THREAT BULLETINS

# Russian State-Sponsored Cyber Actors Target Cleared Defense Contractor Networks to Obtain Sensitive US Defense Information and Technology

○○○ TLP:WHITE

Feb 16, 2022

From at least January 2020 through February 2022, the United States Federal Bureau of Investigation (FBI), National Security Agency (NSA), and Cybersecurity and Infrastructure Security Agency (CISA) have observed regular targeting of US cleared defense contractors (CDCs) by Russian state-sponsored cyber actors. The actors have targeted both large and small CDCs and subcontractors with varying levels of cybersecurity protocols and resources.

These CDCs support contracts for the U.S. Department of Defense (DoD) and Intelligence Community in the following areas:

- Command, control, communications, and combat systems.
- Intelligence, surveillance, reconnaissance, and targeting.

- Weapons and missile development.
- Vehicle and aircraft design.
- Software development, data analytics, computers, and logistics.

Historically, Russian state-sponsored cyber actors have used common but effective tactics to gain access to target networks, including spearphishing, credential harvesting, brute force/password spray techniques, and known vulnerability exploitation against accounts and networks with weak security. These actors take advantage of simple passwords, unpatched systems, and unsuspecting employees to gain initial access before moving laterally through the network to establish persistence and exfiltrate data.

In many attempted compromises, these actors have employed similar tactics to gain access to enterprise and cloud networks, prioritizing their efforts against the widely used Microsoft 365 (M365)environment. The actors often maintain persistence by using legitimate credentials and a variety of malware when exfiltrating emails and data.

These continued intrusions have enabled the actors to acquire sensitive, unclassified information, as well as CDC-proprietary and export-controlled technology. The acquired information provides significant insight into US weapons platforms development and deployment timelines, vehicle specifications, and plans for communications infrastructure and information technology. By acquiring proprietary internal documents and email communications, adversaries may be able to adjust their own military plans and priorities, hasten technological development efforts, inform foreign policymakers of US intentions, and target potential sources for recruitment. Given the sensitivity of information widely available on unclassified CDC networks, the FBI, NSA, and CISA anticipate that Russian state-sponsored cyber actors will continue to target CDCs for US defense information in the near future. These agencies encourage all CDCs and related organizations to apply the recommended mitigations in this advisory, regardless of evidence of compromise.

Health-ISAC is releasing this TLP:WHITE advisory for members' increased security awareness, as increased geopolitical tensions, could directly, or indirectly, affect security and business operations within your own environment, as well as third and fourth-party entities that provide services to your healthcare organization. Health-ISAC has also released a separate report on Russian state-sponsored cyber-threats to US critical infrastructure entities, with additional details and recommendations, which can be accessed here. Health-ISAC has also disseminated a member survey inquiring about member preparedness and observations regarding a recent Ukrainian cyber-attack. The full statistical report, with additional strategic analysis, can be accessed here.

The full, original TLP:WHITE Joint Cyber Security Advisory has been attached to this alert for your reference.

Russian state-sponsored cyber actors have targeted US CDCs from at least January 2020, through February 2022. The actors leverage access to CDC networks to obtain sensitive data about US defense and intelligence programs and capabilities. Compromised entities have included CDCs supporting the US. Army, US Air Force, US Navy, US Space Force, and DoD and Intelligence programs.

During this two-year period, these actors have maintained persistent access to multiple CDC networks, in some cases for at least six months. In instances when the actors have successfully obtained access, the FBI, NSA, and CISA have noted regular and recurring exfiltration of emails and data. For example, during a compromise in 2021, threat actors exfiltrated hundreds of documents related to the company’s products, relationships with other countries, and internal personnel and legal matters.

Through these intrusions, the threat actors have acquired unclassified CDC-proprietary and export-controlled information. This theft has granted the actors significant insight into US weapons platforms development and deployment timelines, plans for communications infrastructure, and specific technologies employed by the US government and military. Although many contract awards and descriptions are publicly accessible, program developments and internal company communications remain sensitive. Unclassified emails among employees or with government customers often contain proprietary details about technological and scientific research, in addition to program updates and funding statuses.

Russian state-sponsored cyber actors use brute force methods, spearphishing, harvested credentials, and known vulnerabilities to gain initial access to CDC networks.

**Threat Actor Activity:**

Initial Access

- Threat actors use brute force techniques to identify valid account credentials for domain and M365 accounts. After obtaining domain credentials, the actors use them to gain initial access to the networks. Note: For more information, see joint NSA-FBI-CISA Cybersecurity Advisory: Russian GRU Conducting Global Brute Force Campaign to Compromise Enterprise and Cloud Environments.
- Threat actors send spearphishing emails with links to malicious domains and use publicly available URL shortening services to mask the link. Embedding shortened URLs instead of actor-controlled malicious domains is an obfuscation technique meant to bypass virus and spam scanning tools. The technique often promotes a false legitimacy to the email recipient, increasing the probability of a victim's clicking on the link.
- The threat actors use harvested credentials in conjunction with known vulnerabilities—for example, CVE-2020-0688 and CVE-2020-17144—on public-facing applications, such as virtual private networks (VPNs), to escalate privileges and gain remote code execution (RCE) on the exposed applications.1 In addition, threat actors have exploited CVE-2018-13379 on FortiClient to obtain credentials to access networks.
- As CDCs find and patch known vulnerabilities on their networks, the actors alter their tradecraft to seek new means of access. This activity necessitates CDCs maintain constant vigilance for software vulnerabilities and out-of-date security configurations, especially in internet-facing systems.

Credential Access

- After gaining access to networks, the threat actors map the Active Directory (AD) and connect to domain controllers, from which they exfiltrate credentials and export copies of the AD database ntds.dit. In multiple instances, the threat actors have used Mimikatz to dump admin credentials from the domain controllers.

Collection

- Using compromised M365 credentials, including global admin accounts, the threat actors can gain access to M365 resources, including SharePoint pages, user profiles, and user emails.

### Command and Control

- The threat actors routinely use virtual private servers (VPSs) as an encrypted proxy. The actors use VPSs, as well as small office and home office (SOHO) devices, as operational nodes to evade detection.

### Persistence

- In multiple instances, the threat actors maintained persistent access for at least six months. Although the actors have used a variety of malware to maintain persistence, the FBI, NSA, and CISA have also observed intrusions that did not rely on malware or other persistence mechanisms. In these cases, it is likely the threat actors relied on possession of legitimate credentials for persistence, enabling them to pivot to other accounts, as needed, to maintain access to the compromised environments.

| | |
|---|---|
| **Reference(s)** | Defense, Bleeping Computer, HS Today |

## Recommendations

### Detection:

The FBI, NSA, and CISA urge all CDCs to investigate suspicious activity in their enterprise and cloud environments.

### Detect Unusual Activity

- Implement robust log collection and retention. Robust logging is critical for detecting unusual activity. Without a centralized log collection and monitoring capability, organizations have limited ability to investigate incidents or detect the threat actor behavior described in this advisory. Depending on the environment, tools and solutions include:

- Cloud-native solutions, such as cloud-native security incident and event management (SIEM) tools.
- Third-party tools, such as Sparrow, to review Microsoft cloud environments and to detect unusual activity, service principals, and application activity.
  - Note: For guidance on using these and other detection tools, refer to CISA Cybersecurity Advisory Detecting Post-Compromise Threat Activity in Microsoft Cloud Environments

### Look for Evidence of Known TTPs

- Look for behavioral evidence or network and host-based artifacts from known TTPs associated with this activity. To detect password spray activity, review authentication logs for system and application login failures of valid accounts. Look for frequent, failed authentication attempts across multiple accounts.
- To detect the use of compromised credentials in combination with a VPS, follow the steps below:
  - Review logs for suspicious “impossible logins,” such as logins with changing usernames, user agent strings, and IP address combinations or logins where IP addresses do not align to the expected user’s geographic location.
  - Look for one IP used for multiple accounts, excluding expected logins.
  - Search for “impossible travel,” which occurs when a user logs in from multiple IP addresses that are a significant geographic distance apart (i.e., a person could not realistically travel between the geographic locations of the two IP addresses in the time between logins).
    - Note: This detection opportunity can result in false positives if legitimate users apply VPN solutions before connecting to networks.
  - Evaluate processes and program execution command-line arguments that may indicate credential dumping, especially attempts to access or copy the ntds.dit file from a domain controller.

  - Identify suspicious privileged account use after resetting passwords or applying user account mitigations.
  - Review logs for unusual activity in typically dormant accounts.
  - Look for unusual user agent strings, such as strings not typically associated with normal user activity, which may indicate bot activity.

**Mitigations:**

The FBI, NSA, and CISA encourage all CDCs, with or without evidence of compromise, to apply the following mitigations to reduce the risk of compromise by this threat actor. While these mitigations are not intended to be all-encompassing, they address common TTPs observed in these intrusions and will help to mitigate against common malicious activity.

Implement Credential Hardening

- Enable multifactor authentication (MFA) for all users, without exception. Subsequent authentication may not require MFA, enabling the possibility to bypass MFA by reusing single-factor authentication assertions (e.g., Kerberos authentication). Reducing the lifetime of assertions will cause account re-validation of their MFA requirements. Service accounts should not use MFA. Automation and platform features (e.g., Group Managed Service Accounts, gMSA) can provide automatic and periodic complex password management for service accounts, reducing the threat surface against single factor authentication assertions.
- Require accounts to have strong, unique passwords. Passwords should not be reused across multiple accounts or stored on the system where an adversary may have access.
- Enable password management functions, such as Local Administrator Password Solution (LAPS), for local administrative accounts. This will reduce the burden of users' managing passwords and encourage them to have strong passwords.

- Implement time-out and lock-out features in response to repeated failed login attempts.
- Configure time-based access for accounts set at the admin level and higher.
    - For example, the Just-In-Time (JIT) access method provisions privileged access when needed and can support enforcement of the principle of least privilege (as well as the Zero Trust model). This is a process where a network-wide policy is set in place to automatically disable administrator accounts at the AD level when the account is not in direct need. When the account is needed, individual users submit their requests through an automated process that enables access to a system but only for a set timeframe to support task completion.
- Use virtualization solutions on modern hardware and software to ensure credentials are securely stored, and protect credentials via capabilities, such as Windows Defender Credential Guard (CredGuard) and Trusted Platform Module (TPM). Protecting domain credentials with CredGuard requires configuration and has limitations in protecting other types of credentials (e.g., WDigest and local accounts). CredGuard uses TPMs to protect stored credentials. TPMs function as a system integrity observer and trust anchor ensuring the integrity of the boot sequence and mechanisms (e.g., UEFI Secure Boot). Installation of Windows 11 requires TPM v2.0. Disabling WDigest and rolling expiring NTLM secrets in smartcards will further protect other credentials not protected by CredGuard.
- Create a centralized log management system. Centralized logging applications allow network defenders to look for anomalous activity, such as out-of-place communications between devices or unaccountable login failures, in the network environment.
    - Forward all logs to a SIEM tool.
    - Ensure logs are searchable.
    - Retain critical and historic network activity logs for a minimum of 180 days.
- If using M365, enable Unified Audit Log (UAL)—M365’s logging capability—which contains events from Exchange Online, SharePoint online, OneDrive, Azure AD, Microsoft Teams,
- PowerBI, and other M365 services.
- Correlate logs, including M365 logs, from network and host security devices. This correlation will help with detecting

anomalous activity in the network environment and connecting it with potential anomalous activity in M365.
- Ensure PowerShell logging is turned on. Threat actors often use PowerShell to hide their malicious activities.
- Update PowerShell instances to version 5.0 or later and uninstall all earlier versions of PowerShell. Logs from prior versions are either non-existent or do not record enough detail to aid in enterprise monitoring and incident response activities.
- Confirm PowerShell 5.0 instances have module, script block, and transcription logging enabled.
- Monitor remote access/Remote Desktop Protocol (RDP) logs and disable unused remote access/RDP ports.

## Initiate a Software and Patch Management Program

- Consider using a centralized patch management system. Failure to deploy software patches in a timely manner makes an organization a target of opportunity, increasing its risk of compromise. Organizations can ensure timely patching of software vulnerabilities by implementing an enterprise-wide software and patch management program.

## Employ Antivirus Programs

- Ensure that antivirus applications are installed on all organizations' computers and are configured to prevent spyware, adware, and malware as part of the operating system security baseline.
- Keep virus definitions up to date.
- Regularly monitor antivirus scans.

## Review Trust Relationships

- Review existing trust relationships with IT service providers, such as managed service providers (MSPs) and cloud service providers (CSPs). Threat actors are known to exploit trust relationships between providers and their customers to gain access to customer networks and data.
- Remove unnecessary trust relationships.

- Review contractual relationships with all service providers, and ensure contracts include:
    - Security controls the customer deems appropriate.
    - Appropriate monitoring and logging of provider-managed customer systems.
    - Appropriate monitoring of the service provider’s presence, activities, and connections to the customer network.
    - Notification of confirmed or suspected security events and incidents occurring on the provider’s infrastructure and administrative networks.

## Encourage Remote Work Environment Best Practices

- With the increase in remote work and the use of VPN services due to COVID-19, the FBI, NSA, and CISA encourage regularly monitoring remote network traffic, along with employing the following best practices.
    - Regularly update VPNs, network infrastructure devices, and devices used for remote work environments with the latest software patches and security configurations.
    - When possible, require MFA on all VPN connections. Physical security tokens are the most secure form of MFA, followed by authenticator applications. When MFA is unavailable, mandate that employees engaging in remote work use strong passwords.
    - Monitor network traffic for unapproved and unexpected protocols.
    - Reduce potential attack surfaces by discontinuing unused VPN servers that may be used as a point of entry by adversaries.

## Establish User Awareness Best Practices

- Cyber actors frequently use unsophisticated methods to gain initial access, which can often be mitigated by stronger employee awareness of indicators of malicious activity. The FBI, NSA, and CISA recommend the following best practices to improve employee operational security when conducting business:

  - Provide end-user awareness and training. To help prevent targeted social engineering and spearphishing scams, ensure that employees and stakeholders are aware of potential cyber threats and how they are delivered. Also, provide users with training on information security principles and techniques.
  - Inform employees of the risks of social engineering attacks, e.g., risks associated with posting detailed career information to social or professional networking sites.
  - Ensure that employees are aware of what to do and whom to contact when they see suspicious activity or suspect a cyber intrusion to help quickly and efficiently identify threats and employ mitigation strategies.

Apply Additional Best Practice Mitigations

- Deny atypical inbound activity from known anonymization services, including commercial VPN services and The Onion Router (TOR).
- Impose listing policies for applications and remote access that only allow systems to execute known and permitted programs under an established security policy.
- Identify and create offline backups for critical assets.
- Implement network segmentation.
- Review CISA Alert AA20-120A: Microsoft Office 365 Security Recommendations for additional recommendations on hardening M365 cloud environments.

**Sources**
Joint Cyber Security Advisory: Russian State-Sponsored Cyber Actors Target Cleared Defense Contractor Networks to Obtain Sensitive U.S. Defense Information and Technology

BleepingComputer: US Says Russian State Hackers Breached Cleared Defense Contractors

Homeland Security Today: New Cybersecurity Advisory on Protecting Cleared Defense Contractor Networks Against Years-Long Activity by Russian State-Sponsored Actors

**Alert ID** 58e45899

This Alert has 1 attachment(s). To view or download the attachment(s), click "View Alert" to login to the web portal.

**View Alert**

**Tags** Defense Contractor Networks, Russian APT, Defense, Russia, Russian

**TLP:WHITE** Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction.

**CISA** CISA is the Nation's risk advisor, working with partners to defend against today's threats and collaborating to build more secure and resilient infrastructure for the future.

**Access the Health-ISAC Intelligence Portal** Enhance your personalized information-sharing community with improved threat visibility, alert notifications, and incident sharing in a trusted environment delivered to you via email and mobile apps. Contact membership@h-isac.org for access to Cyware.

**For Questions or Comments** Please email us at toc@h-isac.org

**FBI** The FBI encourages recipients of this document to report information concerning suspicious or criminal activity to their local FBI field office or the FBI's 24/7 Cyber Watch (CyWatch). Field office contacts may be identified at www.fbi.gov/contact-us/field. Contact CyWatch by telephone at 855-292-3937 or by email at CyWatch@fbi.gov.

Download Health-ISAC's Information Sharing App.

For more update and alerts, visit: **https://health-isac.cyware.com**

If you are not supposed to receive this email,
please contact us at **toc@h-isac.org**.