INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-03-29 18:42 UTC

EU Formalizes Sanctions Against Chinese and Iranian Cyber Contractors, What It Means for Enterprise Risk Teams

GOVERNANCE | MEDIUM | CVSS 5.0

SCC Item ID	SCC-GOV-2026-0002
Type	Governance
Severity	MEDIUM
CVSS Base Score	5.0
Affected Products	Critical infrastructure (EU member states), SMS services (Sweden), advertising billboard systems, Charlie Hebdo subscriber platform; no specific vendor products named
Published	2026-03-21

Executive Summary

The European Union has formally sanctioned three companies and two individuals tied to Chinese and Iranian state-sponsored cyber operations, per official EU designation. Designated entities include Integrity Technology Group (attributed by U.S. authorities to Flax Typhoon / Raptor Train botnet operations), i-Soon (Chinese hack-for-hire contractor), and Emennet Pasargad (linked by prior intelligence reporting to election interference and hack-and-leak campaigns). The sanctions impose asset freezes and travel bans, converting prior U.S. DOJ and CISA attributions into binding EU legal designations. Organizations operating in the EU or with EU-connected supply chains must now conduct sanctions screening against these entities and their known affiliates to avoid compliance exposure.

Technical Analysis

This action is a diplomatic and legal designation, not a technical vulnerability disclosure. No new CVEs or patches are associated with this item. The sanctioned entities are linked to previously documented TTPs: Integrity Technology Group / Flax Typhoon operated the Raptor Train botnet using compromised SOHO routers and IoT devices (documented in CISA and FBI advisories, 2024); i-Soon conducted hack-for-hire intrusions targeting governments and NGOs, relying heavily on valid account abuse (T1078) and phishing (T1566); Emennet Pasargad conducted influence operations and hack-and-leak campaigns. Weakness classes associated with historically attributed operations (documented in CISA and FBI advisories, including the Raptor Train advisory): CWE-284 (Improper Access Control), CWE-287 (Improper Authentication), CWE-306 (Missing Authentication for Critical Functions). Relevant MITRE techniques include T1078 (Valid Accounts), T1566

(Phishing), T1583.005 / T1584.005 (Botnet infrastructure acquisition and compromise), T1190 (Exploit Public-Facing Application), T1491.002 (External Defacement), T1498 (Network Denial of Service), T1567 (Exfiltration Over Web Service), T1071 (Application Layer Protocol), T1591 / T1589.002 (Reconnaissance), and T1588.001 (Malware acquisition). Confidence in attribution: high, corroborated by U.S. and EU government sources. Confidence in new technical disclosure: low, this is a legal action, not a new TTP release.

Action Checklist

1. Step 1, Sanctions Screening (Immediate): Run all third-party vendor, supplier, and technology provider lists against the newly designated entities, Integrity Technology Group, i-Soon (also known as Anxun Information Technology), and Emennet Pasargad, and their known subsidiaries or affiliates. Engage your legal or compliance team to confirm screening scope under applicable EU sanctions regulations.
2. Step 2, Supply Chain Review: Identify any direct or indirect contractual relationships, software licensing agreements, or managed service arrangements that could involve designated entities. Flag for legal review any relationship that cannot be immediately cleared.
3. Step 3, Detection Posture Check: Cross-reference existing threat intelligence feeds and SIEM rules against Flax Typhoon / Raptor Train IOCs published in prior CISA and FBI advisories. Verify detection coverage for T1078 (Valid Accounts) and T1566 (Phishing) given their documented prevalence in i-Soon and Flax Typhoon operations.
4. Step 4, Stakeholder Notification: Brief legal, procurement, and executive leadership on the sanctions designations and compliance obligations. If your organization operates under EU jurisdiction or has EU-based clients, confirm reporting or due diligence obligations with in-house or external counsel.
5. Step 5, Policy and Control Updates (Long-Term): Update third-party risk management and vendor onboarding policies to include sanctions list screening as a standing control. Review authentication and access control posture against CWE-284, CWE-287, and CWE-306, the weakness classes tied to historically attributed TTPs of these actors, using NIST SP 800-53 AC and IA control families as a benchmark.

IR / Forensic Enrichment

Triage Priority	URGENT
Escalation Criteria	Escalate to legal and CISO immediately if any designated entity relationship is confirmed; escalate to external IR firm if potential data exfiltration by these actors is detected or if compliance timeline is missed.
Recovery Notes	Post-containment: (1) Revoke access and credentials for any accounts linked to the compromised vendor or sanctions entity. (2) Force password resets for all users who accessed systems via credentials from that vendor. (3) Rotate all API keys, SSH keys, and service account credentials used by the compromised third party. (4) Conduct 90-day forensic review of logs for any lateral movement or data staging by detected threat actors; retain chain-of-custody evidence for potential law enforcement reporting.

Forensic Artifacts	Windows Event Log 4624 (Successful Logon), 4625 (Failed Logon), 4768 (Kerberos TGT Request) — required for detecting T1078 Valid Accounts exploitation | Sysmon Event ID 1 (Process Creation), 3 (Network Connection), 11 (File Created) — required to detect T1566 phishing payloads and suspicious process execution post-click | DNS query logs and firewall logs (last 90 days) — required to correlate against CISA-published Flax Typhoon IOCs (domains, IPs) | Mail server logs (SMTP, Exchange) with full message metadata and attachment hashes — required for T1566 phishing detection and forensic attribution | Third-party vendor access logs, VPN logs, and API usage logs — required to establish timeline of vendor involvement and lateral movement post-compromise

Per-Action IR Details

Step 1 — Sanctions Screening (Immediate): Run all third-party vendor, supplier, and technology provider lists against the newly designated entities — Integrity Technology Group, Anxun Information Technology (i-Soon), and Emennet Pasargad — and their known subsidiaries or affiliates. Engage your legal or compliance team to confirm screening scope under applicable EU sanctions regulations.

NIST Phase: Preparation

Reference: NIST 800-61r3 §2.1 (Preparation — establish processes and tools)

Controls: NIST 800-53 SA-3 (System Development Life Cycle), NIST 800-53 SA-12 (Supply Chain Protection), CIS 6.2 (Establish and Implement a Third-Party Risk Assessment Process)

Compensating: Export vendor roster to CSV. Cross-reference against EU Official Journal sanctions list (https://eur-lex.europa.eu) and OFAC SDN list using grep or Excel VLOOKUP. Maintain audit log (timestamp, screener name, cleared vendors) in shared spreadsheet with change tracking enabled. Monthly re-screening using free sanctioned entity databases.

Evidence: Capture baseline vendor roster with last-update timestamp before screening begins. Document screening methodology (tool, datasource, date run). Retain cleared vendor list and any flagged matches with denial reason — this becomes your compliance audit trail if sanctions violations are later alleged.

Step 2 — Supply Chain Review: Identify any direct or indirect contractual relationships, software licensing agreements, or managed service arrangements that could involve designated entities. Flag for legal review any relationship that cannot be immediately cleared.

NIST Phase: Preparation

Reference: NIST 800-61r3 §2.2 (Identify tools and resources needed for incident response)

Controls: NIST 800-53 SA-9 (External Information System Services), NIST 800-53 IR-4(a) (Incident Handling Implementation), CIS 6.2 (Third-Party Risk Assessment)

Compensating: Request procurement and IT to export all active contracts (SaaS, MSP, cloud services, software licenses) with vendor name, contract date, and service description. Cross-reference against designated entity list and known shell companies (i-Soon subsidiaries are documented in public U.S. DOJ indictments). Create a gap matrix: contracts requiring legal review vs. cleared contracts. Store in shared access-controlled document with sign-off log.

Evidence: Archive all contract documentation, vendor onboarding records, and licensing agreements with dates. Capture screenshots of contract management system showing vendor relationships and payment flows — this becomes your supply chain baseline for forensic reconstruction if a breach is later tied to a compromised vendor.

Step 3 — Detection Posture Check: Cross-reference existing threat intelligence feeds and SIEM rules against Flax Typhoon / Raptor Train IOCs published in prior CISA and FBI advisories (September 2024 Raptor Train advisory). Verify detection coverage for T1078 (Valid Accounts) and T1566 (Phishing) given their documented prevalence in i-Soon and Flax Typhoon operations.

NIST Phase: Detection Analysis

Reference: NIST 800-61r3 §3.2 (Detection and Analysis) and §3.2.4 (Analysis)

Controls: NIST 800-53 SI-4 (Information System Monitoring), NIST 800-53 CA-7 (Continuous Monitoring), CIS 8.1 (Establish and Maintain Detailed Asset Inventory), CIS 8.6 (Address Unauthorized Software)

Compensating: Download CISA AA23-352A (Flax Typhoon) and FBI/CISA Raptor Train advisory from cisa.gov. Extract IOCs (IPs, domains, file hashes). Use free tools: grep for IP/domain matches in firewall logs and DNS queries (if available); grep for file hashes in Sysmon logs (Event ID 1, 3, 11). For T1078 detection without SIEM: run 'wevtlog query' for Event IDs 4624 (successful login), 4625 (failed login), 4768 (Kerberos TGT request) on domain controllers. For T1566 detection: parse mail server logs (postfix, Exchange) for external mail sources + credential-like patterns in subject lines.

Evidence: Preserve firewall logs (last 90 days minimum), DNS logs, mail server logs (full message metadata), and Windows Event Logs 4624, 4625, 4768, 4769 from all domain controllers and critical systems. Create IOC baseline (hashes, IPs, domains) and timestamp when detection rules were deployed — this proves detection coverage gap or existenceat time of rule deployment, critical for post-breach forensics.

Step 4 — Stakeholder Notification: Brief legal, procurement, and executive leadership on the sanctions designations and compliance obligations. If your organization operates under EU jurisdiction or has EU-based clients, confirm reporting or due diligence obligations with in-house or external counsel.

NIST Phase: Preparation

Reference: NIST 800-61r3 §2.3 (Establish mitigation and response controls and procedures)

Controls: NIST 800-53 IR-1 (Incident Response Policy), NIST 800-53 IR-2 (Incident Response Training), CIS 19.1 (Establish and Maintain an Incident Response Process)

Compensating: Create a one-page stakeholder briefing document: threat name, designated entities, compliance deadline (typically 10-14 days from EU Official Journal publication), required actions, and legal risk if non-compliant. Schedule synchronous briefing with legal, procurement, and CISO. Document attendance, action owners, and completion dates in a tracked action register. Escalate any uncleared vendor relationships to legal within 48 hours with due date for remediation.

Evidence: Retain meeting minutes, attendee list, and distribution of the briefing document with email timestamps. This documentation proves timely notification if compliance is later audited by EU regulators. Store in secure, timestamped location (email archive, document repository with retention lock).

Step 5 — Policy and Control Updates (Long-Term): Update third-party risk management and vendor onboarding policies to include sanctions list screening as a standing control. Review authentication and access control posture against CWE-284, CWE-287, and CWE-306 — the weakness classes tied to historically attributed TTPs of these actors — using NIST SP 800-53 AC and IA control families as a benchmark.

NIST Phase: Recovery

Reference: NIST 800-61r3 §4 (Post-Incident Activities) and §4.2 (Lessons Learned)

Controls: NIST 800-53 AC-2 (Account Management), NIST 800-53 IA-2 (Authentication), NIST 800-53 IA-5 (Authentication and Identification), NIST 800-53 SA-9 (External Information System Services), CIS 5.2 (Use Multifactor Authentication), CIS 5.4 (Restrict Administrator Privileges)

Compensating: Audit current authentication posture manually: (1) Enumerate all active accounts with admin or service account privileges using 'net group', 'Get-LocalGroupMember' (Windows) or 'getent group' (Linux). (2) Check password policies: 'net accounts /domain' (Windows) should enforce 12+ character length, 90-day max age. (3) Verify MFA adoption by querying Active Directory for users with MFA enabled vs. total user count. (4) Disable legacy auth protocols: disable NTLM logins (Event ID 4625 + disable NTLM registry key), require Kerberos. (5) Remove accounts with T1078 risk: identify unused service accounts and remove them; implement credential rotation (quarterly) for remaining service accounts. Document findings in a matrix: control name, current state, target state, owner, due date.

Evidence: Create a baseline access control audit report before policy changes: account inventory (count by privilege level), authentication method distribution (password-only vs. MFA), and legacy protocol usage. Archive this baseline and the updated policies side-by-side — this becomes your remediation proof for post-incident review and regulator audits.

Detection Guidance

No new IOCs are released with this sanctions designation. Detection guidance is based on previously published advisories for the attributed threat actors. For Flax Typhoon / Raptor Train: review CISA and FBI advisories for IP ranges and domains associated with Raptor Train C2 infrastructure; query firewall and proxy logs for outbound connections to those indicators. For i-Soon TTPs: monitor for unusual valid account activity (T1078), failed authentications followed by successful logins from new geolocations or unusual hours; review VPN and remote access logs for anomalous patterns. For Emennet Pasargad: if your organization handles public-facing web content or has exposure to Iranian influence operation targets, monitor for unauthorized content modification (T1491.002) and unusual exfiltration activity over web services (T1567). General: ensure SIEM alerting covers MITRE techniques T1078, T1566, T1190, and T1583.005 / T1584.005. Botnet-associated traffic often presents as distributed, low-volume connections from SOHO device IP ranges; review NetFlow or proxy logs for this pattern. For current indicators, consult the CISA Raptor Train advisory and FBI i-Soon reporting.

Indicators of Compromise

Type	Value	Context	Confidence
URL	`https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-249a`	CISA/FBI advisory on Flax Typhoon and Raptor Train botnet infrastructure — primary source for previously published IOCs associated with Integrity Technology Group operations. Verify URL resolves before use.	HIGH

Framework Mappings

MITRE-ATTACK

- **T1078** — Valid Accounts
- **T1566** — Phishing
- **T1583.005** — Botnet
- **T1491.002** — External Defacement
- **T1591** — Gather Victim Org Information
- **T1190** — Exploit Public-Facing Application
- **T1498** — Network Denial of Service
- **T1567** — Exfiltration Over Web Service
- **T1584.005** — Botnet
- **T1589.002** — Email Addresses
- **T1588.001** — Malware
- **T1071** — Application Layer Protocol

NIST-800-53R5

- **AC-2** — Account Management

- **AC-6** — Least Privilege
- **IA-2** — Identification and Authentication (Organizational Users)
- **IA-5** — Authenticator Management
- **AT-2** — Literacy Training and Awareness
- **CA-7** — Continuous Monitoring
- **SC-7** — Boundary Protection
- **SI-3** — Malicious Code Protection
- **SI-4** — System Monitoring
- **SI-8** — Spam Protection
- **CA-8** — Penetration Testing
- **RA-5** — Vulnerability Monitoring and Scanning
- **SI-2** — Flaw Remediation
- **SI-7** — Software, Firmware, and Information Integrity
- **IA-8** — Identification and Authentication (Non-Organizational Users)
- **AC-3** — Access Enforcement
- **SR-2** — Supply Chain Risk Management Plan

OWASP-TOP10-2021

- **A07:2021** — Identification and Authentication Failures
- **A01:2021** — Broken Access Control

CIS-V8

- **6.3**
- **6.4**
- **6.5**
- **6.1**
- **6.2**
- **15.1** — Establish and Maintain an Inventory of Service Providers

SOC2-TSC

- **CC6.1** — The entity implements logical access security software, infrastructure, and architectures over protected information assets
- **CC9.2** — Manages risks associated with vendors and business partners

HIPAA-SECURITY

- **164.312(d)** — Person or Entity Authentication
- **164.312(a)(1)** — Access Control
- **164.308(a)(6)(ii)** — Response and Reporting

NIST-CSF-2

- **RS.CO-03** — Recovery activities and progress communicated
- **GV.SC-01** — Cybersecurity supply chain risk management program

ISO-27001-2022

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

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1078	Valid Accounts	Defense-Evasion
T1566	Phishing	Initial-Access
T1583.005	Botnet	Resource-Development
T1491.002	External Defacement	Impact
T1591	Gather Victim Org Information	Reconnaissance
T1190	Exploit Public-Facing Application	Initial-Access
T1498	Network Denial of Service	Impact
T1567	Exfiltration Over Web Service	Exfiltration
T1584.005	Botnet	Resource-Development
T1589.002	Email Addresses	Reconnaissance
T1588.001	Malware	Resource-Development
T1071	Application Layer Protocol	Command-And-Control

Sources

Source	URL	Tier
Security News	https://www.bleepingcomputer.com/news/security/europe-sanctions-chi...	T3
EU Sanctions on Chinese and Iranian Firms: Raptor Train Botnet ...	https://www.rescana.com/post/eu-sanctions-on-chinese-and-iranian-fi...	T3
Risky Bulletin: EU finally imposes more cyber sanctions	https://risky.biz/risky-bulletin-eu-finally-imposes-more-cyber-sanc...	T3
Hacktivist group responsible for cyberattacks on critical infrastructure ...	https://www.eurojust.europa.eu/news/hacktivist-group-responsible-cy...	T1

Source	URL	Tier
European Commission's mobile management software hacked	https://www.thestack.technology/european-commissions-mobile-managem...	T3

Generated 2026-03-29 18:42 UTC by TJS Security Command Center