Issues in Information Systems
Volume 26, Issue 4, pp. 348-357, 2025

DOI: https://doi.org/10.48009/4_iis_2025_128

Protecting the U.S. defense industrial base against advanced persistent threat attacks

Amy Kulikowski, *Robert Morris University, kulikowski@rmu.edu*

Abstract

The Defense Industrial Base (DIB) is one of 16 segments of U.S. Critical Infrastructure. Its confidentiality, integrity and availability of information, products and services are of vital importance to the United States national security. Due to the significance of the DIB it is an attractive high value target for nation states wishing to steal technology, disrupt and do harm. The purpose of this research paper is to highlight the imminent danger of Advanced Persistent Threats (APTs) from four nations states: China, Russia, North Korea and Iran. The author will highlight through literature review the preferred tactics, techniques, and procedures (TTPs) of these bad actors in gaining and maintaining persistence in the Defense Industrial Base networks. Research into the nation states APT's and their methodical attack paths will be identified and compared to the MITRE ATT&CK framework.

Keywords: APTs, national security, defense industrial base, U.S. critical infrastructure

Introduction

The Defense Industrial Base is made up of more than 220,000 companies and their subcontractors both domestic and foreign. (U.S. Department of Defense, 2022) The DIB is a worldwide industrial complex that provides research and development, products and services for the Department of Defense that are essential to supplying the U.S. Military. These companies provide cutting edge technology to the U.S. Government enabling the U.S. to remain dominant. (Defense Industrial Base Sector | Cybersecurity and Infrastructure Security Agency CISA, n.d.) Advanced persistent threats on the U.S. Defense Industrial Base by nation states continue for the purposes of espionage, disruption, and destruction. According to former Deputy Defense Secretary Kathleen H. Hicks "These cyber-attacks threaten the U.S. and the rules-based order on which the global economy relies. Markets cannot function effectively in an environment where adversarial countries are leveraging their national power to steal intellectual property, to sabotage commercial activity, and to threaten supply chains." (U.S. Department of Defense, 2022) There is also evidence of nation-states lurking in critical infrastructure to attack in later days. Experts call the impending threat the "9-11" of our critical infrastructure. "CISA Director Jen Easterly said that based on discussions CISA has had with industry partners in the Joint Cyber Defense Collaborative (JCDC), the intrusions are not being leveraged "to steal specific high value information—in sum, as we understand it, this attack is largely an opportunistic one." (Today, 2023)

The Defense Industrial Base relies on a host of third-party vendors for equipment, materials, parts and services. The supply chain of the DIB is made up of approximately 12,000 subcontractors, often small to medium sized businesses with small cybersecurity budgets that can be a vulnerable entry point for nation states trying to gain access to larger contractors. (Rocha & O'Hanlon, 2024) In the action paper "Securing Defense-Critical Supply Chains," in response to Executive Order 14017, one particular recommendation, CP4.1, is to enhance DIB cybersecurity information management. To "…provide useful information on cyber readiness, including a special focus on enhancing information sharing with small and medium enterprises, which tend to have few cyber professionals on staff." (Hicks & National Defense Industrial Association, 2022) The breadth of this segment of providers to the U.S. military makes a large attack surface for U.S. enemies.

This study will provide insight into the DIB's persistent threat actors and their common attack vectors through a literature review of academic research papers, U.S. Government agency advisories and white papers. Common attack paths used by the four nation states for the purpose of stealing U.S. trade secrets, intellectual property and to disrupt and destroy will be highlighted using the combined literature and studies. The research presented in this case study will shed light on the Defense Industrial Base segment of the U.S. Critical Infrastructure and will show the importance of a strong cybersecurity defense for all contractors to shore up U.S. national interests.

RQI: *What are the most common APT attacks affecting the Defense Industrial Base between 2020-2024?*

Literature Review

The Defense Industrial Base is a large and crucial component to protecting the United States homeland. Without the vital materials, equipment, and services that the DIB provides, U.S. warfighters would not be able to maintain technical and tactical superiority. In the present time of great power competition with China, two regional wars and global instability, research on APT's by nation states is imperative. The findings from research provide up to date information to the DIB and the cybersecurity teams that protect their networks.

In 2022 a study using three open data sources (DeBlasio et al) including the MITRE ATT&CK, Kaggle, and General Services Administration, aimed to find and rank the top two nation state sponsors in terms of number of APT attacks. China, given the name APT1, was the highest ranked nation state for Advanced Persistent Attacks and utilized 23 tactics, techniques, and procedures. Number two for most APTs was Russia, named APT28, and used 84 TTPs in their attacks. Lastly, the third highest occurring group referred to as APT29, used 32 TTPs. The 3rd ranking nation state was not attributed to a particular country in the study, however, upon further research APT29 is classified by MITRE ATT&CK as associated with Russia's Foreign Intelligence Service (SVR). This threat group has been credited with the Solar Winds attack and allegedly breached the Democratic National Committee's network in 2015. APT29 also is known by other names including Cozy bear, NOBELIUM, DarkHalo and others. (MITRE ATT&CK, n.d.)

In 2023, CISA conducted The Risk and Vulnerability Assessment which included 143 RVA assessments in conjunction with the U.S. Coast Guard, the federal civilian executive branch (FCEB), high priority private and public sector critical infrastructure (CI) operators, and select state, local, tribal, and territorial (SLTT) stakeholders. The assessors devised an attack path for the RVAs that used 11 of the 14 MITRE ATT&CK steps but was loosely geared to the common attack paths. The main purpose of conducting RVAs was to give the DIB contractors and other participants an actionable plan using collected data and insight on national threats and vulnerabilities.

This large study was valuable, lending insight into security gaps within a single participants' cybersecurity posture and the critical sector as a whole. RVA assessors found that APTs using valid accounts were the most successful access point with Spear Phishing as the second. What was gleaned through this research is that attackers are gaining access through simple measures and that critical infrastructure sectors of all types were vulnerable to the same attacks. (CISA, 2024)

The information provided to participating contractors shows the significance of cyber awareness training for all DIB employees regardless of their job duties and a comprehensive cyber management plan for third party vendors. Gaining initial network access through phishing and valid accounts is the low barrier to entry; ingeniously exploiting human weakness leading to catastrophic damage. “Threat intelligence plays a crucial role in this process, enabling organizations to stay informed of emerging threats, vulnerabilities, and attack techniques, and to adapt their security strategies accordingly.” (Gihon, 2024) Once in the network these nefarious actors can lie in wait, gain access to confidential information, and exfiltrate data to be used for political or economic harm. “When threat actors are persistent on a network, they retain the ability to re-infect machines and/or maintain their existing foothold within a network. Persistence on a network allows threat actors to go undetected for months, enabling them to carry out malicious activity or continuously compromise confidential data.” (CISA, 2024)

In February of 2024, CISA in conjunction with the NSA and FBI published a Cybersecurity Advisory paper titled, “PRC State-Sponsored Actors Compromise and Maintain Persistent Access to U.S. Critical Infrastructure.” An advisory provides technical details, TTPs of the threat actor, detection/ hunt recommendations, incident response, and mitigation suggestions. The 2024 report focused on the People’s Republic of China’s state-sponsored cyber group known as Volt Typhoon. Volt Typhoon commonly uses VPN sessions [T1133] and exploits vulnerabilities in networking applications [T1190] to gain initial access, however, they also utilize valid accounts [T1078] to maintain persistence in a network.

Volt Typhoon’s “hallmark” technique is living off the land (LOTL) for defense evasion [TA0005]. Living off the land is accomplished when an attacker can remain obfuscated by blending into the native traditional security tools within a system meaning that they can live within a network system for months or even years by camouflaging their malicious activities. “Specifically, Chinese cyber actors, including a group known as “Volt Typhoon,” are burrowing deep into our critical infrastructure to be ready to launch destructive cyber-attacks in the event of a major crisis or conflict with the United States.” (Opening Statement by CISA Director Jen Easterly | CISA, 2024)

In early summer of 2023 Microsoft was breached by Storm - 00058 a group affiliated with China impacting over 22 organizations and over 500 individuals. Microsoft became aware of the situation after customer reports and began investigating one month later. Silvers and Alperovitch from the Cyber Safety Review Board (CSRB) commented, “it struck the espionage equivalent of gold. The threat actors accessed the official email accounts of many of the most senior U.S. government officials managing our country’s relationship with the People’s Republic of China.” (Ribeiro, 2024) APT breaches of all critical infrastructure including the DIB and any U.S. Government entities must be studied for optimal prevention and mitigation. There are many cybersecurity frameworks for practitioners to choose from including the MITRE ATT&CK, the Cyber Kill Chain, OWASP TOP 10, and the NIST Cybersecurity Framework and others. The MITRE ATT&CK framework, MITRE D3FEND, and National Security Agency Zero Trust model are all incorporated by the DoD’s Cybersecurity Reference Architecture intended for the DoD’s modernization of Cybersecurity. (Department of Defense (DoD) & DoD CIO Cybersecurity Architecture Division, 2023b)

Basra and Kaushik (2020) report that over 80% of enterprises utilize the MITRE ATT&CK framework. The open and accessible information provided by MITRE enables private companies and governments to utilize the foundation of proven adversarial behaviors through their tactics, techniques, and procedures. (Strom et al., 2020) “The widespread adoption of the MITRE ATT&CK framework, as evidenced by its integration into technologies from vendors like LogRhythm SIEM, Check Point, ServiceNow, Splunk, and

F5, underscores its utility." ("THE APPLICATION OF MITRE ATT&Amp;CK FRAMEWORK IN MITIGATING CYBERSECURITY THREATS IN THE PUBLIC SECTOR," 2024b) Although, the MITRE ATT&CK framework is widely adopted, Basra and Kaushik's work (2020) also discovered that 45% of respondents claimed the interoperability of their security products was challenging with the ATT&CK framework.

In the *Defense Industrial Base Cybersecurity Strategy 2024*, the report unveils a vision and strategy to enhance DIB information systems cybersecurity for fiscal years 2024 through 2027. As part of the DIB Cybersecurity Strategy, DIB contractors are encouraged to "fully integrate" the NIST CSF 2.0 framework into their cybersecurity operational plans. According to the Defense Industrial Base - Sector Specific Plan, 2010, Cybersecurity is identified as "arguably the most urgent infrastructure protection issue facing the Nation." (The Honorable Kathleen H Hicks, 2024b)

The report also outlines DFARS, the Defense Federal Acquisition Regulation Supplement, regarding the cybersecurity rules that need to be adhered to. DFARS is a set of regulations not a framework that outlines specific requirements for contractors and subcontractors doing business with the DoD and U.S. Government. Pertinent regulations that apply include the following.

- DFARS 252.204–7012, "Safeguarding Covered Defense Information and Cyber Incident Reporting
- DFARS 252.204-7020, "NIST SP 800-171 DoD Assessment Requirements
- DFARS 252.239-7010, "Cloud Computing Services
- DFARS 252.204- 7012 requires that NIST Special Publication (SP) 800-171, "Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations," and the "Cloud Computing Security Requirements Guide. This is a guide to contractors and subcontractors who process, transmit and store CUI. (*Suggested Search - Defense Federal Acquisition Regulation Supplement (DFARS)*, n.d.)

Some contractors in the DIB will have to add additional requirements of NIST 800- 172 for added security against the threat of APTs.

Danger of APTs

Advanced Persistent Threats to the United States Defense Industrial Base, are threatening to the U.S. Military, U.S. Economy, and American citizens through the nefarious access to classified and unclassified information that can be stolen, altered, or destroyed. Advanced Persistent Threats are defined as "a sophisticated, sustained cyber-attack in which an intruder establishes an undetected presence in a network in order to steal sensitive data over a prolonged period of time. An APT attack is carefully planned and designed to infiltrate a specific organization, evade existing security measures, and fly under the radar." (What Is an Advanced Persistent Threat (APT)? | CrowdStrike, n.d.) The advanced persistent threats that are being launched at Defense Industrial Base contractors are purposefully detrimental to U.S. National Security by way of espionage, advancements in technology by stealing information, gathering data on employees, in addition to maintaining persistent access on networks. Nation state adversaries perpetuate these long-standing attacks and have the cyber manpower, capital, and patience to continuously pursue valuable DIB assets for their countries benefit and the United States demise. The four nation states that are most concerning for APT threats are China, Russia, North Korea, and Iran. "The governments of China, Russia, Iran, North Korea, and other autocratic states with revisionist intent are aggressively using advanced cyber capabilities to pursue objectives that run counter to our interests and broadly accepted international norms. Their reckless disregard for the rule of law and human rights in cyberspace is threatening U.S. national security and economic prosperity." (Joe Biden, 2023)

Nation states, most notably China, perpetuate continual access to networks and are essentially playing the "long game". They are waiting for the most advantageous time to attack U.S. critical infrastructure's own networks from within to cause mass disruption and unrest to the United States. "The PRC has undertaken significant military modernization and reorganization efforts in pursuit of this goal. In the event of conflict, the PRC likely intends to launch destructive cyber-attacks against the U.S. Homeland to hinder military mobilization, sow chaos, and divert attention and resources." (2023 Cyber Strategy of the Department of Defense, 2023)

One notable large-scale confirmed attack on the Defense Industrial Base was the SolarWinds attack in 2020. Hundreds of companies were affected due to the software provider, SolarWinds, being subject to an injection attack that loaded malware into a released software update. This was an effective supply chain attack linked to the Russian government. SolarWinds was targeted because of their extensive list of customers including multinational corporations and the U.S. Government. The FBI suspected that the purpose was to access emails from the White House and State Department, the other entities affected were unfortunate collateral damage. (Kerner, 2023)

More recently in 2024 three IRGC (Islamic Revolutionary Guard Corps) cyber actors were indicted by the U.S. Justice Department for their attempt to influence the 2024 United States Presidential Election. The Iranian nationals were said to be attempting to sow discord amongst voters, create distrust in the election process and were continuing efforts to avenge the death of IRGC's former leader, Qasem Soleimani. It is alleged that these individuals had compromised former U.S. Government officials and employed the same TTPs to gain access to current campaign officials. The Iranian nationals' efforts enabled them to hack and leak private campaign information to members of the media. "As alleged in the indictment, beginning in or around January 2020, Jalili, Aghamiri, and Balaghi, working on behalf of the IRGC, commenced a wide-ranging hacking campaign that used spear phishing and social engineering techniques to target and compromise victims' computers and accounts." (*Three IRGC cyber actors indicted for 'Hack-and-Leak' operation*, 2024)

Methodology

The data collected by the author was secondary qualitative data obtained through multiple published advisory papers authored by CISA and the MITRE ATT&CK framework. The research question the author sought to answer was "What are the most common APT attacks affecting the Defense Industrial Base between the years 2020-2024?" Sparse academic research was found based on these particular parameters highlighting that more research needs to be conducted in this area. Therefore, the findings from U.S. Government reports and validated research papers from Mitre Corporation and CISA were chosen using the key search terms relevant to RQ1.

According to a study by CISA (2023) in a risk and vulnerability assessment comparing 142 Risk and Vulnerability Assessments were conducted mapping the results of 11 out of the 14 tactics in the MITRE ATT&CK Framework. Of these 11 TTP's selected in the CISA study this author chose to focus on the top four most frequent tactics, techniques, and procedures which are highlighted in this study. These findings were compared and mapped to the four nations states; China, Russia, North Korea, and Iran to uncover similarities and differences in their preferred tactics of accessing high priority critical infrastructure operators. These results were then compared with four separate CISA Advisory Reports on individual nation states to determine the commonality between nation states in four selected TTPs from the RVA study: Initial Access, Persistence, Command & Control (C2) and Exfiltration. The four CISA advisory reports studied were:

- PRC State-Sponsored actors compromise and maintain persistent access to U.S. critical infrastructure | CISA. (2024, February 7)
- Russian military cyber actors target U.S. and global critical infrastructure | CISA. (2024, September 5)
- North Korea Cyber Group conducts global espionage campaign to advance regime's military and nuclear programs | CISA. (2024, July 25)
- Iranian cyber actors' brute force and credential access activity compromises critical infrastructure organizations | CISA. (2024, October 16)

Results and Discussion

Findings in the research show similarities, differences, as well as unique qualities in attack patterns of APTs that set them apart from one another. The author's research results are focused on four key tactics of the attack path: Initial Access, Persistence, Command & Control, and Exfiltration. In researching Advanced Persistent Threat intrusions within critical infrastructure one common theme of the breaches was the simplicity of the attack techniques. Similarities among nation states TTPs will also be reviewed in detail using figures 2-5 utilizing the CISA cybersecurity advisory whitepapers.

The results in Figure.1 illustrate a visual representation of four important parts of a successful adversarial attack mapped to 11 of the 14 MITRE ATT&CK tactics in the RVA study. This study compared 142 Risk and Vulnerability Assessments conducted for the federal civilian executive branch (FCEB), high priority private and public sector critical infrastructure (CI) operators, and select state, local, tribal, and territorial (SLTT) stakeholders including maritime (CI) operators by CISA and the USCG.

143 Risk and Vulnerability Assessments Conducted			
Initial Access [TA0001]	Persistence [TA0003]	Exfiltration [TA0010]	Command & Control [TA0011]
Valid Accounts [T1078] 41%	Valid Accounts [T1078] 42%	Over C2 Channel [T1041] 41%	Commonly Used Ports [T1571] 19%

Figure 1. Successful Attack TTPs

Assessors found that Valid Accounts were successful 41% of the time in gaining initial access into a system and was successful in Persistence 42% of the time. Additionally, the C2 channel was successful 41% of the time for Exfiltration of data. One of the surprising findings in this study was that Valid Accounts [T1078] was the most successfully used technique across multiple tactics; in addition to Initial Access and Persistence it also provided opportunity in Lateral movement, Evading defenses and Privilege escalation.

In separate findings, review of four cybersecurity advisory reports by CISA and their domestic and international allied government agencies showed some similar and varied findings. The following research will be presented reviewing the same four highlighted areas of the MITRE Att&ck path comparing the tactics, techniques, and procedures that nation state adversaries use to gain access to a system, remain undetected, and successfully exfiltrate data. The following data has been compiled comparing how each nation state has their own preferred methods using the following 4 studies. PRC State-Sponsored actors compromise and maintain persistent access to U.S. critical infrastructure | CISA. (2024, February 7); Russian military cyber actors target U.S. and global critical infrastructure. (2024); Iranian cyber actors' brute force and credential access activity compromises critical infrastructure organizations | CISA. (2024, October 16); North Korea Cyber Group conducts global espionage campaign to advance regime's military and nuclear programs | CISA. (2024, July 25).

Table 2. Initial Access

Nation State	Type	Tactic
CHINA – Volt Typhoon	T1190	Exploit Public Facing Application
RUSSIA – Unit 29155	T1078.001 T1190	Valid Accounts/ Default Accounts Exploit Public Facing Applications
IRAN	T1078 T1078.004 T1133	Valid Accounts Valid Accounts/ Cloud Accounts External Remote Services
NORTH KOREA – RGB 3rd Bureau	T1190	Exploit Public Facing Application

In Table 2, the four nation states and their commonly used tactics are detailed to gain initial access into a network system. Three of the four countries utilize [T1190] choosing to exploit public facing applications, and in the previously discussed case, (CISA, 2023). Valid Accounts [T1190] were successful 41% of the time in the RVA study out of 142 assessments. The Figure 3 graph illustrates the tactic of Persistence whereby a threat actor can maintain a discrete presence in the system despite disruptions. China's state-sponsored group, Volt Typhoon is known for its technique of living-off-the land when targeting critical infrastructure. "The group also relies on valid accounts and leverages strong operational security, which combined, allows for long-term undiscovered persistence." (PRC State-Sponsored Actors Compromise and Maintain Persistent Access to U.S. Critical Infrastructure | CISA, 2024)

CHINA – Volt Typhoon	T1078	Valid Accounts/ Credentials
RUSSIA – Unit 29155	T1505.003 T1078	Server Software Component Web Shell Valid Accounts
IRAN	T1098.005 T1556 T1556.006	Account Manipulation/Device Registration Modify Authentication Process Modify Authentication Process/ MFA
NORTH KOREA – RGB 3rd Bureau	N/A	Information could not be found. DPRK seemingly uses custom RATs and dual use common applications used for LOTL

Figure 3. Persistence

Older research from a CISA whitepaper in 2020 shows that the North Korean state-sponsored hacking group, Kimsuky, demonstrates Persistence through multiple routes including remote desktop protocol, utilizing the autostart, and utilizing malicious browser extensions however, more current results could not be found. (North Korean Advanced Persistent Threat Focus: Kimsuky | CISA, 2020)

In Figure 4 The Command and Control (C2) tactic shows that each nation state has their own unique way that they prefer to communicate and control the compromised devices on the network. The only two similarities amongst the four nation states are between Iran and North Korea both utilizing the Application Layer Protocol; however, Iran chooses to use with Web Protocols. Russia and North Korea also similarly utilize Proxy for C2 but Russia-Unit 29155 additionally uses Multi Hop Proxy.

CHINA – Volt Typhoon	T1573 T1105	Encrypted Channel Ingress Tool Transfer
RUSSIA – Unit 29155	T1090.003	Proxy – Multi Hop Proxy
IRAN	T1071.001 T1105 T1572	Application Layer Protocol/ Web Protocols Ingress Tool Transfer Protocol Tunneling
NORTH KOREA – RGB 3rd Bureau	T1071 T1090	Application Layer Protocol Proxy

Figure 4. Command & Control

Shown in Table 5, North Korea, and Russia are the only two nation states who prefer to use web services to exfiltrate data. This study aimed to answer the research question “What are the most common APT attacks affecting the Defense Industrial Base between 2020-2024?” The research showed that attack pathways are often successful using simplistic techniques such as utilizing valid accounts and credentials, phishing, and other forms of social engineering to gain credentials. Additionally, the most common APT attacks between this period were used by several nation states and were not only successful for gaining access but can be useful for privilege escalation and moving laterally around a network system.

Table 5. Exfiltration

Nation State	Type	Tactic
CHINA – Volt Typhoon	T1048	Exfiltration over alternative protocol. Exfiltrates data via Server Message Block (SMB)
RUSSIA – Unit 29155	T1567.002	Sends over web service to cloud storage & file hosting service, MEGA using Rclone
IRAN	T1005	Data from local system
NORTH KOREA – RGB 3rd Bureau	T1039 T1048 T10560 T1567	Data from Network Shared Drive Exfiltration over Alternative Protocol Archive Collected Data Exfiltration over Web Service

This study focuses on the Advanced Persistent Threats plaguing the U.S. Defense Industrial Base; and discovering information related to the APTs tactics, techniques, and procedures. Findings in the research show similarities, differences, as well as unique qualities in attack patterns of APTs that set them apart from one another. The author’s research results are focused on four areas of the attack path: Initial Access; Persistence; Command & Control and Exfiltration. In researching advanced persistent threat intrusions within the DIB one common theme into the breaches was the simplicity of the attack vectors.

Discussion of Findings

A key takeaway from this study for all businesses, not only DIB contractors, is that mitigating access to valid accounts is imperative and should always employ strong passwords, MFA validation to prevent Phishing attacks, implement Identity Access Management, and to monitor access and network communication logs. Following these manageable implemetations will enable detection and swift action of atypical interactions. It is also recommended that contractors employ threat mitigations such as using cyber threat intelligence platforms to assist in detection, remediation and utilizing network security architecture including firewalls, segmentation, encryption, and use of SIEM/SOAR.

Conclusion and Future Research

There is more work that needs to be done in the study of Advanced Persistent Threats to U.S. Critical Infrastructure, particularly in the sector of the Defense Industrial Base. However, there are lessons that can be learned by DIB contractors and down-stream vendors reviewing and utilizing detailed information on APTs tactics, techniques, and procedures. APT's are more than script kiddies or hacktivists looking to prove a point. The adversarial nations that support and fund breaches into the United States most critical systems mean to disrupt and do harm to the American people. Without important and continuous research to gain insight into Advanced Persistent Threats by our nation's enemies, the breaches to Defense Industrial Base networks could cause catastrophic consequences for decades.

Ongoing research into the crisis of Advanced Persistent Threats and methods to combat and mitigate them is imperative due to the fast-paced advancements in technology. Advancements such as quantum computing, artificial intelligence and machine learning will escalate the cyber weapons that nation state actors have in their toolbox. The defensive teams protecting the DIB need to be one step ahead in combating the proliferation of cyber weaponization. Limitations to the study could be seen as lack of timely research into APT's maintaining persistence in the DIB networks. The ever-changing fast pace of technology will mean that new studies must continually be conducted to remain current on APT's newest advanced tactics, techniques, and procedures.

References

Abo El Rob, M. F., Islam, M. A., Gondi, S., & Mansour, O. (2024). The application of MITRE ATT&CK framework in mitigating cybersecurity threats in the public sector. Issues in Information Systems, 25(3).

APT29, IRON RITUAL, IRON HEMLOCK, NobleBaron, Dark Halo, NOBELIUM, UNC2452, YTTRIUM, The Dukes, Cozy Bear, CozyDuke, SolarStorm, Blue Kitsune, UNC3524, Midnight Blizzard, Group G0016 | MITRE ATT&CK®." Retrieved on 07/14/2025 from https://attack.mitre.org/groups/G0016/

Basra, J., Kaushik, T., MITRE ATT&CK, & Center for Long-Term Cyber Security. (2020). MITRE ATT&CK as a framework for cloud threat investigation. In *CLTC White Paper Series* [Report]. https://cltc.berkeley.edu/wp-content/uploads/2020/10/MITRE_ATTCK_Framework_Report.pdf

Cybersecurity and Infrastructure Security Agency CISA. https://www.cisa.gov/news-events/cybersecurity-advisories/aa20-301a

Cybersecurity and Infrastructure Security Agency (CISA). (2024). Risk and vulnerability assessments. https://www.cisa.gov/sites/default/files/2024-09/FY23_RVA_Analysis_508.pdf

DeBlasio, L. M., Farnsworth, T., Feng, P.-G., McLeod, D. C., & MITRE Corporation. (2022). MITRE TECHNICAL REPORT C-ACT (CMMC v2.0-ATT&CK Compliance Tool) V1.0 Report. In

MITRE TECHNICAL REPORT [Report]. MITRE Corporation. https://apps.dtic.mil/sti/pdfs/AD1188287.pdf

Defense Industrial Base Sector | Cybersecurity and Infrastructure Security Agency CISA. (n.d.). https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience/critical-infrastructure-sectors/defense-industrial-base-sector#:~:text=Sector%20Detail-,The%20Defense%20Industrial%20Base%20Sector%20is%20the%20worldwide%20industrial%20complex,t

Department of Defense (DoD), & DoD CIO Cybersecurity Architecture Division. (2023b). Cybersecurity Reference Architecture. In *Department of Defense (DoD)*. https://dodcio.defense.gov/Portals/0/Documents/Library/CS-Ref-Architecture.pdf

Gihon, S. (2024, April 16). *The weak link: Recent supply chain attacks examined*. Cyberint. https://cyberint.com/blog/research/recent-supply-chain-attacks-examined/

Hicks, K. & National Defense Industrial Association. (2022). *Securing Defense-Critical supply chains* (By United States Deputy Secretary of Defense). https://media.defense.gov/2022/feb/24/2002944158/-1/-1/1/dod-eo-14017-report-securing-defense-critical-supply-chains.pdf

Iranian cyber actors' brute force and credential access activity compromises critical infrastructure organizations | CISA. (2024, October 16). Cybersecurity and Infrastructure Security Agency CISA. https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-290a

Kerner, S. O. S. M. (2023, November 3). SolarWinds hack explained: Everything you need to know. WhatIs. https://www.techtarget.com/whatis/feature/SolarWinds-hack-explained-Everything-you-need-to-know#:~:text=More%20than%2018%2C000%20SolarWinds%20customers,on%20other%20companies%20and%20organizations.

Ribeiro, A. (2024, April 5). *CSRB reports Microsoft Exchange breach by Storm-0558, urges security reforms following espionage incident*. Industrial Cyber. https://industrialcyber.co/reports/csrb-reports-microsoft-exchange-breach-by-storm-0558-urges-security-reforms-following-espionage-incident/

Rocha, A., & O'Hanlon, M. E. (2024, June 20). Strengthening America's defense industrial base. *Brookings*. https://www.brookings.edu/articles/strengthening-americas-defense-industrial-base/#:~:text=Humana%2C%20among%20others.-,1,through%20contracts%20with%20private%20companies.

Strom, B. E., Applebaum, A., Miller, D. P., Nickels, K. C., Pennington, A. G., Thomas, C. B., & MITRE Corporation. (2020). *MITRE ATT&CK: Design and Philosophy*. https://attack.mitre.org/docs/ATTACK_Design_and_Philosophy_March_2020.pdf

U.S. Attorney's Office District of Columbia. and Drug Administration. (2024, September 27). Three IRGC Cyber Actors Indicted for 'Hack-and-Leak' Operation Designed to Influence the 2024 U.S. Presidential Election [Press release]. US Attorney's website. [press release] https://www.justice.gov/usao-dc/pr/three-irgc-cyber-actors-indicted-hack-and-leak-operation-designed-influence-2024-us