AEROJET ROCKETDYNE

2001 Aerojet Road
Rancho Cordova, CA 95742-6418

28 February 2022

Dear Aerojet Rocketdyne Supplier:

Aerojet Rocketdyne, Inc. has received notifications from its customers, such as the one provided below that advise of increased threat potential. We wanted to share the information with you and request that you forward this to your internal information technology and security specialists as well as all lower-tier suppliers and take all appropriate actions to protect your company, its resources and ultimately the United States.

On February 16, 2022, the Cybersecurity & Infrastructure Security Agency (CISA), which is part of the U.S. Department of Homeland Security (DHS), issued Alert (AA22-047A), "Russian State-Sponsored Cyber Actors Target Cleared Defense Contractor Networks to Obtain Sensitive U.S. Defense Information Technology." The Alert contains useful background on the situation and the following guidance for companies on response and risk mitigation efforts:

- CISA and U.S. intelligence and law enforcement agencies have observed an increase in targeting of U.S. cleared defense contractors (CDCs) by Russian state-sponsored cyber threat actors. The targeted CDCs support contracts for the U.S. Department of Defense (DoD) and the U.S. intelligence community. Intrusions to date have given the threat actors access to sensitive, unclassified information and also to CDC-proprietary and export-controlled technology
- The Russia state-sponsored threat actors are using common but effective tactics to gain access to targeted networks. These tactics are also used by many other cyber threat actors, potentially making them difficult to identify as part of these attacks, such as: spear phishing, credential harvesting, brute force/password spraying, and targeting known vulnerabilities in widely used platforms like Microsoft 365 (M365). Both enterprise and cloud networks have been targeted.
- The Alert provides additional, detailed information on threat actor activity and tactics, techniques and procedures (TTPs) known to have been associated with these attacks. The Alert also provides guidance to aid companies' detection efforts to identify such attacks. Companies will be well-served to review this information and incorporate it into their preventative measures, as well as threat hunting and incident investigations.
- The Alert also provides suggested measures companies may consider for immediate response to and mitigation against these threats. While discussed here in the context of these attacks, such measures are also helpful more broadly because they respond to the common but effective tactics in use not only by these Russian attackers but also by many other threat actors. Suggested measures include:
  - resetting passwords in the event of a suspected attack;
  - implementing credential hardening;
  - establishing centralized log management;
  - initiating a software and patch management program;
  - employing antivirus (AV) programs;
  - using endpoint detection and response (EDR) tools;
  - maintaining rigorous configuration management programs;
  - enforcing the principle of least privilege;
  - reviewing trust relationships;
  - encouraging remote work environment best practices; and
  - establishing user awareness best practices and applying additional best practice mitigations.

Companies should consider using this threat intelligence as an opportunity to review their cybersecurity incident response plans (IRPs); ensure they understand and are prepared to meet applicable legal, regulatory, and contractual reporting obligations; and evaluate their ability to detect and respond to attacks such as these.

Sincerely,

Mariel Dennis

Mariel Dennis
Director, Supply Chain Compliance