Threats to the Defense Industrial Base

By Google Threat Intelligence Group

Published: 2026-02-10 · Archived: 2026-04-05 12:51:04 UTC

Introduction

In modern warfare, the front lines are no longer confined to the battlefield; they extend directly into the servers and supply chains of the industry that safeguards the nation. Today, the defense sector faces a relentless barrage of cyber operations conducted by state-sponsored actors and criminal groups alike. In recent years, Google Threat Intelligence Group (GTIG) has observed several distinct areas of focus in adversarial targeting of the defense industrial base (DIB). While not exhaustive of all actors and means, some of the more prominent themes in the landscape today include:

- Consistent effort has been dedicated to targeting defense entities fielding technologies on the battlefield in the Russia-Ukraine War. As next-generation capabilities are being operationalized in this environment, Russia-nexus threat actors and hacktivists are seeking to **compromise defense contractors** alongside military assets and systems, with a focus on organizations involved with unmanned aircraft systems (UAS). This includes targeting defense companies directly, using themes mimicking their products and systems in intrusions against military organizations and personnel.
- Across global defense and aerospace firms, the **direct targeting of employees and exploitation of the hiring process** has emerged as a key theme. From the North Korean IT worker threat, to the spoofing of recruitment portals by Iranian espionage actors, to the direct targeting of defense contractors' personal emails, GTIG continues to observe a multifaceted threat landscape that centers around personnel, and often in a manner that evades traditional enterprise security visibility.
- Among state-sponsored **cyber espionage** intrusions over the last two years analysed by GTIG, threat activity from **China-nexus groups continues to represent by volume the most active** threat to entities in the defense industrial base. While these intrusions continue to leverage an array of tactics, campaigns from actors such as UNC3886 and UNC5221 highlight how the targeting of edge devices and appliances as a means of initial access has increased as a tactic by China-nexus threat actors, and poses a significant risk to the defense and aerospace sector. In comparison to the Russia-nexus threats observed on the battlefield in Ukraine, these could support more preparatory access or R&D theft missions.
- Lastly, contemporary national security strategy relies heavily on a secure supply chain. Since 2020, **manufacturing has been the most represented sector across data leak sites** (DLS) that GTIG tracks associated with ransomware and extortive activity. While dedicated defense and aerospace organizations represent a small fraction of similar activity, the broader manufacturing sector includes many companies that provide dual-use components for defense applications, and this statistic highlights the cyber risk the industrial base supply chain is exposed to. The ability to surge defense components in a wartime environment can be impacted, even when these intrusions are limited to IT networks. Additionally, the

global resurgence of hacktivism, and actors carrying out hack and leak operations, DDoS attacks, or other forms of disruption, has impacted the defense industrial base.

Across these themes we see further areas of commonality. Many of the chief state-sponsors of cyber espionage and hacktivist actors have shown an interest in autonomous vehicles and drones, as these platforms play an increasing role in modern warfare. Further, the “evasion of detection” trend first highlighted in the Mandiant M-Trends 2024 report continues, as actors focus on single endpoints and individuals, or carry out intrusions in a manner that seeks to avoid endpoint detection and response (EDR) tools altogether. All of this contributes to a contested and complex environment that challenges traditional detection strategies, requiring everyone from security practitioners to policymakers to think creatively in countering these threats.

1. Longstanding Russian Targeting of Critical and Emerging Defense Technologies in Ukraine and Beyond

Russian espionage actors have demonstrated a longstanding interest in Western defense entities. While Russia's full-scale invasion of Ukraine began in February 2022, the Russian government has long viewed the conflict as an extension of a broader campaign against Western encroachment into its sphere of influence, and has accordingly targeted both Ukrainian and Western military and defense-related entities via kinetic and cyber operations.

Russia's use of cyber operations in support of military objectives in the war against Ukraine and beyond is multifaceted. On a tactical level, targeting has broadened to include individuals in addition to organizations in order to support frontline operations and beyond, likely due at least in part to the reliance on public and off-the-shelf technology rather than custom products. Russian threat actors have targeted secure messaging applications used by the Ukrainian military to communicate and orchestrate military operations, including via attempts to exfiltrate locally stored databases of these apps, such as from mobile devices captured during Russia's ongoing invasion of Ukraine. This compromise of individuals' devices and accounts poses a challenge in various ways—for example, such activity often occurs outside spaces that are traditionally monitored, meaning a lack of visibility for defenders in monitoring or detecting such threats. GTIG has also identified attempts to compromise users of battlefield management systems such as Delta and Kropyva, underscoring the critical role played by these systems in the orchestration of tactical efforts and dissemination of vital intelligence.

More broadly, Russian espionage activity has also encompassed the targeting of Ukrainian and Western companies supporting Ukraine in the conflict or otherwise focused on developing and providing defensive capabilities for the West. This has included the use of infrastructure and lures themed around military equipment manufacturers, drone production and development, anti-drone defense systems, and surveillance systems, indicating the likely targeting of organizations with a need for such technologies.

APT44 (Sandworm, FROZENBARENTS)

APT44, attributed by multiple governments to Unit 74455 within the Russian Armed Forces' Main Intelligence Directorate (GRU), has attempted to exfiltrate information from Telegram and Signal encrypted messaging applications, likely via physical access to devices obtained during operations in Ukraine. While this activity extends back to at least 2023, we have continued to observe the group making these attempts. GTIG has also identified APT44 leveraging WAVESIGN, a Windows Batch script responsible for decrypting and exfiltrating data

from Signal Desktop. Multiple governments have also reported on APT44's use of INFAMOUSCHISEL, malware designed to collect information from Android devices including system device information, commercial application information, and information from Ukrainian military apps.

TEMP.Vermin

TEMP.Vermin, an espionage actor whose activity Ukraine's Computer Emergency Response Team (CERT-UA) has linked to security agencies of the so-called Luhansk People's Republic (LPR, also rendered as LNR), has deployed malware including VERMONSTER, SPECTRUM (publicly reported as Spectr), and FIRMACHAGENT via the use of lure content themed around drone production and development, anti-drone defense systems, and video surveillance security systems. Infrastructure leveraged by TEMP.Vermin includes domains masquerading as Telegram and involve broad aerospace themes including a domain that may be a masquerade of an Indian aerospace company focused on advanced drone technology.

Figure 1: Lure document used by TEMP.Vermin

UNC5125

UNC5125 has conducted highly targeted campaigns focusing on frontline drone units. Its collection efforts have included the use of a questionnaire hosted on Google Forms to conduct reconnaissance against prospective drone operators; the questionnaire purports to originate from Dronarium, a drone training academy, and solicits personal information from targets, notably including military unit information, telephone numbers, and preferred mobile messaging apps. UNC5125 has also conducted malware delivery operations via these messaging apps. In one instance, the cluster delivered the MESSYFORK backdoor (publicly reported as COOKBOX) to an UAV operator in Ukraine.

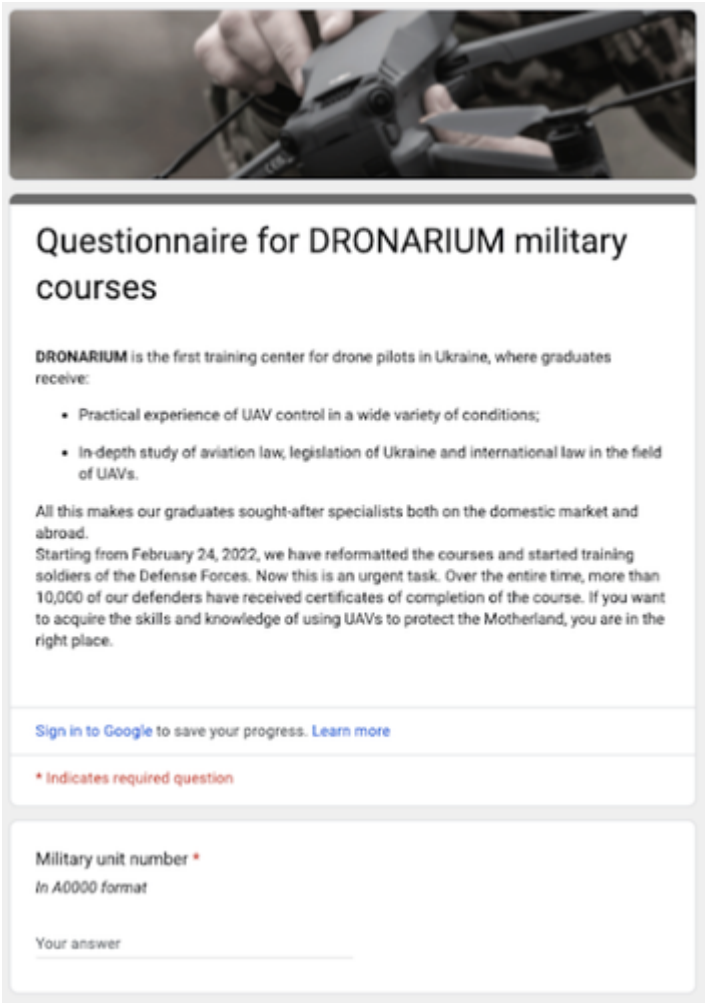


Figure 2: UNC5125 Google Forms questionnaire purporting to originate from Dronarium drone training academy

We also identified suspected UNC5125 activity leveraging Android malware we track as GREYBATTLE, which was delivered via a website spoofing a Ukrainian military artificial intelligence company. GREYBATTLE, a customized variant of the Hydra banking trojan, is designed to extract credentials and data from compromised devices.

Note: Android users with Google Play Protect enabled are protected against the aforementioned malware, and all known versions of the malicious apps identified throughout this report.

UNC5792

Since at least 2024, GTIG has identified this Russian espionage cluster exploiting secure messaging apps, targeting primarily Ukrainian military and government entities in addition to individuals and organizations in Moldova, Georgia, France, and the US. Notably, UNC5792 has compromised Signal accounts via the device-linking feature. Specifically, UNC5792 sent its targets altered "group invite" pages that redirected to malicious URLs crafted to link an actor-controlled device to the victim's Signal accounts allowing the threat actor to see victims' message in real time. The cluster has also leveraged WhatsApp phishing pages and other domains masquerading as Ukrainian defense manufacturing and defense technology companies.

UNC4221

UNC4221, another suspected Russian espionage actor active since at least March 2022, has targeted secure messaging apps used by Ukrainian military personnel via tactics similar to those of UNC5792. For example, the cluster leveraged fake Signal group invites that redirect to a website crafted to elicit users to link their account to an actor-controlled Signal instance. UNC4221 has also leveraged WhatsApp phishing pages intended to collect geolocation data from targeted devices.

UNC4221 has targeted mobile applications used by the Ukrainian military in multiple instances, such as by leveraging Signal phishing kits masquerading as Kropyva, a tactical battlefield app used by the Armed Forces of Ukraine for a variety of combat functions including artillery guidance. Other Signal phishing domains used by UNC4221 masqueraded as a streaming service for UAVs used by the Ukrainian military. The cluster also leveraged the STALECOOKIE Android malware, which was designed to masquerade as an application for Delta, a situational awareness and battlefield management platform used by the Ukrainian military, to steal browser cookies.

UNC4221 has also conducted malware delivery operations targeting both Android and Windows devices. In one instance, the actor leveraged the "ClickFix" social engineering technique, which lured the target into copying and running malicious PowerShell commands via instructions referencing a Ukrainian defense manufacturer, in a likely attempt to deliver the TINYWHALE downloader. TINYWHALE in turn led to the download and execution of the MESHAGENT remote management software against a likely Ukrainian military entity.

UNC5976

Starting in January 2025, the suspected Russian espionage cluster UNC5976 conducted a phishing campaign delivering malicious RDP connection files. These files were configured to communicate with actor-controlled domains spoofing a Ukrainian telecommunications entity. Additional infrastructure likely used by UNC5976 included hundreds of domains spoofing defense contractors including companies headquartered in the UK, the US, Germany, France, Sweden, Norway, Ukraine, Turkey, and South Korea.

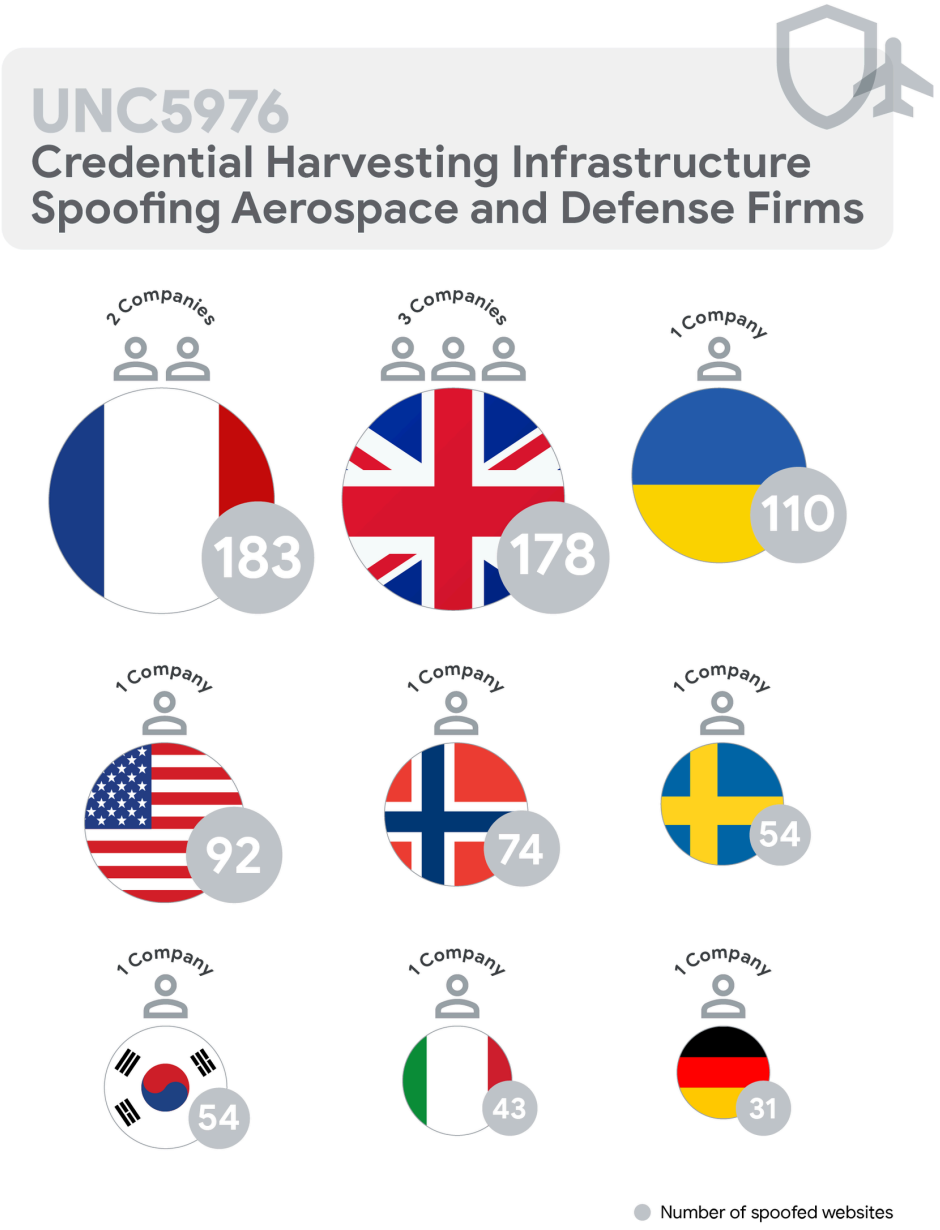


Figure 3: Identified UNC5976 credential harvesting infrastructure spoofing aerospace and defense firms

Wider UNC5976 phishing activity also included the use of drone-themed lure content, such as operational documentation for the ORLAN-15 UAV system, likely for credential harvesting efforts targeting webmail credentials.

Figure 4: Repurposed PDF document used by UNC5976 purporting to be operational documentation for the ORLAN-15 UAV system

UNC6096

In February 2025, GTIG identified the suspected Russian espionage cluster UNC6096 conducting malware delivery operations via WhatsApp Messenger using themes related to the Delta battlefield management platform. To target Windows users, the cluster delivered an archive file containing a malicious LNK file leading to the download of a secondary payload. Android devices were targeted via malware we track as GALLGRAB, a modified version of the publicly available "Android Gallery Stealer". GALLGRAB collects data that includes locally stored files, contact information, and potentially encrypted user data from specialized battlefield applications.

UNC5114

In October 2023, the suspected Russian espionage cluster UNC5114 delivered a variant of the publicly available Android malware CraxsRAT masquerading as an update for the Kropyva app, accompanied by a lure document mimicking official installation instructions.

Overcoming Technical Limitations with LLMs

GTIG has recently discovered a threat group suspected to be linked to Russian intelligence services which conducts phishing operations to deliver CANFAIL malware primarily against Ukrainian organizations. Although the actor has targeted Ukrainian defense, military, government, and energy organizations within the Ukrainian regional and national governments, the group has also shown significant interest in aerospace organizations, manufacturing companies with military and drone ties, nuclear and chemical research organizations, and international organizations involved in conflict monitoring and humanitarian aid in Ukraine.

Despite being less sophisticated and resourced than other Russian threat groups, this actor recently began to overcome some technical limitations using LLMs. Through prompting, they conduct reconnaissance, create lures for social engineering, and seek answers to basic technical questions for post-compromise activity and C2 infrastructure setup.

In more recent phishing operations, the actor masqueraded as legitimate national and local Ukrainian energy organizations to target organizational and personal email accounts. They also imitated a Romanian energy company that works with customers in Ukraine, targeted a Romanian organization, and conducted reconnaissance on Moldovan organizations. The group generates lists of email addresses to target based on specific regions and industries discovered through their research.

Phishing emails sent by the actor contain a lure that based on analysis appears to be LLM-generated, uses formal language and a specific official template, and Google Drive links which host a RAR archive containing CANFAIL malware, often disguised with a .pdf.js double extension. CANFAIL is obfuscated JavaScript which executes a PowerShell script to download and execute an additional stage, most commonly a memory-only PowerShell dropper. It additionally displays a fake “error” popup to the victim.

This group’s activity has been documented by SentinelLABS and the Digital Security Lab of Ukraine in an October 2025 blog post detailing the “PhantomCaptcha" campaign, where the actor briefly used ClickFix in their operations.

Hacktivist Targeting of Military Drones

A subset of pro-Russia hacktivist activity has focused on Ukraine’s use of drones on the battlefield. This likely reflects the critical role that drones have played in combat, as well as an attempt by pro-Russia hacktivist groups to claim to be influencing events on the ground. In late 2025, the pro-Russia hacktivist collective KillNet, for example, dedicated significant threat activity to this. After announcing the collective’s revitalization in June, the first threat activity claimed by the group was an attack allegedly disabling Ukraine’s ability to monitor its airspace for drone attacks. This focus continued throughout the year, culminating in a December announcement in which the group claimed to create a multifunctional platform featuring the mapping of key infrastructure like Ukraine’s drone production facilities based on compromised data. We further detail in the next section operations from pro-Russia hacktivists that have targeted defense sector employees.

2. Employees in the Crosshairs: Targeting and Exploitation of Personnel and HR Processes in the Defense Sector

Throughout 2025, adversaries of varying motivations have continued to target the "human layer" including within the DIB. By exploiting professional networking platforms, recruitment processes, and personal communications, threat actors attempt to bypass perimeter security controls to gain insider access or compromise personal devices. This creates a challenge for enterprise security teams, where much of this activity may take place outside the visibility of traditional security detections.

North Korea’s Insider Threat and Revenue Generation

Since at least 2019, the threat from the Democratic People's Republic of Korea (DPRK) began evolving to incorporate internal infiltration via "IT workers" in addition to traditional network intrusion. This development, driven by both espionage requirements and the regime's need for revenue generation, continued throughout 2025 with recent operations incorporating new publicly available tools. In addition to public reporting, GTIG has also observed evidence of IT workers applying to jobs at defense related organizations.

- In June 2025, the US Department of Justice announced a disruption operation that included searches of 29 locations in 16 states suspected of being laptop farms and led to the arrest of a US facilitator and an indictment against eight international facilitators. According to the indictment, the accused successfully gained remote jobs at more than 100 US companies, including Fortune 500 companies. In one case, IT workers reportedly stole sensitive data from a California-based defense contractor that was developing AI technology.
- In 2025, a Maryland-based individual, Minh Phuong Ngoc Vong, was sentenced to 15 months in prison for their role in facilitating a DPRK ITW scheme. According to government documents, in coordination with a suspected DPRK IT worker, Vong was hired by a Virginia-based company to perform remote software development work for a government contract that involved a US government entity's defense program. The suspected DPRK IT worker used Vong's credentials to log in and perform work under Vong's identity, for which Vong was later paid, ultimately sending some of those funds overseas to the IT worker.

The Industrialization of Job Campaigns

Job-themed campaigns have become a significant and persistent operational trend among cyber threat actors, who leverage employment-themed social engineering as a high-efficacy vector for both espionage and financial gain. These operations exploit the trust inherent in the online job search, application, and interview processes, masquerading malicious content as job postings, fake job offers, recruitment documents, and malicious resume-builder applications to trick high-value personnel into deploying malware or providing credentials.

North Korean Cyber Operations Targeting Defense Sector Employees

North Korean cyber espionage operations have targeted defense technologies and personnel using employment themed social engineering. GTIG has directly observed campaigns conducted by APT45, APT43, and UNC2970 specifically target individuals at organizations within the defense industry.

- GTIG identified a suspected APT45 operation leveraging the SMALLTIGER malware to reportedly target South Korean defense, semiconductor, and automotive manufacturing entities. Based on historical activity, we suspect this activity is conducted at least in part to acquire intellectual property to support the North Korean regime in its research and development efforts in the targeted industries; South Korea's National Intelligence Service (NIS) has also reported on North Korean attempts to steal intellectual property toward the aims of producing its own semiconductors for use in its weapons programs.
- GTIG identified suspected APT43 infrastructure mimicking German and U.S. defense-related entities, including a credential harvesting page and job-themed lure content used to deploy the THINWAVE backdoor. Related infrastructure was also used by HANGMAN.V2, a backdoor used by APT43 and suspected APT43 clusters.

- UNC2970 has consistently focused on defense targeting and impersonating corporate recruiters in their campaigns. The cluster has used Gemini to synthesize open-source intelligence (OSINT) and profile high-value targets to support campaign planning and reconnaissance. UNC2970's target profiling included searching for information on major cybersecurity and defense companies and mapping specific technical job roles and salary information. This reconnaissance activity is used to gather the necessary information to create tailored, high-fidelity phishing personas and identify potential targets for initial compromise.

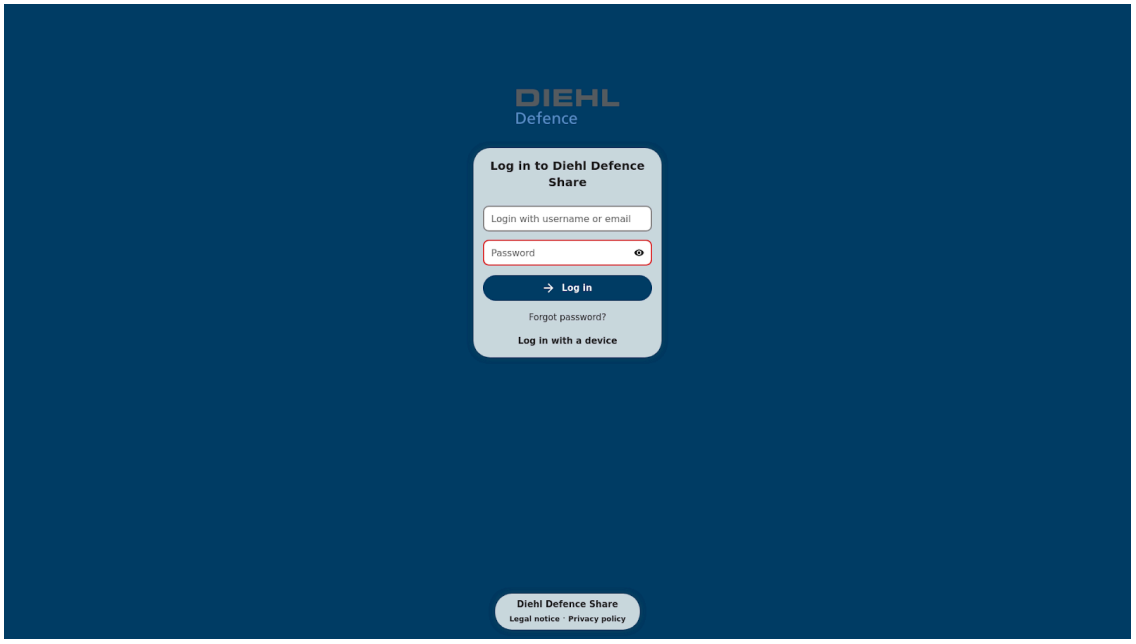


Figure 5: Content of a suspected APT43 phishing page

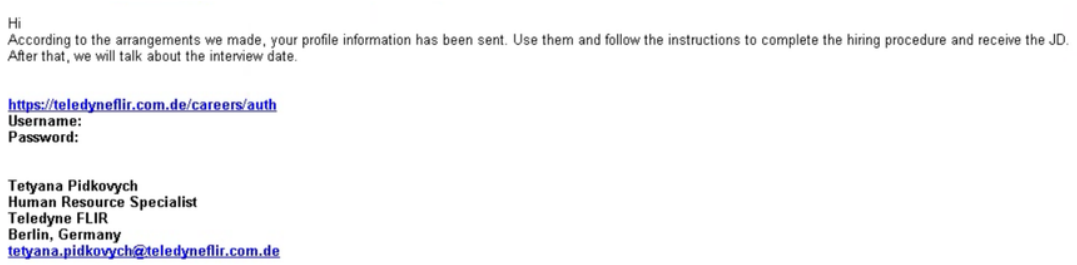
Iranian Threat Actors Use Recruitment-Themed Campaigns to Target Aerospace and Defense Employees

GTIG has observed Iranian state-sponsored cyber actors consistently leverage employment opportunities and exploit trusted third-party relationships in operations targeting the defense and aerospace sector. Since at least 2022, groups such as UNC1549 and UNC6446 have used spoofed job portals, fake job offer lures, as well as malicious resume-builder applications for defense firms, some of which specialize in aviation, aerospace, and UAV technology, to trick users/personnel into executing malware or giving up credentials under the guise of legitimate employment opportunities.

- GTIG has identified fake job descriptions, portals, and survey lures hosted on UNC1549 infrastructure masquerading as aerospace, technology, and thermal imaging companies, including drone manufacturing entities, to likely target personnel interested in major defense contractors. Likely indicative of their intended targeting, in one campaign UNC1549 leveraged a spoofed domain for a drone-related conference in Asia.
    - UNC1549 has additionally gained initial access to organizations in the defense and aerospace sector by exploiting trusted connections with third-party suppliers. The group leverages compromised third-party accounts to exploit legitimate access pathways, often pivoting from service providers to their customers. Once access is gained, UNC1549 has focused on privilege escalation by targeting IT staff with malicious emails that mimic authentic processes to steal administrator credentials, or

by exploiting less-secure third-party suppliers to breach the primary target's infrastructure via legitimate remote access services like Citrix and VMware. Post-compromise activities often include credential theft using custom tools like CRASHPAD and RDP session hijacking to access active user sessions.

Since at least 2022, the Iranian-nexus threat actor UNC6446 has used resume builder and personality test applications to deliver custom malware primarily to targets in the aerospace and defense vertical across the US and Middle East. These applications provide a user interface - including one likely designed for employees of a UK-based multinational aerospace and defense company - while malware runs in the background to steal initial system reconnaissance data.



Hi
According to the arrangements we made, your profile information has been sent. Use them and follow the instructions to complete the hiring procedure and receive the JD.
After that, we will talk about the interview date.

https://teledyneflir.com.de/careers/auth
Username:
Password:

Tetyana Pidkovych
Human Resource Specialist
Teledyne FLIR
Berlin, Germany
tetyana.pidkovych@teledyneflir.com.de

Figure 6: Hiring-themed spear-phishing email sent by UNC1549

Project Manager Job Description

Job Summary:

A project manager plans, organizes and oversees a project from start to finish. They should guarantee that the project is finalized to the contentment of all stakeholders, within the designated budget and timeline.

Duties/Responsibilities:

- Determine and define project scope and objectives
- Predict resources needed to reach objectives and manage resources in an effective and efficient manner
- Prepare budget based on scope of work and resource requirements
- Track project costs in order to meet budget
- Develop and manage a detailed project schedule and work plan
- Provide project updates on a consistent basis to various stakeholders about strategy, adjustments, and progress
- Manage contracts with vendors and suppliers by assigning tasks and communicating expected deliverables
- Utilize industry best practices, techniques, and standards throughout entire project execution
- Monitor progress and make adjustments as needed
- Use appropriate verification techniques to manage changes in project scope, schedule and costs
- Measure project performance using appropriate systems, tools and techniques to identify areas for improvement
- Report and escalate to management as needed
- Manage the relationship with the client and all stakeholders

Figure 7: UNC1549 fake job offer on behalf of DJI, a drone manufacturing company

China-Nexus Actor Targets Personal Emails of Defense Contractor Employees

China-nexus threat actor APT5 conducted two separate campaigns in mid to late 2024 and in May 2025 against current and former employees of major aerospace and defense contractors. While employees at one of the companies received emails to their work email addresses, in both campaigns, the actor sent spearphishes to employees' personal email addresses. The lures were meticulously crafted to align with the targets' professional roles, geographical locations, and personal interests. Among the professional, industry, and training lures the actor leveraged included:

- Invitations to industry events, such as CANSEC (Canadian Association of Defence and Security Industries), MilCIS (Military Communications and Information Systems), and SHRM (Society for Human Resource Management).
- Red Cross training courses references.
- Phishing emails disguised as job offers.

Additionally, the actor also leveraged hyper-specific and personal lures related to the locations and activities of their targetings, including:

- Emails referencing a "Community service verification form" from a local high school near one of the contractor's headquarters.
- Phishing emails using "Alumni tickets" for a university minor league baseball team, targeting employees who attended the university.
- Emails purporting to be "open letters" to Boy Scouts of America camp or troop leadership, targeting employees known to be volunteers or parents.
- Fake guides and registration information leveraging the 2024 election cycle for the state where the employees lived.

RU Hacktivists Targeting Personnel

Doxxing remains a cornerstone of pro-Russia hacktivist threat activity, targeting both individuals within Ukraine's military and security services as well as foreign allies. Some groups have centered their operations on doxxing to uncover members across specific units/organizations, while others use doxxing to supplement more diverse operations.

For example, in 2025, the group Heaven of the Slavs (Original Russian: НЕБО СЛАВЯН) claimed to have doxxed Ukrainian defense contractors and military officials; Beregini alleged to identify individuals who worked at Ukrainian defense contractors, including those that it claimed worked at Ukrainian naval drone manufacturers; and PalachPro claimed to have identified foreign fighters in Ukraine, and the group separately claimed to have compromised the devices of Ukrainian soldiers. Further hacktivist activity against the defense sector is covered in the last section of this report.

3. Persistent Area of Focus For China-Nexus Cyber Espionage Actors

The defense industrial base has been an important target for China-nexus threat actors for as long as cyber operations have been used for espionage. One of the earliest observed compromises attributed to the Chinese military's APT1 group was a firm in the defense industrial sector in 2007. While historical campaigns by actors such as APT40 have at times shown hyper-specific focus in sub-sectors of defense, such as maritime related technologies, in general the areas of defense targeting from China-nexus groups has spanned all domains and supply chain layers. Alongside this focus on defense systems and contractors, Chinese cyber espionage groups have steadily improved their tradecraft over the past several years, increasing the risk to this sector.

GTIG has observed more China-nexus cyber espionage missions directly targeting defense and aerospace industry than from any other state-sponsored actors over the last two years. China-nexus espionage actors have used a broad range of tactics in operations, but the hallmark of many operations has been their exploitation of edge devices to gain initial access. We have also observed China-nexus threat groups leverage ORB networks for reconnaissance against defense industrial targets, which complicates detection and attribution.

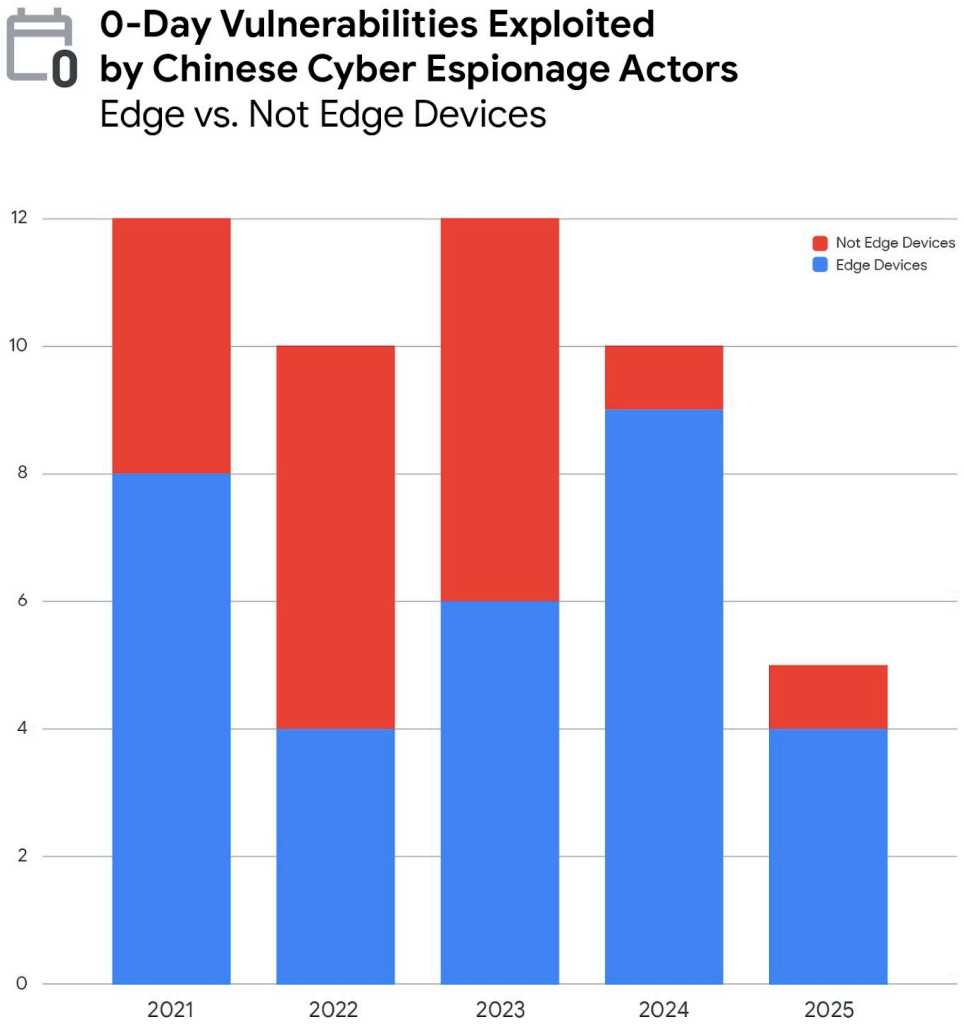


Figure 8: Edge vs. not edge zero-days likely exploited by CN actors 2021 — September 2025

Drawing from both direct observations and open-source research, GTIG assesses with high confidence that since 2020, Chinese cyber espionage groups have exploited more than two dozen zero-day (0-day) vulnerabilities in edge devices (devices that are typically placed at the edge of a network and often do not support EDR monitoring, such as VPNs, routers, switches, and security appliances) from ten different vendors. This observed emphasis on exploiting 0-days in edge devices likely reflects an intentional strategy to benefit from the tactical advantages of reduced opportunities for detection and increased rates of successful compromises.

While we have observed exploitation spread to multiple threat groups soon after disclosure, often the first Chinese cyber espionage activity sets we discover exploiting an edge device 0-day, such as UNC4841, UNC3886, and UNC5221, demonstrate extensive efforts to obfuscate their activity in order to maintain long-term access to targeted environments. Notably, in recent years, both UNC3886 and UNC5221 operations have directly impacted the defense sector, among other industries.

- UNC3886 is one of the most capable and prolific China-nexus threat groups GTIG has observed in recent years. While UNC3886 has targeted multiple sectors, their early operations in 2022 had a distinct focus on

aerospace and defense entities. We have observed UNC3886 employ 17 distinct malware families in operations against DIB targets. Beyond aerospace and defense targets, UNC3886 campaigns have been observed impacting the telecommunications and technology sectors in the US and Asia.

- UNC5221 is a sophisticated, suspected China-nexus cyber espionage actor characterized by its focus on exploiting edge infrastructure to penetrate high-value strategic targets. The actor demonstrates a distinct operational preference for compromising perimeter devices—such as VPN appliances and firewalls—to bypass traditional endpoint detection, subsequently establishing persistent access to conduct long-term intelligence collection. Their observed targeting profile is highly selective, prioritizing entities that serve as "force multipliers" for intelligence gathering, such as managed service providers (MSPs), law firms, and central nodes in the global technology supply chain. The BRICKSTORM malware campaign uncovered in 2025, which we suspect was conducted by UNC5221, was notable for its stealth, with an average dwell time of 393 days. Organizations that were impacted spanned multiple sectors but included aerospace and defense.

In addition to these two groups, GTIG has analysed other China-nexus groups impacting the defense sector in recent years.

UNC3236 Observed Targeting U.S. Military and Logistics Portal

In 2024, GTIG observed reconnaissance activity associated with UNC3236 (linked to Volt Typhoon) against publicly hosted login portals of North American military and defense contractors, and U.S. and Canadian government domains related to North American infrastructure. The activity leveraged the ARCMAZE obfuscation network to obfuscate its origin. Netflow analysis revealed communication with SOHO routers outside the ARCMAZE network, suggesting an additional hop point to hinder tracking. Targeted entities included a Drupal web login portal used by defense contractors involved in U.S. military infrastructure projects.

UNC6508 Search Terms Indicate Interest in Defense Contractors and Military Platforms

In late 2023, China-nexus threat cluster UNC6508 targeted a US-based research institution through a multi-stage attack that leveraged an initial REDCap exploit and custom malware named INFINITERED. This malware is embedded within a trojanized version of a legitimate REDCap system file and functions as a recursive dropper. It is capable of enabling persistent remote access and credential theft after intercepting the application's software upgrade process to inject malicious code into the next version's core files.

The actor used the REDCap system access to collect credentials to access the victim’s email platform filtering rules to collect information related to US national security and foreign policy (Figure 10). GTIG assesses with low confidence that the actors likely sought to fulfill a set of intelligence collection requirements, though the nature and intended focus of the collection effort are unknown.

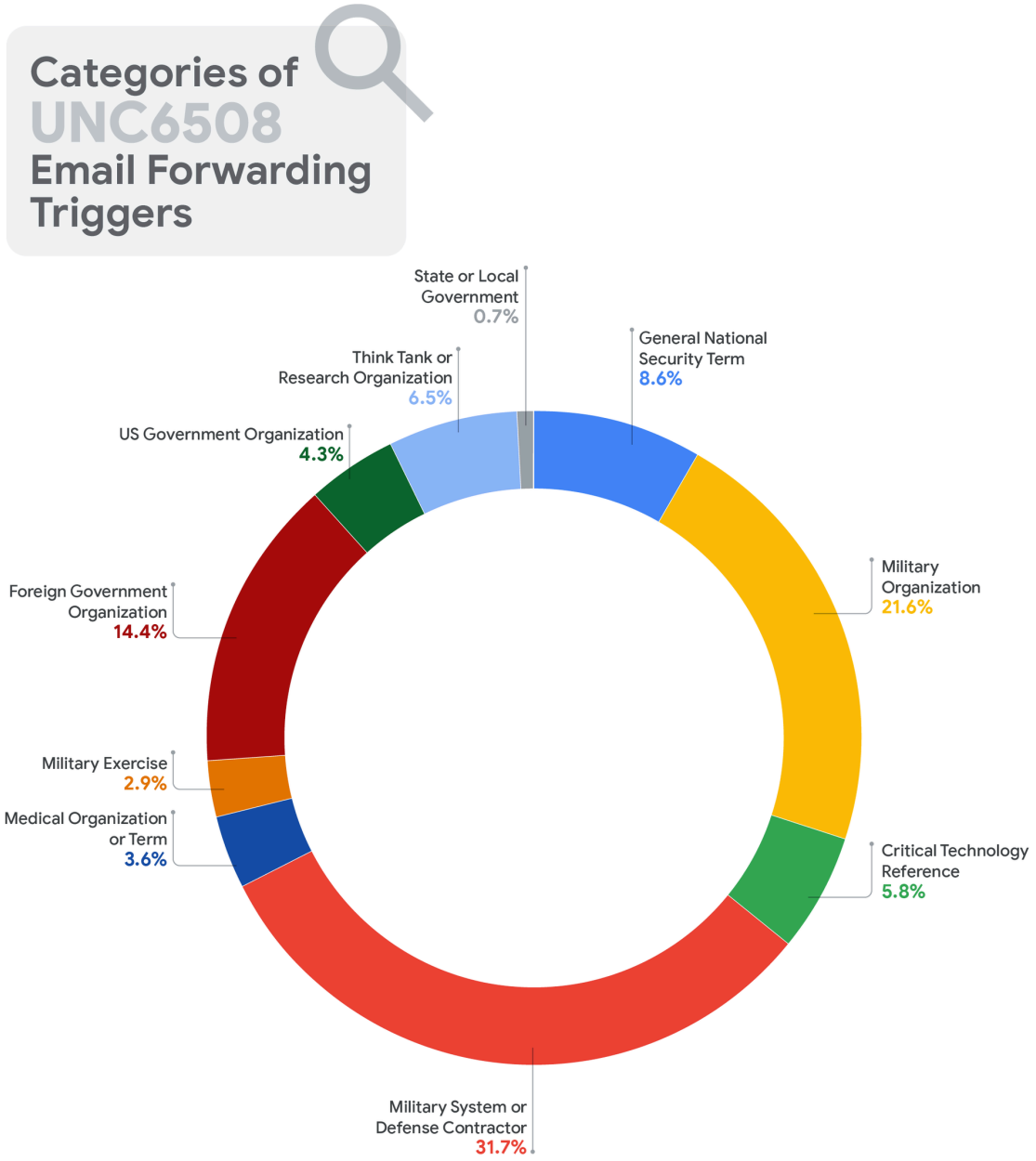


Figure 9: Categories of UNC6508 email forwarding triggers

By August 2025, the actors leveraged credentials obtained via INFINITERED to access the institution's environment with legitimate, compromised administrator credentials. They abused the tenant compliance rules to dynamically reroute messages based on a combination of keywords and or recipients. The actors modified an email rule to BCC an actor-controlled email address if any of 150 regex-defined search terms or email addresses appeared in email bodies or subjects, thereby facilitating data exfiltration by forwarding any email that contained at least one of the terms related to US national security, military equipment and operations, foreign policy, and medical research, among others. About a third of the keywords referenced a military system or a defense contractor, with a notable amount related to UAS or counter-UAS systems.

4. Hack, Leak, and Disruption of the Manufacturing Supply Chain

Extortion operations continue to represent the most impactful cyber crime threat globally, due to the prevalence of the activity, the potential for disrupting business operations, and the public disclosure of sensitive data such as personally identifiable information (PII), intellectual property, and legal documents. Similarly, hack-and-leak operations conducted by geopolitically and ideologically motivated hacktivist groups may also result in the public disclosure of sensitive data. These data breaches can represent a risk to defense contractors via loss of intellectual property, to their employees due to the potential use of PII for targeting data, and to the defense agencies they support. Less frequently, both financially and ideologically motivated threat actors may conduct significant disruptive operations, such as the deployment of ransomware on operational technology (OT) systems or distributed-denial-of-service (DDoS) attacks.

Cyber Crime Activity Impacting the Defense Industrial Base and Broader Manufacturing and Industrial Supply Chain

While dedicated aerospace & defense organizations represent only about 1% of victims listed on data leak sites (DLS) in 2025, manufacturing organizations, many of which directly or indirectly support defense contracts, have consistently represented the largest share of DLS listings by count (Figure 11). This broader manufacturing sector includes companies that may provide dual-use components for defense applications. For example, a significant 2025 ransomware incident affecting a UK automotive manufacturer, who also produces military vehicles, disrupted production for weeks and reportedly affected more than 5,000 additional organizations. This highlights the cyber risk to the broader industrial supply chain supporting the defense capacity of a nation, including the ability to surge defense components in a wartime environment can be impacted, even when these intrusions are limited to IT networks.

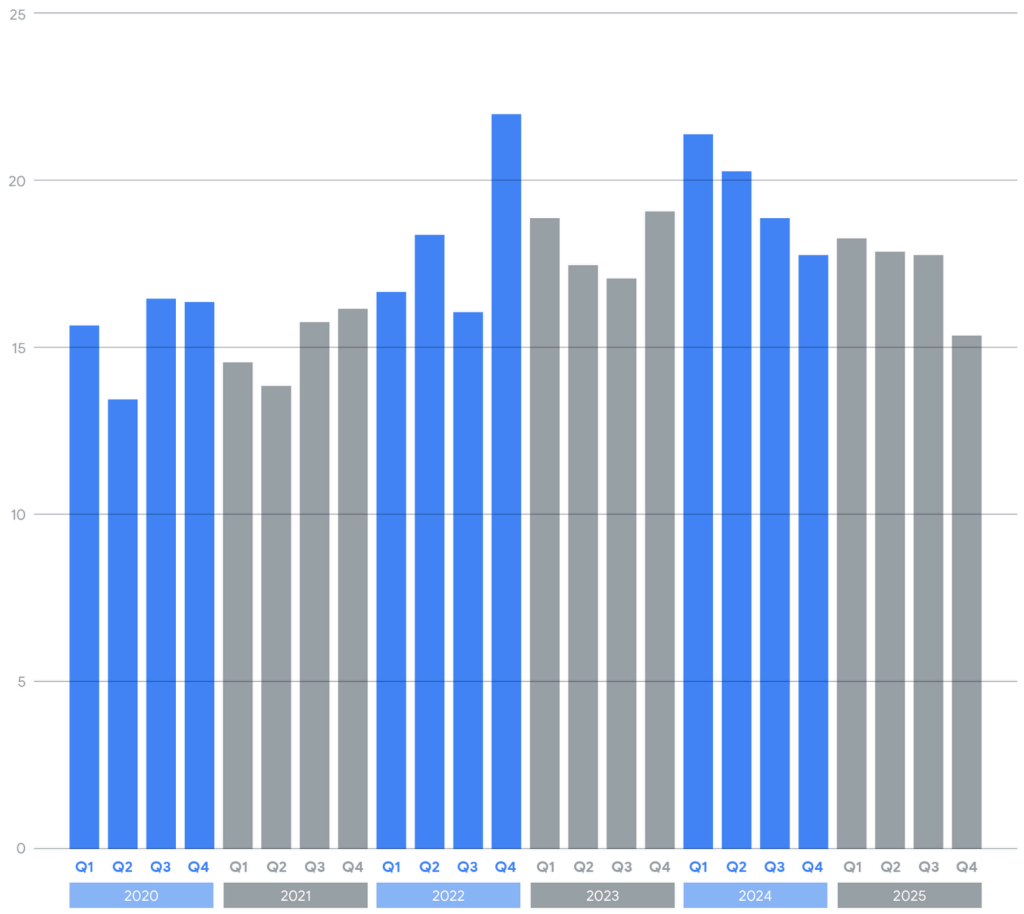


Figure 10: Percent of DLS victims in the manufacturing industry by quarter

Threat actors also regularly share and/or advertise illicit access to or stolen data from aerospace and defense sector organizations. For example, the persona “miyako,” who has been active on multiple underground forums based on the use of the same username and Session ID, has advertised access to multiple, unnamed, defense contractors over time (Figure 11). While defense contractors are likely not attractive targets for many cyber criminals, given that these organizations typically maintain a strong security posture, a small subset of financially motivated actors may disproportionately target the industry due to dual motivations, such as a desire for notoriety or ideological motivations. For example, the BreachForums actor “USDoD” regularly shared or advertised access to data claimed to have been stolen from prominent defense-related organizations. In a bizarre 2023 interview, USDoD claimed the threat was misdirection and that they were actually targeting a consulting firm, NATO, CEPOL, Europol, and Interpol. USDoD further indicated that they had a personal vendetta and were not motivated by politics. In October 2024, Brazilian authorities arrested an individual accused of being USDoD.

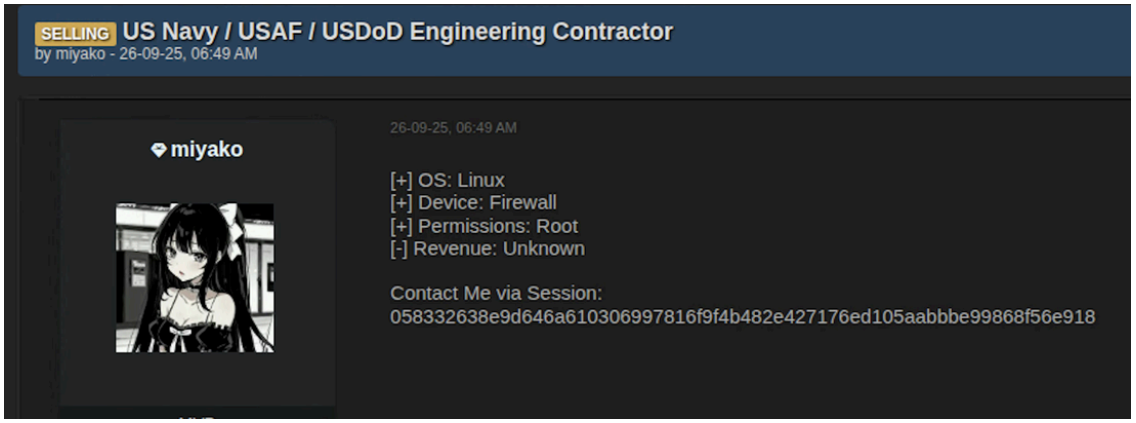


Figure 11: Advertisement for “US Navy / USAF / USDoD Engineering Contractor”

Hacktivist Operations Targeting the Defense Industrial Base

Pro-Russia and pro-Iran hacktivism operations at times extend beyond simple nuisance-level attacks to high-impact operations, including data leaks and operational disruptions. Unlike financially motivated activity, these campaigns prioritize the exposure of sensitive military schematics and personal personnel data—often through "hack-and-leak" tactics—in an attempt to erode public trust, intimidate defense officials, and influence geopolitical developments on the ground. Robust geopolitically motivated hacktivist activity works not only to advance state interests but also can serve to complicate attribution of threat activity from state-backed actors, which are known to leverage hacktivist tactics for their own ends.

2025	Actor	Claim Category	Summary
DEC 20	Handala Hack	Doxxing	Doxxed 14 individuals allegedly associated with Israeli drone programs.
	Cyber Toufan	Hack-and-Leak	Released data purportedly stolen from a "key supplier" for Israeli defense contractors.
DEC 17	NoName057(16)	DDoS Attack	Claimed DDoS attacks targeting Ukrainian manufacturers of military equipment.
DEC 16	Beregini	Information Operations	"Leaked" a publicly available UAV detector manual as part of a post portraying Ukraine as an aggressive state.
	NoName057(16)	DDoS Attack	Claimed a DDoS attack targeting a Ukrainian manufacturer of military vehicles.
DEC 12	Cyber Toufan	Hack-and-Leak	Leaked intellectual property and PII allegedly obtained from a key supplier for Israeli defense contractors.
DEC 11	Cyber Toufan	Hack-and-Leak	Leaked intellectual property allegedly stolen from a key supplier for Israeli defense contractors.
NOV 22	Cyber Toufan	Hack-and-Leak	Shared videos as "proof" of access to a database belonging to a manufacturer that supports Israel's military defense complex.
NOV 13	Infrastructure Destruction Squad	Attempted Intrusion	Threatened to hack and sell data from US defense contractor after citing failed initial attempt to breach company.
NOV 8	Beregini	Hack-and-Leak	Published a purported Ukrainian MoD document to allege corruption within Ukrainian defense contracting.
	Handala Hack	Doxxing	Doxxed individuals purportedly supporting Israel's defense industry.
OCT 29	Cyber Toufan	Hack-and-Leak	Shared stolen data purportedly related to various Israeli defense technologies.
OCT 9	Cyber Toufan	Hack-and-Leak	Shared images possibly from an Israeli engineering company's security cameras and announced forthcoming data leak.
OCT 16	JokerDNR (aka JokerDPR)	Information Operations	Published propaganda videos criticizing a US defense contractor and its and role in Western strategy.
SEP 15	Cyber Toufan	Hack-and-Leak	Leaked data allegedly proving an Israeli manufacturer's business dealings with Israeli defense contractors.
AUG 07	Cyber Isnaad Front	Hack-and-Leak	Announced they would leak data stolen from an organization that allegedly works with the US military and Israeli defense contractors.
JUL 31	NoName057(16)	Hack-and-Leak	Shared two screenshots as "proof" of compromising a French defense contractor.
JUN 27	NoName057(16)	DDoS Attack	Claimed DDoS attacks against Israeli defense contractors.
APR 13	Diplomat	DDoS Attack	Claimed DDoS attacks against French and German defense contractors and manufacturers.
MAR 25	Diplomat	DDoS Attack	Claimed DDoS attacks against Israeli defense contractors and nonfunctional .il domains.
	BLOCKWEB	DDoS Attack	Claimed DDoS attacks against Israeli defense contractors.

Figure 12: Notable 2025 hacktivist claims allegedly involving the defense industrial base

Pro-Russia Hacktivism Activity

Pro-Russia hacktivist actors have collectively dedicated a notable portion of their threat activity to targeting entities associated with Ukraine’s and Western countries’ militaries and in their defense sectors. As we have

previously reported, GTIG observed a revival and intensification of activity within the pro-Russia hacktivist ecosystem in response to the launch of Russia's full-scale invasion of Ukraine in February 2022. The vast majority of pro-Russia hacktivist activity that we have subsequently tracked has likewise appeared intended to advance Russia's interests in the war. As with the targeting of other high-profile organizations, at least some of this activity appeared primarily intended to generate media attention. However, a review of the related threat activity observed in 2025 also suggest that actors targeting military/defense sectors had more diverse objectives, including seeding influence narratives, monetizing claimed access, and influencing developments on the ground. Some observed attack/targeting trends over the last year include the following:

- **DDoS Attacks:** Multiple pro-Russia hacktivist groups have claimed distributed denial-of-service (DDoS) attacks targeting government and private organizations involved in defense. This includes multiple such attacks claimed by the group NoName057(16), which has prolifically leveraged DDoS attacks to attack a range of targets. While this often may be more nuisance-level activity, it demonstrates at the most basic level how defense sector targeting is a part of hacktivist threat activity that is broadly oriented toward targeting entities in countries that support Ukraine.
- **Network Intrusion:** In limited instances, pro-Russia groups claimed intrusion activity targeting private defense-sector organizations. Often this was in support of hack and leak operations. For example, in November 2025, the group PalachPro claimed to have targeted multiple Italian defense companies, alleging that they exfiltrated sensitive data from their networks—in at least one instance, PalachPro claimed it would sell this data; that same month, the group Infrastructure Destruction Squad claimed to have launched an unsuccessful attack targeting a major US arms producer.
- **Document Leaks:** A continuous stream of claimed or otherwise implied hack and leak operations has targeted the Ukrainian military and the government and private organizations that support Ukraine. Beregini and JokerDNR (aka JokerDPR) are two notable pro-Russia groups engaged in this activity, both of which regularly disseminate documents that they claim are related to the administration of Ukraine's military, coordination with Ukraine's foreign partners, and foreign weapons systems supplied to Ukraine. GTIG cannot confirm the potential validity of all the disseminated documents, though in at least some instances the sensitive nature of the documents appears to be overstated.
    - Often, Beregini and JokerDNR leverage this activity to promote anti-Ukraine narratives, including those that appear intended to reduce domestic confidence in the Ukrainian government by alleging things like corruption and government scandals, or that Ukraine is being supplied with inferior equipment.

Pro-Iran Hacktivism Activity

Pro-Iran hacktivist threat activity targeting the defense sector has intensified significantly following the onset of the Israel-Hamas conflict in October 2023. These operations are characterized by a shift from nuisance-level disruptive attacks to sophisticated "hack-and-leak" campaigns, supply chain compromises, and aggressive psychological warfare targeting military personnel. Threat actors such as Handala Hack, Cyber Toufan, and the Cyber Isnaad Front have prioritized the Israeli defense industrial base—compromising manufacturers, logistics providers, and technology firms to expose sensitive schematics, personnel data, and military contracts. The

objective of these campaigns is not merely disruption but the degradation of Israel's national security apparatus through the exposure of military capabilities, the intimidation of defense sector employees via "doxxing," and the erosion of public trust in the security establishment.

- The pro-Iran persona Handala Hack, which GTIG has observed publicize threat activity associated with UNC5203, has consistently targeted both the Israeli Government, as well as its supporting military-industrial complex. Threat activity attributed to the persona has primarily consisted of hack-and-leak operations, but has increasingly incorporated doxxing and tactics designed to promote fear, uncertainty, and doubt (FUD).
    - On the two-year anniversary of al-Aqsa Flood, the day which Hamas-led militants attacked Israel, Handala launched "Handala RedWanted," an actor-controlled website supporting a concerted doxxing/intimidation campaign targeting members of Israel's Armed Forces, its intelligence and national security apparatus, and both individuals and organizations the group claims to comprise Israel's military-industrial complex.
    - Following the announcement of RedWanted, the persona has recently signaled an expansion of its operations vis-a-vis the launch of "Handala Alert." Significant in terms of a potential expansion in the group's external targeting calculus, which has long prioritized Israel, is a renewed effort by Handala to "support anti-regime activities abroad."
- Ongoing campaigns such as those attributed to the Pro-Iran personas Cyber Toufan (UNC5318) and الجبهة الإسناد السيبرانية (Cyber Isnaad Front) are additionally demonstrative of the broader ecosystem's longstanding prioritization of the defense sector.
    - Leveraging a newly-established leak channel on Telegram (ILDefenseLeaks), Cyber Toufan has publicized a number of operations targeting Israel's military-industrial sector, most of which the group claims to have been the result of a supply chain compromise resulting from its breach of network infrastructure associated with an Israeli defense contractor. According to Cyber Toufan, access to this contractor resulted in the compromise of at least 17 additional Israeli defense contractor organizations.
    - While these activities have prioritized the targeting of Israel specifically, claimed operations have in limited instances impacted other countries. For example, recent threat activity publicized by Cyber Isnaad Front also surrounding the alleged compromise of the aforementioned Israeli defense contractor leaked information involving reported plans by the Australian Defense Force to purchase Spike NLOS anti-tank missiles from Israel.

Conclusion

Given global efforts to increase defense investment and develop new technologies the security of the defense sector is more important to national security than ever. Actors supporting nation state objectives have interest in the production of new and emerging defense technologies, their capabilities, the end customers purchasing them, and potential methods for countering these systems. Financially motivated actors carry out extortion against this sector and the broader manufacturing base like many of the other verticals they target for monetary gain.

While specific risks vary by geographic footprint and sub-sector specialization, the broader trend is clear: the defense industrial base is under a state of constant, multi-vector siege. The campaigns against defense contractors in Ukraine, threats to or exploitation of defense personnel, the persistent volume of intrusions by China-nexus actors, and the hack, leak, and disruption of the manufacturing base are some of the leading threats to this industry today. To maintain a competitive advantage, organizations must move beyond reactive postures. By integrating these intelligence trends into proactive threat hunting and resilient architecture, the defense sector can ensure that the systems protecting the nation are not compromised before they ever reach the field.

Posted in

- Threat Intelligence
