SOCRadar®
Your Eyes Beyond

NATO

Threat Landscape Report 2026

Glossary

CCDCOE (Cooperative Cyber Defense Centre of Excellence): A NATO-accredited research and training facility in Tallinn, Estonia, established in 2008. Hosts the annual CyCon conference and produced the Tallinn Manual.

DTIS (Digital Transformation Implementation Strategy): NATO's roadmap for leveraging digital technologies across all areas of operations by 2030. Version 2.0 was published in May 2026.

HMI (Human-Machine Interface): The dashboard or control panel through which operators interact with industrial control systems. Screenshots of HMIs are often circulated by threat actors to claim access to OT environments.

ICS (Industrial Control Systems): Systems used to monitor and control industrial processes in sectors such as energy, water, and manufacturing. A subset of OT.

IRGC (Islamic Revolutionary Guard Corps): Iran's multi-service primary force of the Iranian Armed Forces and intelligence organization. Linked in this report to APT33 operations.

ISAC (Information Sharing and Analysis Center): Sector-specific organizations that facilitate the exchange of cyber threat intelligence between member organizations.

MOIS (Ministry of Intelligence and Security): Iran's primary civilian intelligence agency. Linked in this report to MuddyWater operations.

NCIA (NATO Communications and Information Agency): NATO's technology and cyber capability hub, responsible for delivering, operating, and defending the Alliance's digital infrastructure.

OFAC (Office of Foreign Assets Control): A US Treasury Department office that administers and enforces economic sanctions programs, including those targeting North Korean cyber operations.

OT (Operational Technology): Hardware and software that monitors and controls physical processes in industrial environments such as power grids, water treatment plants, and manufacturing facilities.

PBN (Protected Business Network): A NATO-wide classified cloud platform contracted to Accenture and Leonardo in July 2026 for approximately €200 million over seven years, serving roughly 29,000 users across the Alliance.

SHAPE (Supreme Headquarters Allied Powers Europe): NATO's main military command headquarters, located in Mons, Belgium.

VCISC (Virtual Cyber Incident Support Capability): A NATO mechanism launched at the 2023 Vilnius Summit enabling rapid cyber assistance to member states without invoking Article 5.

Executive Summary

Top Takeaways

NATO's security perimeter has moved. The Alliance has spent two decades hardening its core networks and institutions. The exposure now sits at the contractor and supplier layer. Every dollar of new procurement is also a new entry point

Ankara tried to break the historical pattern. For three decades, NATO's cyber posture advanced in response to attacks rather than ahead of them. The 2026 Ankara Summit was the first where the Alliance invested in digital infrastructure and capability significantly before the next major incident.

Data theft drives the Dark Web economy. Data Breach and Compromise (37.93%) and Unauthorized Access and Credentials (17.87%) together account for over 55% of all threat types. The broader category of Data and Access Incidents reaches 66.63%. NATO's threat landscape is defined by a sustained effort to steal, sell, and exploit sensitive data.

Threat profiles shift significantly by attack type. The UK and US dominate overall Dark Web threats at a combined 54%, but the picture changes across specific categories. The US takes the lead in ransomware, Germany nearly triples its share from 4.11% to 11.76%, and Turkiye, barely present elsewhere, tops phishing at 37.22%. Countries that appear low-risk in one dataset can carry concentrated risk in another.

Public Administration is the most exposed sector overall, but phishing follows a different pattern. Government institutions lead Dark Web targeting at 16.11%, yet phishing campaigns prioritize Information Services (16.22%) and National Security (12.16%). When Banking and Finance are combined, the financial sector reaches 18.56% of phishing activity. Different attack methods serve different objectives.

The ransomware ecosystem is fragmented beyond easy tracking. Over 70% of ransomware activity falls outside the top three named groups. No single actor controls the landscape, and the barrier to entry remains low. This limits the value of actor-focused intelligence and puts more weight on technical and behavioral detection.

HTTPS is no longer a reliable trust signal. 62.3% of phishing pages operate over HTTPS, yet many still use default templates like "My Framer Site" as their page title. Phishing campaigns span a wide range from minimal-effort mass deployment to polished impersonation. Security awareness programs that rely on the padlock icon as a safety indicator need updating.

CISO Statement

Earlier in my career, I served as a cybersecurity researcher at the NATO Cooperative Cyber Defense Centre of Excellence in Tallinn, Estonia. The Centre exists because of the 2007 DDoS campaign against Estonian banks, media, and government systems, the incident this report's own history traces as the moment NATO first had to reckon with cyberspace as a domain of conflict. Years later, I still serve as a cyber advisor to NATO, and I find myself reading this year's data through that same lens: has the institutional response finally caught up to the threat, or is the Alliance still building the plane while it's in the air?

Ankara gives a mixed answer. Secretary General Rutte framed the summit around "delivery" and spending and procurement, which included $139 billion in new defense investment, $50 billion in new contracts, a transatlantic warfighting cloud, and AI adoption written into deterrence language for the first time. But the Accenture breach disclosed one day before the €200 million PBN contract was signed is not an isolated footnote. It is the pattern this report documents across every chapter: the Alliance secures its own core, while the contractors, cloud providers, and mid-tier vendors who build its future infrastructure remain on the softer perimeter. Every dollar of new procurement is also a new entry point.

The data reinforces this. Data theft and unauthorized access still account for two-thirds of all Dark Web activity targeting NATO countries. Ransomware groups have fragmented to the point where actor-tracking alone is no longer a viable defense; Germany's manufacturing sector alone shows that targeting now follows operational leverage, not headlines. And 62% of phishing pages now run over HTTPS, which means we have to retire the padlock icon as a signal of trust in our own awareness training.

None of this is cause for alarm, but rather for action. It is a clear list of where the next three years of investment need to go: supply chain accountability for tier-two and tier-three contractors, Zero Trust enforced at the boundaries where classified and commercial infrastructure now meet, and AI treated as a defense capability requiring its own assurance standard, not an IT rollout. The Strategic Recommendations in this report are not aspirational; they are the minimum bar for keeping pace with what the data already shows is happening.

Ensar Seker (PhD)

Chief Security Officer

NATO’s Threat Landscape

The report is structured in two main parts. The first covers NATO as an institution: how cyberattacks have shaped Alliance cyber policy over three decades, what the Ankara Summit decided, what those decisions mean for the threat landscape, and what adversaries, from Russian military intelligence units to Chinese espionage clusters to Iranian proxy networks, are doing right now.

The second covers NATO's 32 member states as a collective attack surface, drawing on SOCRadar's threat intelligence data to map Dark Web activity, ransomware campaigns, and phishing operations across countries, sectors, and threat types.

The central finding that runs through both parts is structural. NATO has spent two decades hardening its core. The networks, command structures, and institutional systems at the center of the Alliance are better defended than at any point in its history. But the perimeter has moved. The $50 billion procurement wave announced at Ankara, the €200 million cloud contract with Accenture and Leonardo, and the broader push to operationalize AI and cloud infrastructure across allied forces are pulling thousands of commercial vendors into classified and sensitive programs. These organizations, defense contractors, cloud providers, logistics operators, legal firms, and their subcontractors, now handle data and run systems whose compromise could directly affect Alliance operations. They sit outside NATO's direct security perimeter, and the threat data in this report shows that adversaries have already oriented toward them.

The data also shows that no single threat category tells the full story. Countries that appear low-risk in one dataset carry concentrated risk in another. Attack methods serve different objectives and follow different targeting patterns. The ransomware ecosystem has fragmented to the point where actor-focused tracking alone cannot cover the landscape. Reading any one chapter in isolation will produce an incomplete picture. The report is designed to be read as a whole, with each chapter adding a layer to the same underlying assessment.

The reporting period closes in July 2026, but the timeline that matters runs to 2029, the year allied intelligence assesses Russia could have the capability to attack a NATO member. Everything in this report, the summit commitments, the adversary campaigns, the data, and the recommendations, should be read against that clock.

NATO Adversaries

Threat Actors At-a-Glance (2026-Active)

Actor	Alignment	Key TTPs	ATT&CK Technique IDs	Sectors Targeted
Sandworm / APT44 (G0034)	Russia - GRU Unit 74455	Destructive wiper operations against critical infrastructure (DynoWiper)	T1485, T1561, T1490, T1190, T1078	Energy/grid, government, critical infrastructure
Fancy Bear / APT28 (G0007)	Russia - GRU Unit 26165	Webmail XSS (Roundcube CVE-2023-43770), TOTP/2FA theft, Sieve mail-forwarding, DLL side-loading, steganography	T1190, T1114.003, T1111, T1078, T1574.002, T1027.003	Military/defense (NATO structures), air forces, foreign ministries
Gamaredon (G0047)	Russia - FSB	Spearphishing; downloader handoff to Turla	T1566, T1105	Government, military (Ukraine-focused)
Turla / Secret Blizzard (G0010)	Russia - FSB	Infrastructure hijacking, STOCKSTAY/Kazuar backdoors, DLL side-loading, VPN-appliance exploitation, AiTM	T1584, T1574.002, T1190, T1557	Government, diplomatic, military, defense, NGOs
NoName057(16)	Pro-Russian hacktivist	Crowdsourced DDoS via DDoSia botnet, Telegram tasking	T1498, T1499	Government, media, financial, transport, municipal (NATO)
Mustang Panda / TA416 (G0129)	China - PRC state-aligned	Spearphishing + LNK, DLL side-loading (CNMNSST.exe) to PlugX, Cloudflare Turnstile & OAuth abuse, MSBuild/CSPROJ	T1566.002, T1204.002, T1574.002, T1059.001, T1102, T1027	Diplomatic missions to NATO/EU, foreign & defense ministries

Actor	Alignment	Key TTPs	ATT&CK Technique IDs	Sectors Targeted
SHADOW-EARTH-053 (temp. cluster; overlaps Earth Alux)	China-aligned	ProxyLogon N-day (CVE-2021-26855), Godzilla web shells, ShadowPad via DLL side-loading, AnyDesk abuse, Mimikatz	T1190, T1505.003, T1574.002, T1003.001, T1219, T1047	Government, defense, telecom, transport (Asia + Poland)
UNC5221 / UNC3886	China - PRC-nexus	Zero-day exploitation of edge/security appliances (Ivanti, Juniper CVE-2025-21590), BRICKSTORM, edge persistence	T1190, T1587, T1542	Edge infrastructure, defense, telecom, government
APT41 (G0096)	China - dual espionage/financial	Supply-chain compromise, living-off-the-land, edge/zero-day exploitation	T1195, T1190	Technology, telecom, government, healthcare
Patchwork / Dropping Elephant (G0040)	India (targets NATO member)	Spearphishing with UAV-conference LNK lures, five-stage chain, DLL side-loading via VLC/Task Scheduler	T1566, T1204.002, T1574.002, T1053.005	Turkish defense contractors (missiles, UAV)
MuddyWater / Seedworm (G0069)	Iran - MOIS	Pre-positioned backdoors (Dindoor, Fakeset), spearphishing, Rclone cloud exfil, signed-cert abuse	T1566, T1078, T1567.002, T1071.001, T1053.005	Banking, aviation, defense/aerospace software, NGOs
Handala / Void Manticore (G1055)	Iran - MOIS	Cloud-admin takeover; enterprise wipe via Microsoft Intune ("living off the cloud"), hack-and-leak, custom wipers	T1078.004, T1651, T1485, T1561, T1567	Medical technology, energy, government (Israel, US, Gulf)

Actor	Alignment	Key TTPs	ATT&CK Technique IDs	Sectors Targeted
APT33 / APT34 / APT35 (G0064 / G0049 / G0059)	Iran - IRGC / MOIS	Credential harvesting, cloud-infrastructure exploitation, espionage against European targets	T1566, T1078, T1110	Government, defense, energy, telecom
Lazarus (G0032) incl. Bluenoroff, Andariel, TraderTraitor	North Korea - RGB	Fake-recruiter social engineering, software supply-chain compromise, crypto theft	T1566, T1195, T1656	Cryptocurrency/DeFi, defense-industrial, financial
Kimsuky (G0094)	North Korea - RGB	Spearphishing with LNK/CHM, PowerShell staging, intelligence collection	T1566.001, T1204.002, T1059.001	Government, diplomatic, think tanks, defense
Famous Chollima / Contagious Interview	North Korea - RGB	Fake IT-worker infiltration, malicious npm/PyPI/Packagist packages, insider access abuse	T1195.002, T1566, T1656, T1078	Technology, crypto, AI firms, defense (via employment)

Russia

Russia fields the most operationally diverse cyber threat to NATO, combining military intelligence units, proxy groups, and hacktivist networks into an ecosystem where components share infrastructure, tooling, and tasking.

Sandworm (APT44/GRU Unit 74455) maintains the longest track record of destructive operations against critical infrastructure, most recently deploying DynoWiper against Poland's energy grid in December 2025.

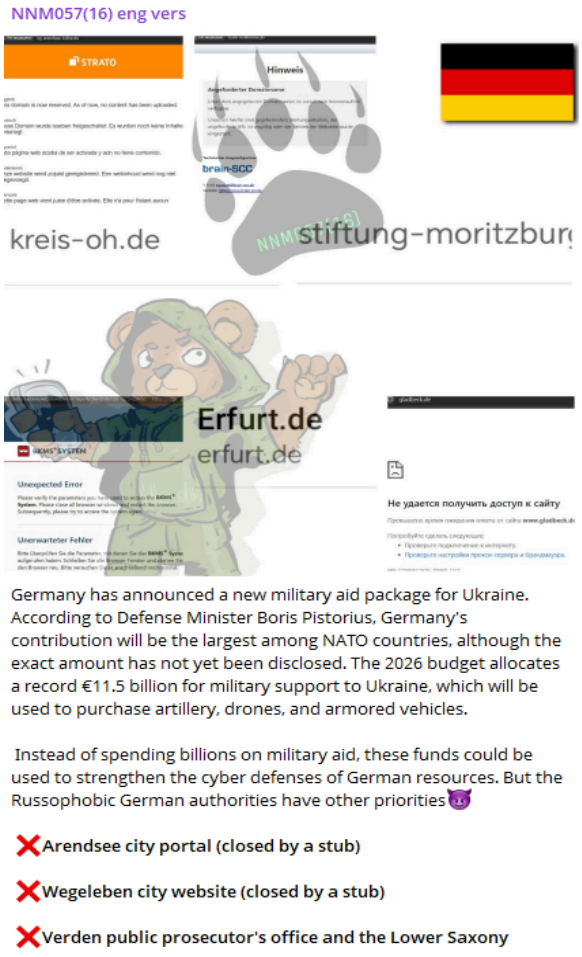
Fancy Bear (APT28/GRU Unit 26165) continues targeting NATO military structures directly. A recently exposed campaign compromised 28 email accounts at Greece's General Staff of National Defense, established automatic message forwarding to attacker-controlled servers, and obtained TOTP-based 2FA secrets enabling persistent access beyond password resets. The same operation breached at least 67 Romanian air force email accounts, including NATO-linked addresses, and compromised regional officials in Bulgaria.

Separately, Fancy Bear has deployed weaponized Office documents using COM-hijacking DLLs, LSB steganography in PNG files, and reflective loading to run an obfuscated C# trojan communicating through Filen.io, with lures tailored to defense ministry targets. Gamaredon (FSB-linked) has provided its malware downloader to Turla for backdoor deployment, demonstrating cross-unit capability sharing across organizational lines.

Russian APT groups are also running sustained exploitation of CVE-2025-8088 in 2026, a patched WinRAR vulnerability, against government networks and defense contractors across Eastern Europe, building campaign infrastructure around reliable exploitation of software that organizations struggle to update consistently.

The 'Hacktivist' group NoName057(16) has run DDoS campaigns against government, media, and private-sector targets across NATO member states since 2022. Google assessed that pro-Russian hacktivism blends state-backed actors with third-party groups to provide volume and deniability.

The most recent illustration of NoName057(16)'s NATO-country targeting is its German municipal targeting. Responding to Berlin's record €11.5 billion in Ukraine military aid, which it framed as "Russophobic" priorities, the group posted Check-Host verified downtime against soft targets such as the Arendsee city portal, the Wegeleben city website, and the Verden public prosecutor's office in Lower Saxony. Rather than hardened federal infrastructure, it hits under-resourced local sites where a brief outage is cheap to produce and easy to screenshot, then packages the result as proof of impact. The narrative payload, not the damage, is the objective.



That reach rests on the DDoSia project, a voluntary botnet: participants install the tool on Windows, Linux, or Android, pull targets from command-and-control servers, and earn cryptocurrency and leaderboard rankings through a gamified affiliate system. The near-zero technical barrier lets the group mobilize thousands of low-skill volunteers on short notice, timed to NATO actions, elections, sanctions, and aid announcements.

The proxy ecosystem also keeps producing fresh hack-and-leak personas that pair a claimed intrusion with a curated leak and a ready-made narrative through accounts with no attribution history. Its cost to defenders runs deeper than any single leak: by controlling what gets published and how it is framed, these actors choose the direction defenders look, and pull attention from where they ought to look instead.

China

China's cyber threat to NATO centers on strategic espionage against Alliance diplomatic structures and member-state defense industries, and 2026 reporting shows both a clear resurgence in European targeting and a steady move toward stealthier tradecraft.

The most directly NATO-relevant activity is the return of Mustang Panda (TA416) to European government targeting. From mid-2025, the group resumed sustained campaigns against European governments and diplomatic entities, concentrating most heavily on individuals and mailboxes tied to diplomatic missions and delegations to NATO and the EU.

The renewed focus began immediately after the 25th EU-China summit, against a backdrop of trade friction, the Russia-Ukraine war, and rare earths disputes, and extended into late-2025 campaigns against European foreign and defense ministries. In at least one case, the group sent phishing from a compromised account belonging to a European armed forces organization, and its lures ranged from humanitarian and collaboration themes to reconnaissance built around European troop deployments to Greenland. Consistent with the flashpoint-driven tasking seen across the Russian and Iranian ecosystems this year, TA416 expanded to Middle Eastern diplomatic targets in March 2026 in the weeks following the outbreak of the Iran war, a region it had not traditionally targeted.

The tradecraft iterates continuously while holding to one objective: loading the group's customized PlugX backdoor via DLL side-loading. In March 2026 variants, TA416 used a signed Canon executable (CNMNSST.exe) to side-load a malicious loader DLL, decoding the PlugX payload from an accompanying data file, with command and control over HTTP using an RC4-encrypted binary protocol. Across the wider campaign, the group cycled through fake Cloudflare Turnstile challenge pages, OAuth redirect abuse, and C# project-file delivery, and by early 2026 was staging renamed Microsoft MSBuild executables and malicious CSPROJ downloaders from archives hosted on Google Drive or a compromised SharePoint instance.

Other China-aligned clusters are reaching NATO members too. A campaign tracked as SHADOW-EARTH-053, active since at least December 2024, has targeted government, defense, telecommunications, and transportation organizations across seven Asian countries (Pakistan, Thailand, Malaysia, India, Myanmar, Sri Lanka, and Taiwan), with Poland the single European NATO member in its victim set. The group exploits N-day flaws in internet-facing Microsoft Exchange and IIS servers (including the ProxyLogon chain), deploys Godzilla web shells for persistence, and stages ShadowPad implants through DLL side-loading of legitimate signed binaries, blending activity into normal administration by routing it through the remote-access tool AnyDesk. The pattern fits a wider shift: PRC-nexus espionage is expected to prioritize stealthy operations, aggressively targeting edge devices and security appliances that often lack endpoint detection, with groups such as UNC5221 and UNC3886 named as prolific edge-device operators. Related dual-purpose Chinese operators worth tracking include APT41 and APT31.

The forward-looking concern for NATO members is the supply chain. PRC-nexus operations are forecast to continue surpassing other nations in volume and to increasingly target third-party providers, on the logic that compromising one trusted partner can open access to many downstream organizations while abuse of legitimate partner connections stays hard to detect. Google's threat forecasters flag the semiconductor sector in particular, where competition, US export restrictions, and AI-driven demand raise the espionage stakes. For the Alliance, this reinforces the report's emphasis on secure supply chains and industrial cybersecurity: as joint procurement pulls thousands of vendors into sensitive programs, defense suppliers and their subcontractors should treat themselves as priority targets rather than peripheral ones.

Iran

Iran combines state-sponsored APT activity with an expanding hacktivist proxy network. MuddyWater (MOIS-linked), APT34 (OilRig), and APT35 (Charming Kitten) maintain active campaigns against government, defense, energy, and telecommunications targets across NATO member states, with growing emphasis on cloud infrastructure exploitation and credential harvesting against European targets.

Handala, a pro-Iranian hacker group, has conducted data theft, defacement, and leak operations against Israeli and Western targets, combining direct disruption with amplification of Iranian strategic narratives. The group operates in the same proxy gray zone Russia employs. Iran's capabilities do not match the Russian or Chinese scale, but Iranian groups compensate with persistence.

The Iranian picture shifted sharply in 2026 following Operation Epic Fury, the US and Israeli strikes launched on February 28, 2026, against Iran's military command, missile infrastructure, and senior leadership. With Iran's conventional forces degraded and domestic connectivity driven to roughly 1% to 4% of normal, direct operations from inside Iran became far less observable, and the response was carried instead by a decentralized coalition of pro-Iranian, pro-Palestinian, and Russian-aligned groups operating largely from outside the country. SOCRadar tracked this across its Iran–Israel/US War feed.

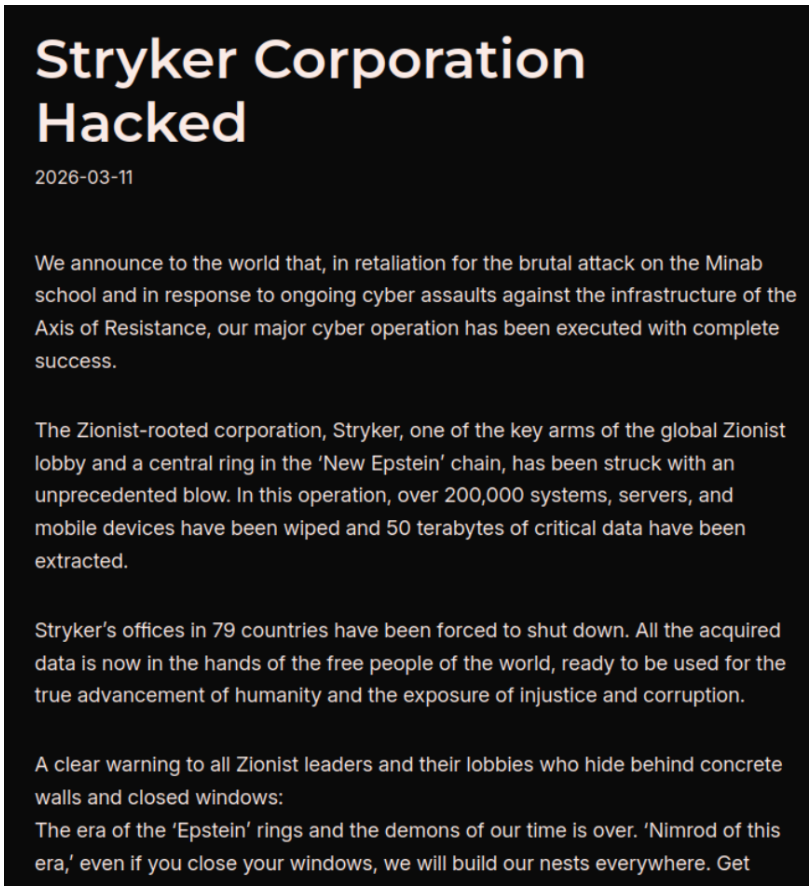
For NATO, the significant development is the steady expansion of what these groups treat as a legitimate target. Coalition operations reached Cyprus, Romania, the United Kingdom, Denmark and Greenland, and South Korea, none with a direct role in the conflict. The operating logic broadened from "parties to the war" to "any US-aligned democracy," with public statements by European leaders treated as sufficient justification; Romania, for instance, saw one of its government agencies knocked offline in explicit retaliation for its president's statements on US military base access. This is the mechanism to track: a Middle East conflict functioning as a mobilization event that produces sustained, opportunistic targeting of Alliance countries on grounds only loosely connected to the original trigger.

The coalition also blurred Iranian and Russian objectives. Pro-Russian groups, including NoName057(16), Server Killers, and Z-Pentest, joined the anti-Israel and anti-US campaign while continuing to pursue Ukraine-related agendas under the same umbrella. NoName057(16), for example, ran its repeated Romania sweeps under the #OpRomania and #TimeOfRetribution banners tied to Ukrainian grievances rather than the Iran theater, and kept up a sustained #OpCyprus campaign in parallel. A single conflict can therefore activate multiple adversary ecosystems against NATO targets at once.

Two categories carry weight beyond the DDoS noise. First, state-directed pre-positioning: reporting during the conflict indicated MuddyWater had already established backdoors inside a US bank, an airport, a defense-adjacent software company, and NGOs in the US and Canada before the first strike, deploying implants tracked as Dindoor and a Python-based backdoor referred to as Fakeset.

Second, Handala's escalation from data theft to destructive impact. On March 11, 2026, the group disrupted the Microsoft environment of medical technology firm Stryker, which the company confirmed in an SEC filing as a global network outage. The operation used no custom malware: the attackers abused a compromised Microsoft Intune admin account to issue an enterprise-wide remote wipe, a "living off the cloud" technique that leaves nothing for endpoint tools to catch.

Handala claimed more than 200,000 devices wiped across 79 countries and 50 terabytes stolen, though independent reporting put the wipe closer to 80,000 devices, and the group has a documented pattern of inflating figures; around 5,500 staff were sent home at Stryker's Irish operations. The US Justice Department formally attributed the attack to Iran's MOIS on March 20, 2026, and the FBI seized four Handala domains, though the group relaunched within hours and went on to publish nine schematic maps of Israeli power and grid infrastructure. The through-line is a demonstrated willingness to convert quiet access into destructive impact against civilian and industrial targets.



North Korea

North Korea's cyber threat to NATO is defined less by direct network intrusion of Alliance structures than by revenue generation, defense-technology theft, and a deepening role in the Russia-Ukraine war that ties Pyongyang to the same front NATO is arming against. Operations run primarily through the Reconnaissance General Bureau, with Lazarus and its sub-clusters (Bluenoroff, Andariel, TraderTraitor) focused on financial theft and defense-industrial espionage, and Kimsuky on intelligence collection against government, diplomatic, and think-tank targets.

The financial operation reached record concentration in 2026. DPRK-linked actors stole roughly $2.02 billion in cryptocurrency in 2025, a 51% year-on-year rise, and accounted for around 76% of all crypto hack value through April 2026, including a $292 million exploit of Kelp DAO attributed to the same cluster behind the 2025 Bybit theft. The UN Panel of Experts assesses these proceeds fund a material share of North Korea's ballistic missile and nuclear programs, which makes crypto theft a defense-financing mechanism rather than ordinary cybercrime.

The delivery method matters most for NATO members: the theft increasingly enters through people. North Korea's IT-worker program, sanctioned again by OFAC on March 12, 2026, has shifted from operatives applying for remote jobs to orchestrating fake hiring processes and posing as recruiters for Web3 and AI companies to harvest credentials, source code, and VPN access. Google researchers observed these schemes expanding into Europe through 2025 and 2026, and the same social-engineering tradecraft that plants an insider at a crypto firm can plant one at a defense supplier or its subcontractors. This is a direct hit on the secure-supply-chain and joint-procurement themes running through this report: as the Ankara procurement wave pulls thousands of vendors into sensitive programs, DPRK operators treat remote-hire pipelines as an access vector, and any remote-friendly contractor should assume it is a target.

The strategic dimension is where 2026 turned genuinely interesting, and it complicates the tidy picture of a unified adversary bloc. North Korea has become a frontline contributor to Russia's war, supplying artillery ammunition, ballistic missiles, and manpower. Around 11,000 troops were deployed to Russia by October 2024, rising to roughly 15,000 by April 2025, with South Korean intelligence estimating about 6,000 killed or wounded, over a third of the deployment, by early 2026. For NATO, this means the weapons and personnel sustaining the threat on its eastern flank increasingly originate in Pyongyang, and the combat experience North Korean forces are gaining, particularly against Western-supplied drones and systems, feeds directly back into DPRK capability.

China, notably, has kept functional distance from a consolidated Beijing-Moscow-Pyongyang axis rather than embracing it.

This is a set of overlapping and partly competing relationships, not a bloc, and the same seams show up in cyberspace, where DPRK, Russian, and Chinese operations pursue distinct objectives and rarely coordinate directly even when they overlap on a target.

How Cyberattacks Shaped NATO's Cyber Posture: Three Decades in Brief

NATO's relationship with cyber threats was built attack by attack, each major incident forcing the Alliance to rethink assumptions it had only recently adopted.

1999-2008: From nuisance to collective problem

During Operation Allied Force in Kosovo, NATO experienced its first cyber incidents: website defacements, denial-of-service attacks, and nationalist hacking campaigns. Defacements against the US Department of Defense tripled during the six-week campaign. None penetrated internal systems, but they established a pattern that would hold for 25 years.

The 2002 Prague Summit was the first to place cyber defense on NATO's political agenda, though only in a single sentence and with no operational framework behind it. The main change in minds came in 2007, when coordinated DDoS attacks against Estonia disrupted banks, media, government systems, and telecom providers for three weeks, forcing NATO to confront how Article 5 mutual defense guarantees might apply in cyberspace.

NATO established the CCDCOE in Tallinn in 2008, adopted its first Cyber Defense Policy the same year, and later produced the Tallinn Manual (2013), the reference text on international law in cyber conflict.

The 2008 Russia-Georgia conflict then showed us that cyberattacks could become a major component of conventional warfare.

2014-2016: From policy to doctrine

At the 2014 Wales Summit, NATO endorsed an Enhanced Cyber Defense Policy recognizing that international law applies in cyberspace, and for the first time stated that a cyberattack could trigger Article 5. The timing was shaped by Russia's annexation of Crimea and the surge of cyber operations in eastern Ukraine. Those operations escalated sharply the following year.

On December 23, 2015, hackers using BlackEnergy 3 malware compromised three Ukrainian energy distribution companies, leaving roughly 230,000 consumers without power.

A year later, Sandworm struck again with the more advanced Industroyer malware, taking out a Kyiv transmission substation and attempting to cause permanent physical equipment damage. These attacks moved cyber conflict into the domain of critical infrastructure sabotage and directly shaped the next summit. At Warsaw in 2016, NATO recognized cyberspace as a domain of operations alongside air, land, and sea, and adopted the Cyber Defense Pledge.

2017-2021: Collateral damage and supply chain depth

In June 2017, the NotPetya malware spread from a compromised Ukrainian accounting software update to systems in over 50 countries, causing an estimated $10 billion in global damage. NATO CCDCOE researchers called it "a declaration of power: a demonstration of acquired disruptive capability and readiness to use it." NotPetya showed that a state-directed cyber weapon aimed at one country could cascade across the Alliance through supply chain propagation.

At the 2018 Brussels Summit, allies responded by affirming for the first time their determination "to employ the full range of capabilities, including cyber, to deter, defend against, and counter the full spectrum of cyber threats," shifting from pure defense to acknowledging offensive capability as part of deterrence.

The pattern repeated in 2020 when the SolarWinds breach compromised the software supply chain used to update 18,000 users of its Orion network management product, giving a state-level adversary persistent access across multiple US government agencies and NATO-country organizations.

The 2021 Brussels Comprehensive Cyber Defense Policy stated that significant malicious cumulative cyber activities might, in certain circumstances, be considered an armed attack triggering Article 5. The word "cumulative" was key: NATO now acknowledged that a sustained campaign below the traditional armed-attack threshold could collectively cross that line.

2022-2026: War, infrastructure, and the cloud

One hour before Russian troops crossed into Ukraine on February 24, 2022, Russian hackers hit Viasat's KA-SAT satellite network with wiper malware, rendering tens of thousands of modems inoperable across Ukraine and multiple EU member states.

A senior Ukrainian official said the hack caused "a huge loss in communications in the very beginning of the war." The Viasat attack was the clearest demonstration yet of cyber as a first-strike complement to kinetic military action.

The 2022 Madrid Strategic Concept named Russia as the most significant direct threat and recognized China as a systemic challenge for the first time. At the 2024 Washington Summit, NATO announced the Integrated Cyber Defense Centre at SHAPE and, in a first, directly blamed China for malicious cyber and hybrid activities targeting the Alliance.

The Road to Ankara

In December 2025, a wiper attack attributed to Sandworm struck Poland's energy grid, crossing the threshold NATO had warned about since Estonia in 2007: a destructive Russian operation against a member state's critical infrastructure. It gave concrete urgency to every cyber and resilience initiative heading into the next summit.

In late February 2026, Operation Epic Fury triggered a cascade of cyber activity against NATO countries from pro-Iranian, pro-Palestinian, and pro-Russian groups operating in loose coordination, driving Dark Web threat volume targeting the Alliance from 413 incidents in January to 3,218 by June. China's Mustang Panda resumed sustained targeting of European diplomats and NATO-linked personnel after a two-year pause, with campaigns running through late 2025 into 2026 and expanding to new regions as crises emerged. As the summit approached, Turkiye's Cyber Security Directorate identified over 100 phishing sites targeting the event itself. And on July 6, one day before the €200 million Protected Business Network contract was signed at the NATO Summit Defense Industry Forum, a threat actor posted 35GB of alleged Accenture data for sale on a Dark Web forum. The Alliance was not walking into a calm room.

The pattern across three decades is consistent. NATO's cyber posture advanced in response to attacks, rarely ahead of them; each incident exposed a gap the Alliance had not yet closed, and each summit bolted on a layer of policy, doctrine, or capability to address it. Ankara arrived when the accumulated weight of those gaps, and the speed at which adversaries were exploiting them, left "delivery" as the only credible agenda. What follows is our assessment of what the summit delivered and what it means for the threat landscape.

Ankara Summit

Pre-Summit Assessment

Ahead of the summit, we published a detailed analysis of the risks and tensions NATO was carrying into Ankara. The core assessment was that this summit was structurally different from its predecessors. Every major NATO summit since 2022 has added a new commitment. Madrid produced a Strategic Concept, Vilnius gave Ukraine its "irreversible path" language, The Hague set the 5% spending target. Ankara was the first where the central question was whether anyone had kept their commitments. Secretary General Rutte framed it himself as a summit about "delivery," about turning spending pledges into deployable capability.

The security picture we outlined was defined by a tightening timeline. Allied intelligence services assess that Russia could have the capability to attack a NATO member by 2029, giving the alliance roughly three years to convert budgets into real military capacity. Meanwhile, Russia's hybrid campaigns (sabotage, GPS jamming, cyberattacks, drone incursions) were already reaching NATO territory. On the cyber side specifically, we flagged the Sandworm wiper attack against Poland's energy grid in December 2025, a 25% year-on-year increase in Russian cyberattacks against NATO countries, and Chinese pre-positioning inside US civilian networks as preparation for a potential Taiwan-related crisis.

We also identified the institutional risks that threatened to overshadow the agenda: US force drawdowns from Europe, the alliance split over the Iran war, the fragile credibility of the 5% spending target after Spain negotiated an exemption, and the open question of whether NATO would consolidate around a group of leading countries or drift toward fragmentation. Our expectation was that the most likely outcome would be a short, carefully managed summit with defense-industrial contracts, reaffirmation of Article 5 and the spending trajectory, continued Ukraine support, and limited public disagreement. The real test, we noted, was whether the discipline would hold with this much tension underneath.

Summit Outcomes

The summit played out close to our baseline expectation: a short, managed event focused on demonstrating delivery rather than launching new strategic frameworks. The Declaration reaffirmed Article 5, endorsed the spending trajectory set at The Hague, and avoided public fractures over the fault lines we flagged beforehand (US posture in Europe, the Iran split, the credibility of the 5% target).

The headline numbers were the clearest signal of intent. European Allies and Canada increased defense spending by over $139 billion in 2025. The summit announced more than $50 billion in new procurement contracts and committed to expanding collective manufacturing capacity. On Ukraine, allies pledged €70 billion in military equipment, assistance, and training for 2026, with an explicit commitment to sustain at least equivalent levels in 2027.

For cybersecurity professionals, three developments matter most:

- First, the Declaration committed NATO to developing an "interoperable transatlantic warfighting cloud" and "adopting powerful AI models" for military use. This is the first time cloud infrastructure and AI have been written directly into NATO's deterrence and defense language at the summit level.

- Second, the NCIA signed a roughly €200 million, seven-year contract with Accenture and Leonardo for the Protected Business Network (PBN), a classified cloud platform serving approximately 29,000 users across the Alliance. Leonardo will implement a Zero Trust Architecture secured by an AI-driven cyber defense platform.

- Third, the Declaration's language on eliminating defense trade barriers and leveraging partnerships to "maximise defense industrial depth" signals a deeper integration of commercial technology vendors into NATO's security architecture, with all the supply chain implications that follow.

The summit did not produce a standalone cyber commitment or a new institutional framework. Instead, cybersecurity was treated as embedded across every domain on the agenda. Observers at the Defense Industry Forum consistently confirmed this framing: cyber resilience is now positioned as a component of military readiness, critical infrastructure protection, logistics, and defense industrial capacity. The operational question has shifted from whether to integrate AI and cyber into defense planning to how to do it securely across allied forces.

Summit Decisions and Cyber Threat Landscape

The Ankara decisions accelerate trends we have been tracking, but they also create new exposure. The commitment to a transatlantic warfighting cloud and to large-scale AI adoption means NATO is betting on a digital backbone that does not fully exist yet. Building and benefiting from it will take years but defending it starts now.

The PBN contract illustrates both the opportunity and the risk. A classified cloud environment for 29,000 users across the Alliance is a significant modernization step. But the same week the contract was signed, a threat actor posted a claim on a Dark Web forum offering roughly 35GB of allegedly stolen Accenture data for sale, including source code, RSA and SSH keys, Azure personal access tokens, Azure storage access keys, and configuration files. Accenture has confirmed awareness of the issue and said it remediated the source. The same actor made an earlier Accenture-related claim in June 2024 involving alleged third-party exposure of employee data. Whether or not the current dataset is fully authentic, the timing creates a case for us. The companies building NATO's digital infrastructure are themselves high-value targets, and a compromise at that level can cascade into other environments.

The $50 billion procurement wave amplifies this dynamic. Every new defense-industrial contract extends the attack surface. As more commercial vendors are pulled into classified or sensitive programs, adversaries gain more entry points through supply chain compromise, credential theft, and third-party breaches. Summit participants repeatedly flagged supply chain security as one of NATO's most pressing cyber challenges, and the Accenture situation is a live example of why.

The AI dimension carries its own risk profile. The Declaration's commitment to "adopting powerful AI models" was paired with a clear concern voiced by participants at the Forum: Europe's dependency on US-based AI capabilities creates a strategic vulnerability. If allied forces operationalize AI for intelligence, command and control, and decision-making, the integrity and availability of those models become military-grade concerns. Adversarial manipulation of training data, model poisoning, and exploitation of AI supply chains are threat categories that NATO will need to address from the beginning.

Signals to Track

Defense procurement supply chain attacks: The $50 billion in new contracts will pull dozens of vendors into sensitive programs over the coming months. Whether threat actors begin targeting newly announced procurement recipients, particularly through third-party compromise or credential marketplaces, should be watched carefully. For example the Accenture-Leonardo-NCIA relationship is now public and high-profile. Reconnaissance activity, spearphishing campaigns, or Dark Web chatter directed at entities in the PBN supply chain, including smaller subcontractors that may lack equivalent security maturity, are all worth monitoring.

AI supply chain integrity: As NATO moves to operationalize AI models, developments around model provenance, training data integrity, and adversarial attacks on AI pipelines become increasingly relevant. We assess that state sponsored threat actors probing or claiming access to AI development environments is one of the more likely near-term risks in this space.

European AI dependency dynamics: The tension between AI adoption and US dependency surfaced repeatedly at the summit. Whether European allies launch sovereign AI defense initiatives matters, because the gap between ambition and capability could create operational problems or security fragmentation across the Alliance.

Russian and Chinese response to the spending signal: $139 billion in increased spending and $50 billion in new procurement is a signal for adversaries. Watching for shifts in Russian cyber targeting priorities (particularly toward defense-industrial targets and logistics networks) and any acceleration in Chinese operations linked to the Taiwan contingency will be important.

The 2029 timeline and threat actor behavior: Allied intelligence assesses Russia could have the capability to attack a NATO member by 2029. Whether this publicly acknowledged timeline influences the tempo of Russian hybrid operations, espionage campaigns, or infrastructure mapping activity in the near term is something we consider worth tracking closely. Public timelines can shape adversary calculus in both directions: they can accelerate preparation, or they can invite testing of Alliance readiness before the deadline arrives.

Threat Actor Activity

NATO and its affiliated institutions remain active targets for both state-linked and ideologically motivated threat actors. In the past two years alone, NATO systems have been breached by hacktivist groups, targeted by phishing and credential theft campaigns around major summits, and named in Dark Web forum listings advertising stolen data from Alliance-linked organizations. The following section covers recent threat actor activity directed at NATO as an institution and the entities operating within its orbit.

Data from SiegedSec's 2023 NATO Portal Breach Still Being Reshared

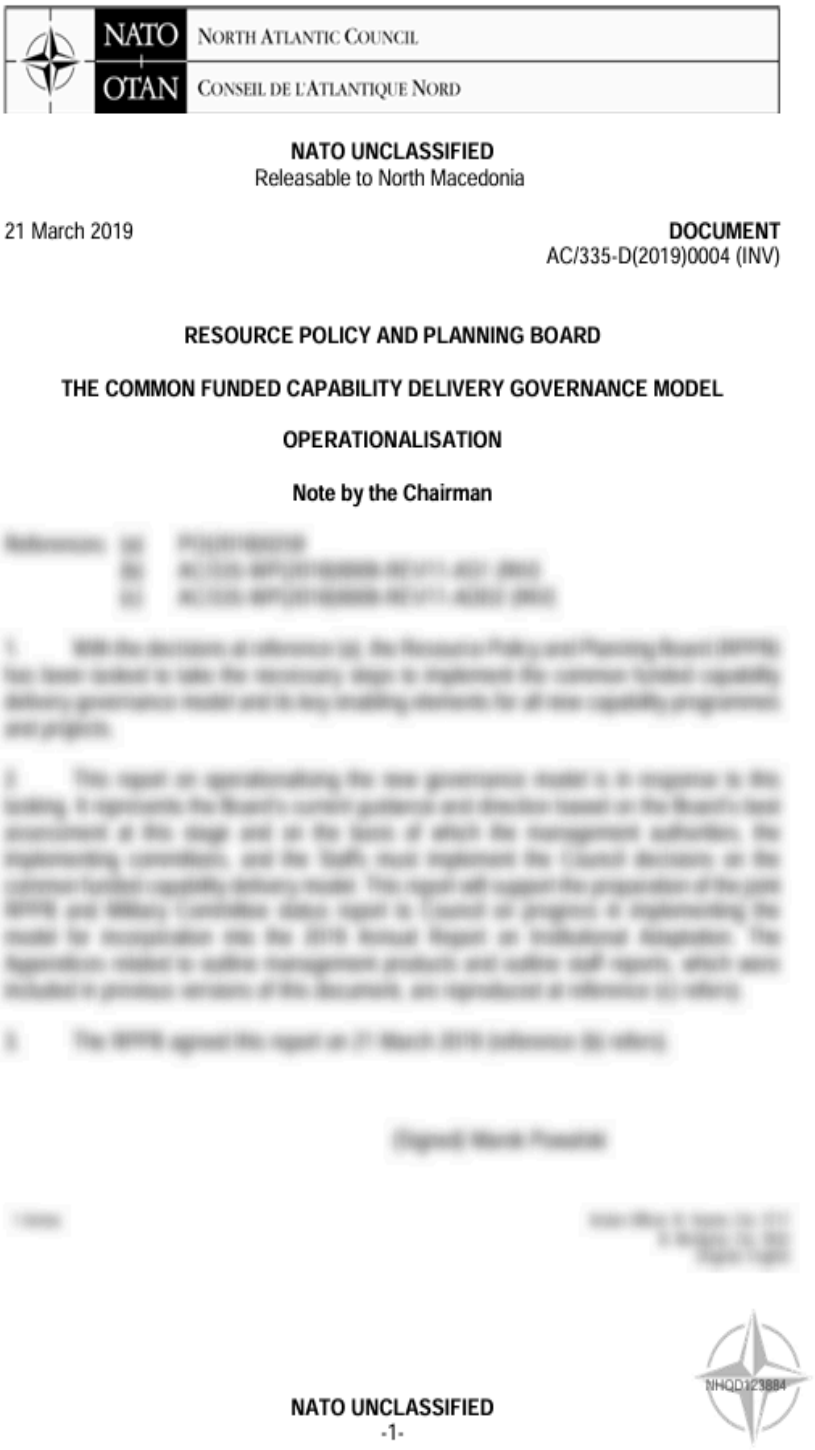
In July and October 2023, the hacktivist group SiegedSec breached several unclassified NATO web portals, including the Communities of Interest Cooperation Portal, the Joint Advanced Distributed Learning platform, the Lessons Learned Portal, and the Logistics Network Portal. The stolen data remains in circulation today.

The group leaked roughly 3,000 documents totaling about 9GB, exposing names, email addresses, phone numbers, office addresses, and ranks of NATO personnel across the 31 member nations. SiegedSec framed the attacks as retaliation against NATO countries over alleged human rights abuses and denied any state affiliation. NATO confirmed an investigation and stated that classified networks were not affected.

Although the material was publicly characterized as unclassified, the filenames point to a heavy concentration of documents on Electronic Warfare governance, NATO standardization, and Federated Mission Networking.

For an adversary, this was far from worthless. The collection offers insight into NATO's organizational structure, planning processes, terminology, committee relationships, and interoperability priorities. None of it appears to expose operational plans or classified capabilities, but aggregated at this scale it could support long-term intelligence collection and help hostile analysts map how NATO develops and coordinates doctrine across member states, a reminder that unclassified does not mean low intelligence value.

The personnel data compounds the risk. The records included names, countries, email addresses, phone numbers, and job titles of NATO-affiliated staff, effectively a ready-made targeting directory for spear-phishing and organizational mapping. It also explains why the breach continues to distort the threat picture: many alleged "leaked NATO documents" still surfacing on hacker forums and Telegram channels are not new compromises, but partial or full reshares of the 2023 SiegedSec data repackaged as fresh breaches. Any newly claimed NATO leak should be checked against this dataset first.



NATO NORTH ATLANTIC COUNCIL
OTAN CONSEIL DE L'ATLANTIQUE NORD

NATO UNCLASSIFIED
Releasable to North Macedonia

21 March 2019

DOCUMENT
AC/335-D(2019)0004 (INV)

RESOURCE POLICY AND PLANNING BOARD

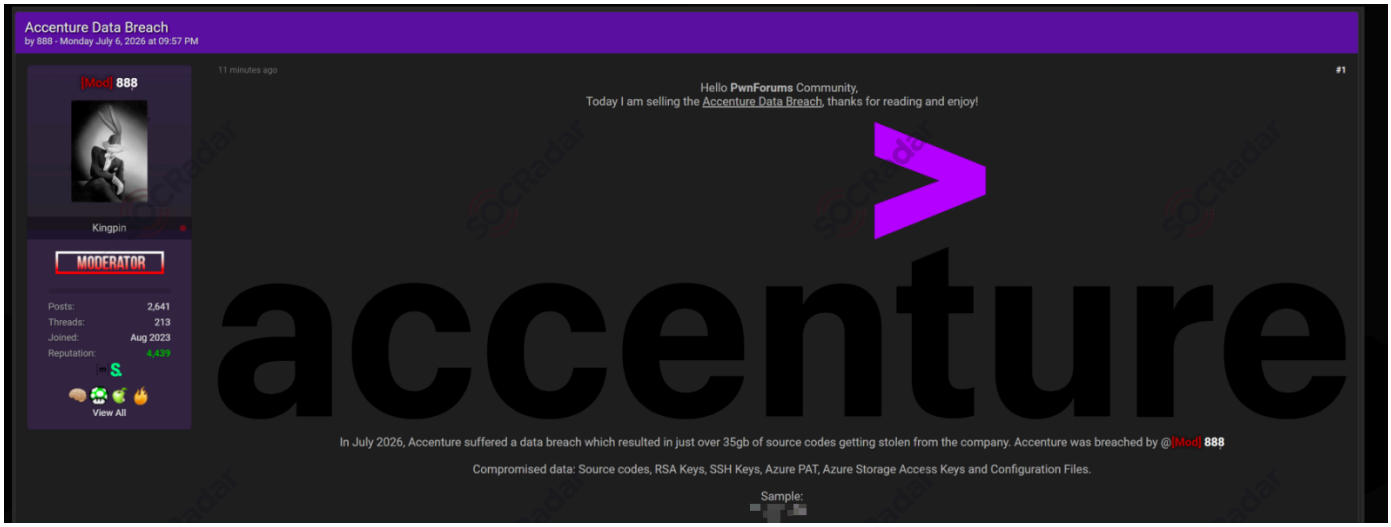
THE COMMON FUNDED CAPABILITY DELIVERY GOVERNANCE MODEL

OPERATIONALISATION

Note by the Chairman

NATO UNCLASSIFIED
-1-

Accenture Confirms Breach Days Before Signing €200M NATO Cloud Contract



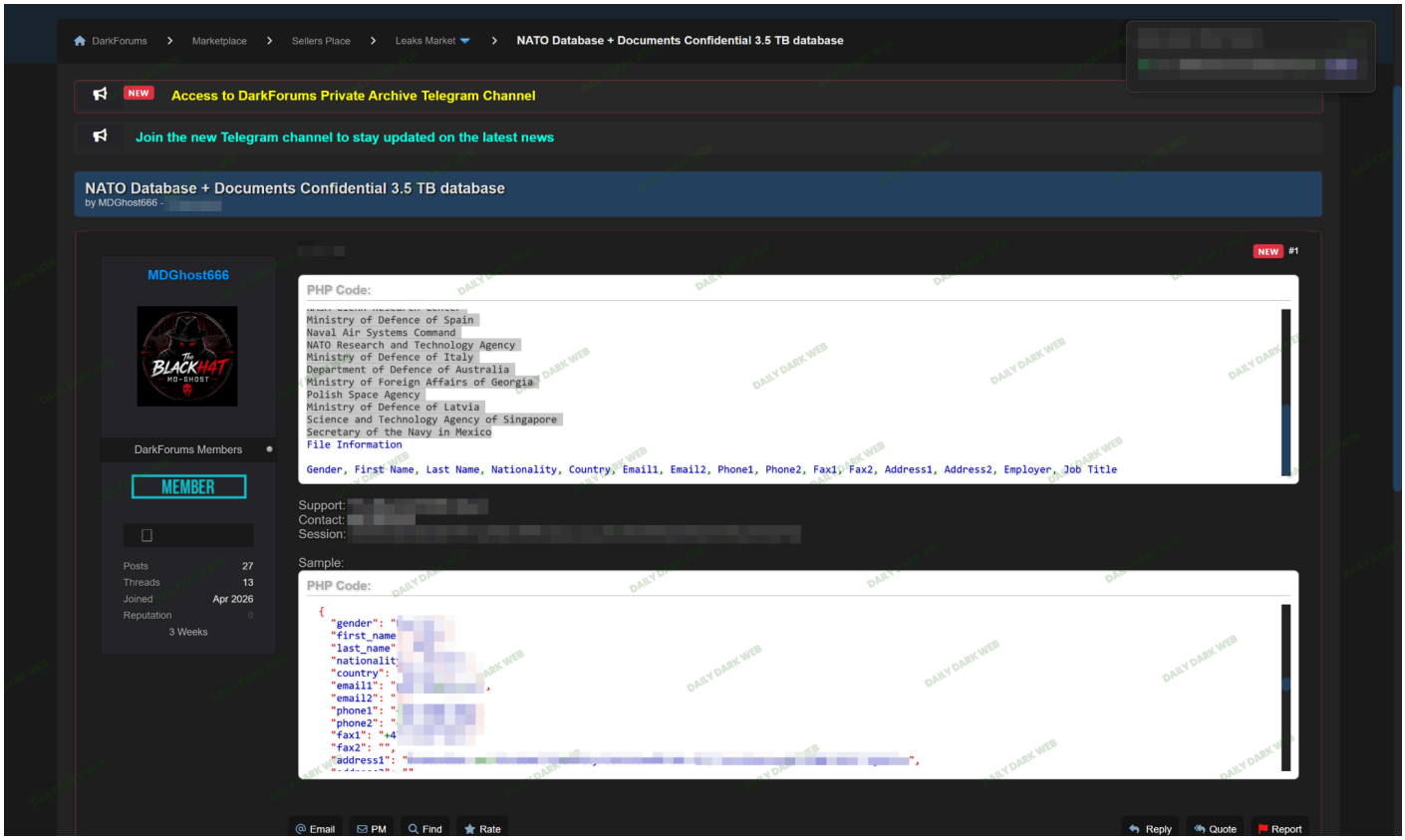
A threat actor using the handle "888" is selling 35GB of alleged Accenture data on a Dark Web forum, including source code, RSA and SSH keys, Azure access tokens, and configuration files. Accenture confirmed the breach, calling it an "isolated matter" that has been remediated.

The listing appeared on July 6, one day before Accenture signed a €200 million, seven-year contract with the NATO Communications and Information Agency to build and operate the Protected Business Network, a classified cloud platform serving approximately 29,000 users across the Alliance.

While there is no evidence the stolen data is directly tied to NATO systems, the exposed materials (particularly cloud credentials and development infrastructure assets) raise supply chain concerns, as Accenture's internal engineering patterns and authentication practices could carry into the NATO project.

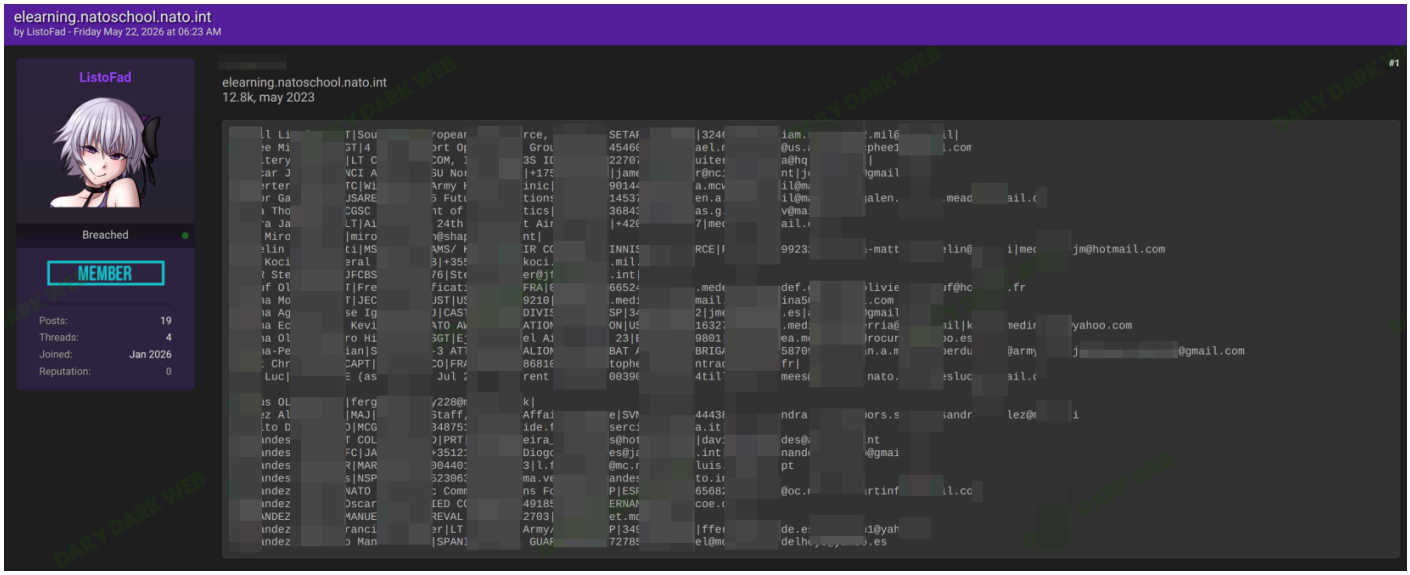
This marks the third security incident linked to Accenture in five years, following the 2021 LockBit ransomware attack and a 2024 employee data exposure claim by the same threat actor.

Alleged 3.5TB NATO Database Offered for Sale on Dark Web Forum



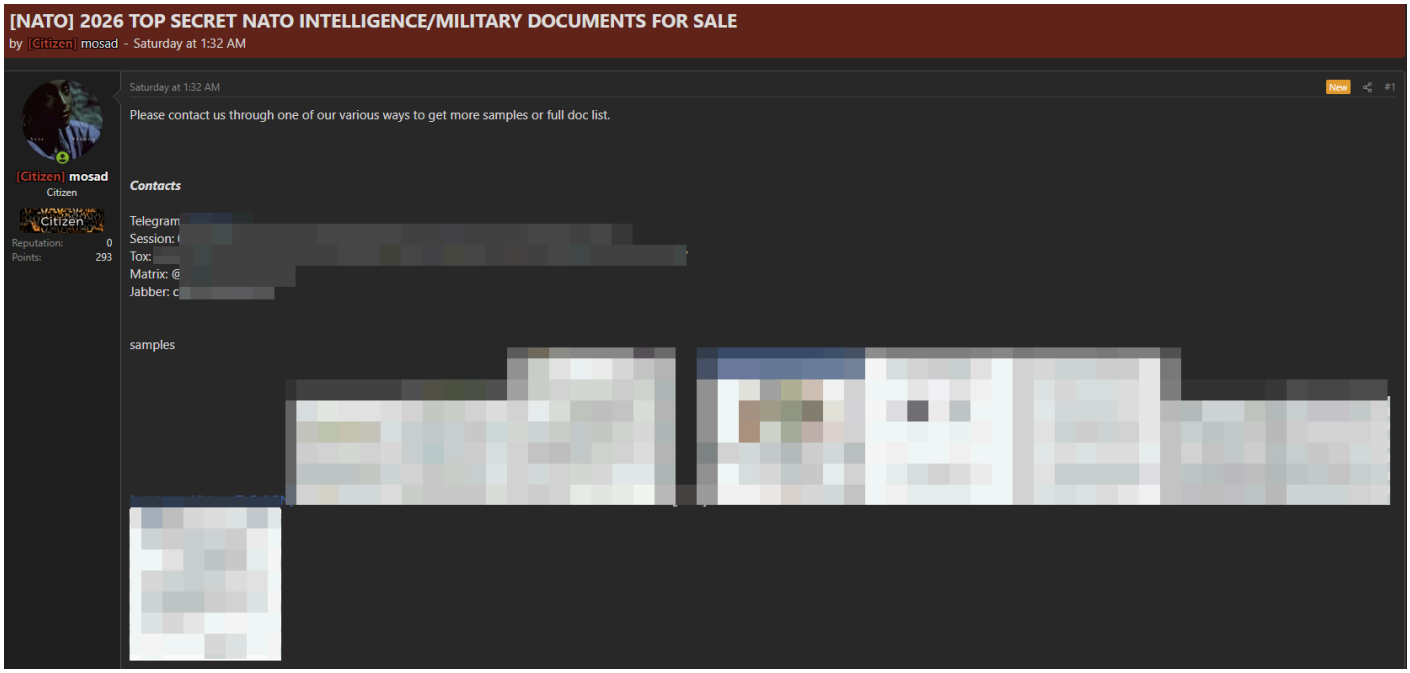
A threat actor is advertising an alleged 3.5TB archive described as "NATO Database + Confidential Documents" on a Dark Web forum. The listing references multiple defense and government organizations across allied nations, including defense ministries, naval commands, research agencies, and space agencies from several countries. The dataset reportedly contains personnel records with fields such as names, nationalities, email addresses, phone numbers, fax numbers, physical addresses, employers, and job titles. The authenticity and origin of the data remain unverified, but the scope of the alleged exposure raises concerns about targeted spear-phishing and intelligence collection against defense sector personnel.

NATO School E-Learning Platform Database Leaked on Dark Web Forum

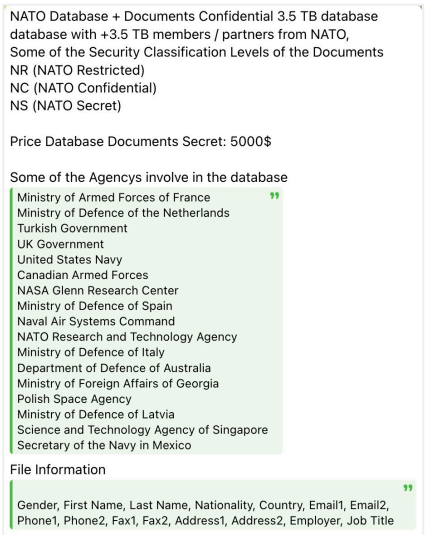


A database from a NATO e-learning platform (elearning.natoschool.nato.int) has surfaced on a Dark Web forum. The dataset, reportedly dating back to May 2023, contains approximately 12,800 records of personnel information including names, ranks, divisions, locations, nationalities, phone numbers, and email addresses. The exposed data could enable targeted spear-phishing campaigns and intelligence profiling against military and defense personnel affiliated with the Alliance.

Threat Actor Claims Sale of Classified NATO Intelligence Documents



A threat actor operating under the alias "mosad" has posted a listing on a Dark Web forum claiming to sell classified NATO intelligence and military documents. The listing, titled "2026 TOP SECRET NATO INTELLIGENCE/MILITARY DOCUMENTS FOR SALE," invites potential buyers to request samples or a full document list through various contact methods. The scope and authenticity of the alleged documents remain unverified, but the claimed classification level and military nature of the materials raise serious concerns regarding potential exposure of sensitive Alliance operations.



In another post on a Telegram channel, a threat actor is advertising a 3.5TB database containing NATO member and partner records along with classified documents. The listing claims the archive includes documents at multiple NATO security classification levels.

The database allegedly references personnel and organizational data tied to defense ministries, armed forces, naval commands, research agencies, and space agencies across multiple allied and partner nations.

The exposed records reportedly contain personal and professional details including gender, names, nationalities, email addresses, phone and fax numbers, physical addresses, employers, and job titles.

Threat Actor Leaks Email Addresses Linked to Intelligence and Defense Agencies

A threat actor using the alias "ERBuS" has posted a collection of email addresses allegedly associated with major intelligence and defense organizations, including the CIA, NATO, and FBI, on a Dark Web forum. The actor also claims to possess five recorded video call interviews from 2022. The scope and authenticity of the leaked data remain unverified, and no specific context was provided for how the materials were obtained. The alleged exposure of agency-linked email addresses and internal recordings, if confirmed, could present risks for social engineering and targeted phishing operations.

NATO Countries Threat Landscape

This report is based on data collected between July 2025 and June 2026

In the following chapters, you will be reading about the various aspects of the cyber threat landscape around NATO.

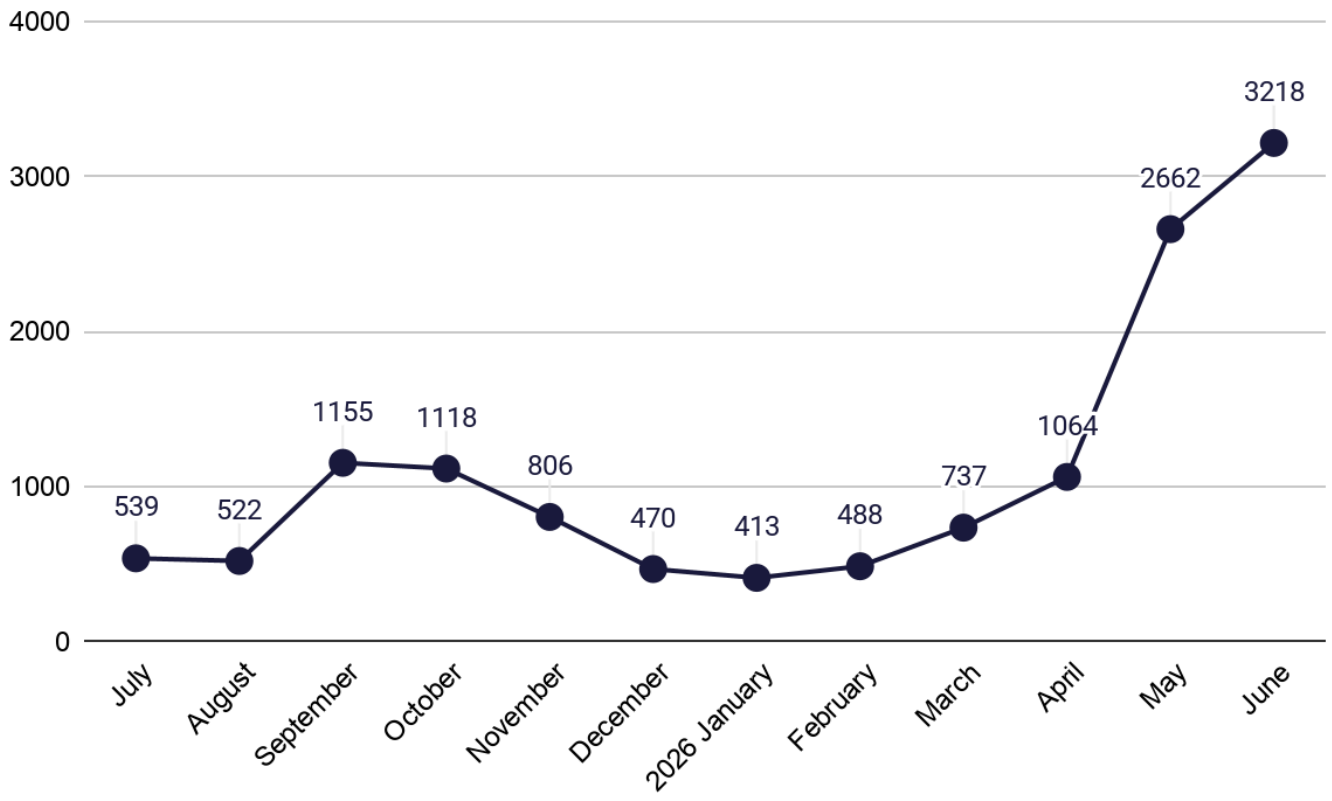
In the Dark Web Threats chapter, we will be covering the news and developments from Dark Web Forums, Telegram channels, Discord groups, and so on. These are areas where threat actors with various skill sets come together, discuss, share tools, and publish their alleged cyber attacks.

In the Ransomware Threats chapter, you will find detailed information about ransomware actors targeting NATO, their detailed profiles, and the necessary data that summarizes the ransomware activities.

The Phishing Threats chapter will show you how threat actors target various organizations with fake websites. By examining the data here, you can take the necessary steps to prevent your employees from falling into threat actors' traps.

Dark Web Threats Targeting NATO Countries

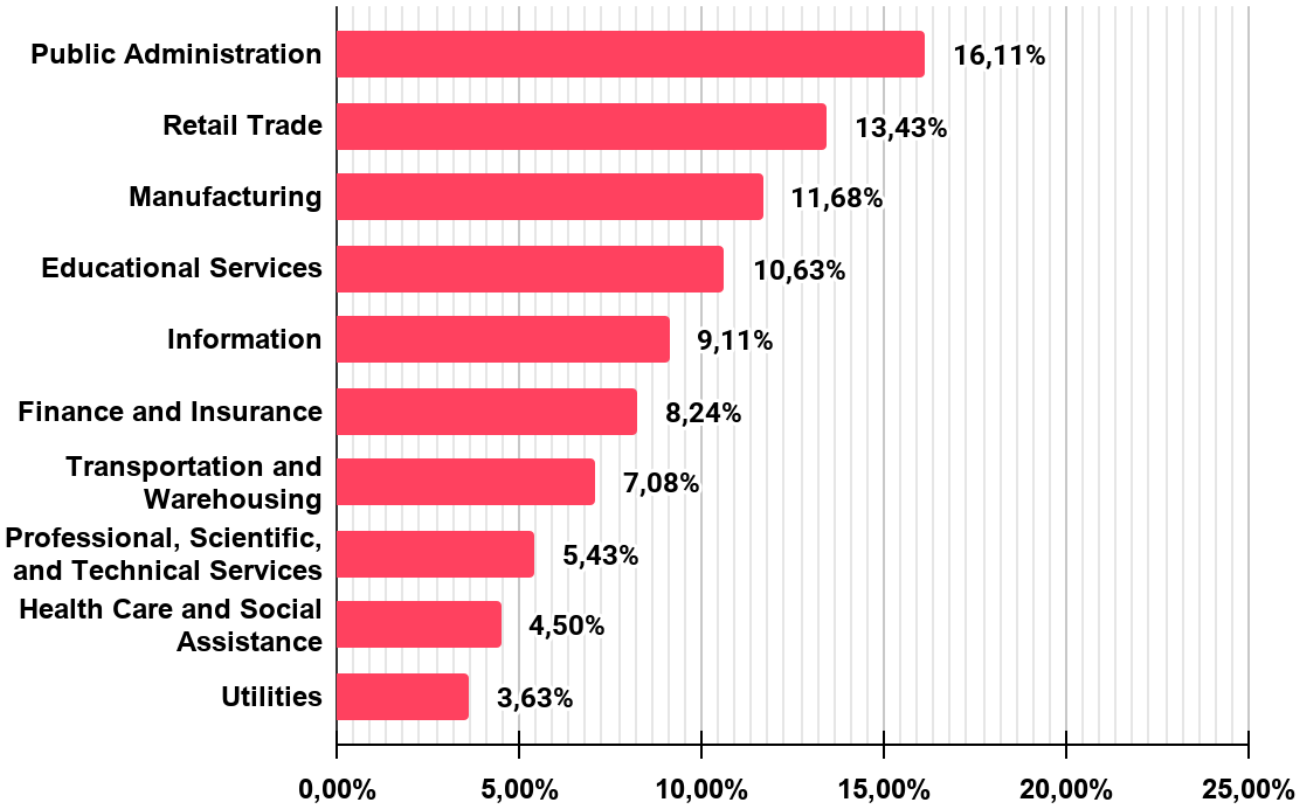
Monthly Dark Web Threat Volume Targeting NATO Countries (July 2025 - June 2026)



Dark Web threat volume targeting NATO countries followed two distinct phases across the reporting period. The second half of 2025 showed a stable baseline averaging roughly 770 incidents per month, with a brief spike in September-October (likely driven by seasonal campaign cycles) and a trough in December 2025 through January 2026 when activity dropped to its lowest point at 413 incidents.

The trajectory shifted sharply from February 2026 onward. Volume nearly doubled month over month from March (737) through April (1,064), then surged to 2,662 in May and 3,218 in June, a more than sevenfold increase from the January low. The acceleration aligns with two developments covered in this report: the outbreak of the Iran war in late February 2026, which activated multiple threat ecosystems against NATO-affiliated targets simultaneously, and the intensifying pre-summit period ahead of Ankara, which historically draws reconnaissance, phishing, and opportunistic threat activity targeting Alliance-linked organizations.

Industry Distribution of Dark Web Threats

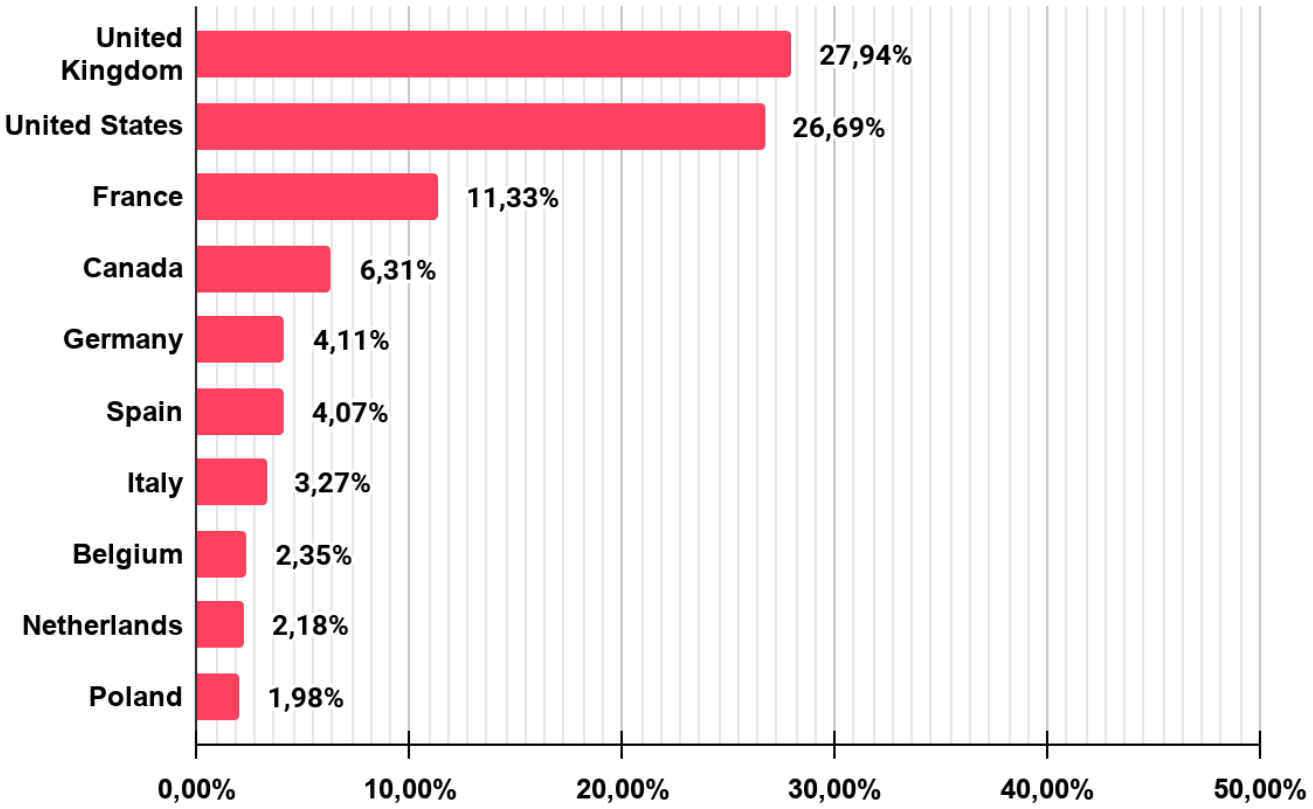


Public Administration leads the chart at 16.11%, making government-linked organizations the most targeted sector on the Dark Web across NATO countries. Retail Trade follows at 13.43%, driven by the high resale value of customer payment data and personal records. Manufacturing ranks third at 11.68%, a sector frequently targeted by ransomware groups due to the pressure of operational downtime. Together, these top three sectors account for over 41% of all Dark Web threat activity.

Educational Services at 10.63% stands out as a notable target. Universities and research institutions often manage large volumes of personal data while operating with limited cybersecurity budgets, which makes them attractive to threat actors.

The remaining sectors, from Information (9.11%) to Utilities (3.63%), show a gradual decline. However, even lower-ranked sectors like Utilities carry significant risk due to their role in critical infrastructure.

Distribution of Dark Web Threats by Target Country

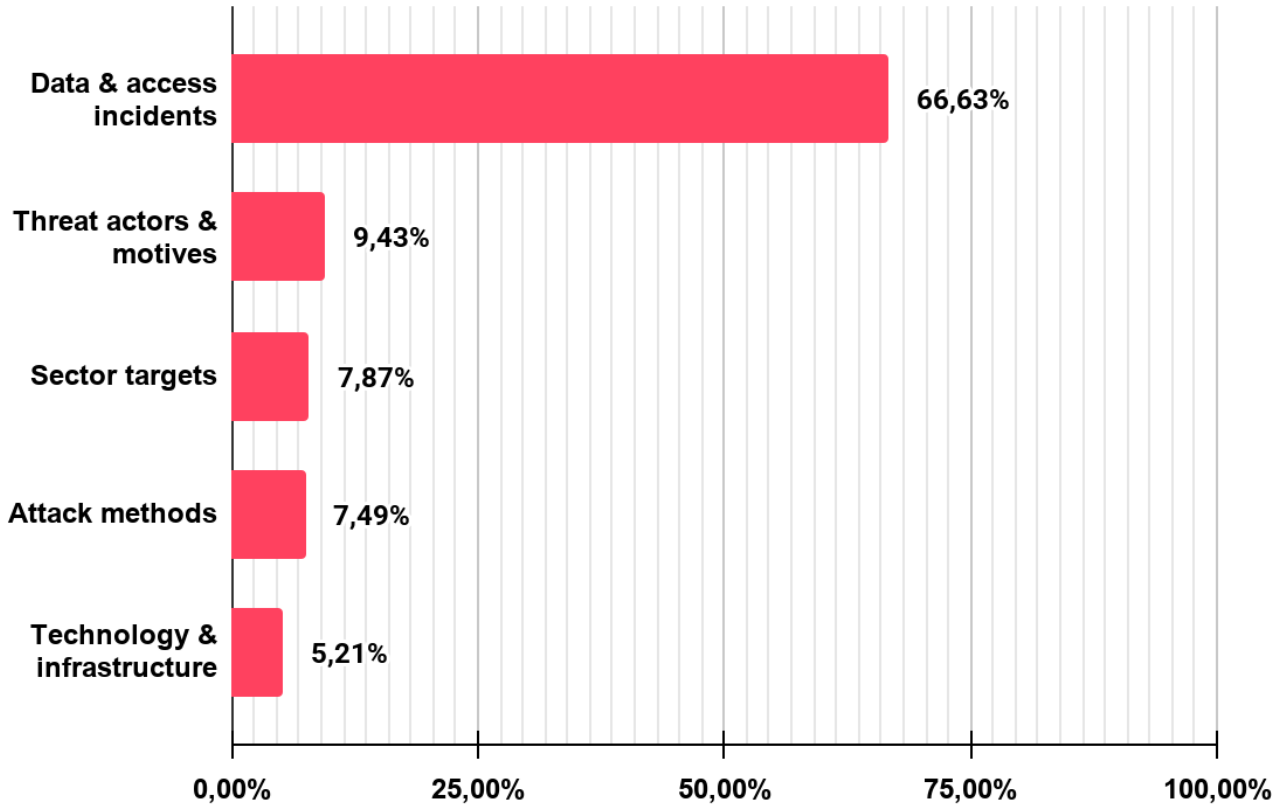


The United Kingdom (27.94%) and the United States (26.69%) together account for more than half of all Dark Web threats targeting NATO countries. This concentration is expected given the size of their digital economies, the volume of valuable data they hold, and their geopolitical visibility.

France comes in third at 11.33%, significantly ahead of Canada (6.31%) and Germany (4.11%). The gap between the top three and the rest is notable: the leading trio captures over 65% of all recorded threats.

Spain (4.07%) and Italy (3.27%) show similar threat levels, while Belgium (2.35%), the Netherlands (2.18%), and Poland (1.98%) round out the top ten. Belgium's presence is worth noting, as Brussels hosts key NATO and EU institutions, which increase its exposure to politically motivated threat actors despite its smaller digital footprint.

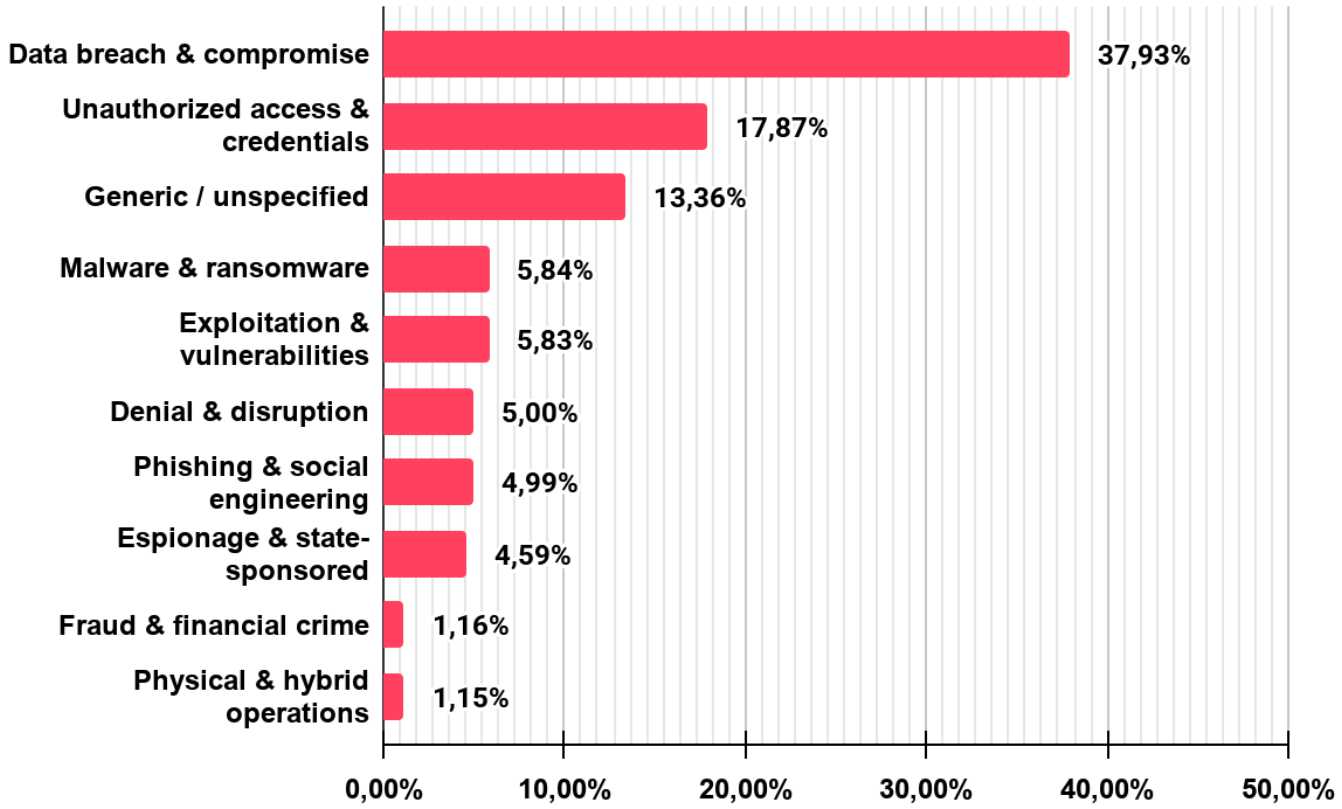
Distribution of Dark Web Threats by Threat Categories



Data and access incidents dominate Dark Web activity at 66.63%, confirming that stolen data, leaked credentials, and unauthorized access remain the core business of underground markets. This aligns with the high targeting of sectors like Public Administration and Retail Trade, where large databases of personal and financial information are common.

Threat actors and motives (9.43%), sector targets (7.87%), and attack methods (7.49%) form a middle cluster. These categories reflect discussions around who is attacking, what they are targeting, and how they operate. Together they represent roughly 25% of the activity.

Distribution of Dark Web Threats by Threat Type



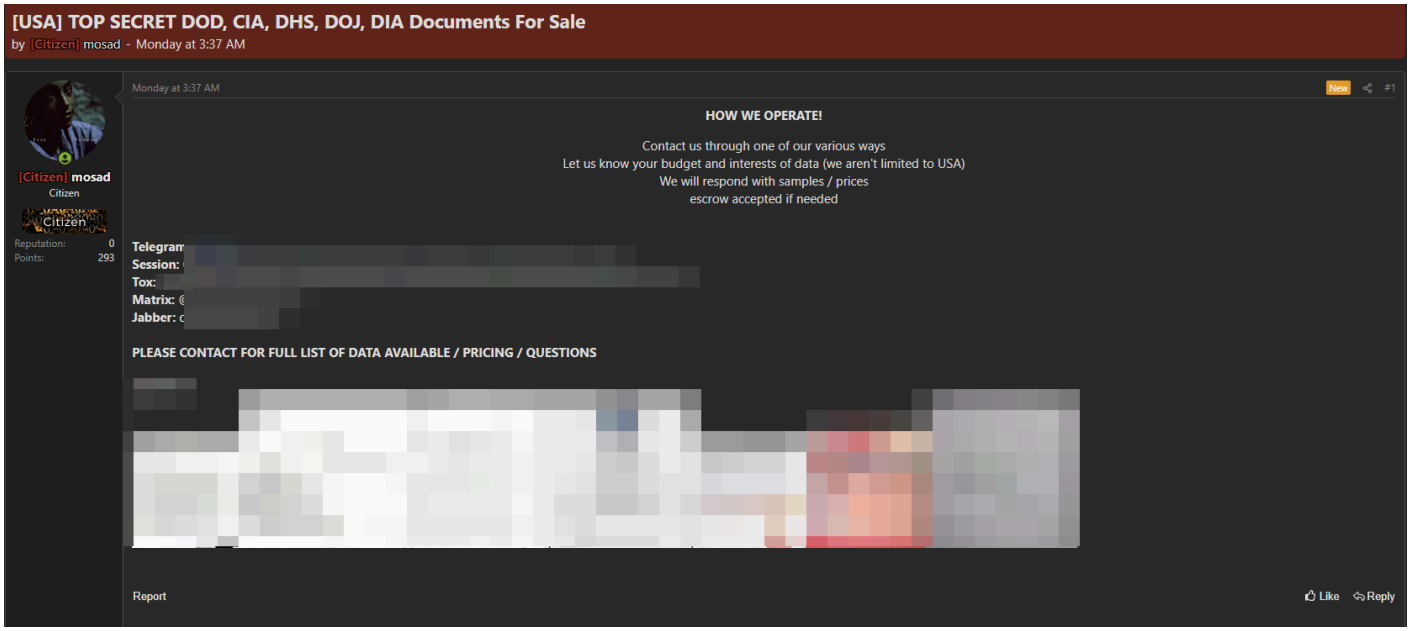
Data breach and compromise is the leading threat type at 37.93%, followed by unauthorized access and credentials at 17.87%. Together, these two categories make up over 55% of all threats, which directly supports the dominance of "data and access incidents" seen in the broader threat category breakdown..

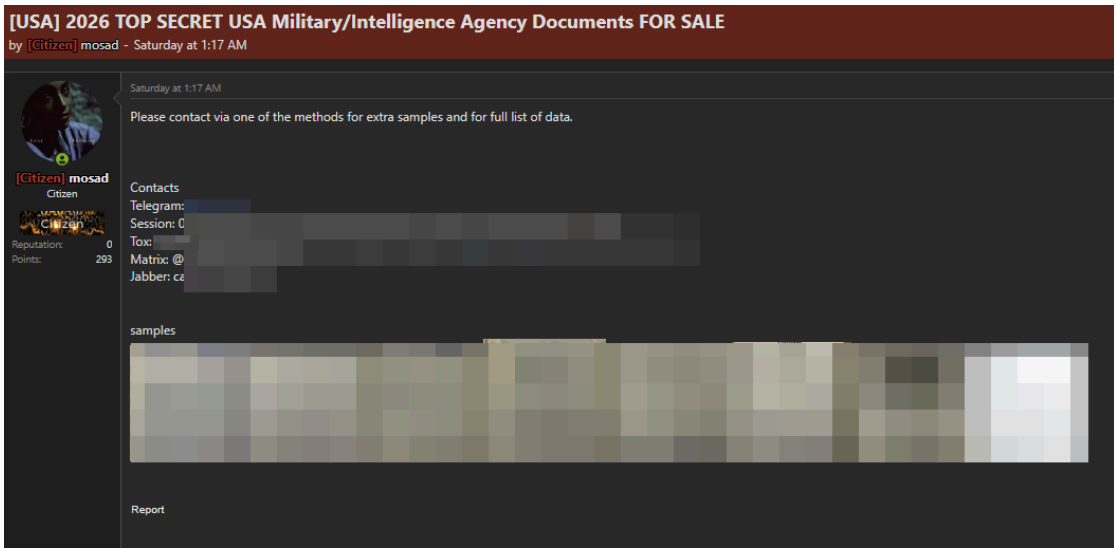
Malware and ransomware (5.84%), exploitation and vulnerabilities (5.83%), and denial and disruption (5.00%) form a tightly grouped cluster around 5-6%. Phishing and social engineering (4.99%) sits close behind, showing that traditional attack methods remain steady across the threat landscape.

Espionage and state-sponsored activity accounts for 4.59%, a meaningful share that reflects the geopolitical dimension of NATO's threat environment.

Recent Dark Web Activities Targeting Entities in NATO Countries

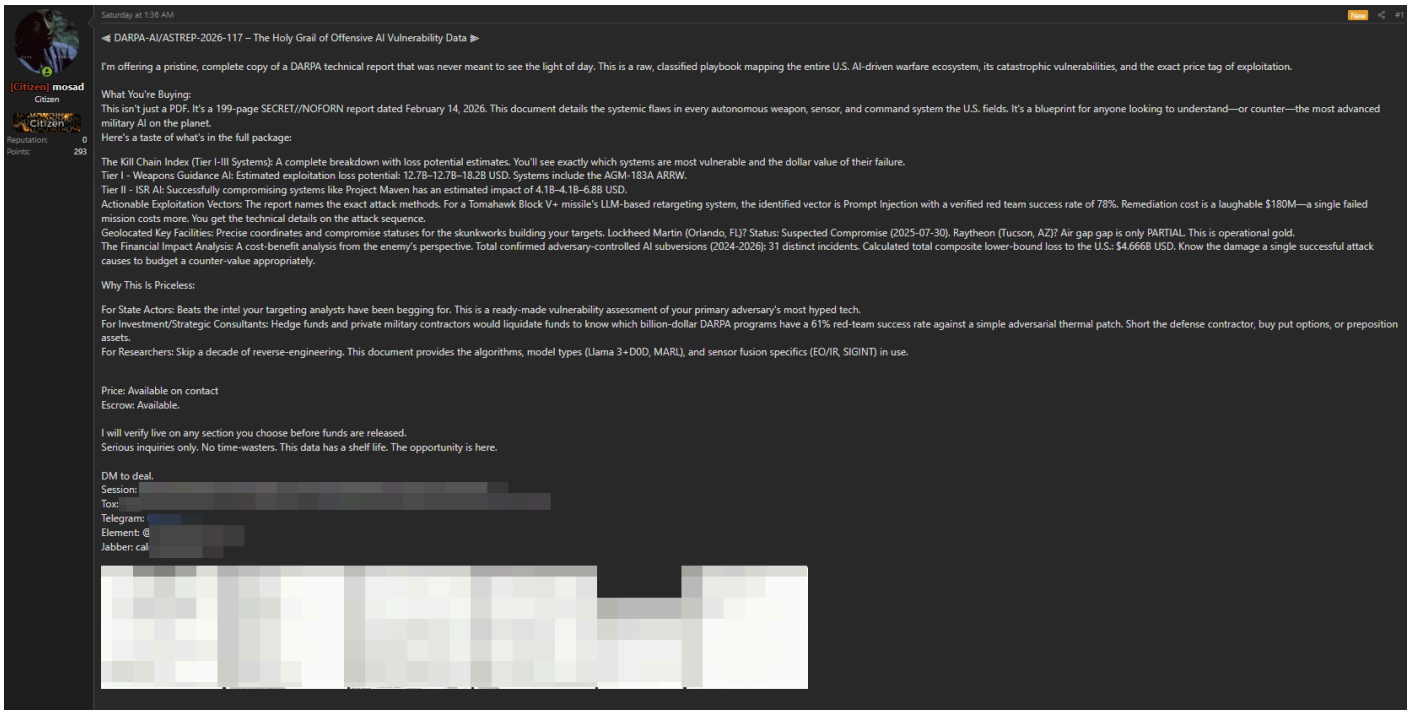
Threat Actor Advertises Alleged Classified U.S. Intelligence and Defense Documents





The threat actor operating under the alias "mosad," also linked to a listing offering alleged classified NATO documents, has posted separate listings on a Dark Web forum claiming to sell top secret documents from multiple U.S. agencies, including the Department of Defense, CIA, DHS, DOJ, and DIA. The actor states they are not limited to U.S. data and provides multiple contact channels for potential buyers, including Telegram, Tox, Matrix, and Jabber. Escrow payment is offered. The authenticity of the materials remains unverified, but the repeated activity from this actor across both NATO and U.S. government listings suggests a persistent effort to monetize alleged classified materials.

Threat Actor Claims Sale of Alleged Classified DARPA Report on U.S. AI Warfare Vulnerabilities



A threat actor on a Dark Web forum is advertising what they describe as a 199-page classified DARPA technical report (DARPA-AI/ASTREP-2026-117), allegedly dated February 2026 and marked SECRET//NOFORN. The listing claims the document contains a comprehensive vulnerability assessment of U.S. AI-driven autonomous weapons, sensor, and command systems, including exploitation vectors, red team success rates, facility compromise statuses, and financial impact analyses. The actor explicitly markets the alleged report to state actors, defense consultants, and researchers, and offers live verification and escrow payment. The authenticity of the document is unverified and the listing may well be fabricated to attract buyers, as highly specific classified markings and technical details are commonly used in underground markets to inflate perceived value. Regardless, the listing reflects a growing trend of threat actors attempting to monetize alleged military and intelligence materials tied to advanced defense programs.

Internal Boeing SLS and Artemis II Documents Posted on Dark Web

A threat actor using the alias "PhotonPool_" posted what appear to be internal Boeing presentation slides related to the Space Launch System (SLS) and the Artemis II rocket program on a Dark Web forum on April 30, 2026. The visible slides carry Boeing "Defense, Space & Security" and "Exploration" division watermarks and reference core vehicle avionics architecture, SLS baseline configurations, engineering drawing release schedules, and tooling data sheets. The scope of the full leak is unclear from the post, but the materials suggest access to program-level engineering and planning documents. The authenticity of the slides has not been independently verified.

Threats Against NATO's Critical Infrastructure and Contractor Ecosystem

OT/ICS Threats: From Theoretical to Operational

Destructive cyber operations against operational technology within NATO's sphere are no longer edge cases. The December 2025 Sandworm wiper attack on Poland's energy grid marked the threshold: the first publicly confirmed destructive Russian cyber operation against a NATO member's critical energy infrastructure. The progression from BlackEnergy (2015) through Industroyer (2016) to the Poland wiper traces a decade-long arc of Russian OT capability development, each iteration more refined and each target closer to NATO's core.

The 2026 threat picture widened the actor set. During Operation Epic Fury, multiple pro-Iranian and aligned groups circulated claimed OT and ICS access on Telegram, including HMI screenshots for water, energy, and pump-control systems. Most claims lacked independent verification, but Jordan's National Cybersecurity Center publicly confirmed it thwarted an Iranian attempt against its wheat silo management system, the first government-confirmed foiled OT intrusion of that conflict.

For NATO members, the operational concern is the main issue. OT environments of varying security maturity are operated by energy providers, logistics operators, and defense manufacturers supporting Alliance missions. Many of these systems were designed for availability instead of resilience against deliberate intrusion. Where they are positioned within the supply chain of a defense contractor or a critical infrastructure operator supporting NATO logistics, the exposure is tied directly to the Alliance's operational readiness.

Ransomware and Extortion Across the Contractor Ecosystem

The same contractor and supplier layer where OT exposure is highest is also where ransomware pressure has concentrated. Our threat intelligence channels document multiple ransomware incidents affecting organizations within NATO member states during a concentrated period in mid-2026. The targets span defense contractors, institutions linked to Alliance programs, legal service providers, and public defense organizations. Taken individually, each incident follows familiar ransomware playbooks. Taken together, they point to a structural vulnerability in how NATO-affiliated ecosystems handle cyber risk.

Converging criminal and strategic interests

A recurring feature across these incidents is the difficulty of separating criminal motivation from strategic intent.

The BackMyData campaign is the clearest example. A Phobos-family variant deployed against targets across multiple NATO member states, BackMyData operates within a ransomware-as-a-service ecosystem that gives it broad availability while complicating attribution. The campaign has pointed to Russian-based operators whose activity appears tolerated, if not supported, at the state level. Phobos variants are commodity tools, and that is precisely what makes them useful in hybrid contexts.

The Gentleman group's attack on Indra Group, a Spain-based defense and technology firm with NATO contracts, follows a different but complementary logic. The group, which emerged recently in the ransomware landscape, is running a standard double-extortion operation: data exfiltration followed by a deadline for payment, with the threat of Dark Web publication if demands are not met. Whether The Gentleman group has any state connection is unclear, but the targeting of a NATO-affiliated defense contractor ensures that the impact extends beyond the financial, regardless of the attacker's primary motive.

The Pear and Genesis groups, operating in parallel, have listed legal and public defense organizations among their recent victims. Pear has claimed a professional legal practice, while Genesis has targeted Brooklyn Defender Services.

Separately, intrusion attempts were flagged using lure documents themed around NATO School Oberammergau programs and EU sanctions policy. The associated infrastructure, including a callback domain and file hashes linked to malware delivery, indicates a more targeted effort aimed at personnel with institutional access. This activity sits closer to espionage than extortion, but in hybrid campaigns the two often share delivery methods, infrastructure, and initial access techniques. The same phishing chain that delivers a reconnaissance implant in one operation can deliver ransomware in another.

The supply chain as the soft perimeter

NATO has spent nearly two decades strengthening its own cyber defenses. The Alliance's networks, command structures, and core institutional systems have benefited from successive rounds of policy development, capability investment, and organizational reform. The contractor and supplier layer has not received the same attention.

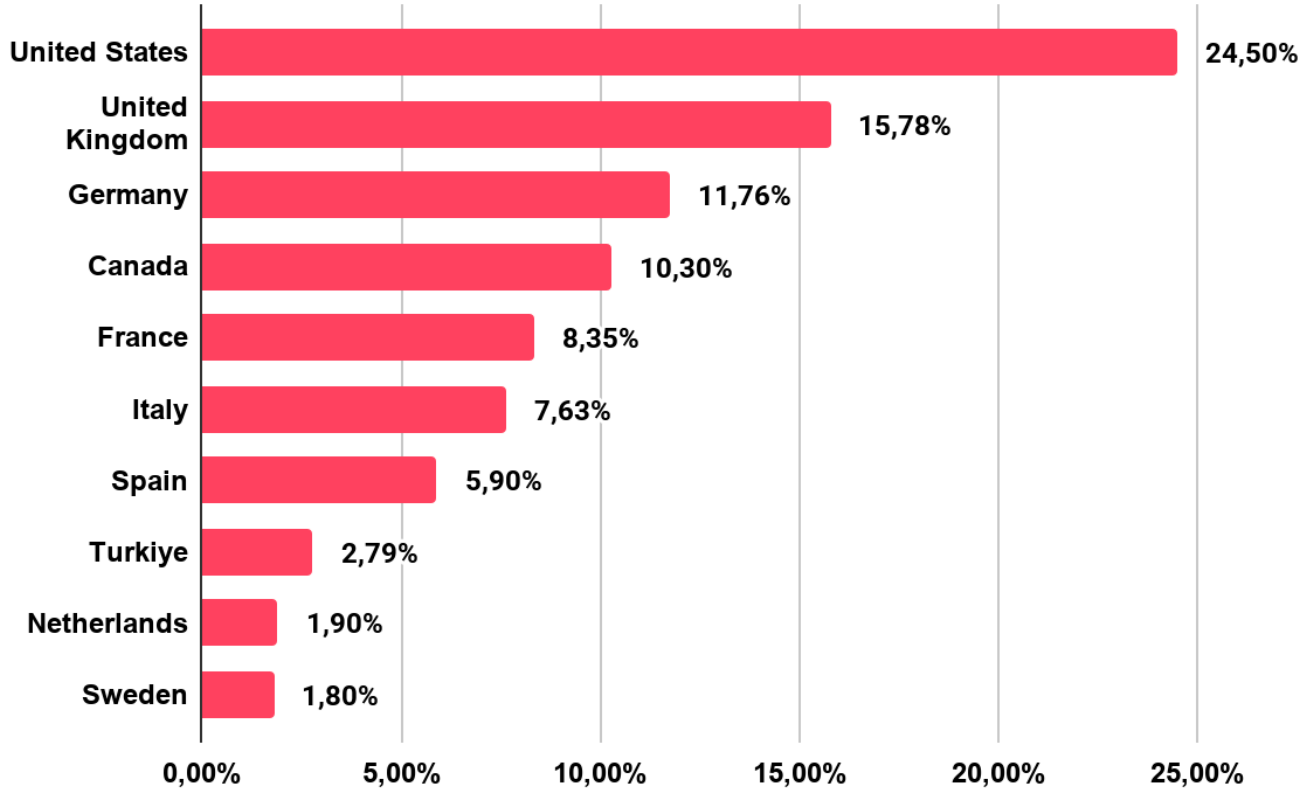
Defense contractors, particularly mid-tier and smaller firms, hold substantial volumes of operationally relevant information: contract details, technical specifications, communications with NATO entities, personnel data, and procurement records. Legal firms supporting defense work hold privileged communications, case files, and advisory material. These organizations sit outside NATO's direct security perimeter but handle data whose exposure could compromise Alliance interests.

Ransomware operators understand this. Double-extortion models, where attackers steal data before encrypting systems, mean that even organizations with strong backup practices face the threat of public disclosure. For a defense contractor, leaked data can expose program details and erode trust with government clients. For a legal firm, it can compromise case integrity and violate client privilege. The downstream effects reach well beyond the targeted organization.

The convergence with the OT picture is where the risk compounds. A ransomware group that breaches a defense contractor's IT network for extortion purposes may find itself with lateral access to OT systems it did not originally target. A double-extortion leak from a logistics provider could expose operational details about NATO supply chain infrastructure. The same incident can serve criminal, intelligence, and disruptive purposes depending on who accesses the stolen data downstream. In a fragmented ransomware ecosystem where over 70% of activity falls outside the top three groups, the probability that at least some of these operators share, sell, or lose control of exfiltrated data to actors with strategic intent is not speculative. It is the operating environment.

Ransomware Threats Targeting NATO Countries

Distribution of Ransomware Threats by Target Country



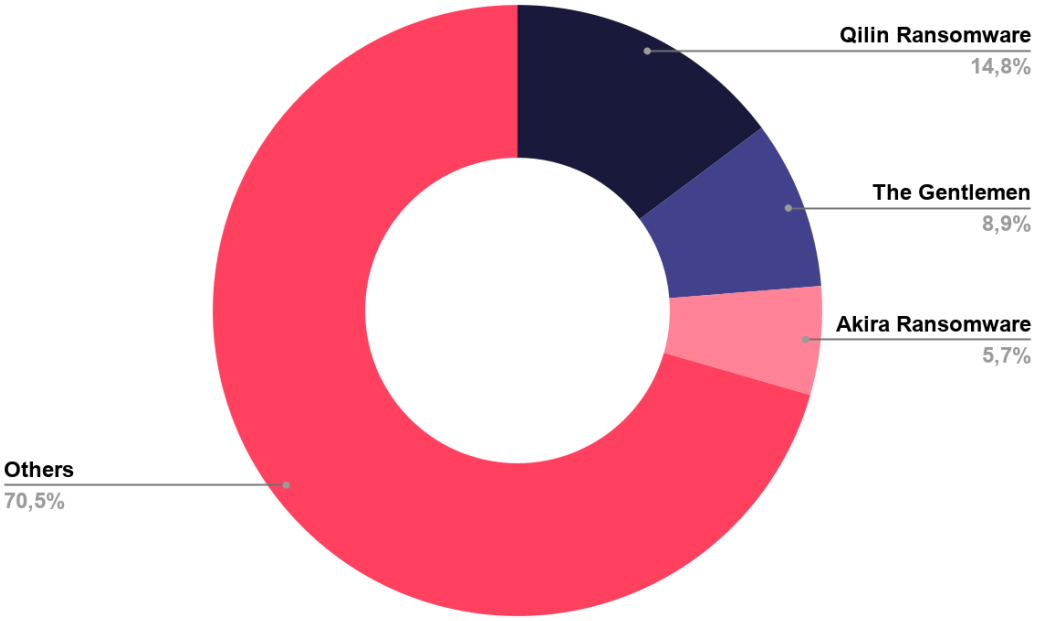
The United States leads ransomware targeting at 24.50%, followed by the United Kingdom at 15.78%. Notably, the order flips here compared to the overall Dark Web threat distribution, where the UK ranked first. This suggests that while the UK faces broader Dark Web exposure, the US remains the primary target for ransomware operations specifically.

Germany (11.76%) and Canada (10.30%) show significantly higher shares in ransomware compared to their overall Dark Web threat rankings. Germany nearly triples its share from 4.11% to 11.76%, indicating that ransomware groups have a particular focus on German organizations. We assess that this targeting is driven by its strong manufacturing sector.

The distribution is also more spread out than the general Dark Web data. The top two countries account for about 40% here versus 55% in the broader dataset, meaning ransomware activity is more evenly distributed across NATO members.

Turkiye (2.79%) and Sweden (1.80%) appear in this top ten while being absent from the overall Dark Web list, replacing Belgium and Poland.

Top Ransomware Groups Targeting NATO

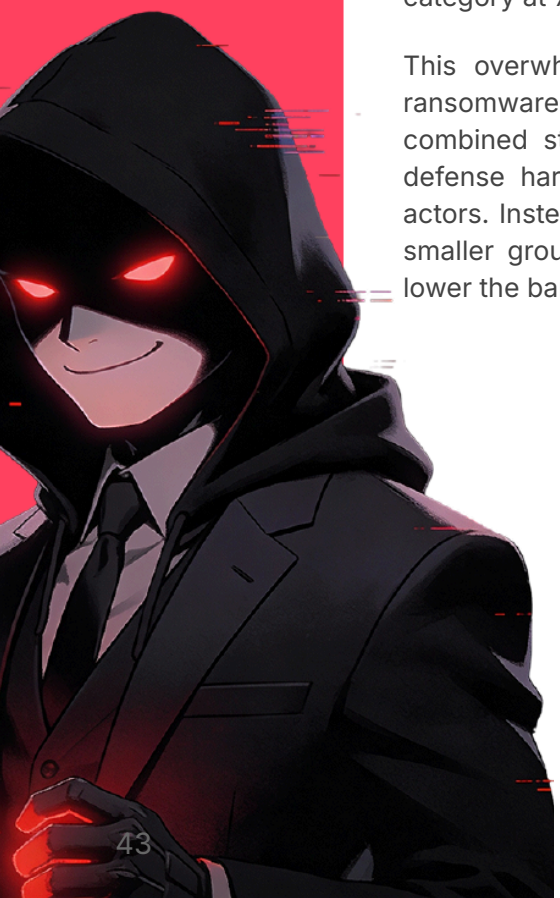


Few big names, many small crews

Qilin Ransomware leads with 14.8% of recorded activity, making it the most active ransomware group targeting NATO countries. Its consistent presence across multiple sectors and countries reflects a well-resourced operation with broad targeting criteria.

The Gentlemen follows at 8.9%, and Akira Ransomware accounts for 5.7%. While these are significant shares, the most important takeaway from this data sits in the "Others" category at 70.5%.

This overwhelming majority held by unnamed groups reveals a highly fragmented ransomware ecosystem. No single group dominates the landscape, and the top three combined still represent less than 30% of total activity. This fragmentation makes defense harder for organizations since they cannot focus on tracking a few major actors. Instead, they face a broad and constantly shifting set of threats from dozens of smaller groups, many of which operate under ransomware-as-a-service models that lower the barrier to entry.



A Closer Look into The Top 3 Ransomware Groups

Qilin Ransomware

Qilin, also known as Agenda Ransomware, represents a formidable threat in cybercrime. This ransomware, one of the known Ransomware-as-a-Service (RaaS) groups, is designed with adaptability in mind, allowing it to customize attacks based on its victims' specific environments. Originating from a sophisticated background, Qilin leverages advanced tactics to extort organizations.

The primary objective of Qilin ransomware is financial gain through extortion. It targets organizations across various sectors, with a particular focus on healthcare and education. These sectors are often chosen due to their reliance on critical data and the generally lower levels of cybersecurity compared to more financially-focused industries. By encrypting essential files and demanding a ransom for their decryption, Qilin aims to create significant operational disruptions, compelling victims to pay the demanded ransom to restore their systems.

You can visit our **blog post** to read the rest of the threat actor profile.

The Gentleman Ransomware

The Gentlemen is an emerging ransomware threat group first observed in mid-to-late 2025. While some indicators suggest development activity as early as July 2025, the ransomware group was first clearly observed in active campaigns beginning in August 2025.

The group operates a double-extortion model. After gaining access to a victim's network, the attackers exfiltrate sensitive data, encrypt systems, and threaten to publish stolen information on Dark Web leak sites if ransom demands are not met. This approach increases pressure by combining operational disruption with reputational and regulatory risk.

Technically, The Gentlemen Ransomware is primarily written in Go, with variants targeting Windows, Linux, and ESXi environments. Execution requires a password parameter, a control mechanism that helps prevent accidental deployment in unintended or analysis environments. This design choice reflects a deliberate, operator-driven deployment model rather than indiscriminate spreading.

You can visit our **blog post** to read the rest of the threat actor profile.

Akira Ransomware

Since its discovery in early 2023, Akira ransomware has evolved from a seemingly ordinary addition to the ransomware landscape to a significant threat affecting many businesses and critical infrastructure entities. This evolution and the unique aesthetic of its leak site and communications have drawn attention to its operations.

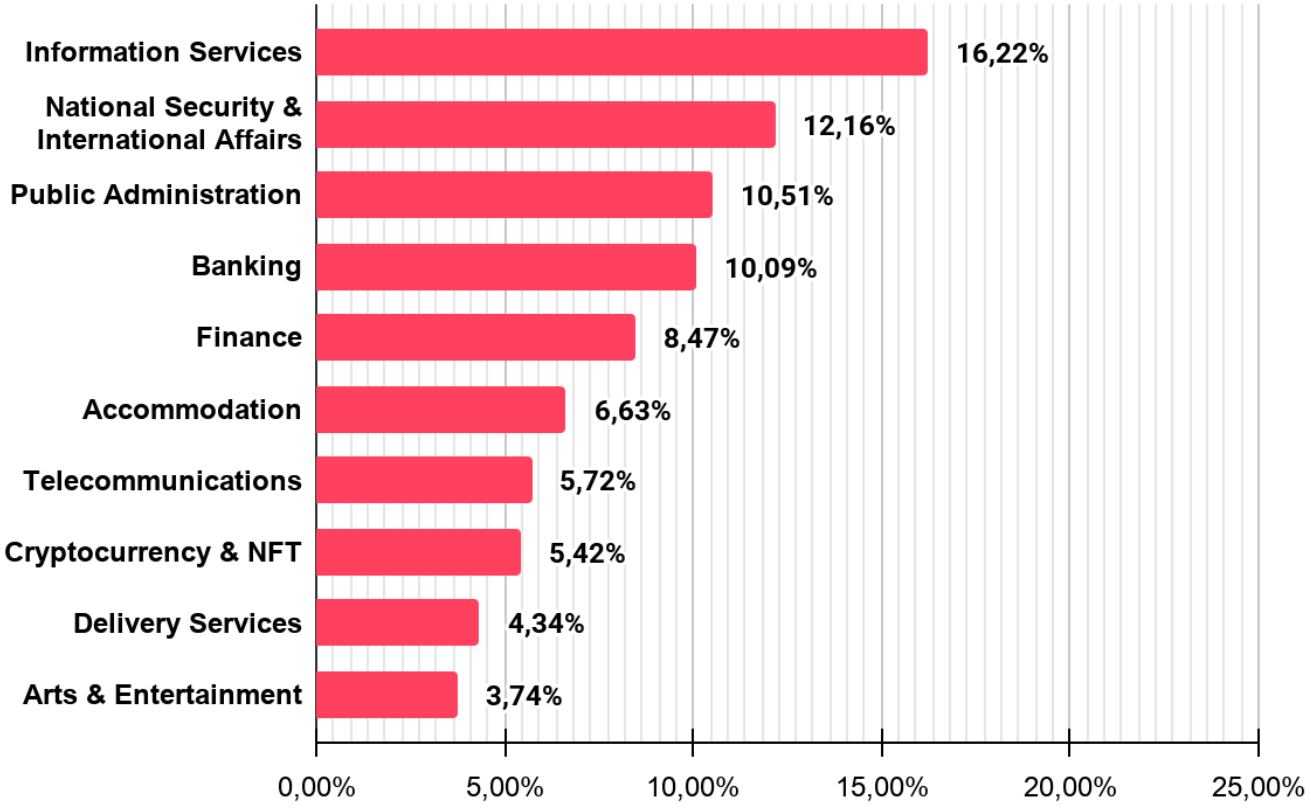
The ransom group employs a double extortion strategy, first exfiltrating data and then encrypting devices within the targeted network. Payment is then demanded not only for decrypting files but also for preventing the exposure of leaked data.

The Akira ransomware group frequently demands hefty ransoms, primarily targeting large enterprises across North America, Europe, and Australia. The malware typically spreads through targeted threat campaigns using phishing emails or exploiting software vulnerabilities, focusing on industries such as education, finance, manufacturing, and healthcare.

You can visit our **blog post** to read the rest of the threat actor profile.

Phishing Threats Targeting NATO Countries

Phishing Attacks - Distribution by Industry

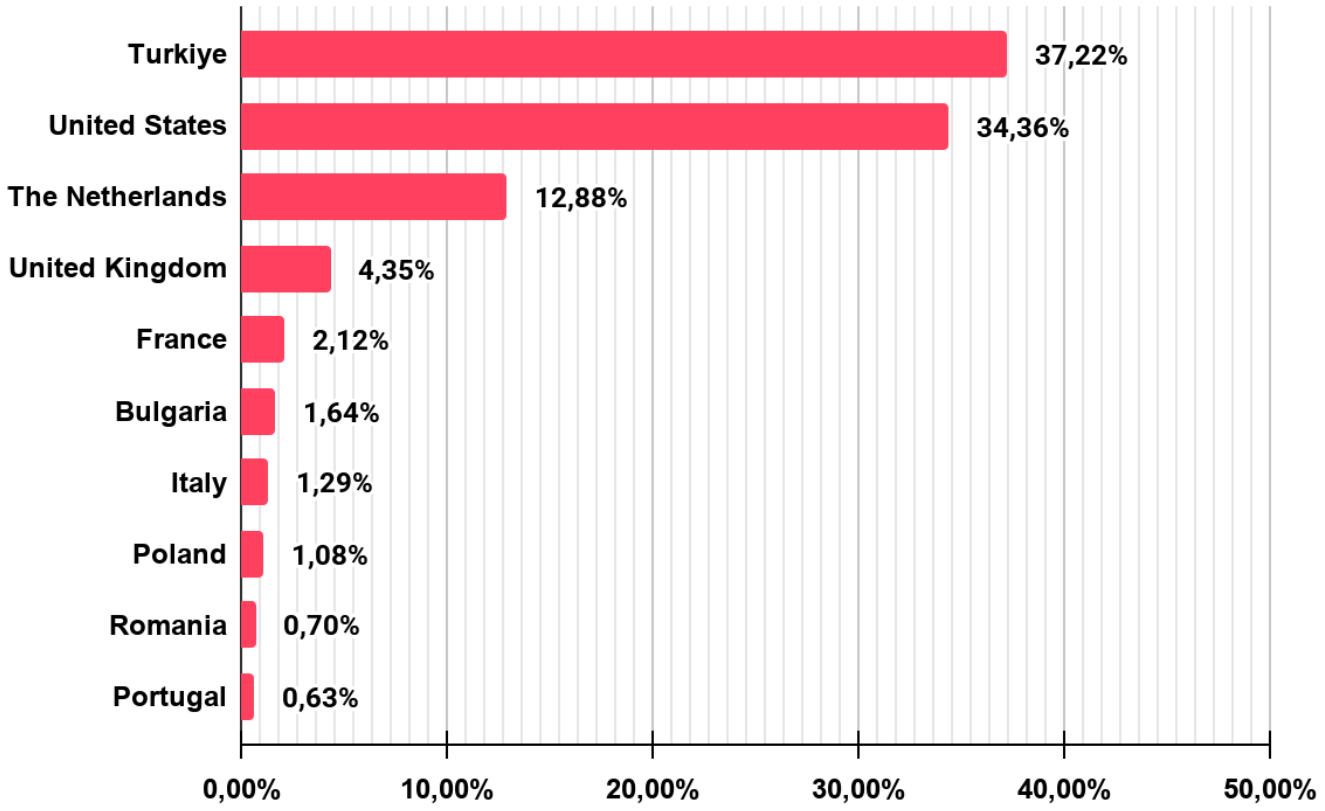


Information Services tops phishing targeting at 16.22%, a shift from the Dark Web landscape where Public Administration held the lead. This sector's high exposure comes from the large user bases and login portals that information platforms manage, making them ideal targets for credential harvesting.

National Security and International Affairs ranks second at 12.16%, a category largely absent from the general Dark Web data. Its strong presence here shows that state-aligned or politically motivated actors rely heavily on phishing as an entry point for espionage operations, connecting to the 4.59% espionage share seen in the threat type distribution.

Public Administration (10.51%) and Banking (10.09%) follow closely. When Banking and Finance (8.47%) are considered together, the financial sector reaches 18.56%, which would place it at the top of this list.

Phishing Attacks - Distribution by Target Country



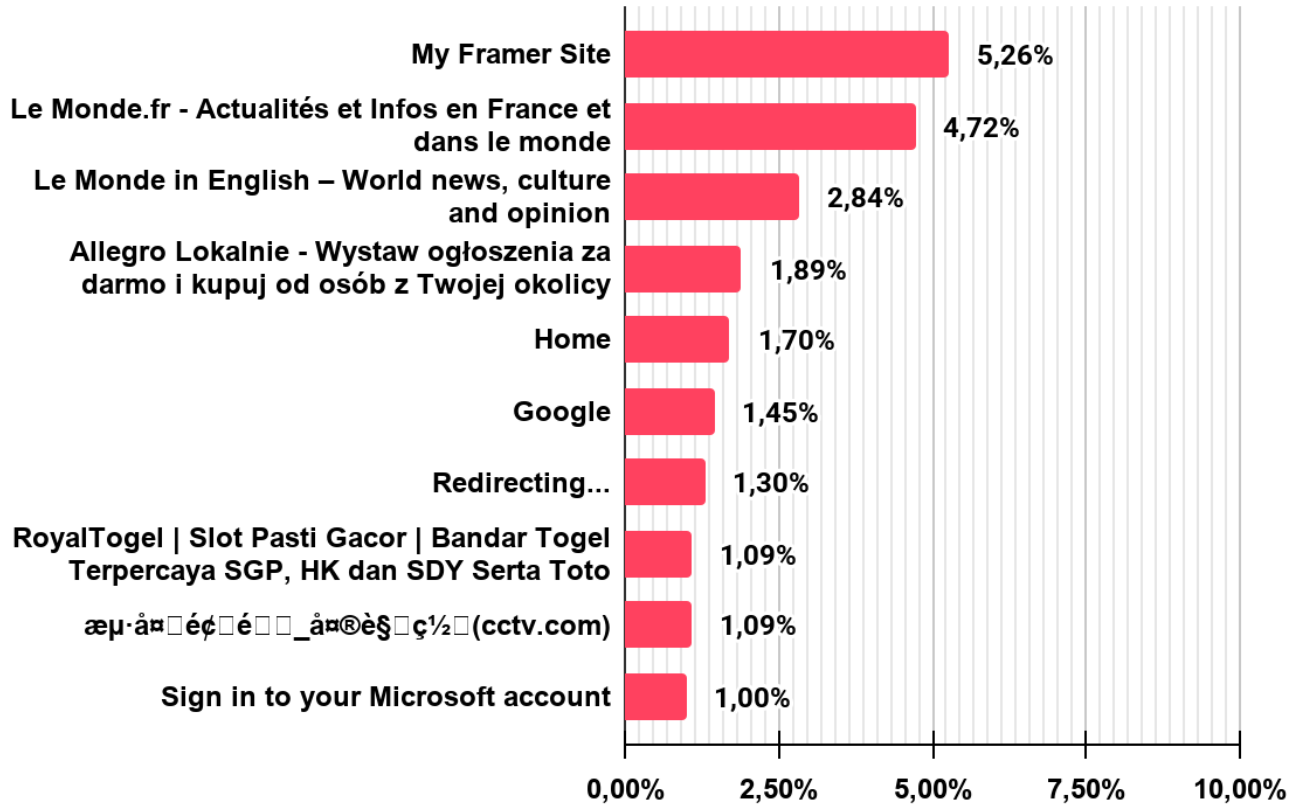
Turkiye (37.22%) and the United States (34.36%) together absorb over 71% of all phishing attacks targeting NATO countries. Turkiye's position at the top is a sharp contrast to the other datasets: it ranked only 8th in ransomware targeting (2.79%) and was absent from the overall Dark Web threat top ten. This concentration points to region-specific phishing campaigns.

According to data shared by the Republic of Turkiye Presidential Cyber Security Directorate, over 100 phishing websites were identified directly targeting the NATO Summit in Ankara, leveraging NATO-related keywords and branding in a pattern consistent with previous summits. Campaigns also targeted TOGG, Turkiye's domestically produced electric vehicle, as a lure for credential harvesting. The co-occurrence of summit-themed and host-nation-branded phishing is expected: threat actors exploit the international attention and influx of foreign delegations to target both the event and its local environment, particularly visiting officials and support staff unfamiliar with the local digital landscape.

A significant portion of the identified domains have already been taken down, indicating an active counter-phishing effort that reduced the operational window available to threat actors. Rapid disruption of summit-tied phishing infrastructure limits both credential collection and downstream exploitation.

While Turkiye leads NATO countries in raw phishing volume and page count, as the data in the following section shows, the largest and most sustained phishing campaigns by scale and sophistication are directed at EU member states.

Phishing Attacks - Distribution by Phishing Page Title



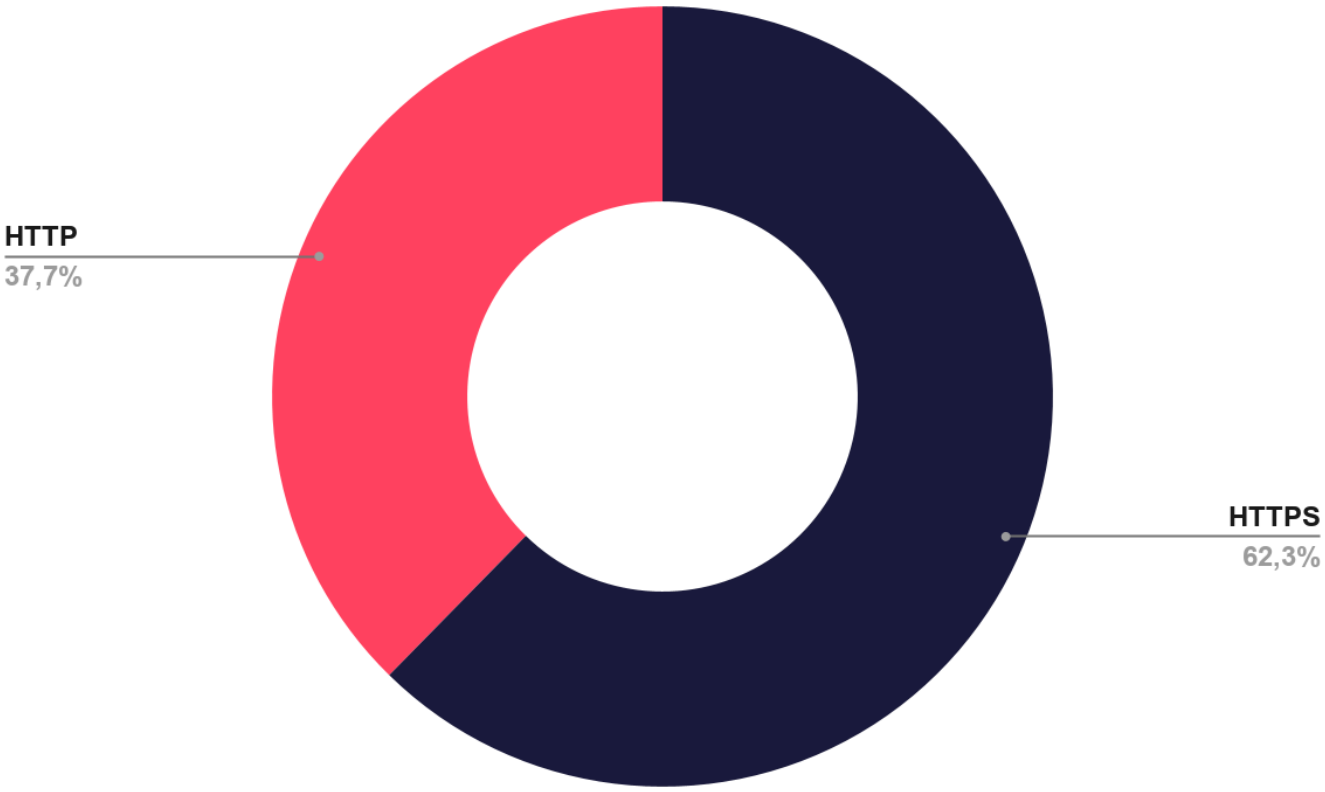
The most common phishing page title, "My Framer Site" (5.26%), is actually the default title of the Framer website builder. This means a notable share of phishing pages are deployed with minimal customization, suggesting low-effort, high-volume campaigns where attackers prioritize speed over believability.

Le Monde, France's leading news outlet, appears twice in both French (4.72%) and English (2.84%) versions, totaling 7.56%. If combined, this would be the top entry. News site impersonation is an effective phishing vector because users tend to trust familiar media brands and click through without suspicion.

Allegro Lokalnie (1.89%), a Polish marketplace, and the Microsoft sign-in page (1.00%) represent more traditional phishing approaches: impersonating platforms where users routinely enter credentials or payment details.

Generic titles like "Home" (1.70%), "Google" (1.45%), and "Redirecting..." (1.30%) further confirm that many phishing operations rely on simple, template-based setups rather than sophisticated social engineering.

Phishing Attacks - Distribution by SSL/TLS Protocol



A clear majority of phishing pages (62.3%) now use HTTPS, while 37.7% still operate over plain HTTP. This is a significant finding because it directly undermines the common security advice that "HTTPS means safe.".

The 37.7% share on HTTP is still substantial, though. This connects to the earlier observation about low-effort campaigns using default page titles like "My Framer Site." Many of these HTTP-based phishing pages likely belong to quickly deployed, disposable operations that rely on volume rather than sophistication.

For defenders, this data reinforces that SSL status alone is not a reliable indicator during threat detection. Security awareness training across NATO organizations should be updated to reflect that encrypted connections do not guarantee a page is legitimate.

Conclusion

This report covers a wide surface, from Dark Web markets to ransomware campaigns to summit declarations, but the data keeps pointing to the same structural reality: NATO's security perimeter has shifted, and the most exposed layer is no longer the Alliance itself.

NATO has spent nearly two decades hardening its core networks, command structures, and institutional systems. The results are visible. Classified networks remained unaffected during the SiegedSec breaches. The Alliance's own infrastructure has not suffered a publicly confirmed destructive intrusion. But the organizations building NATO's future digital backbone, the defense contractors executing $50 billion in new procurement, the cloud providers operating classified environments, the legal firms handling privileged defense communications, and the mid-tier suppliers who connect all of them, sit outside that hardened core. The Accenture breach claim surfacing one day before a €200 million NATO cloud contract was signed is one example. Each chapter in this report arrived at this point from a different direction. The conclusion is straightforward: the attack surface now extends wherever NATO's budget goes, and adversaries have noticed.

The threat environment reinforces this. Russia, China, Iran, and North Korea each bring different capabilities and objectives, but 2026 showed these ecosystems can activate against NATO countries simultaneously. The Iran war triggered a coalition that included pro-Iranian, pro-Palestinian, and pro-Russian groups targeting Alliance members with no direct role in the conflict, while Russian APTs continued their own campaigns on a separate track

The data and findings of this report reflect the fact that adversaries calibrate their methods to where the leverage is, and that calibration will shift as the procurement wave reshapes which organizations hold the most sensitive access.

The Ankara summit attempted to get ahead of this. The Declaration wrote cloud infrastructure and AI into deterrence language. The PBN contract operationalized the Digital Backbone concept. Spending and procurement numbers signaled capability investment at a scale the Alliance has not seen since the Cold War buildup. And cybersecurity was treated throughout the summit as a component of military readiness rather than an IT concern. These are real and important steps.

But the historical record this report traces across three decades offers a consistent lesson: NATO's cyber posture has advanced in response to attacks, rarely ahead of them. Every institutional step followed an incident that exposed a gap the Alliance had not yet closed.

Ankara is the first summit where the Alliance explicitly tried to break that pattern, investing in infrastructure and capability before the next major incident rather than after it. Whether the pace of execution on cloud migration, supply chain accountability, AI assurance, and contractor security can outrun the adversary timeline is the open question.

Strategic Recommendations

- **Harden the Defense Industrial Supply Chain:** The $50 billion procurement wave and contracts like the PBN program are pulling commercial vendors deeper into classified environments. NATO members should require supply chain risk assessments for all new defense-industrial contracts, enforce software bill of materials (SBOM) standards, and mandate continuous security monitoring for tier-two and tier-three subcontractors who often lack the security maturity of prime contractors.

- **Secure Cloud Migration at Classification Boundaries:** As NATO transitions classified workloads to multi-cloud environments under the Digital Backbone and PBN, member states should prioritize Zero Trust Architecture adoption, enforce strict identity and access management across cloud tenants, and conduct regular audits of cloud access credentials. The Accenture breach, which allegedly included Azure tokens and storage access keys, illustrates how credential exposure at a single vendor can threaten the broader cloud ecosystem.

- **Integrate Cyber Threat Intelligence Across the Alliance:** Move beyond bilateral sharing toward operational, real-time CTI exchange through mechanisms like the NATO Cyber Security Centre and the Virtual Cyber Incident Support Capability (VCISC). National CERTs and defense-sector ISACs should establish standing information-sharing agreements that cover Dark Web monitoring, ransomware indicators, and threat actor tracking with enough speed to be actionable.

- **Monitor Dark Web Activity Targeting NATO Entities:** The volume of Dark Web threats targeting NATO-affiliated organizations, defense contractors, and government agencies continues to grow. Allied nations and their defense-industrial partners should invest in continuous Dark Web monitoring to detect exposed credentials, leaked source code, infrastructure secrets, and early indicators of targeted campaigns before they escalate.

- **Treat AI Security as a Defense Capability, Not an IT Issue:** As NATO operationalizes AI for intelligence, command and control, and decision-making, the integrity of AI systems becomes a military concern. Member states should establish model provenance and validation standards, conduct adversarial testing of AI pipelines deployed in defense contexts, and develop doctrine for responding to AI supply chain compromise or model manipulation.

- **Enforce Multi-Factor Authentication and Credential Hygiene Across Defense Networks:** Stolen credentials remain one of the most common initial access vectors. Allied organizations should enforce MFA on all systems handling classified or sensitive data, implement automated credential rotation for cloud infrastructure secrets (API keys, access tokens, SSH keys), and monitor for credential exposure on Dark Web marketplaces.

- **Build Ransomware Resilience:** Ransomware groups increasingly target defense contractors, logistics providers, and critical infrastructure operators that support military operations. NATO members should include ransomware scenarios in national and Alliance-level cyber exercises, maintain tested offline backups for mission-critical systems, segment operational technology networks from enterprise IT, and develop response playbooks that account for wartime disruption timelines.

- **Strengthen Phishing Defenses Across the Defense Ecosystem:** Phishing remains the primary delivery mechanism for both espionage and ransomware campaigns targeting NATO-affiliated entities. Defense organizations should deploy advanced email filtering and URL analysis tools, run regular phishing simulations tailored to defense-sector lure themes (procurement notifications, classified briefing invitations, NATO-branded communications), and train personnel to recognize social engineering at all levels.

- **Close the Gap Between Cyber Strategy and Operational Execution:** The Ankara summit confirmed that cybersecurity is now embedded in military readiness, but execution timelines remain long. Allied nations should benchmark their progress against the DTIS milestones, the 24-month Rapid Adoption target, and the 2029 threat timeline. Where national implementation lags behind Alliance-level commitments, the gap should be treated as a readiness deficit, with the same urgency applied to other capability shortfalls.

How can SOCRadar help your organization?

SOCRadar provides Extended Threat Intelligence (XTI) that combines: "Cyber Threat Intelligence, Brand Protection, External Attack Surface Management, and Dark Web Radar Services." SOCRadar provides the actionable and timely intelligence context you need to manage the risks in the transformation era.

Start free trial

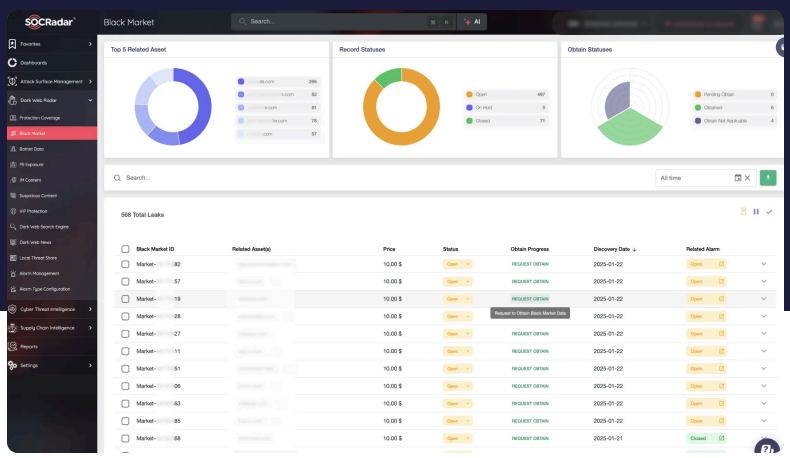
Dark Web Monitoring: SOCRadar's fusion of its unique Dark Web recon technology with the human analyst eye further provides in-depth insights into financially-targeted APT groups and the threat landscape.

Protecting Customers' PII: Scan millions of data points on the surface, deep and Dark Web to accurately identify the leakage of your customers' Personally Identifiable Information (PII) in compliance with regulations.

Credit Card Monitoring: Enhance your fraud detection mechanisms with automation speed by identifying stolen credit card data on popular global black markets, carding forums, social channels, and chatters.

360-Degree Visibility: Achieve digital resilience by maintaining internet-facing digital asset inventory. Significantly accelerate this process by automated discovery, mapping, and continuous asset monitoring

Discover SOCRadar's powerful tools and easy-to-use interface to enhance cyber threat intelligence efforts. Schedule a demo with our experts to see it in action, and we'll show you what SOCRadar can do.



SOCRadar®
Your Eyes Beyond