CROWDSTRIKE

2025 EUROPEAN THREAT LANDSCAPE REPORT

Table of Contents

Executive Overview

The CrowdStrike 2025 European Threat Landscape Report provides key insights into observed cyber activity and related geopolitical developments across the region. It summarizes the nation-state, eCrime, and hacktivism threats impacting Europe to inform public and private sector stakeholders.

Europe is a primary target for eCrime adversaries, likely due to the relative profitability of Europe-based entities, the region's legal framework, and the political motivations of eCrime actors. While big game hunting (BGH) poses a persistent threat, Europe-based entities are also contending with evolving eCrime techniques, including campaigns leveraging voice phishing (vishing) and CAPTCHA lures. Adversaries both originating from and targeting Europe benefit from a highly organized and resilient underground ecosystem, accessible via English- and Russian-language clearnet and darknet forums. This ecosystem facilitates collaboration and accommodates enabling services that provide network access, ready-made malware, and violence as a service (VaaS).

Russia's full-scale invasion of Ukraine in February 2022 triggered a surge of targeted cyber intrusions focused on Ukrainian entities. Though Russia-nexus and Russia-aligned threat actors conducted most of these, DPRK-nexus adversaries have also conducted operations targeting Ukrainian entities. Beyond conflict-specific operations, Russia, Iran, the Democratic People's Republic of Korea (DPRK), China, Türkiye, Kazakhstan, and India persistently target European entities through cyber operations driven by motives including strategic intelligence collection, information operations (IO), intellectual property theft, and opportunistic financial gain.

Geopolitical events, including the ongoing Russia-Ukraine and Israel-Hamas conflicts, were the primary drivers of global hacktivist activity directed at European countries. This activity primarily consisted of distributed denial-of-service (DDoS) attacks, hack-and-leak campaigns, and website defacements.

This report offers an in-depth view of the European threat landscape based on CrowdStrike Intelligence reporting from January 2024 to September 2025. It is produced by the CrowdStrike Counter Adversary Operations team, which integrates two closely aligned groups: CrowdStrike Intelligence and CrowdStrike OverWatch. The CrowdStrike Intelligence team delivers actionable reporting that identifies new adversaries, tracks their activities, and monitors emerging cyber threats in real time. Leveraging this intelligence, the CrowdStrike OverWatch team conducts proactive threat hunting across customer telemetry to detect and address malicious activity before it escalates.

As Europe's cyber threat landscape continues to evolve, organizations must stay vigilant against a diverse array of adversaries, from cybercriminal groups to state-backed threat actors and hacktivists. With intelligence-driven security strategies, regional stakeholders can strengthen their defenses, mitigate risks, and stay ahead of emerging threats in an increasingly complex threat landscape.

NAMING CONVENTIONS

ADVERSARY	NATION-STATE OR CATEGORY
BEAR	RUSSIA
BUFFALO	VIETNAM
CHOLLIMA	DPRK (NORTH KOREA)
CRANE	ROK (REPUBLIC OF KOREA)
HAWK	SYRIA
JACKAL	HACKTIVIST
KITTEN	IRAN
LEOPARD	PAKISTAN
LYNX	GEORGIA
OCELOT	COLOMBIA
PANDA	PEOPLE'S REPUBLIC OF CHINA
SAIGA	KAZAKHSTAN
SPHINX	EGYPT
SPIDER	eCRIME
TIGER	INDIA
WOLF	TÜRKIYE

eCrime Overview

Big Game Hunting

Europe-based victims constitute nearly 22% of entities named on DLSs that CrowdStrike Intelligence tracks, making it the second most targeted region after North America. According to the dataset, entities in Europe are more than twice as likely to be targeted than entities in the Asia Pacific and Japan region. Europe-based entities are attractive targets for BGH adversaries, likely due to the following factors:

- **Legal pressures:** Threat actors have leveraged the EU's General Data Protection Regulation (GDPR) data breach penalties to pressure victims into paying ransoms; several threat actors have threatened to report entities for regulatory noncompliance via their DLS, in ransom notes, or during negotiations.
- **Lucrative targets:** Europe contains five of the world's 10 most valuable companies across France, Germany, the Netherlands, Switzerland, and the U.K. As BGH adversaries typically base their ransom demands on a victim organization's revenue, they likely perceive that European organizations can pay sizable ransoms.
- **Political motives:** Though BGH adversaries are predominantly financially motivated, some have expressed political stances and threatened politically motivated activity. WIZARD SPIDER, for example, supported the 2022 Russian invasion of Ukraine, and EU organizations such as Europol have also warned that eCrime threat actors and hybrid threat actors[1] are cooperating for mutual benefit.[2]

SINCE JANUARY 1, 2024, BGH THREAT ACTORS HAVE NAMED APPROXIMATELY 2,100 EUROPE-BASED VICTIMS ON MORE THAN 100 DATA EXTORTION AND RANSOMWARE DEDICATED LEAK SITES (DLSs).

1 Hybrid threat actors conduct activity supporting a combination of motivations, including eCrime, nation-state, hacktivist, and information operations.

2 https://www.europol.europa.eu/cms/sites/default/files/documents/EU-SOCTA-2025.pdf

According to DLS data, the U.K., Germany, Italy, France, and Spain were the most targeted European nations. These countries represent Europe's largest economies — excluding Russia, which is absent from the dataset (see the *Prohibitions on Targeting Entities in Russia and the CIS Region* section on page 12). Between January 2024 and September 2025, the most targeted sectors were manufacturing, professional services, technology, industrials and engineering, and retail. DLS entries naming Europe-based entities have increased nearly 13% year-over-year, from approximately 1,220 entries to 1,380 (Figure 1).

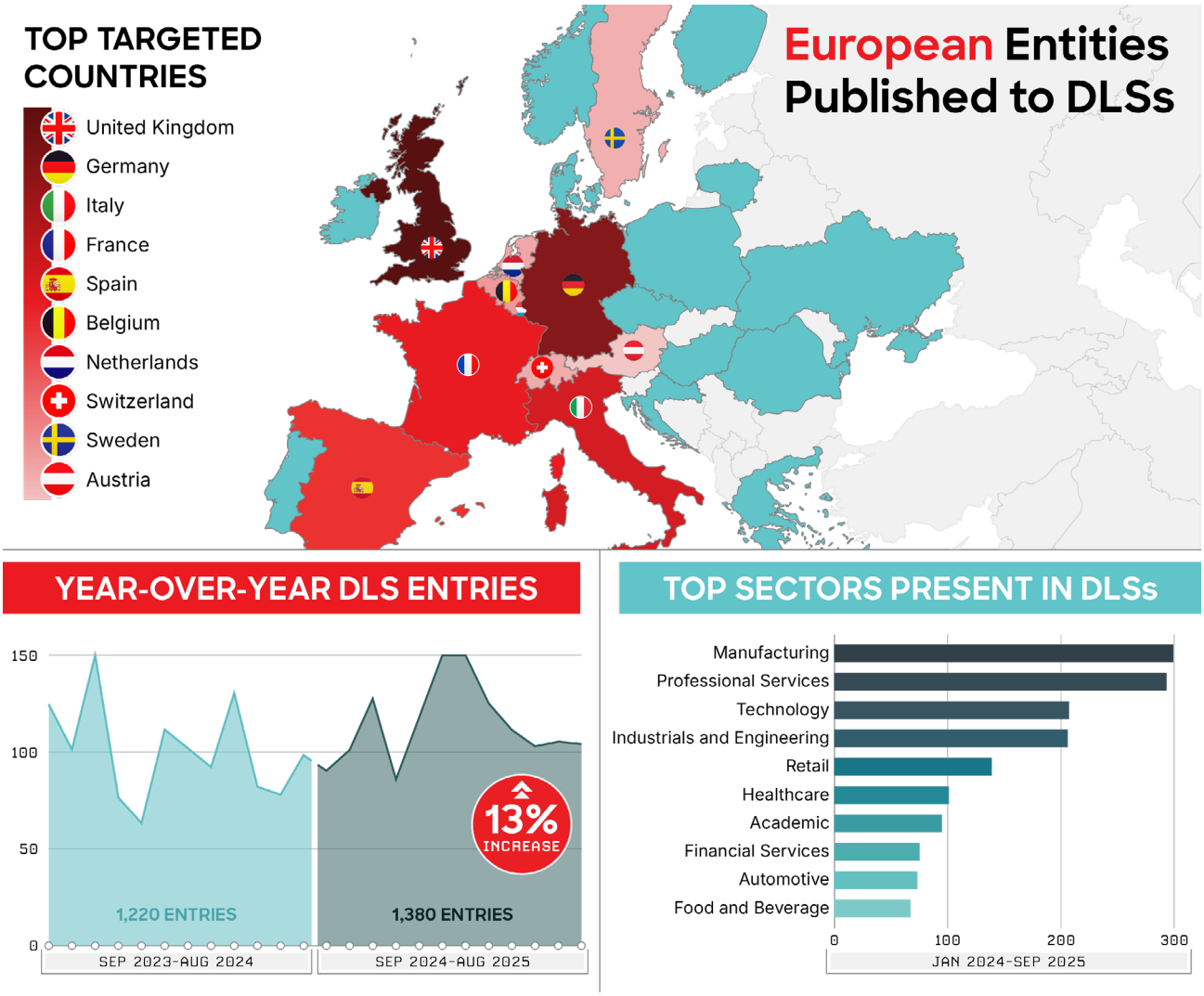


Figure 1. DLS entries by country, sector, and time period

Of those Europe-based victims, 92% were named on ransomware-associated DLSs (e.g., BITWISE SPIDER's *LockBit* DLS); typically, adversaries operating these DLSs use a combination of ransomware and data theft to extort victims. The remaining 8% of victims were named on DLSs belonging to adversaries that rely solely on data theft (e.g., GRACEFUL SPIDER's *Clop* DLS).

During the reporting period, BITWISE SPIDER, PUNK SPIDER, OCULAR SPIDER, TRAVELING SPIDER, and BRAIN SPIDER impacted the highest number of European victims (Figure 2). Also during this time frame, law enforcement operations severely impacted some of these adversaries' operations.

For example, BITWISE SPIDER affiliates' activity levels have significantly decreased following the multinational law enforcement effort Operation Cronos. Another multinational effort, Operation Phobos Aetor, seized BRAIN SPIDER's *8BASE* DLS and arrested four alleged *8BASE* ransomware operators. Additionally, OCULAR SPIDER closed their *RansomHub* ransomware as a service (RaaS) following conflicts between *RansomHub* affiliates and the *DragonForce* RaaS administrator.

However, prolific adversaries such as PUNK SPIDER, TRAVELING SPIDER, and unnamed threat actors — including *Qilin* RaaS affiliates — continue to pose a significant threat to European entities.

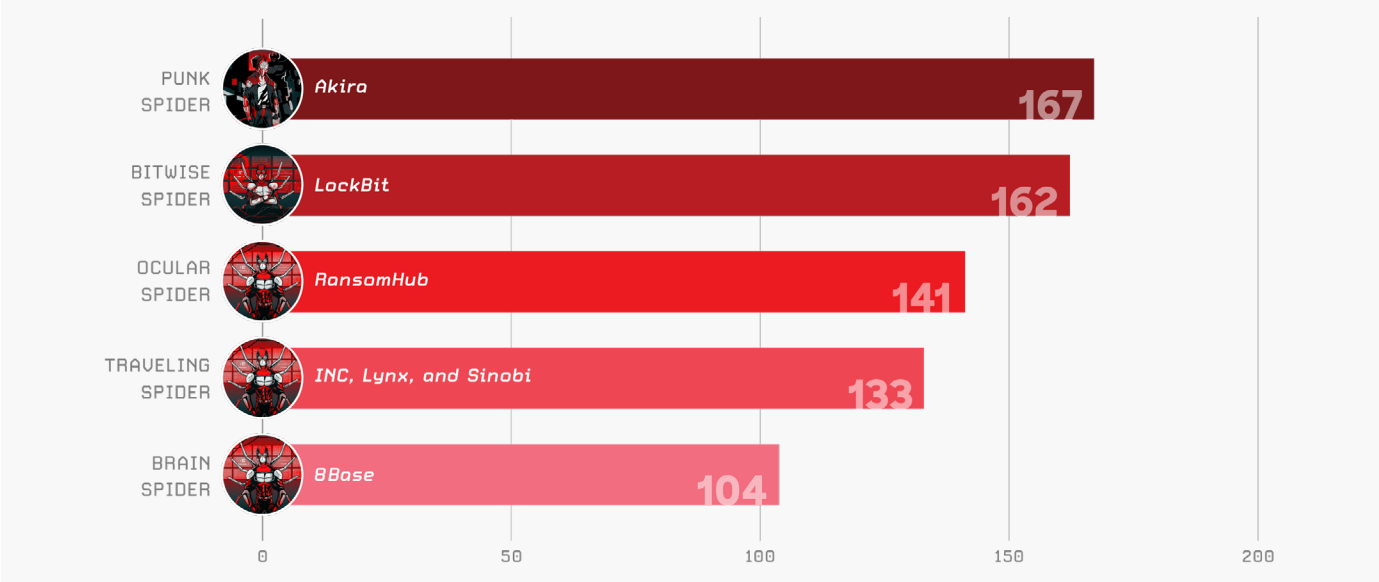


Figure 2. Dominant ransomware and extortion adversaries targeting European Entities, January 2024-September 2025

Regardless of where victims are located, BGH adversaries typically use the same tactics, techniques, and procedures (TTPs). During the reporting period, BGH actors heavily employed the following TTPs:

- Dumping credentials from backup and restore configuration databases, which often store credentials used to access hypervisor infrastructure
- Remotely encrypting files, executing ransomware — often from an unmanaged system[3] — and running the file encryption process outside of the targeted system
- Leveraging access to unmanaged systems to steal data and deploy ransomware
- Deploying Linux ransomware on VMware ESXi infrastructure

3 An unmanaged system is a system that does not feature any installed endpoint detection and response (EDR) software.

SCATTERED SPIDER Targets U.K. Retail Sector in 2025

Active since 2022, SCATTERED SPIDER has become one of the most aggressive and disruptive eCrime adversaries. SCATTERED SPIDER conducts a range of financially motivated activity, including cryptocurrency theft, SIM swapping, and extortion. Since 2023, the adversary has predominantly targeted high-value enterprise organizations in ransomware and data theft campaigns. SCATTERED SPIDER's intrusions are characterized by the sophisticated help desk vishing campaigns they use to gain initial access, their innovative cloud-conscious tradecraft, and — most especially — their speed.

Although SCATTERED SPIDER predominantly targets private sector companies based in North America, they have targeted entities in Finland, France, Germany, Luxembourg, Sweden, and the U.K. After a period of inactivity between December 2024 and March 2025, the adversary targeted numerous U.K.-based retail entities in April 2025 with the intent to deploy *DragonForce* ransomware.

The April 2025 activity included a possible attempted close-access operation in which a threat actor linked to the eCrime ecosystem often referred to as "The Com" — a primarily English-speaking online ecosystem comprising multiple interconnected subgroups — attempted to recruit individuals to visit the corporate headquarters of a U.K.-based retailer that reportedly sustained a SCATTERED SPIDER attack. According to the threat actor's instructions, individuals selected for the operation would need to obtain a "burner" Windows laptop, travel to the U.K.-based entity's corporate headquarters to connect to the onsite Wi-Fi, and provide remote access to the laptop via RDP. Whether the close-access operation occurred remains unconfirmed; however, the discussion of such a technique distinguishes Western eCrime threat actors from their Russian counterparts.

Unlike most prominent BGH adversaries, SCATTERED SPIDER operators are based in Western countries. CrowdStrike Intelligence has identified individual members based in both the U.S. and the U.K. In July 2025, the U.K. National Crime Agency announced the arrests of four individuals, aged between 17 and 20, in relation to recent incidents impacting U.K.-based retailers.[4] In September 2025, two of those individuals were arrested again and charged for their role in a 2024 incident impacting Transport for London.[5] These individuals were active from at least 2022 despite previous arrests, demonstrating the challenges of disrupting eCrime activity even when an adversary's personnel are within an authority's jurisdiction.

4 https://www.nationalcrimeagency.gov.uk/news/retail-cyber-attacks-nca-arrest-four-for-attacks-on-m-s-co-op-and-harrods

5 https://www.nationalcrimeagency.gov.uk/news/two-charged-for-tfl-cyber-attack

Dominant eCrime Techniques

VISHING LIKELY TO BECOME A SIGNIFICANT THREAT

Since 2024, eCrime adversaries have increasingly used vishing to gain initial access. Vishing is a type of social engineering technique in which an adversary calls a victim to encourage them to provide credentials or take action on their endpoint. Along with facilitating fraud, eCrime adversaries — including CURLY SPIDER and MUTANT SPIDER — have used vishing to gain initial access for ransomware groups (see the *Initial Access Brokers* section on page 14). Similarly, operators or affiliates of BGH adversaries ROYAL SPIDER, TUNNEL SPIDER, and WANDERING SPIDER have used vishing in their operations.

In late 2024, a user highly likely associated with MUTANT SPIDER posted on the Russian-language forum Exploit, claiming to prefer North America-based targets over those based in Europe because they were more likely to pay higher ransoms.

However, vishing will likely become a more significant threat to Europe-based entities. This assessment is made with moderate confidence based on the recent high-impact vishing incidents affecting entities in Europe (see the *SCATTERED SPIDER Targets U.K. Retail Sector in 2025* section on page 8) and because eCrime adversaries are increasingly leveraging native speakers of their target regions in their vishing campaigns. For example, PLUMP SPIDER has used native Brazilian Portuguese speakers to target Brazil-based entities, and a February 2025 vishing campaign likely employed German speakers to deliver TeamViewer and *SH RAT* to entities in Germany.

DURING THE REPORTING PERIOD, CROWDSTRIKE OVERWATCH AND THE CROWDSTRIKE FALCON® COMPLETE NEXT-GEN MDR TEAM OBSERVED NEARLY 1,000 VISHING-RELATED INCIDENTS GLOBALLY. MOST INCIDENTS IMPACTED NORTH AMERICA-BASED ENTITIES, LIKELY DUE TO THE UBIQUITY OF THE ENGLISH LANGUAGE AS WELL AS THE TARGETS' HIGHER REVENUE.

FAKE CAPTCHAs REMAIN A COMMON DELIVERY METHOD

Starting in mid-2024, eCrime adversaries have begun widely adopting CAPTCHA lures (aka *ClickFix*) to deliver malware. This social engineering technique involves using pages that imitate CAPTCHA authentication tests to convince victims to copy, paste, and execute malicious code into the Windows Run dialog box or terminal.

Identified campaigns used phishing emails, malicious advertising (malvertising), and search engine optimization (SEO) poisoning to direct targets to fake CAPTCHA pages. While campaigns leveraging CAPTCHA lures are often opportunistic, some eCrime threat actors tailor fake CAPTCHAs to their specific targets, such as hospitality and travel entities.

IN 2024 AND 2025, CROWDSTRIKE IDENTIFIED OVER 1,000 INCIDENTS IMPACTING EUROPE-BASED CUSTOMERS THAT INVOLVED CAPTCHA LURES (FIGURE 3).

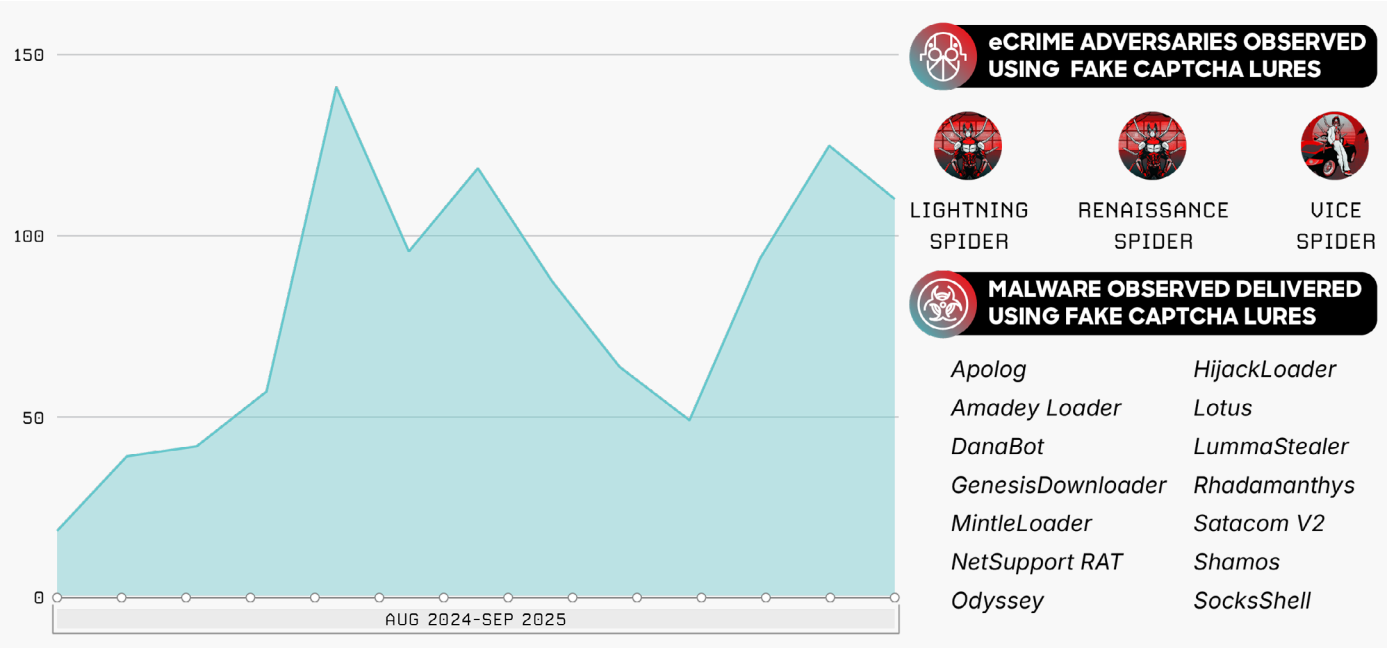


Figure 3. CAPTCHA lure-related incidents at Europe-based customers

eCrime services on the Russian-language eCrime forums Exploit and XSS have advertised several tools that can be used to create customizable or ready-made fake CAPTCHA pages for Windows, macOS, and Linux (see the *Underground Ecosystem* section on page 11). Advertised features included dynamically created code obfuscation, security bypass capabilities, and decoy functionalities (e.g., imitating cryptocurrency management platforms). These eCrime services make CAPTCHA lures readily available for a broad range of threat actors.

LIGHTNING SPIDER, RENAISSANCE SPIDER, and VICE SPIDER have all historically targeted Europe-based entities and used CAPTCHA lures in their campaigns. Additionally, unidentified eCrime threat actors have used CAPTCHA lures to deliver BRASH SPIDER's *Odyssey*, COOKIE SPIDER's *Shamos*, HAZARD SPIDER's *Amadey Loader*, LUNAR SPIDER's *Lotus*, SCULLY SPIDER's *DanaBot*, and *MintleLoader* (aka *MintsLoader*, *MintLoader*) in campaigns targeting Europe and other geographies.

Underground Ecosystem

Though law enforcement operations occasionally seize infrastructure and arrest administrators operating prominent Europe-based eCrime platforms, the European — and specifically the Russian-language — underground ecosystem remains robust. Numerous persistent and emerging forums, marketplaces, and Telegram channels support threat actors of varying sophistication by serving as hubs for collaboration, knowledge and tool sharing, and various eCrime enabling services.

RUSSIAN-LANGUAGE eCRIME FORUMS

For nearly three decades, eCrime threat actors have coalesced on Russian-language underground forums. Although these forums initially provided a platform for carding (i.e., the theft and sale of credit card details), the ecosystem quickly matured to include forums specializing in various eCrime services or monetization methods.[6]

The increasing number of eCrime forums has allowed threat actors to share knowledge on tradecraft and tools as well as advertise and develop their criminal services. Some forums, including Exploit and XSS — which was impacted by recent law enforcement arrests and clearnet domain seizure — accommodate general eCrime discussions; however, numerous forums specialize in specific eCrime services or monetization methods, including the following:

- **Carding:** One of the first major cybercrime activities in the Russian-language underground ecosystem, carding continues to be discussed on generalist and specialized forums (e.g., WWH-Club or the historical CarderPlanet). So-called carders (кардеры) trade payment card data obtained in data breaches or via ATM skimming, point-of-sale (POS) malware, and formjacking.[7]
- **Financial services:** These forums discuss and offer services for financial fraud, money laundering, or cashing out. The DarkMoney forum, administered by a RENAISSANCE SPIDER operator, was historically one of the leading financial services forums, generating an advertising revenue of €200,000 per month.
- **Probiv:** The term “probiv” (пробив) describes a prominent service in the Russian-language underground ecosystem in which users trade personal information obtained from leaked data or recruit insiders with specific data access. Russian authorities have recently cracked down on data leaks and probiv services, partially due to their role in facilitating investigative journalism.[8]
- **Ransomware:** Following CARBON SPIDER’s highly publicized *DarkSide* attack in May 2021, prominent Russian-language eCrime forums banned ransomware-related discussions. As a result, an eCrime threat actor likely linked to the now-defunct *Babuk Locker* created the RAMP forum, which provides a dedicated section for RaaS affiliate programs.

This eCrime ecosystem accommodates a broad base of threat actors and enabling services, including initial access and data brokers, bulletproof hosting providers, cash-out services and cryptocurrency mixers, malware as a service (MaaS) and RaaS operators, and spammers. To govern interactions and ensure trust between buyers, sellers, and other users, Russian-language eCrime forums have developed a self-governance model that includes dispute arbitration, deal guarantors and automated escrow, seller reputation and user tier systems, deposit functionality,[9] and forum rules enforced by administrators and moderators.

---

6 https://www.justice.gov/archives/opa/pr/ukrainian-national-who-co-founded-cybercrime-marketplace-sentenced-18-years-prison
https://www.own.security/ressources/blog/russian-language-cybercriminal-forums---chapter-i-an-excursion-into-the-core-of-the-underground-ecosystem

7 In formjacking (aka Magecart, digital skimming, sniffing) operations, threat actors inject malicious JavaScript code into websites to harvest customer payment card information and/or personally identifiable information (PII) from websites’ front ends.

8 https://meduza.io/en/feature/2025/07/29/too-much-is-slipping-through

9 Often, forum administrators will require sellers to make a deposit of commensurate value to what they are selling; for example, a user attempting to sell a product for 10,000 USD may be asked to deposit that much within a dedicated forum wallet.

Prohibitions on Targeting Entities in Russia and the CIS Region

The prohibition on targeting organizations and citizens of Russia and Commonwealth of Independent States (CIS) countries has long been a tacit and often codified rule in the Russian-language underground ecosystem. Though this prohibition is likely rooted in an attempt to avoid domestic law enforcement, patriotism also likely plays a role, with CIS-based eCrime threat actors preferring to target external entities.

Numerous Russian-speaking MaaS and RaaS operators prohibit their customers and affiliates from targeting Russia and the CIS region. For example, HAZARD SPIDER's *Amadey Loader* XSS forum advertisement stated the loader is "not operational in the Russian Federation and fraternal countries." *Amadey Loader* enforces this prohibition by not executing command-and-control (C2) commands if CIS countries' keyboard layout IDs are identified on the system. Similar guardrails for systems' default UI language are found in *Lumma Stealer*, DEMON SPIDER's *Matanbuchus*, and *Rhadamanthys*.

Though targeting entities in these regions is not always explicitly prohibited on eCrime forums, Russian-speaking eCrime threat actors have ostracized eCrime threat actors that do not adhere to the targeting prohibition. In March 2024, an XSS forum user associated with BRASH SPIDER — developer of the *Doshell Stealer* and *Odyssey* macOS information stealers — accused COOKIE SPIDER of targeting the CIS region and called for their expulsion from the forum.

ENGLISH-LANGUAGE eCRIME FORUMS

English-language eCrime forums have emerged as critical hubs within the broader European eCrime ecosystem, serving as marketplaces and community spaces where threat actors exchange tools, data, and expertise. Unlike Russian-language forums that traditionally dominated high-end malware development and ransomware affiliate recruitment, English-language venues have created accessible gateways for European threat actors with varying skill levels. They provide easy access to compromised data, commoditized tooling, and money laundering services, all supported by trust-building features such as escrow and reputation scores.

On forums such as BreachForums, commodities typically include databases containing compromised personal and corporate data, access credentials for corporate VPNs and cloud environments, and tooling such as infostealers, loaders, and phishing kits. Vendors also offer tutorials, initial access broker listings, and laundering services that enable threat actors to monetize their operations. Transactions are generally conducted using cryptocurrency, and many forums employ escrow services to mediate deals, reducing fraud risk in inherently untrustworthy communities.

BreachForums Leadership, Law Enforcement Action

BreachForums emerged as a critical platform in the English-language eCrime ecosystem after authorities seized its predecessor, RaidForums, in April 2022. After law enforcement arrested RaidForums' administrator Diogo Santos Coelho (known as Omnipotent) in Portugal and seized the domain, the void left was quickly filled by Pompompurin, a well-respected member of the RaidForums community, who launched BreachForums in March 2022.

Pompompurin was arrested in 2023, and the forum's ownership transferred to ShinyHunters, which had conducted many high-profile data theft operations. ShinyHunters is likely based in France, as corroborated by a June 2021 U.S. Department of Justice (DOJ) indictment of several France-based individuals associated with the group. The forum's leadership underwent several transitions until the U.K.-based adversary BUTLER SPIDER (aka *IntelBroker*) became the primary owner and administrator in August 2024.

BUTLER SPIDER was a prominent forum member and claimed responsibility for selling and exposing sensitive U.S. and European government data. In January 2025, BUTLER SPIDER resigned their role as the BreachForums administrator, claiming they lacked the time needed to administer the forum. In February 2025, French authorities reportedly arrested BUTLER SPIDER. Their inactivity since March 2025 led other forum members to speculate whether the adversary had been arrested.

In April 2025, the forum went offline, though the administrators at the time claimed they had intentionally taken the forum down because it had been targeted with a zero-day exploit. In June 2025, the French Cybercrime Brigade reportedly arrested four individuals using the monikers ShinyHunters, Hollow, Noct, and Depressed for their roles in developing and administering BreachForums.

The tumultuous history of BreachForums demonstrates how individual threat actors can significantly shape forum activity while drawing international law enforcement scrutiny.

INITIAL ACCESS BROKERS

Initial access brokers (IABs) are threat actors that gain and sell access to corporate networks on forums and marketplaces. IABs use various TTPs to gain initial access, including abusing compromised credentials, exploiting vulnerabilities, and leveraging social engineering. Europe-based entities are a popular target among IABs and their buyers. Potential buyers most often prefer access to U.S. entities, followed by entities in Europe, Canada, and Australia.

Most advertised entities are in the U.K., Spain, Germany, Italy, and France and in the academia, retail, professional services, manufacturing, and industrials and engineering sectors. Similar to other enabling services, Russian-speaking IABs often have self-imposed restrictions on advertising access to entities in Russia and the CIS region (Figure 4).

SINCE JANUARY 2024, CROWDSTRIKE INTELLIGENCE HAS IDENTIFIED 260 IABS ADVERTISING NETWORK ACCESSES TO MORE THAN 1,400 EUROPE-BASED ENTITIES.

	UNITED KINGDOM	SPAIN	GERMANY	ITALY	FRANCE	NETHERLANDS	BELGIUM	SWEDEN	SWITZERLAND	PORTUGAL	AUSTRIA	POLAND	DENMARK	NORWAY	CZECH REPUBLIC	OTHER	GRAND TOTAL
Academic	40	10	23	19	16	14	5	1	1	9	1	7	0	0	1	15	162
Retail	28	25	10	20	12	2	4	5	6	2	2	5	7	2	0	14	135
Professional Services	34	10	24	6	13	9	2	6	5	3	5	2	4	3	2	6	133
Manufacturing	20	9	16	14	3	6	3	3	5	0	4	1	0	2	0	6	92
Industrials and Engineering	19	5	18	16	4	5	7	3	3	0	3	1	0	0	0	5	85
Technology	14	14	7	10	9	5	2	4	1	6	0	1	3	4	0	3	83
Government	4	7	3	10	9	1	1	5	0	1	1	0	1	1	0	6	50
Financial Services	13	3	1	7	6	5	0	0	2	1	0	1	1	0	3	7	49
Telecommunications	5	5	4	4	5	2	0	1	0	1	1	1	0	0	1	10	40
Healthcare	4	2	4	1	5	8	5	0	1	0	0	1	1	0	1	6	38
Automotive	1	3	7	5	1	4	0	2	1	0	0	0	0	1	0	3	27
Energy	2	1	3	3	3	0	0	0	1	0	0	3	1	1	0	2	20
Media	4	1	1	0	10	0	0	0	1	0	0	0	0	0	1	2	20
Transportation	1	0	1	2	2	6	0	2	0	0	0	0	0	0	1	3	18
Logistics	6	5	1	1	2	0	0	0	0	0	1	0	1	0	0	0	17
Other	100	65	38	40	55	14	18	10	15	5	9	4	7	5	5	72	462
Grand Total	292	161	160	156	153	80	46	42	41	28	27	27	24	19	15	160	1,431

Figure 4. IABs' advertised entities by top European countries and sectors, January 2024-September 2025

Based on this dataset, IABs' most advertised countries and sectors broadly coincide with those named on BGH DLSs (see the *Big Game Hunting* section on page 5). This is likely due to multiple factors, one of which is the close collaboration between IABs and BGH adversaries. For example, HOOK SPIDER — which has operated under several monikers on the Russian-language eCrime forums Exploit, RAMP, and XSS — has highly likely sold access to several BGH adversaries (including BITWISE SPIDER and BRAIN SPIDER) and is historically associated with SCATTERED SPIDER.

MALWARE AS A SERVICE

MaaS is an enabling service that offers malicious software (e.g., banking malware, information stealers, crypters, and loaders), similar to the legitimate software as a service (SaaS) model. The MaaS model makes it significantly easier for eCrime threat actors to access tools they would otherwise lack the time or resources to develop.

MaaS operators offer their tools through various business models, including purchase, rent, or pay-per-install arrangements as well as affiliate programs that involve profit-sharing between MaaS operators and affiliates (Figure 5). Russian-speaking MaaS operators typically offer their services on eCrime forums (notably Exploit), public or private Telegram channels, and — in the case of LUNAR SPIDER — on a referral basis.

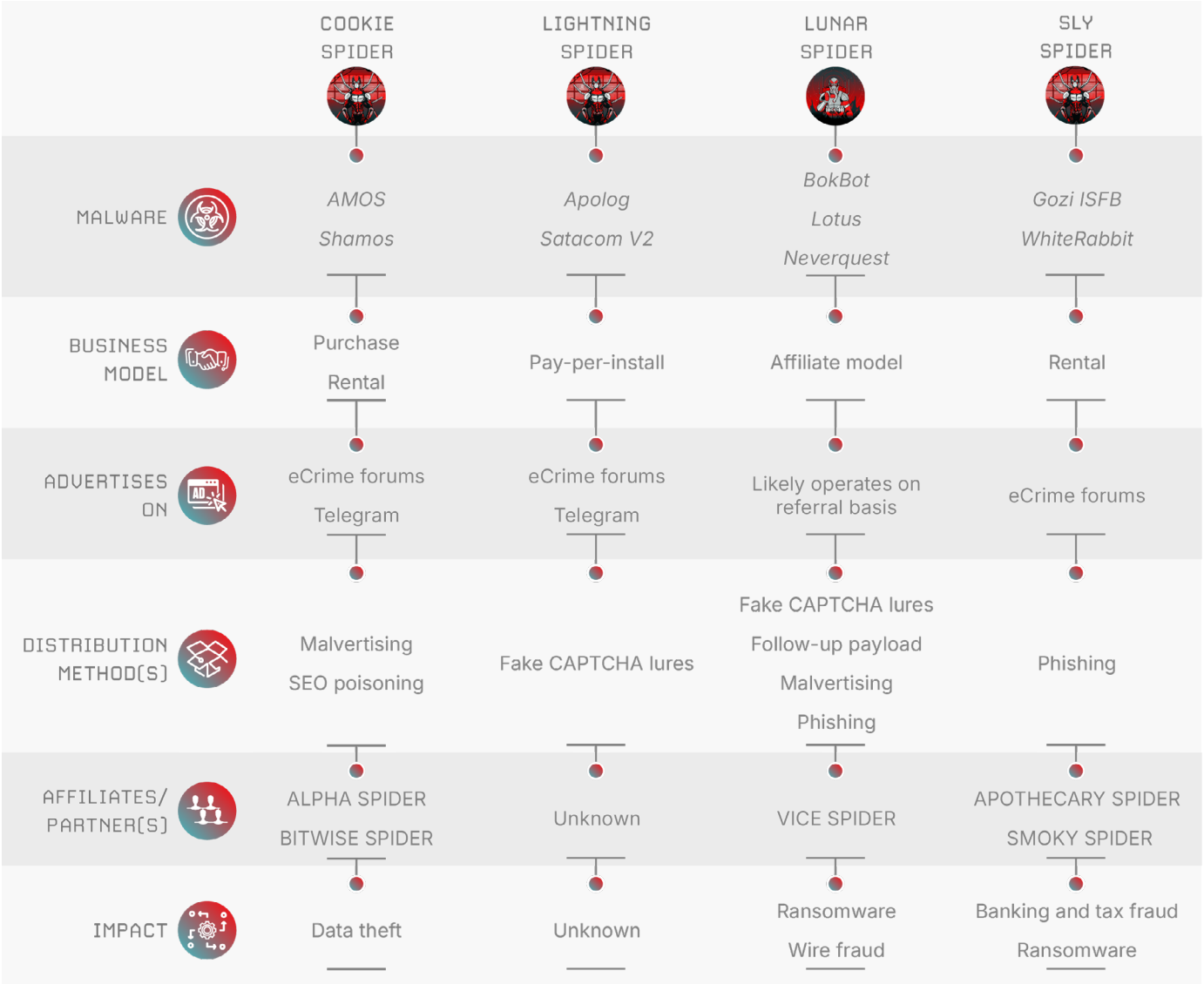


Figure 5. Prominent MaaS operators targeting European countries

While law enforcement operations such as Operation Endgame or the July 2025 XSS seizure regularly disrupt the ecosystem, MaaS operators remain resilient partially due to the persistence of long-standing members that act with near impunity in their jurisdictions. However, LUNAR SPIDER member Vyacheslav Igorevich Penchukov (aka Tank) — active since 2009 and initially a member of the *JabberZeus* gang — was arrested in Geneva, Switzerland, in 2022 and extradited to the U.S. in early 2024.

Apart from enabling other threat actors, the persistence and proliferation of MaaS operators also impede attribution by equipping many threat actors with the same tools, which are often delivered using similar TTPs. Nation-state adversaries exploit this model, such as Russia-nexus adversary EMBER BEAR, which has leveraged DEMON SPIDER's *Matanbuchus*, SMOKY SPIDER's *SmokeLoader*, and *Raccoon Stealer*. In May 2025, the U.S. DOJ indicted 16 members of SCULLY SPIDER's *DanaBot* MaaS, revealing that Russia-nexus threat actors used this criminal service to support military operations and espionage efforts.[10]

Communication Tools Telegram, Tox, and Jabber

Though eCrime services often advertise on eCrime forums, communication with potential customers typically takes place over Telegram. While channel takedowns increased after Telegram CEO Pavel Durov was arrested in August 2024 and Telegram's terms of service were updated, eCrime threat actors largely continue to rely on Telegram as a primary communication platform. Telegram allows eCrime services to communicate updates or service outages as well as offer direct support to customers.

Other common communication methods include Tox and Jabber. Tox messages are immutable, preventing customers from changing agreements after a sale. Additionally, compared to eCrime forums and Telegram, Jabber is less prone to disruption due to its decentralized nature and because eCrime threat actors can operate their own Jabber servers.

VIOLENCE AS A SERVICE AND PHYSICAL CRYPTOCURRENCY THEFT

Since 2024, cryptocurrency thefts involving physical attacks and kidnappings have increased dramatically, particularly in Europe. In January 2025, threat actors kidnapped and attempted to extort the co-founder of Ledger, a prolific cryptocurrency wallet vendor, in France. While the threat actors in this case (and numerous others) have been arrested, the threat persists.[11] Between January 2025 and September 2025, 17 similar incidents occurred in Europe, 13 of which occurred in France.[12]

Individuals involved in physical cryptocurrency theft often operate within eCrime communities affiliated with "The Com." Several of these individuals have previously advertised tools such as one-time password interception bots, which are Telegram-based tools that enable threat actors to automate vishing calls to victims and are often used to target cryptocurrency exchange accounts.

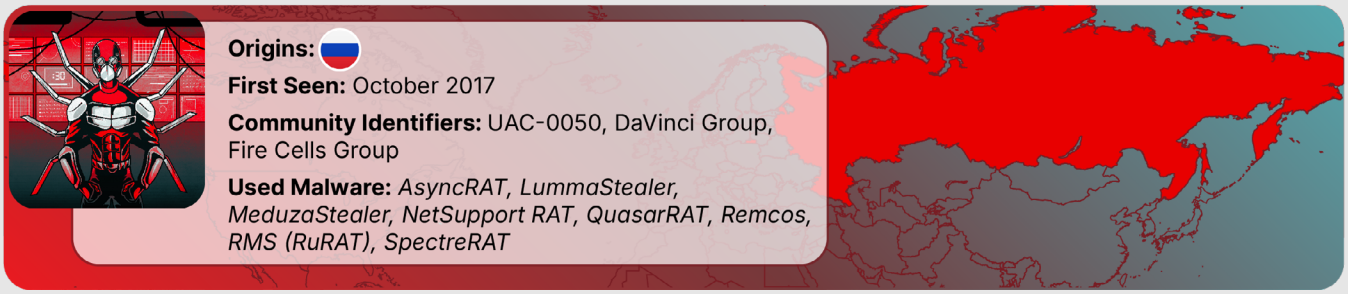
---

10 https://www.crowdstrike.com/en-us/blog/crowdstrike-partners-with-doj-disrupt-danabot-malware-operators/

11 https://www.france24.com/en/france/20250621-france-arrests-five-kidnapping-cryptocurrency-entrepreneur-father

12 https://github.com/jlopp/physical-bitcoin-attacks

RENAISSANCE SPIDER Poses Significant Threat to Europe



RENAISSANCE SPIDER is a Russia-based eCrime adversary that has historically conducted a mix of eCrime, cyber espionage, and influence operations and has facilitated physical sabotage.

- RENAISSANCE SPIDER conducts high-volume phishing campaigns primarily targeting Ukraine's public and private sectors. They have intermittently targeted entities across Europe, including in Germany, Italy, Lithuania, Moldova, Poland, Switzerland, and the U.K. The adversary is likely motivated by both financial gain and intelligence gathering.
- RENAISSANCE SPIDER has targeted entities across Europe in email- and social media-based IO using various personas, including the fake hacktivist *DaVinci Group*, or impersonating real Moldovan journalists by using their compromised email accounts. Most recently, the adversary emailed fake bomb threats to various European entities, likely aiming to undermine support for Ukraine.
- In August 2024, RENAISSANCE SPIDER created the purported VaaS *Fire Cells Group*, hiring individuals to conduct subversion and sabotage in Ukraine. Under the guise of *Fire Cells Group*, the adversary conducted IO, offered payment for assassinating Ukrainian officials, and highly likely paid individuals to conduct arson attacks against Ukrainian military vehicles and civilian infrastructure.

CrowdStrike Intelligence assesses that RENAISSANCE SPIDER operators are likely acting under the direction of, or in coordination with, Russian special services. This assessment is made with moderate confidence based on the adversary's activities (e.g., IO and sabotage), targeting aligned with Russian state interests, the likely arrest of group members in 2021, and other cybercriminals' accusations.

Nation-State Overview

Kinetic conflicts, including the war in Ukraine and conflicts in the Middle East, are major drivers of cyber activity in Europe. Within these contexts, state-sponsored threat actors predominantly employ cyber capabilities in a support role, such as to gain visibility into target government and military entities to support the war effort or to amplify information (and disinformation) operations. Some adversaries have also weaponized their network access to degrade, disrupt, or destroy access to critical infrastructure and essential government functions.

Meanwhile, a broad spectrum of state-sponsored cyber activity persists. These campaigns range from targeted intrusions for traditional espionage — aimed at obtaining geopolitical and operational insight or facilitating intellectual property theft — to opportunistic intrusions for financial gain.

Conflict-Driven Cyber Activity

RUSSIA-ALIGNED CONFLICTS

Russia's full-scale invasion of Ukraine in February 2022 triggered a surge in targeted cyber intrusions from a mix of new and established threat actors. Each adversary's distinct intelligence mandates collectively form a broad intelligence-gathering campaign supporting various strategic objectives. Though most intelligence collection activity related to the conflict is conducted by Russian Intelligence Services (RIS) — primarily the GRU (aka GU, Main Directorate of the General Staff of the Armed Forces of the Russian Federation) and Federal Security Service of the Russian Federation (FSB) — the DPRK's intelligence agencies have also been involved in kinetic and cyber operations targeting Ukraine.

Figure 6. Ukraine war-related adversaries

GRU-Nexus Adversaries Conduct Intelligence Collection and Disruptive Operations

GRU-operated adversary FANCY BEAR has conducted numerous simultaneous campaigns targeting Ukrainian military and government entities. Though the adversary has used their custom credential phishing toolkit for their phishing operations targeting users of the free Ukrainian webmail service **ukr.net** since 2023, they have also leveraged *ClickFix*, malicious RDP files, and open-source large language model capabilities in their campaigns.

FANCY BEAR's intelligence collection focuses on supporting Russia's military objectives in Ukraine on strategic, operational, and tactical levels. The adversary targets important national and local entities across various sectors, such as government entities, as well as individuals, including Ukrainian army service members.

Meanwhile, GRU-operated VOODOO BEAR has focused on Ukrainian critical infrastructure, conducting destructive operations against energy, telecommunications, and utility entities. During instances in which they did not immediately deploy wiper malware, VOODOO BEAR likely maintained their access to move laterally and further compromise networks in support of their intelligence collection and destructive operation requirements.

In early 2025, CrowdStrike OverWatch detected VOODOO BEAR leveraging the *POEMGATE* secure shell (SSH) backdoor and credential logger in the environments of Ukrainian telecommunications entities. In June 2025, the adversary continued initial access operations delivering fake antivirus program installers containing the *Sumbur* backdoor, which downloads and executes additional payloads to facilitate long-term persistence.

FSB-Nexus Adversaries Conduct Intelligence Collection and Information Operations

The targeting priorities for threat actors linked to Russia's FSB have remained consistent since 2022. PRIMITIVE BEAR continues to execute high-volume spear-phishing campaigns against Ukrainian government and military organizations, likely to gather intelligence that supports Russia's war aims, such as bolstering its political and military influence.

GOSSAMER BEAR conducts credential phishing operations targeting Ukrainian government and military entities as well as U.K. and EU nongovernmental organizations (NGOs). CrowdStrike Intelligence assesses with moderate confidence that GOSSAMER BEAR's credential phishing operations likely support IO efforts to undermine the morale of Ukrainian citizens or denigrate and undermine the credibility of U.K. governance and Western institutions.

Other Russia-Aligned Activity Clusters

Since at least 2017, Russia-aligned activity cluster RepeatingUmbra has targeted Ukrainian government and defense entities. In 2024 and 2025, the cluster conducted credential phishing campaigns and used multiple variants of their custom *Pryatki* downloader to deliver *Cobalt Strike* to Ukrainian targets.

Since 2022, the increased need for intelligence to support the Russian war effort has led to the emergence of novel threat actors that often conduct high-volume but low-sophistication operations against Ukrainian government and military targets. For example, CrudeScientist, a likely Russia-nexus activity cluster active since at least November 2023, has maintained a high operational tempo through early 2025 with largely consistent, low-sophistication TTPs.

Similarly, FamishedLibrarian — another likely Russia-nexus activity cluster active since at least November 2022 — relies on relatively unchanged delivery TTPs and continues to make operations security (OPSEC) errors that expose their campaign infrastructure.

AN ACTIVITY CLUSTER IS A GROUPING OF RELATED MALICIOUS BEHAVIORS THAT SHARE COMMON TOOLS, TECHNIQUES, OR INFRASTRUCTURE, TRACKED BY CROWDSTRIKE WHEN THERE ISN'T YET ENOUGH EVIDENCE TO ATTRIBUTE THE ACTIVITY TO A NAMED ADVERSARY.

Throwaway Agents Recruited via Telegram

Since Russia's February 2022 full-scale invasion of Ukraine, Moscow has increasingly leveraged hybrid warfare tactics, including sabotage, against Ukraine and its European allies. In 2024 and 2025, numerous Russia-nexus sabotage instances were reported across Europe. In response, the EU sanctioned Russian GRU Unit 29155 members for their attempted destabilization activities, including cyberattacks.[13]

Russian special services have increasingly relied on so-called throwaway agents to conduct subversion and sabotage. "Throwaway agents" are operatives recruited by an intelligence service, often for a specific, low-level task, with the full expectation that they are expendable. Using throwaway agents offers greater plausible deniability, is low cost and relatively low risk, and has likely been useful in light of European countries' mass expulsion of Russian diplomats and intelligence officers.

Throwaway agents are often recruited and coordinated over Telegram using criminal or extremist intermediaries, complicating attribution.[14] Since October 2024, RENAISSANCE SPIDER has acted as such an intermediary under the guise of the VaaS provider *Fire Cells Group*.

Targeting Ukrainian Allies

Russia-aligned threat actors have also targeted European entities for their public support of Ukraine. For example, in March 2022, RepeatingUmbra demonstrated renewed interest in targeting German and Baltic entities, possibly tied to the support these countries have provided in regard to the conflict. Meanwhile, between late March 2022 and May 2022, PRIMITIVE BEAR temporarily expanded their targeting from Ukraine to include government entities in Latvia, Moldova, and Lithuania, likely in response to their public support for Kyiv immediately after the invasion.[15]

Though other pro-Ukraine European governments have also been targeted, likely in part for their support for Ukraine, CrowdStrike Intelligence assesses these broader campaigns are mainly driven by standing intelligence collection requirements (see the *Russia-Aligned Activity* section on page 26).

13 https://www.economist.com/graphic-detail/2025/07/22/russian-sabotage-attacks-surged-across-europe-in-2024

14 https://www.tv4.se/artikel/5vLIzItKYKnriPm0uJvd1N/saepo-larmar-vaervar-missbrukare-foer-att-utfoera-sabotage-i-sverige
https://www.abw.gov.pl/pl/informacje/2662,Dzialal-na-rzecz-obcego-wywiadu-przeciwko-RP-21-lipca-br-Kolumbijczyk-uslyszal-z.html
https://dossier.center/gru-guide/

15 https://eng.lsm.lv/article/politics/diplomacy/latvian-officials-immediately-condemn-putins-ukraine-invasion.a445051/
https://web.archive.org/web/20220507122804/https://www.bbc.com/ukrainian/features-61155192
https://www.eurointegration.com.ua/rus/news/2022/04/18/7137985/
https://www.delfi.lt/a/89541661

DPRK-Nexus Cyber Activity Targeting Ukraine

Throughout 2024 and 2025, the DPRK has deepened its ties with Russia, offering diplomatic, economic, and military support during Russia's invasion of Ukraine. The alliance reached a high point in October 2024, when the DPRK deployed troops to Russia to aid its war efforts in Ukraine. In exchange for its military support, Russia has reportedly provided North Korea with advanced air defense equipment, anti-aircraft missiles, and electronic warfare systems.[16]

The DPRK's increasing military support for Russia coincides with LABYRINTH CHOLLIMA's targeting of European defense entities in August 2024 and May 2025 as well as VELVET CHOLLIMA's targeting of European diplomatic entities between March 2025 and August 2025. These campaigns were likely motivated by DPRK military intelligence requirements related to the war in Ukraine.[17]

Since entering a new phase of their alliance, the DPRK and Russia have promised to collaborate more closely on military matters, including in the cyber realm. The leaders of each country's intelligence agencies have also met several times. A June 2025 report claimed that both sides are pursuing an intelligence-sharing agreement.[18]

Russia-Nexus Adversaries Focus on Ukraine

During the reporting period, Russia-nexus operations targeting Europe focused almost exclusively on supporting Russia's goals — namely, securing Russia's control over the annexed eastern Ukrainian territories, securing Ukraine's political and military neutrality regarding NATO, and establishing a Russia-friendly government in Ukraine.

Since 2022, at least two Russia state-nexus destructive operations primarily targeting Ukrainian entities or capabilities have impacted entities outside of Ukraine, demonstrating the potential for impacts to other European entities.[19] One operation involved collateral damage, while the other intentionally targeted Poland, whose government supports Ukraine.

Unless Western support for Ukraine changes significantly — including if Western military forces become directly involved in operations against Russian forces — Russian threat actors are unlikely to target non-Ukrainian entities in Europe with destructive attacks. However, CrowdStrike Intelligence assesses that the Russian government will likely accept the risk of minor collateral damage to entities outside Ukraine resulting from cyber operations targeting Ukrainian military capabilities.

---

16 https://assets.korearisk.com/uploads/2025/05/Unlawful-Military-Cooperation-including-Arms-Transfers-between-North-Korea-and-Russia-MSMT_2025_1-1.pdf

17 https://www.trellix.com/blogs/research/dprk-linked-github-c2-espionage-campaign/

18 https://www.dailynk.com/english/n-korea-uses-moscow-security-meeting-to-advance-intelligence-cooperation-with-russia/

19 https://www.sentinelone.com/labs/acidrain-a-modem-wiper-rains-down-on-europe/ https://www.microsoft.com/en-us/security/blog/2022/10/14/new-prestige-ransomware-impacts-organizations-in-ukraine-and-poland/

SPILLOVER FROM MIDDLE EASTERN CONFLICTS

Kinetic conflicts in the Middle East, particularly between Israel and Hamas, were the primary drivers of Iran-backed cyber operations and pro-Iran hacktivism toward European entities. Though Iranian cyber activity has primarily focused on Israel-based entities, tense diplomatic relations between Iran and European nations drove a limited number of Iran-nexus threat actors to target European entities. Iran-nexus adversaries have conducted various operations in the region, including espionage, hack-and-leak, and destructive campaigns. As Israel-Iran tensions remain high, Iran-nexus adversaries will likely continue to target Israel and its Western allies involved in the conflict through impersonation efforts and spear-phishing campaigns.

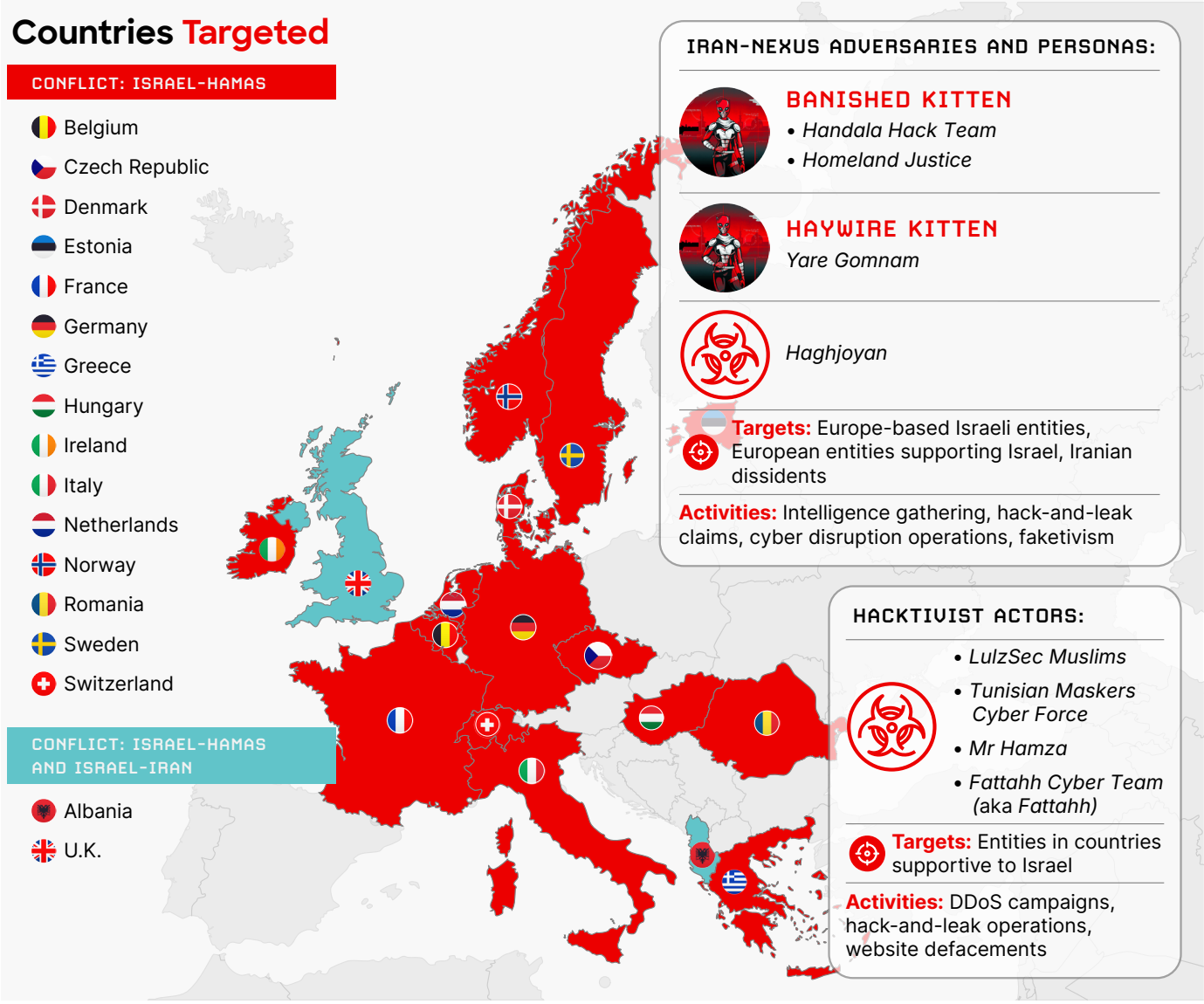


Figure 7. Iran-nexus and hacktivist spillover from Middle Eastern conflicts

Intelligence-Gathering Operations

Between late July 2025 and mid-August 2025, spear-phishing campaigns — almost certainly conducted by an Islamic Revolutionary Guard Corps (IRGC)-affiliated Iran-nexus threat actor — targeted a U.K.-based academic institution, likely to gather intelligence. The adversary likely used employment-themed messages to lure the victims into downloading and executing *AIDente* malware. This operation coincided with heightened tensions between the U.K. and Iran over nuclear negotiations and the decision by Germany, France, and the U.K. (known collectively as the E3) to trigger "snapback" sanctions against Iran in late August 2025. Although Iran is unlikely to conduct overt disruptive or destructive operations during negotiations, Iran very likely remains focused on intelligence collection as the snapback sanctions process continues.[20]

Hack-and-Leak Operations

Since 2024, Iran-linked cyber groups have increasingly conducted hack-and-leak operations under the guise of inauthentic hacktivist personas (aka faketivists), targeting Israeli entities or entities in countries that publicly support Israel. This tactic serves as a low-cost form of asymmetric warfare, allowing Iran to retaliate, destabilize its adversaries, and shape public perception while maintaining plausible deniability and avoiding conventional military conflict.

In July 2025, two Iran-linked cyber groups — pro-IRGC hacktivist group *Gomnaman Team* and BANISHED KITTEN's *Handala Hack Team* persona — claimed responsibility for hack-and-leak operations targeting a U.K.-based Iranian opposition media outlet. The groups claimed to have leaked employees' PII as well as sensitive emails and files. This activity was allegedly conducted in response to the outlet's cooperation with Israeli intelligence agencies. *Handala Hack Team*'s and *Gomnaman Team*'s July 2025 claims are part of a larger IO campaign likely intended to control information and suppress dissidents outside of Iran as well as damage trust in opposition media at a politically sensitive time for the regime.

Cyber Disruption Operations

In January 2024, likely HAYWIRE KITTEN persona *YareGomnam* (aka *Yare Gomnam Cyber Team*) claimed responsibility for a DDoS attack against a Dutch government news organization and a defense-related organization's English-language website. *YareGomnam* stated the DDoS attacks were in response to Dutch participation in the U.S.-led coalition responsible for military strikes against Houthi military sites in Yemen in January 2024. However, the mid-January 2024 news that a Dutch engineer had assisted Iranian nuclear sabotage in 2007 may have also influenced the group's targeting priorities.

CONFLICT-DRIVEN HACKTIVIST ACTIVITY

Between January 2024 and September 2025, global conflicts — including those between Russia and Ukraine, Israel and Hamas, and Israel and Iran — provoked widespread hacktivist activity, including DDoS attacks, hack-and-leak operations, website defacements, and destructive activity. Though these attacks predominantly targeted entities within the countries or regions actively engaged in the conflicts, some activity impacted European nations. Hacktivist attacks aligned with perceived support for Ukraine or Israel and targeted European financial, telecom, government, energy, logistics, law enforcement, and critical infrastructure entities.

20 https://www.iranintl.com/en/202507268188

Hacktivist Entity	Regional Activity
BOUNTY JACKAL	Between January 2024 and September 2025, pro-Russia hacktivist adversary BOUNTY JACKAL conducted extensive and near-daily DDoS campaigns against European entities in response to military or financial support for Ukraine or perceived Russo-phobic sentiments. The adversary's targeting was almost certainly largely opportunistic, and they used their *DDoSia* attack toolkit to coordinate campaigns with their global volunteer network. In addition to the DDoS support provided by volunteers, BOUNTY JACKAL collaborated with like-minded hacktivists — including *UserSec*, *People's Liberation Front*, *Cyber Army of Russia (CARR)*, *HackNeT*, and *Z-Alliance* — on multiple occasions to target European financial, telecom, government, energy, logistics, law enforcement, and critical infrastructure entities, as well as a Western military alliance. Numerous BOUNTY JACKAL campaigns were almost certainly timed to coincide with ongoing elections or protests in Europe. This highlights the adversary's broader anti-EU motivations — while still aligned with countries' perceived support for Ukraine — and desire to gain attention for campaigns by synchronizing attacks with major events in the target geography.
Cyber Army of Russia (aka *CARR*)	Throughout 2024, pro-Russia hacktivist *CARR* claimed to have conducted numerous DDoS campaigns against European entities in retaliation for Western military and financial support for Ukraine. *CARR* also claimed to have conducted multiple campaigns alongside BOUNTY JACKAL and *Z-Alliance*, including April 2024 DDoS attacks against Spanish government, energy, and logistics entities' websites. In September 2024 and October 2024, *CARR* claimed responsibility for industrial control system (ICS) compromises in Poland, France, the U.S, and Taiwan. In December 2024, *CARR* deleted their public Telegram channel and announced that group members would continue to conduct DDoS attacks under the *Z-Alliance* moniker.
Fattahh Cyber Team (aka *Fattahh*)	In January 2024, pro-IRGC hacktivist group *Fattahh Cyber Team* defaced a Dutch manufacturing website with pro-Houthi messaging. Although the hacktivist remains active through October 2025, this incident is the only known instance in which they targeted Europe.
LulzSec Muslims	Through at least August 2024, pro-Palestine and pro-Islam hacktivist group *LulzSec Muslims* claimed to have targeted numerous entities globally, including countries in Western, Northern, and Southern Europe but none in Eastern Europe other than Ukraine. Activity consisted of hack-and-leak operations, DDoS attacks, and website defacements against entities in countries the group perceives to directly or indirectly support Israel in the conflict with Hamas.
Mr Hamza	In January 2025, pro-Islam hacktivist *Mr Hamza* claimed to have conducted DDoS attacks against federal and national police, security and intelligence entities, a ministry of defense, and military services in Belgium, the Czech Republic, Denmark, Estonia, Germany, Hungary, Ireland, Italy, the Netherlands, Norway, Romania, Sweden, and the U.S. This activity was motivated by these countries' perceived support for Israel.
Tunisian Maskers Cyber Force	From May 2025 to June 2025, pro-Palestine hacktivist group *Tunisian Maskers Cyber Force* conducted their #Dark_Pulse_V2 campaign targeting U.K.-based entities in response to the U.K.'s support for Israel in the Israel-Hamas conflict. The hacktivist claimed to have conducted DDoS attacks against U.K.-based financial, professional services, hospitality, and retail entities and shared links to website-monitoring tools to prove the campaign was successful. As part of this campaign, *Tunisian Maskers Cyber Force* threatened to leak emails from an unspecified government entity (possibly based in Europe) and data allegedly obtained from a previously targeted professional services entity. However, because the hacktivist did not subsequently mention these threats or post the data to their known social media channels, whether they followed through with these threats remains unknown.
Z-Alliance (aka *Z-Pentest*)	In late 2024 and early 2025, *Z-Alliance* claimed to have breached the supervisory control and data acquisition (SCADA) systems of at least six entities in the U.S., France, Germany, Ukraine, and Taiwan and claimed responsibility for compromising ICSs in France, Greece, Lithuania, Italy, Poland, Spain, and Sweden. These breaches were motivated by the group's pro-Russia, anti-Ukraine, and anti-West sentiments and likely intended to gain notoriety.

Table 1. Hacktivist activity against European targets

Ongoing and emerging conflicts will highly likely continue to motivate hacktivist activity — both within conflict areas and globally — as hacktivists seek to retaliate for perceived support, spread their ideologies, or leverage media coverage to garner attention. This assessment is made with high confidence based on observed hacktivist activity in response to global conflicts since at least 2022.

Non-Conflict-Driven Nation-State Cyber Activity

Though major conflicts have altered the targeting priorities and operational tempo of some nation-state adversaries, the underlying drivers of cyber espionage remain constant. Nation-states' persistent demand for intelligence to inform national policy, support state-owned enterprises, or finance autocratic regimes ensures a range of cyber operations will continue.

RUSSIA-ALIGNED ACTIVITY

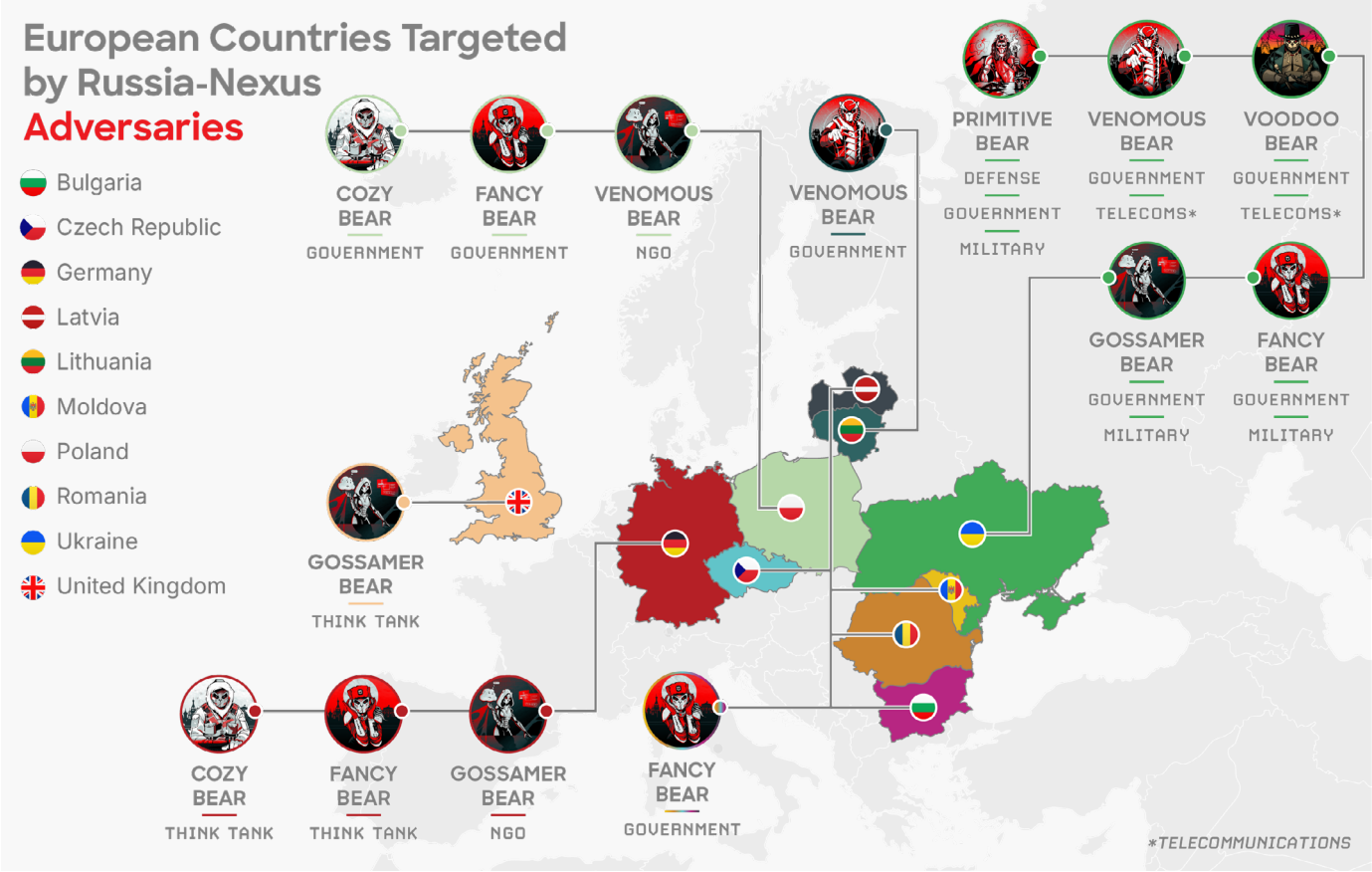


Figure 8. Russia-nexus targeting of European countries

Though most Russia-nexus nation-state adversaries and threat actors are focusing on targeting Ukraine, strategic targeting of other European states — particularly NATO member countries — remains a priority.

Russia-nexus adversaries' intelligence collection targeting patterns across different sectors align with Russia's political and military objectives in Europe. To further support Russia's war effort in Ukraine, these adversaries collect strategic, operational, and tactical intelligence, allowing Russia to track military aid to Ukraine. Targeting entities also highly likely enables Russia to gather political intelligence to exploit internal divisions that undermine European support for Ukraine and fracture the cohesion of NATO and the EU.

Russia-aligned threat actors' cyber operations against entities in non-NATO European countries likely serve distinct strategic goals. For entities in Western-aligned countries, these intrusions likely primarily aim to collect intelligence and monitor relationships with the EU and NATO. For countries actively seeking to integrate with these institutions, these threat actors likely intend to monitor and potentially disrupt their accession and reassert Russia's regional sphere of influence.

These operations demonstrate Russia's integration of its intelligence collection and influence operations, focusing on NATO activities, energy relationships, and policy development. The threat actors' persistence and large volume of campaigns indicate Russia is allocating high-level resources to these campaigns and prioritizing European intelligence collection and influence operations.

European Government Sector Targeting

FANCY BEAR, a GRU-operated adversary, has maintained a high operational tempo against European government entities. Throughout 2024, the adversary exploited vulnerabilities and conducted malware campaigns likely targeting government entities in European nations including Poland, Moldova, the Czech Republic, Bulgaria, and Latvia. Throughout 2025, FANCY BEAR has continued to exploit vulnerabilities in webmail clients such as Zimbra, Roundcube, and MDaemon to capture authentication data as well as redirect and exfiltrate emails.

FANCY BEAR highly likely targeted Czech Republic government entities with NATO cooperation lures and exploited NTLM vulnerabilities against Romanian government entities, highlighting the adversary's persistent intelligence collection goals. NATO member states and countries that have formal partnerships and cooperative agreements with NATO will remain a primary long-term target for FANCY BEAR's future operations.

Since October 2020, the Foreign Intelligence Service of the Russian Federation (SVR)-operated adversary COZY BEAR has continued their DiplomaticOrbiter campaign targeting European ministries of foreign affairs (MFAs) to collect intelligence consistent with the SVR's diplomatic and strategic intelligence objectives. The adversary resumed operations in January 2025, in which they highly likely used spear-phishing emails to deliver their novel custom downloader *BoomTwins*. In October 2024, COZY BEAR likely targeted European government entities during a separate large-scale phishing campaign. The adversary distributed malicious RDP files and registered more than 180 domains mimicking defense ministries, armed forces, and think tanks.

Between 2023 and 2025, VENOMOUS BEAR deployed their *CoreTech* implant and *Kazuar RAT* in campaigns against multiple Eastern European government entities, including those in Ukraine. Since Russia's full-scale invasion, CrowdStrike Intelligence has observed only limited VENOMOUS BEAR activity targeting Eastern European countries, including Ukraine. However, CrowdStrike Intelligence assesses with moderate confidence that VENOMOUS BEAR has targeted and will continue to target Eastern European government entities — likely due to the adversary's routine intelligence collection requirements, which were established alongside their intelligence collection capabilities prior to February 2022.

Throughout 2024 and 2025, Russia-aligned activity cluster RepeatingUmbra has targeted individuals and entities in Eastern Europe via sustained credential phishing and malware campaigns. The activity cluster conducted extensive credential phishing operations against Polish, Lithuanian, Latvian, and Ukrainian individuals and public entities as well as Russian-speaking individuals.

Additionally, RepeatingUmbra continued using malicious documents to deliver various loaders such as *Pryatki*, ultimately delivering a *Cobalt Strike* beacon, to Eastern European entities. RepeatingUmbra highly likely continues to collect intelligence while conducting IO — such as compromising politicians' social media accounts and laundering stolen data through hacktivist groups — to destabilize Eastern European countries.

In August 2025 and September 2025, a likely Russia-nexus eCrime threat actor conducted WhatsApp phishing campaigns targeting entities and individuals in Moldova, including a likely Moldovan Armed Forces member. The threat actor abused device-linking features to access victims' WhatsApp accounts. In September 2025, the threat actor reportedly used the Signal messaging application to distribute a link that led to a malicious website spoofing a legitimate Moldovan economic manifesto petition. The website enticed targets to sign in to WhatsApp to "prevent electoral fraud."

Also in September 2025, another likely Russia-nexus eCrime threat actor leveraged opportunistically compromised Zimbra Collaboration servers to collect emails. The threat actor indicated their target scope comprises government, nonprofit, political, and logistics entities located in Europe, particularly those in Moldova. CrowdStrike Intelligence assesses the unidentified threat actor is likely collecting intelligence on behalf of the FSB.

European Defense Sector Targeting

In October 2024, COZY BEAR leveraged domain spoofing — using domains registered since at least August 2024 — to likely target an international defense organization as well as European and North American government and private entities. Additionally, in July 2025, U.K. government sanctions against GRU Unit 26165 operators alleged that the group had accessed private IP cameras near military facilities, ports, border crossings, and other transportation infrastructure across several European countries, including Moldova. This highlights Russia's wide-ranging intelligence collection requirements against military and critical infrastructure targets.

European Energy Sector Used in Lure Content

In an April 2024 campaign, FANCY BEAR used renewable energy-themed lures, likely indicating that energy is a significant RIS collection priority due to heavy sanctions on Russia's oil and gas sector. FANCY BEAR used a subdomain hosting a lure document spoofing an energy sector intergovernmental organization's "energy profile" of Austria.

As of December 2023, Austria imported 98% of its gas from Russia.[21] Austria's Energy Minister announced in February 2024 that the country was seeking to end its import contract with Gazprom. Though the campaign's exact target scope remains unknown, the lure indicates FANCY BEAR was potentially targeting European energy entities. The operation demonstrates Russia's long-term intelligence requirements regarding European energy relationships and policy developments.

European Think Tank Sector Targeting

Between late 2023 and Q2 2024, FSB-operated group GOSSAMER BEAR conducted credential phishing campaigns against U.K. think tanks specializing in international affairs, defense, and security. The adversary likely weaponized the obtained data in subsequent hack-and-leak influence operations. FANCY BEAR also exploited NTLM vulnerabilities against a Romanian government entity and likely against a German think tank as part of their intelligence collection operations. Meanwhile, COZY BEAR's DiplomaticOrbiter campaign targeted Western think tanks as part of routine intelligence collection.

DURING THEIR OCTOBER 2024 PHISHING CAMPAIGN, COZY BEAR REGISTERED MORE THAN 180 DOMAINS SPOOFING THINK TANKS AND DEFENSE ENTITIES, INDICATING THE LIKELY HIGH PRIORITY PLACED ON MONITORING HIGH-VALUE WESTERN GOVERNMENT, TECHNOLOGY, DEFENSE, AND NONPROFIT ENTITIES FOR STRATEGIC INTELLIGENCE COLLECTION.

European Media and NGO Sector Targeting

GOSSAMER BEAR has targeted European media and NGO entities through hack-and-leak campaigns, weaponizing stolen documents for IO. From January 2025 to August 2025, GOSSAMER BEAR continued credential phishing operations likely targeting think tank, dissident, and NGO entities in Europe and Africa. Consistent with the adversary's historical focus on "undesirable organizations,"[22] in 2025, GOSSAMER BEAR targeted at least one NGO that promotes civil society relations between Germany and Eastern European countries.

Following the October 2023 start of the Israel-Hamas conflict, GOSSAMER BEAR registered multiple domains spoofing a European law enforcement entity to capture Microsoft Outlook credentials from associated individuals. In early February 2024, GOSSAMER BEAR registered domains spoofing a European military training entity focused on Africa, which aligns with Moscow's growing strategic interest in Africa. Russia has been positioning itself as an alternative to Western partners for Africa as EU and U.S. forces reduce their continental presence. GOSSAMER BEAR's intelligence collection and IO campaigns often involve hack-and-leak operations weaponizing stolen documents from government, media, think tank, and NGO entities.

In January 2024, VENOMOUS BEAR targeted a Polish NGO with a novel backdoor named *dcmd*. This activity aligned with the adversary's long-term intelligence collection requirements and with their increased targeting of Polish entities, likely due to Poland receiving refugees from and providing aid to Ukraine.

---

21 https://www.reuters.com/markets/europe/austria-seeking-end-russian-gas-import-contract-energy-minister-says-2024-02-12/

22 Russia designates organizations that it perceives as a foreign threat to Russian state interests as "undesirable," prohibiting those organizations from conducting business within Russia.

IRAN-NEXUS ACTIVITY

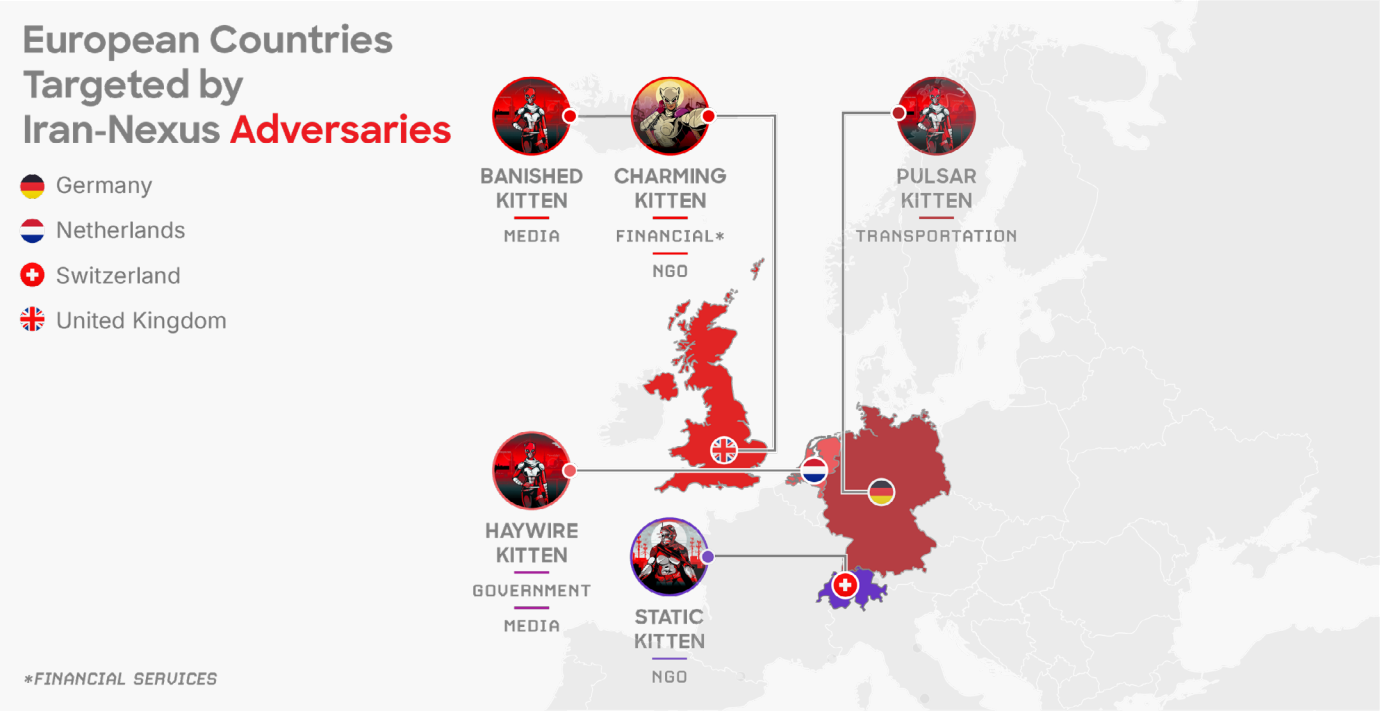


Figure 9. Iran-nexus targeting of European countries

Iran-nexus adversaries have predominantly targeted Israel, its allies, and other targets in the Middle East due to ongoing regional tensions. However, they have also continued to collect intelligence from European targets, particularly those in opposition to Iran's state interests. Though Iran will likely refrain from disruptive or destructive offensive cyber activity during its ongoing attempts to return to nuclear negotiations, Iran-nexus threat actors still pose a heightened threat to European nations.

In late August 2025, the E3 initiated the "snapback" sanctions process against Iran.[23] Iran likely does not perceive intelligence-gathering activity to be overtly offensive cyber activity, so the "snapback" sanction process initiation will likely drive Iran-nexus adversaries to specifically target E3 countries to gather intelligence.

European Government Sector Targeting

Iran-nexus adversaries have consistently targeted European government entities, particularly those opposing Iranian state interests. Likely beginning in January 2025 through March 2025, an unattributed Iran-nexus threat actor conducted a spear-phishing campaign targeting a prominent EU parliament representative from Germany who leads efforts supporting Iranian opposition groups.

The campaign leveraged voice calls and elaborate social engineering, with the German politician's staff reportedly receiving messages and phone calls from unknown threat actors impersonating a legitimate contact associated with a U.S.-based think tank. Eventually, the threat actors compromised and installed malicious software on a laptop from the politician's office. Though the threat actors successfully compromised the target's systems, EU parliament security measures reportedly prevented any sensitive data theft.

The German politician was likely selected as a phishing target due to their political position and professional proximity to Iranian dissidents.

23 https://www.iranintl.com/en/202507268188

European Financial Services Sector Targeting

In May 2024, CHARMING KITTEN targeted U.K.-based financial entities with phishing campaigns to gather intelligence. The adversary tailored their operations using spoofed infrastructure, target-specific social engineering, and websites spoofing legitimate entities. The adversary also consistently abused legitimate services such as Microsoft OneDrive to deliver their custom malware.

European Transportation Sector Targeting

In mid-July 2025, PULSAR KITTEN likely conducted a spear-phishing operation targeting the German branch of a U.S.-based transportation company. The adversary used aviation-themed job offers to deliver their sophisticated *SilkySand* malware through the legitimate file-sharing service ONLYOFFICE. The adversary conducted this operation amid rising tensions between Iran and Germany, particularly following controversial statements about the Israel-Iran conflict and European threats of renewed sanctions. The operation served both political and intelligence-gathering purposes, advancing Iran's counterintelligence interests in Western Europe. PULSAR KITTEN has previously spoofed German automotive manufacturer websites but has not previously been observed targeting transportation entities.

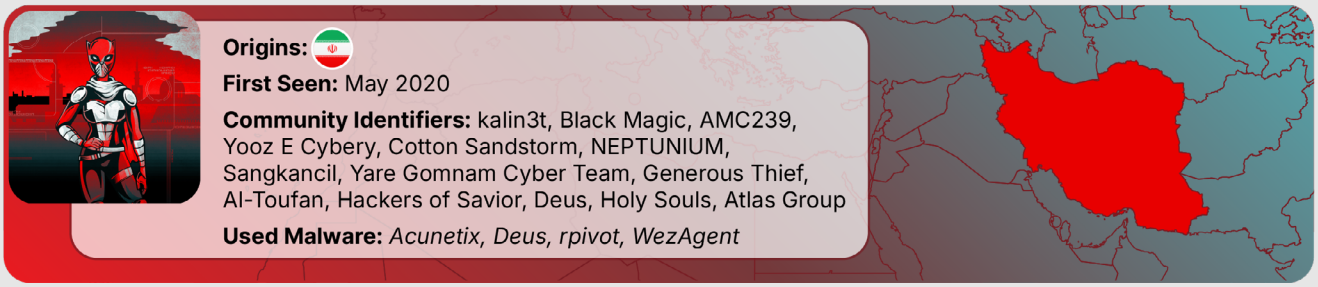
Iran-nexus adversaries affiliated with the IRGC — including PULSAR KITTEN, IMPERIAL KITTEN, an unattributed Iran-nexus threat actor, and HAYWIRE KITTEN — have likely spoofed or targeted Germany-based entities as of early to mid-2025.

European NGO Sector Targeting

In August 2025, STATIC KITTEN conducted an intelligence-gathering campaign targeting the Southeast Asia branch of a Switzerland-based NGO. The adversary likely gained initial access to the entity through a web server compromise; however, the NGO has not confirmed this.

Once STATIC KITTEN established a foothold, they used a compromised service account to move laterally through the network. Using their elevated access, the adversary invoked PowerShell to download a malicious payload from an adversary-controlled IP address. Lastly, they attempted to write registry hives to disk and harvest credentials, almost certainly in preparation for exfiltration.

HAYWIRE KITTEN Likely Phishing Campaign Targets Western Europe



Starting in at least December 2024 through July 2025, HAYWIRE KITTEN likely conducted an extensive Microsoft-themed phishing campaign targeting Western organizations across various sectors. Their operation focused on technology, renewable energy, manufacturing, and hospitality entities. Some evidence suggests the adversary targeted entities in France, Germany, Spain, Switzerland, and the U.S. The group deployed Microsoft-themed credential harvesting pages and likely used spear-phishing emails with a PDF attachment lure containing a request for quote (RFQ) for an event space in Germany that hosts various trade shows and conferences.

HAYWIRE KITTEN's targeting of technology, renewable energy, and hospitality entities reflects Iran's strategic interests and follows historical targeting patterns against the West. The adversary likely conducted this activity to collect intelligence.

This activity is also consistent with HAYWIRE KITTEN's pattern of targeting Western entities and highlights their ability to develop infrastructure domains. CrowdStrike Intelligence assesses that HAYWIRE KITTEN likely controls the infrastructure associated with this Microsoft-themed phishing campaign; however, whether this infrastructure was operationalized and successfully implemented remains unclear.

CHINA-NEXUS ACTIVITY

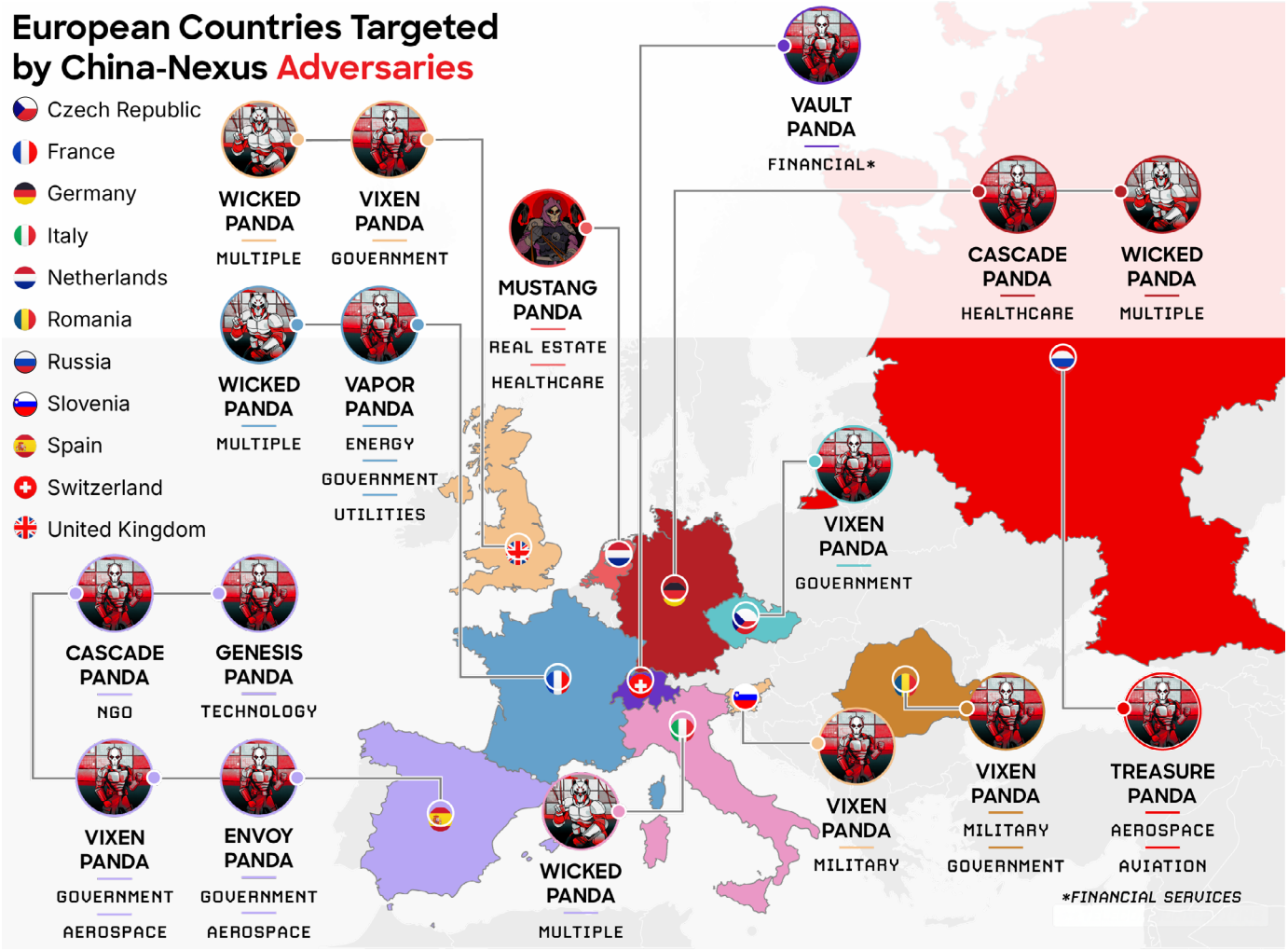


Figure 10. European countries targeted by China-nexus adversaries

The EU — one of China's largest trading partners and investment destinations — plays a key role in China's aspirations to improve regional integration via trade in Central Asia and Eastern Europe. China's cyber activity targeting Europe has remained consistently focused on likely intelligence collection to inform Beijing's political and economic engagement with the region. Beijing also aims to support the government's strategic priorities amid a currently turbulent period in the EU-U.S. relationship regarding trade and defense issues. China-nexus threat actors have continued to target European government, defense, industrial, and aerospace entities.

China-nexus threat actors' operations targeting Europe likely aim to support China's strategic priorities, such as boosting the economy and avoiding foreign interference. China also aims to achieve self-reliance in key science and technology areas, particularly as the country's access to advanced technologies made outside of China is increasingly restricted.

European Healthcare and Biotechnology Sector Targeting

Multiple China-nexus adversaries continue to persistently target the healthcare and biotechnology sector, which is one of the most consistently targeted sectors in Europe. In April 2024, CASCADE PANDA attempted to deploy *WinDealer* malware at a German biotechnology entity with operations in China, demonstrating the adversary's ongoing focus on entities with a cross-border presence.

MUSTANG PANDA's operations impacted several European healthcare organizations throughout 2023 and 2024. These operations deploy USB-spread modular malware, including the *LubanBall* USB drive infector, *Tangram* and *Foregram* loaders, and *LingerRAT* remote access tool (RAT). The adversary's capabilities have continued to evolve, and they most recently deployed *LubanBall* at a Netherlands-based healthcare organization in August 2024.

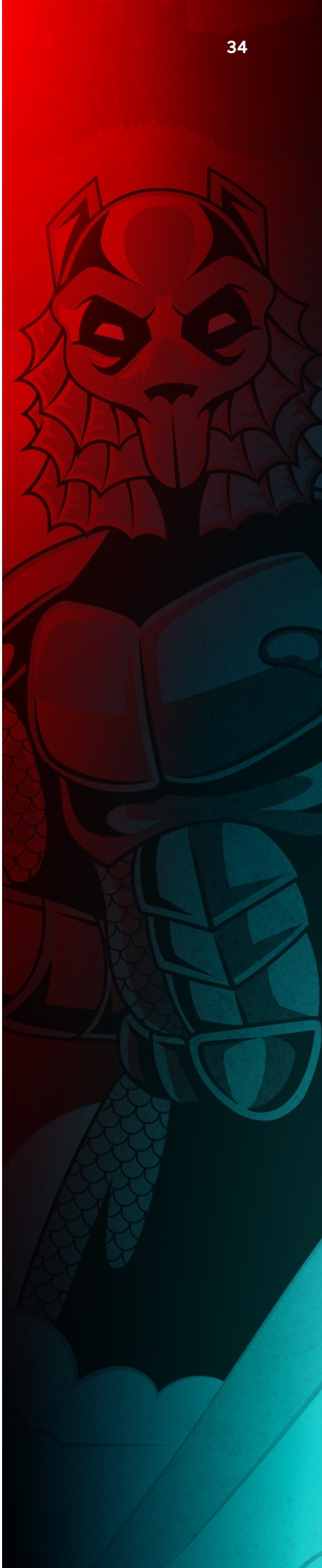
China-nexus threat actors likely target this sector to collect intelligence, obtain PII, and steal intellectual property regarding research and development in vaccines and biomedical technologies. This targeting pattern aligns with China's strategic interest in advancing its biotechnology capabilities and understanding Western medical innovations that are critical to national health security.

European Government and Defense Sector Targeting

During the reporting period, VIXEN PANDA has been the most prolific threat to government and defense entities in Europe. From early 2024 through early 2025, VIXEN PANDA engaged in systematic scanning operations using an operational relay box (ORB) network tracked as ORB02, demonstrating the adversary's operational persistence and scope.

VIXEN PANDA's activities in the latter half of 2024 progressed from broad reconnaissance efforts against hundreds of network security devices across multiple European countries to targeted attempts to exploit perimeter appliances at government and defense entities in Slovenia, Romania, the Czech Republic, and EU institutions. VIXEN PANDA's February 2025 targeting of a U.S. government agency's European operations indicates the adversary is maintaining their operational tempo and focusing on high-value government and defense targets.

Between September 2024 and March 2025, observations in third-party network telemetry data indicate TREASURE PANDA likely targeted Russian aerospace and defense entities developing military radar systems. The adversary's broad target scope has extended into Eastern Europe, likely due to Russia's invasion of Ukraine in 2022.



In January 2024, an unattributed China-nexus threat actor targeted an Italian government entity and engaged in hands-on-keyboard activity involving reconnaissance, LSASS memory dumping, and *PlugX* implant deployment. This activity occurred shortly after Italy formally withdrew from China's Belt and Road Initiative in December 2023, suggesting the threat actor potentially had retaliatory or intelligence-gathering motivations.

China-nexus threat actors' targeting of multiple EU institutions and NATO-aligned countries likely reflects Beijing's priority to monitor European defense coordination and policy development. China considers European government and defense entities critical sources for understanding Western alliance dynamics, defense capabilities, and policy development processes. China-nexus adversaries also continue to target European countries that are not aligned with Western politics. These adversaries have targeted Russian entities — which aligns with the geographic mission of the People's Liberation Army (PLA) Northern Theater Command units — likely to collect intelligence regarding national security and defense.

European Manufacturing Sector Targeting

VERTIGO PANDA has targeted the European manufacturing sector with USB-based exploitation techniques. In February 2024, VERTIGO PANDA targeted a Western European manufacturing entity's Vietnam-based operations using an infected USB drive containing multiple malicious components, including the adversary's signature *InstituteX* implant. Given the persistent nature of malware delivery via removable media, CrowdStrike Intelligence cannot determine whether these samples represent ongoing novel VERTIGO PANDA attempts to deploy *InstituteX* or continuing reinfections.

European Financial Services Sector Targeting

Financial services entities face targeted intelligence collection efforts from China-nexus adversaries, with VAULT PANDA conducting reconnaissance against Swiss financial institutions in January 2024. The adversary used *Acunetix* for initial reconnaissance to identify exploitable vulnerabilities.

In August 2024, WICKED PANDA conducted a large-scale phishing campaign targeting insurance entities across multiple European countries, including the U.K., France, Italy, and Germany. The adversary used compromised tax authority emails to deliver the *Voldemort* malware.

China-nexus adversaries appear to target financial institutions to collect intelligence and steal PII. The collected data is likely useful for assessing monetary assets and facilitating follow-on intelligence activities. This suggests China's interest in understanding European financial capabilities and potentially identifying targets for future economic espionage operations.

European Academic Sector Targeting

Academic institutions and research organizations face systematic targeting as part of broader multi-sector campaigns, with VIXEN PANDA conducting reconnaissance against academic entities and EU research institutions in April 2024. WICKED PANDA also targeted European academic institutions in an August 2024 phishing campaign that impacted more than 70 global targets. Targeting EU research institutions alongside government and military entities suggests China recognizes academia's critical role in European technological advancement and defense capabilities.

European Technology Sector Targeting

In June 2025 and July 2025, CrowdStrike OverWatch and CrowdStrike Services responded to GENESIS PANDA's intrusion activity at a Spain-based technology firm. The adversary likely gained initial access by compromising a Microsoft SQL Server instance. During the intrusion, GENESIS PANDA engaged in basic reconnaissance activity, attempted to move laterally via Windows Remote Shell, and downloaded multiple implants and tools — including *Sliver* and *Cobalt Strike* — from known adversary-controlled infrastructure.

During the reporting period, China-nexus activity targeting Europe-based technology organizations was low; however, China-nexus adversaries consistently targeted technology entities more than any other sector worldwide. Technology organizations are routinely targeted to fulfill adversaries' traditional intelligence collection and industrial espionage requirements, highlighting that cyber espionage is integral to China's national information-gathering efforts. Given that China-nexus adversaries have historically significantly targeted technology entities worldwide, the European technology sector is likely a high-priority target for them.

European Nonprofit and NGO Sector Targeting

In June 2024, CASCADE PANDA successfully deployed *WinDealer* malware at a Western European nonprofit's China-based offices. This targeting demonstrated China's interest in monitoring international NGOs operating in Chinese territory and suggests potential concerns regarding foreign influence operations or intelligence collection activities conducted through nonprofit organizations.

DPRK-NEXUS ACTIVITY

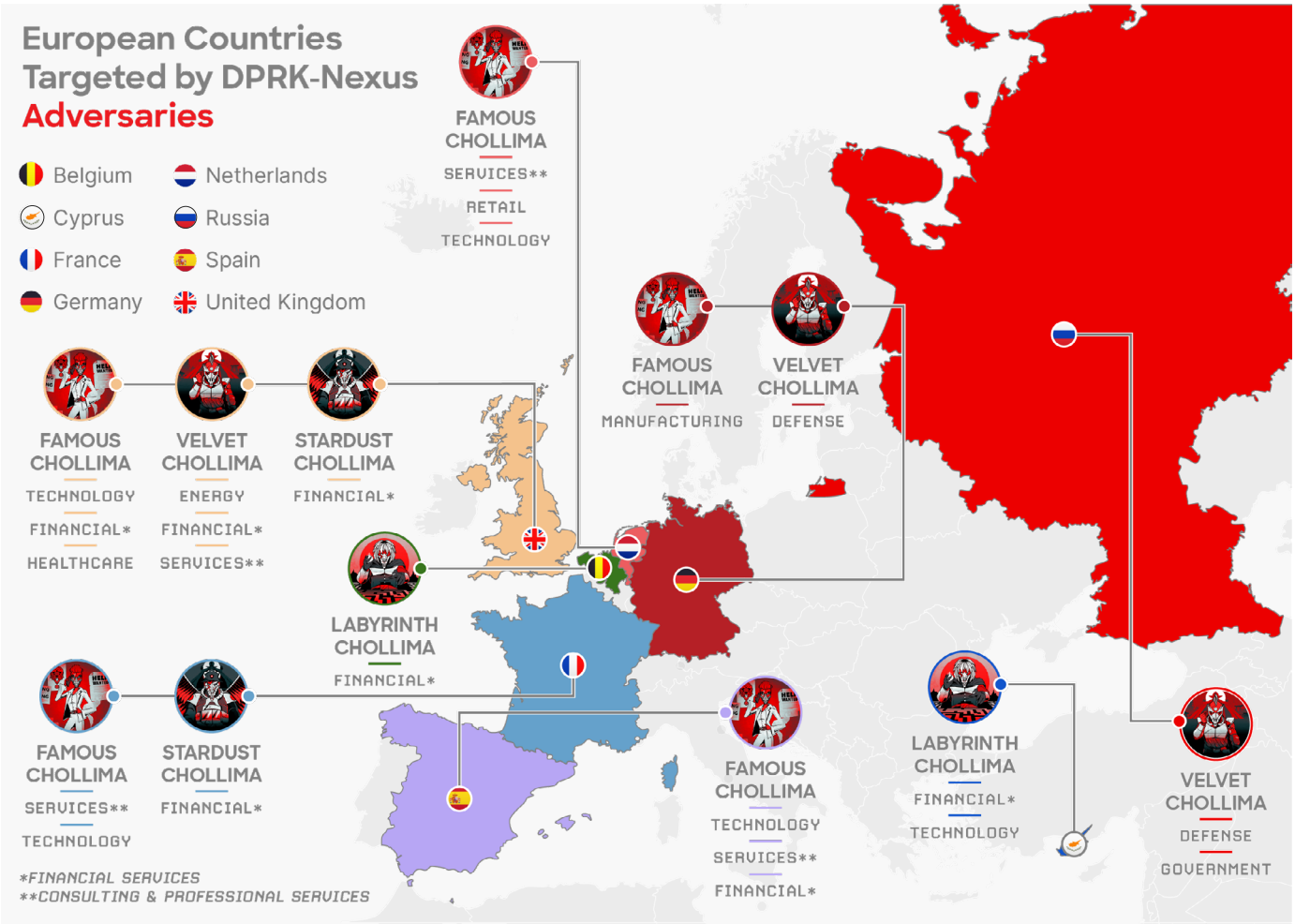


Figure 11. DPRK-nexus targeting of European countries

North Korea has historically targeted European entities due to the region's status as an economic, diplomatic, and military hub with deep influence on Korean Peninsula issues. DPRK-nexus adversaries are motivated by collecting intelligence on policy affairs, military issues, and currency generation and have targeted various European government, defense, financial services, and consulting entities. This targeting aligns with North Korea's priorities of obtaining nuclear weapons and advanced military technology and gaining regional influence in Northeast Asia.

European Defense Sector Targeting

Since at least April 2024, DPRK-nexus adversaries VELVET CHOLLIMA and LABYRINTH CHOLLIMA have targeted European defense entities to possibly steal intellectual property and/or fulfill military intelligence requirements. This activity likely supports North Korea's military technology and allows the country to obtain tactical intelligence on European weapons systems, which Ukrainian forces may use against DPRK soldiers fighting in alliance with Russia.

Additionally, several European countries contribute forces and material to the UN Command stationed in the Republic of Korea (ROK). The UN Command is a multi-lateral body formed in 1950 to counter the DPRK's aggression against the ROK during the Korean War. The Korean War ended in an armistice, and the belligerents remain in a legal state of war, making European defense and military organizations an attractive target in the DPRK's cyber espionage operations.

Between May 2024 and at least September 2024, VELVET CHOLLIMA likely targeted a German defense manufacturer's employees via a credential phishing campaign deploying their *HTTPSpy* malware. Targeting defense manufacturing entities to collect intellectual property or military intelligence aligns with VELVET CHOLLIMA's known target scope and motivations.

In August 2024, LABYRINTH CHOLLIMA posed as a job recruiter to entice an employee at a European defense entity into downloading a malicious job-themed ZIP file hosted on a cloud file sharing service. This defense entity — which works in areas of high interest to the North Korean regime (e.g., satellites and aerial reconnaissance) — aligns with the DPRK's intelligence requirements.[24] Subsequently, in May 2025, the adversary targeted a European defense entity with an employment-themed ZIP file delivered via WhatsApp.

European Financial Services Targeting

European financial institutions and financial technology (fintech) companies are high-value targets for financially motivated DPRK operations, as Europe contains many well-developed financial and fintech entities. Many European jurisdictions have also relaxed financial regulations, which could contribute to a perception of lower security levels or reluctance to report cybersecurity incidents. Both scenarios likely heighten DPRK-nexus adversaries' interest in targeting these entities.

Between January 2025 and June 2025, STARDUST CHOLLIMA, which has an exclusive currency-generating mandate, targeted European cryptocurrency and finance entities. In several incidents, the adversary leveraged video conference-themed phishing lures masquerading as venture capital opportunities. These lures enticed targets to download and execute AppleScript payloads that purportedly correct meeting access or audio issues. STARDUST CHOLLIMA's campaigns are very likely motivated by the DPRK's need for digital assets and to evade international sanctions.

In Q3 2024, LABYRINTH CHOLLIMA impersonated a job recruiter on LinkedIn to entice an employee at a Western Europe-based fintech company into joining a Slack workspace for the fake company. The victim downloaded a trojanized Python project containing *SnakeBaker* that masqueraded as a skills assessment. After the victim executed the project, LABYRINTH CHOLLIMA accessed the victim's cloud environment access key, conducted reconnaissance, moved laterally, and ultimately diverted cryptocurrency funds.

24 https://kcnawatch.org/newstream/1610155111-665078257/on-report-made-by-supreme-leader-kim-jong-un-at-8th-congress-of-wpk/

European Energy Sector Targeting

Between April 2024 and October 2024, VELVET CHOLLIMA spoofed U.K. energy entities and numerous organizations in the U.S. and Japan. Whether VELVET CHOLLIMA was specifically targeting the energy sector — or whether they were attempting to compromise an individual accessing public-facing energy websites — remains unclear. If the former, the collected data could support the DPRK's likely long-standing intelligence requirements on energy technology. Additionally, nuclear energy technology is inherently dual use, and North Korea could plausibly use any stolen information to support its military nuclear program.

However, this activity is an anomaly for VELVET CHOLLIMA. DPRK adversaries do not currently pose a significant threat to European energy companies.

European Professional Services Sector Targeting

Also during the April 2024 to October 2024 campaign, VELVET CHOLLIMA targeted U.K. professional services entities using spoofed domains. This activity likely supports the adversary's broader intelligence collection objectives regarding Western policy positions and accessing entities that influence diplomatic and economic decision-making processes.

FAMOUS CHOLLIMA

During the reporting period, FAMOUS CHOLLIMA used malware and insider threats to target Europe-based entities in opportunistic and sector-agnostic activity. FAMOUS CHOLLIMA's operations appear to be financially motivated, as their activity consistently involves small-value cryptocurrency theft or credit card fraud as well as receiving illicit salaries. FAMOUS CHOLLIMA uses employment-themed lures to entice targets into downloading and executing malicious payloads hosted on GitHub and Bitbucket. The adversary also lures targets into visiting malicious infrastructure that masquerades as virtual interviewing or skills assessment platforms.

European individuals have also helped facilitate FAMOUS CHOLLIMA's insider threat operations. In May 2024, the U.S. DOJ indicted and coordinated the arrest of a Ukrainian national for running a service that operated three laptop farms and sold profiles on popular freelancing websites, enabling FAMOUS CHOLLIMA operators to falsify their identities.

Additionally, CrowdStrike Intelligence identified a Poland-based laptop farm that the adversary used in June 2025. The U.S. DOJ has also sanctioned a Russian national for working with a Russia-based DPRK consular official to facilitate payments to an entity employing DPRK IT workers in Russia and Laos.

In September 2024, the U.K.'s Office of Financial Sanctions Implementation (OFSI) issued an advisory describing FAMOUS CHOLLIMA's first-known operations targeting the U.K. Since then, CrowdStrike Intelligence has observed several insider threat operations targeting European-based entities.

REST-OF-WORLD ACTIVITY

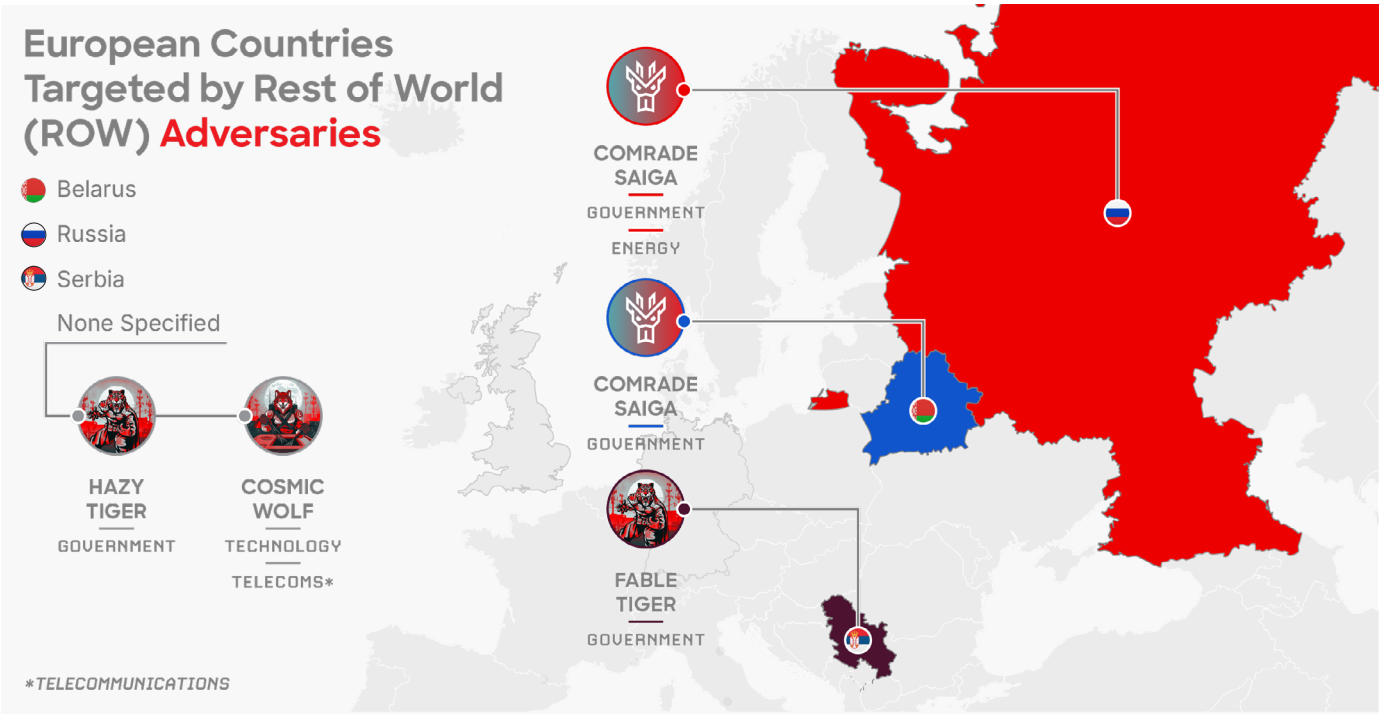


Figure 12. European countries targeted by the rest of the world

Between January 2024 and September 2025, CrowdStrike Intelligence observed few instances of rest-of-world (ROW) adversaries targeting European entities. However, two adversaries — COSMIC WOLF and COMRADE SAIGA — remain relevant threats to specific sectors based on their historical activity, target scopes, and motivations.

Türkiye-Nexus Adversaries

Despite minimal observed activity since early 2024, Türkiye-nexus adversary COSMIC WOLF remains a relevant threat to European entities, particularly to technology and telecommunications entities. In December 2023, COSMIC WOLF deployed the *Torchlight* Linux implant and used living-off-the-land techniques at a Europe-based technology company. Though the adversary's initial access method is unknown, CrowdStrike Intelligence research indicates they obtained a private SSH key for a server in the target environment.

Based on COSMIC WOLF's activity since 2022, the adversary likely focuses on European telecom and technology entities. Compromising these entities likely enables COSMIC WOLF to target downstream entities more directly relevant to Türkiye's intelligence requirements, such as minority groups and political dissidents in Türkiye.

Kazakhstan-Nexus Adversaries

Kazakhstan-nexus adversary COMRADE SAIGA has not been observed targeting European entities between January 2024 and September 2025. However, the adversary is a relevant threat to European MFAs, particularly those with embassies in Kazakhstan. Outside of Russia, COMRADE SAIGA predominantly targets government and energy entities associated with or operating in the CIS region.

Among government entities, COMRADE SAIGA most commonly targets MFAs, almost certainly to collect intelligence on diplomatic issues relevant to Kazakhstan and the CIS region. In late January 2023, COMRADE SAIGA likely targeted a European embassy in Astana, Kazakhstan, using a phishing email containing a malicious attachment. The adversary's focus on MFAs — which has not been observed against European entities since 2023 — highly likely indicates that COMRADE SAIGA aims to collect intelligence regarding Kazakhstan's diplomatic efforts.

India-Nexus Adversaries

From January 2024 to September 2025, India-nexus adversaries only conducted one incident targeting European entities. In November 2024, HAZY TIGER targeted diplomatic entities in China — including representatives from a European trade mission — likely using spear-phishing emails with search connector files linked to malicious WebDAV directories. HAZY TIGER was likely continuing their intelligence collection efforts regarding Chinese diplomatic relations rather than specifically targeting the trade mission.

In late 2023, FABLE TIGER likely targeted a Serbian government entity using a credential harvesting website spoofing the organization's webmail login page. FABLE TIGER typically targets South Asian entities, and CrowdStrike Intelligence cannot currently assess the adversary's motivation for this activity.

India-nexus activity against the region will highly likely remain infrequent or tangential over the next year. This assessment is made with high confidence based on India-nexus adversaries' predominant focus on South and Southeast Asian targets, with minimal activity against European entities.

Hacktivism and Non-State Overview

Between January 2024 and September 2025, CrowdStrike Intelligence observed numerous hacktivist groups claiming to target industrial control systems (ICSs) across Europe both in response to conflicts and in non-conflict-related activity. Pro-Russia hacktivist group *Z-Alliance* conducted most of this activity against countries perceived to be hostile toward Russia. Hacktivists' growing interest in targeting ICSs is likely due to the potential significant impact and the associated media attention.

During this reporting period, international law enforcement — including European authorities — disrupted multiple hacktivist groups' infrastructure and arrested hacktivist members. This law enforcement activity aligns with broader European goals to combat cybercrime, such as the European Multidisciplinary Platform Against Criminal Threats' (EMPACT) classification of cybercrime as a high priority in EMPACT 2022-2025.[25]

25 https://www.europol.europa.eu/crime-areas-and-trends/eu-policy-cycle-empact

Industrial Control System Targeting

Between January 2024 and September 2025, numerous hacktivist groups claimed to target ICSs, SCADA systems, internet of things (IoT) devices, and operational technology (OT) across Europe. The purported activity primarily consisted of device setting manipulation, defacements, DDoS attacks against externally facing systems, and credential theft.

Hacktivists stated that political grievances were the primary driver for ICS targeting, with *Z-Alliance* responsible for the largest volume of claims during this time. The group reportedly used publicly available tools such as Shodan and RealVNC Viewer in their attacks.

Additional hacktivist groups — including *APT Iran*, *Cyber Av3ngers*, *Infrastructure Destruction Squad (IDS)*, *GhostSec*, *Golden Falcon Team*, *Maxious Greyhat*, *Russian Partisan*, and *Laneh | Dark* — also claimed to target ICS devices during this time. Though their purported activity focused on non-European entities, these claims highlighted hacktivists' growing interest in targeting ICS devices.

Hacktivist groups will likely continue demonstrating interest in targeting ICSs globally over the next 12 months. However, most will likely demonstrate limited technical capabilities and rely on exaggerated claims or publicly available malware designed to target ICS devices. These assessments are made with moderate confidence based on an observed increase in claimed hacktivist activity against these devices and systems during the reporting period as well as hacktivists' desire for attention.

Hacktivist Response to European Law Enforcement Actions

Between January 2024 and September 2025, European law enforcement agencies conducted numerous operations against hacktivist groups, resulting in hundreds of arrests and significant infrastructure seizures across multiple countries. Hacktivists responded to law enforcement activity through retaliatory campaigns against entities in the targeted countries, OPSEC adjustments, and strategic social media messaging to downplay the impact of law enforcement activity.

During this time, multiple law enforcement actions targeted BOUNTY JACKAL. In July 2024, Spanish authorities arrested BOUNTY JACKAL members. These arrests prompted the adversary to implement new OPSEC procedures and launch coordinated DDoS attacks against Spanish websites.

Similarly, after the Europol-led Operation Eastwood disrupted BOUNTY JACKAL's infrastructure in July 2025, the adversary quickly initiated Operation Time of Retribution. The adversary targeted countries associated with Operation Eastwood with DDoS attacks, website defacements, and purported infrastructure breaches and claimed the Europol operation caused limited impact to the group.

As global law enforcement agencies continue to target cybercrime, hacktivists will likely continue to respond with retaliatory campaigns, operational changes, and social media posts.

Conclusion

eCrime adversaries will almost certainly continue to prioritize targeting Europe-based entities in the foreseeable future due to financial motivations. Data extortion and ransomware will highly likely remain the most critical eCrime threat facing Europe, given the impact of successful intrusions and BGH adversaries' sustained targeting preference for the region.

While the potential impact of successful intrusions remains high, eCrime adversaries benefit from historical and evolving initial access and malware delivery techniques, as demonstrated by adversaries' abrupt and broad adoption of vishing and CAPTCHA lures. The popularity of AI will likely further this evolution.

Since 2024, international law enforcement operations have impacted eCrime adversaries' operations, forums (e.g., BreachForums and XSS), and enabling services. However, the English- and Russian-language underground ecosystems are resilient, as they are decentralized and involve threat actors that operate without consequences in apparent safe haven countries.

Therefore, eCrime threat actors based in and targeting Europe will continue to benefit from an ecosystem that enables threat actors of varying sophistication and lowers the entry barrier for eCrime. Given the ecosystem's anonymity and enabling services' indiscriminate nature, non-eCrime threats (including hybrid threat actor RENAISSANCE SPIDER and Russia-nexus EMBER BEAR) also benefit from these networks.

State-nexus adversaries will almost certainly continue to collect intelligence to shape national policy and engagement with European entities. Adversarial states are highly motivated to target European entities likely because they offer lucrative political, economic, and technological information that can be exploited to advance strategic interests.

Geopolitical developments can rapidly alter an adversary's intelligence requirements and operational scope. For countries such as Russia and Iran, cyber capabilities are integral for responding to conflicts perceived as threats to their sovereignty. Both countries conduct a full spectrum of operations, from passive espionage and reconnaissance campaigns to destructive hack-and-leak campaigns disguised as hacktivism and overtly destructive attacks. These operations offer plausible deniability, hinder attribution efforts, and reduce financial and human costs, allowing these states to project power and influence beyond conventional capabilities.

Additionally, other state-nexus threat actors target European entities due to economic and financial motives. China-nexus adversaries often conduct intellectual property theft to bolster China's international competitive edge and avoid costly internal research and development. In addition to intelligence collection efforts, DPRK-nexus adversaries often conduct opportunistic revenue-generation activities (such as cryptocurrency theft) to finance the DPRK regime.

Global conflicts will likely continue to motivate hacktivist activity against European entities over the next 12 months. To maximize their public impact, some hacktivist groups will likely claim to target critical OT, including ICSs and SCADA systems, across Europe and globally. As international law enforcement agencies intensify their operations against cybercrime, hacktivists will likely respond via retaliatory campaigns, tactical shifts, and coordinated social media activity.

Recommendations

1 Adopt agentic AI to scale security operations

As threat actors adopt AI to strike faster, scale operations, and evade detection, defenders face mounting pressure to keep pace. Security teams are already stretched thin, grappling with growing alerts, contending with skills shortages, and racing to respond at speed. To close these widening gaps, security teams should operationalize agentic AI — specialized agents capable of reasoning, adapting, and acting within defined guardrails and organizational policies. Agentic AI allows teams to apply expert reasoning and machine speed to accelerate outcomes and automate work. These capabilities can scale intelligence-driven operations by applying emerging threat intelligence and expertise to triage alerts, conduct investigations, and execute response actions. By offloading time-intensive, repetitive tasks, agentic AI empowers human analysts to focus on proactive threat hunting and hypothesis-driven investigation, elevating both strategic impact and operational efficiency.

2 Secure the entire identity ecosystem

Adversaries increasingly target identities using credential theft, multifactor authentication bypass, and social engineering while moving laterally between on-premises, cloud, and SaaS environments via trusted relationships. This allows them to impersonate legitimate users, escalate privileges, and evade detection.

Organizations should adopt phishing-resistant multifactor authentication solutions, such as hardware security keys, to prevent unauthorized access. Strong identity and access policies are essential, including just-in-time access, regular account reviews, and conditional access controls. Identity threat detection tools must monitor behavior across endpoints and on-premises, cloud, and SaaS environments to flag privilege escalation, unauthorized access, and backdoor account creation. Integrating these tools with extended detection and response (XDR) platforms enables comprehensive visibility and a unified defense against adversaries.

Additionally, organizations should educate users to recognize vishing and phishing attempts while maintaining proactive monitoring to detect and respond to identity-based threats.

3 Eliminate cross-domain visibility gaps

Adversaries' growing use of hands-on-keyboard techniques and legitimate tools makes detection and response more difficult. Unlike traditional malware, these methods allow attackers to bypass legacy security measures by executing commands and using legitimate software to mimic normal operations.

To counter this, organizations must modernize their detection and response strategies. Solutions like next-gen security information and event management (SIEM) provide unified visibility across endpoints, networks, cloud environments, and identity systems, enabling analysts to correlate suspicious behaviors and see the full attack path. Agentic AI-powered triage and investigations can extend these capabilities, autonomously analyzing signals across domains to surface high-fidelity insights and prioritize real threats.

Proactive threat hunting and threat intelligence further enhance detection by identifying potential attack patterns and providing insights into adversary TTPs. With real-time intelligence, organizations can stay informed about emerging threats, anticipate attacks, and prioritize critical security efforts.

4 Defend the cloud as core infrastructure

Cloud-focused adversaries are exploiting misconfigurations, stolen credentials, and cloud management tools to infiltrate systems, move laterally, and maintain persistent access for malicious activities like data theft and ransomware deployment.

Cloud-native application protection platforms (CNAPPs) with cloud detection and response (CDR) capabilities are critical to counter these threats. These solutions provide operators with a unified view of their cloud security posture, helping them rapidly detect, prioritize, and remediate misconfigurations, vulnerabilities, and adversary threats. Additionally, enforcing strict access controls — such as role-based access and conditional policies — limits exposure to critical systems while continuously monitoring for anomalies, including logins from unexpected locations.

Regular audits are also critical to maintaining security. Automated tools can uncover overly permissive storage settings, exposed APIs, and unpatched vulnerabilities. Frequent reviews of cloud environments allow teams to promptly address unused permissions and outdated configurations.

5 Prioritize vulnerabilities with an adversary-centric approach

Adversaries are increasingly exploiting publicly disclosed vulnerabilities and using exploit chaining, combining multiple vulnerabilities to gain rapid access, escalate privileges, and bypass defenses. These multi-stage attacks often rely on public resources like proof-of-concept exploits and technical blogs, enabling adversaries to craft effective and hard-to-detect payloads.

To counter these threats, organizations must prioritize regular patching or upgrading of critical systems, especially frequently targeted internet-facing services like web servers and VPN gateways. Monitoring for subtle signs of exploit chaining, such as unexpected crashes or privilege escalation attempts, can help detect attacks before they progress.

Tools like CrowdStrike Falcon® Exposure Management, built with native AI prioritization, enable teams to reduce noise and focus on the vulnerabilities that matter most, specifically those affecting critical and high-risk systems. By adopting proactive security approaches, discovering exposures across the attack surface, and leveraging automation, organizations can mitigate sophisticated threats and limit adversary opportunities.

6 Know the adversary and be prepared

When a cyberattack unfolds in minutes — or even seconds — being prepared can be the difference between containment and catastrophe. An intelligence-driven approach enables security teams to move beyond reactive defense by understanding which adversary is targeting them, how they operate, and what their objectives are. With threat intelligence, adversary profiling, and tradecraft analysis, security teams can prioritize resources, adapt defenses, and actively hunt for threats before they escalate. CrowdStrike's threat intelligence doesn't just detect known threats — it anticipates new and evolving tradecraft, keeping defenders one step ahead. By seamlessly integrating intelligence into security workflows, organizations can accelerate response times, disrupt adversaries, and turn intelligence into action.

Though technology is critical to detect and stop intrusions, the end user remains a crucial link in the chain to stop breaches. Organizations should initiate user awareness programs to combat the continued threat of phishing and related social engineering techniques. For security teams, practice makes perfect. Encourage an environment that routinely performs tabletop exercises and red/blue teaming to identify gaps and eliminate weaknesses in your cybersecurity practices and response.

About CrowdStrike

CrowdStrike (Nasdaq: CRWD), a global cybersecurity leader, has redefined modern security with the world's most advanced cloud-native platform for protecting critical areas of enterprise risk — endpoints and cloud workloads, identity and data.

Powered by the CrowdStrike Security Cloud and world-class AI, the CrowdStrike Falcon® platform leverages real-time indicators of attack, threat intelligence, evolving adversary tradecraft and enriched telemetry from across the enterprise to deliver hyper-accurate detections, automated protection and remediation, elite threat hunting and prioritized observability of vulnerabilities.

Purpose-built in the cloud with a single lightweight-agent architecture, the Falcon platform delivers rapid and scalable deployment, superior protection and performance, reduced complexity and immediate time-to-value.

CrowdStrike: We stop breaches.

Learn more: www.crowdstrike.com

Follow us: Blog | X | LinkedIn | Facebook | Instagram | YouTube

Start a free trial today: www.crowdstrike.com/free-trial-guide