web console) for outbound connections from internal router IPs to non-whitelisted external destinations over ports 443, 22, 8080, 9999, or unusual high-numbered ports. Command example: 'grep -E "(SRC=192\.168\.|SRC=10\.).*DST=" firewall.log | grep -vE "(8\.8\.8\.8|1\.1\.1\.1|your-ISP-gateway)" | sort | uniq -c'. Export DHCP logs from your router web UI or syslog server and grep for MAC addresses with excessive address changes in short time windows (indicator of device reboot/infection). Cross-check SSH/RDP authentication logs (Windows Event ID 4624, Linux /var/log/auth.log) for successful logins outside normal business hours or from internal-to-internal connections originating from edge device subnets.

Evidence: Capture immediately: firewall egress logs (full packet capture or netflow) for last 30 days, DHCP lease history and current leases, router syslog output, Windows Event Log 4624/4625 (logon/logoff), SSH auth.log, VPN access logs with source IPs and timestamps, any device management logs from router admin interfaces. Preserve these before conducting hunt to establish clean baseline.

Step 3 — Assessment: Inventory all internet-exposed SOHO routers, edge devices, and remote access endpoints; identify devices running end-of-life firmware or using default/hardcoded credentials (CWE-798, CWE-306); prioritize remediation for devices in OT-adjacent or critical infrastructure network segments.

NIST Phase: Containment

Reference: NIST 800-61r3 §3.3 (containment strategy — contain scope of incident)

Controls: NIST 800-53 CA-7 (continuous monitoring), NIST 800-53 IA-4 (identifier management), NIST 800-53 SC-7 (boundary protection), CIS 5.1 (inventory of assets)

Compensating: Conduct network scan using free tools (nmap, Shodan query, or IP camera/router discovery sites). Command: 'nmap -p 22,23,80,443,8080,8443 --script ssh-hostkey,http-title 192.168.0.0/16 -oX router-inventory.xml'. For each device: SSH/telnet into the device and run 'show version' or 'cat /proc/version' to extract firmware version; check vendor EOL date against current date. Document default credentials via datasheet lookup or test (SSH admin/admin, admin/password). Create a spreadsheet ranking devices by: (1) internet exposure (ping from external), (2) firmware age (>2 years = critical), (3) location (OT-adjacent = higher priority), (4) credential status (default = critical). Devices scoring high on multiple factors get immediate firmware update or replacement.

Evidence: Preserve before remediation: snapshots of current firmware versions (SSH banner captures), credential test results (what was attempted and succeeded), network topology diagrams showing device placement relative to OT/critical infrastructure, historical firmware update logs if available, any device configuration backups. This preserves evidence of the vulnerable state pre-remediation.

Step 4 — Communication: Brief legal and compliance teams on sanctions designations; if your organization operates in EU member states or transacts with entities in the affected sectors, coordinate with counsel on obligations under EU restrictive measures; notify relevant sector-specific regulators if a compromise is identified.

NIST Phase: Preparation

Reference: NIST 800-61r3 §2.3.1 (communications and information sharing)

Controls: NIST 800-53 IR-4 (incident handling), NIST 800-53 SA-15 (development process, standards, and tools), CIS 18.1 (incident response plan)

Compensating: Create a one-page brief (template: threat name, affected systems, sanctions entities involved, your organization's exposure per Step 1 findings, regulatory requirements in your jurisdiction). Send to legal immediately with links to EU Official Journal (sanctions text), OFAC SDN list, and sector-specific guidance (e.g., CISA advisories for critical infrastructure). If your organization is in healthcare, finance, or critical infrastructure, identify your sector regulator (e.g., BaFin for Germany, FCA for UK) and prepare notification template per their incident reporting SLA (typically 72 hours post-discovery). Document all communications for audit trail.

Evidence: Preserve: outbound communication log (email headers, delivery receipts), legal memo or compliance sign-off documenting regulatory obligations analysis, regulatory notification draft with timestamp, any external IR firm or law firm engagement letters. This creates defensible record of due diligence.

Step 5 — Long-term: Implement SOHO and edge device hardening aligned to CIS Benchmarks for network devices; enforce credential rotation policies that eliminate default and shared credentials; establish recurring threat intelligence reviews mapping Flax Typhoon, i-Soon, and Emennet Pasargad TTPs (per MITRE ATT&CK entries above) to your detection rule set and control gaps.

NIST Phase: Recovery

Reference: NIST 800-61r3 §3.4 (eradication and recovery); NIST 800-53r5 §3.5 (system and information integrity controls)

Controls: NIST 800-53 SI-2 (flaw remediation), NIST 800-53 IA-5 (authentication), NIST 800-53 SC-7 (boundary protection), CIS 4.5 (hardening routers and switches), CIS 6.3 (maintain vendor/patch updates)

Compensating: Download CIS Benchmark for your router model (free PDF from cisecurity.org). For each control: export current device config (SSH 'show running-config' or web UI backup), compare against benchmark checklist, implement gaps via CLI or web interface, test connectivity post-change. For credential rotation without enterprise tools: use router SSH to change admin password via CLI command 'username admin privilege 15 password ', store in

encrypted password manager (Bitwarden, free tier), audit successful logins monthly. For threat intelligence: subscribe to free CISA alerts (cisa.gov email list), MITRE ATT&CK threat intel summaries, and your vendor's security bulletins. Quarterly: extract TTPs for Flax Typhoon (T1021.004, T1021.005, T1133, T1078 per public ATT&CK entries) and map to your current detection rules (grep rule files for these technique IDs); flag gaps and draft new rules or monitoring procedures.

Evidence: Preserve for post-recovery audit: pre- and post-hardening device configs, credential rotation logs with timestamps and admin usernames, CIS Benchmark compliance checklist with sign-off, threat intelligence subscription confirmations, detection rule change log showing new/updated rules for Flax Typhoon/i-Soon/Emennet TTPs.

Detection Guidance

Focus detection on three behavioral clusters aligned to the confirmed TTPs. For Flax Typhoon botnet activity: monitor for unusual outbound traffic volumes from SOHO routers to non-business VPS ranges; alert on new SSH or RDP sessions originating from SOHO network segments (T1133); detect scripting interpreter execution on network appliances (T1059); look for service termination events (T1489) on edge infrastructure. For i-Soon contractor TTPs: monitor web-facing application logs for exploitation attempts against public-facing services (T1190); alert on large outbound transfers to cloud storage or web services (T1567); review DNS and proxy logs for C2 over HTTP/S to low-reputation domains (T1071.001). For Emennet Pasargad influence operations: monitor inbound phishing indicators at the email gateway (T1598); if your organization manages SMS delivery infrastructure, review for unauthorized API access or bulk message injection (T1650). Cross-reference outbound traffic against CISA and OFAC published IOC lists for Flax Typhoon and i-Soon. Confidence on behavioral detections is medium without environment-specific tuning; IOC-based detections against published government advisories are high confidence.

Indicators of Compromise

Type	Value	Context	Confidence
DOMAIN	`See CISA Advisory AA24-249A`	Flax Typhoon botnet C2 infrastructure — CISA published network IOCs in the August 2024 joint FBI/NSA/CISA advisory. Retrieve current IOC list directly from CISA at cisa.gov.	HIGH
IP	`See CISA Advisory AA25-071A`	i-Soon (Anxun) infrastructure IOCs — CISA published indicators in advisory AA25-071A. Retrieve current IOC list directly from CISA at cisa.gov.	HIGH
URL	`See OFAC SDN List — Integrity Technology Group, Anxun Information Technology, Emennet Pasargad entries`	Sanctioned entity identifiers and associated infrastructure references are maintained in the OFAC Specially Designated Nationals list at home.treasury.gov/policy-issues/financial-sanctions/sdn-list.	HIGH

Framework Mappings

MITRE-ATTACK

- **T1496** — Resource Hijacking
- **T1133** — External Remote Services
- **T1567** — Exfiltration Over Web Service
- **T1584.005** — Botnet
- **T1583.003** — Virtual Private Server
- **T1102** — Web Service
- **T1583.005** — Botnet
- **T1059** — Command and Scripting Interpreter
- **T1489** — Service Stop
- **T1078** — Valid Accounts
- **T1598** — Phishing for Information
- **T1190** — Exploit Public-Facing Application
- **T1650** — Acquire Access
- **T1486** — Data Encrypted for Impact
- **T1071.001** — Web Protocols

NIST-800-53R5

- **AC-17** — Remote Access
- **AC-20** — Use of External Systems
- **IA-2** — Identification and Authentication (Organizational Users)
- **IA-5** — Authenticator Management
- **SC-7** — Boundary Protection
- **CM-7** — Least Functionality
- **SI-3** — Malicious Code Protection
- **SI-4** — System Monitoring
- **SI-7** — Software, Firmware, and Information Integrity
- **CM-6** — Configuration Settings
- **AC-2** — Account Management
- **AC-6** — Least Privilege
- **CA-8** — Penetration Testing
- **RA-5** — Vulnerability Monitoring and Scanning
- **SI-2** — Flaw Remediation
- **CP-9** — System Backup
- **CP-10** — System Recovery and Reconstitution
- **IA-8** — Identification and Authentication (Non-Organizational Users)

OWASP-TOP10-2021

- **A07:2021** — Identification and Authentication Failures

CIS-V8

- **6.3**
- **16.10**
- **6.4**
- **6.5**

ISO-27001-2022

- **A.8.28** — Secure coding

SOC2-TSC

- **CC6.1** — The entity implements logical access security software, infrastructure, and architectures over protected information assets

HIPAA-SECURITY

- **164.312(d)** — Person or Entity Authentication

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1496	Resource Hijacking	Impact
T1133	External Remote Services	Persistence
T1567	Exfiltration Over Web Service	Exfiltration
T1584.005	Botnet	Resource-Development
T1583.003	Virtual Private Server	Resource-Development
T1102	Web Service	Command-And-Control
T1583.005	Botnet	Resource-Development
T1059	Command and Scripting Interpreter	Execution
T1489	Service Stop	Impact
T1078	Valid Accounts	Defense-Evasion
T1598	Phishing for Information	Reconnaissance
T1190	Exploit Public-Facing Application	Initial-Access
T1650	Acquire Access	Resource-Development
T1486	Data Encrypted for Impact	Impact
T1071.001	Web Protocols	Command-And-Control

Sources

Source	URL	Tier
Security News	https://www.bleepingcomputer.com/news/security/europe-sanctions-chi...	T3
Risky Bulletin: EU finally imposes more cyber sanctions	https://risky.biz/risky-bulletin-eu-finally-imposes-more-cyber-sanc...	T3
Commission responds to cyber-attack on its central mobile ...	https://ec.europa.eu/commission/presscorner/detail/en/ip_26_342	T1
US, Germany, Canada Disrupt Botnets That Infected Millions of ...	https://www.usnews.com/news/top-news/articles/2026-03-19/us-says-it...	T3
European Commission Hit by Mobile Management Data Breach	https://www.esecurityplanet.com/threats/european-commission-hit-by-...	T3

Generated 2026-03-29 18:39 UTC by TJS Security Command Center