TLP:WHITE

Alert (AA22-047A)

More Alerts

Russian State-Sponsored Cyber Actors Target Cleared Defense Contractor Networks to Obtain Sensitive U.S. Defense Information and Technology

Original release date: February 16, 2022

Summary

Actions to Help Protect Against Russian State-Sponsored Malicious Cyber Activity:

- Enforce multifactor authentication.
- Enforce strong, unique passwords.
- Enable M365 Unified Audit Logs.
- Implement endpoint detection and response tools.

From at least January 2020, through February 2022, the Federal Bureau of Investigation (FBI), National Security Agency (NSA), and Cybersecurity and Infrastructure Security Agency (CISA) have observed regular targeting of U.S. 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; and
- 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.

TLP:WHITE

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 U.S. 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 U.S. 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 U.S. defense information in the near future. These agencies encourage all CDCs to apply the recommended mitigations in this advisory, regardless of evidence of compromise.

For additional information on Russian state-sponsored cyber activity, see CISA's webpage, Russia Cyber Threat Overview and Advisories.

Click here for a PDF version of this report.

Threat Details

Targeted Industries and Assessed Motive

Russian state-sponsored cyber actors have targeted U.S. CDCs from at least January 2020, through February 2022. The actors leverage access to CDC networks to obtain sensitive data about U.S. defense and intelligence programs and capabilities. Compromised entities have included CDCs supporting the U.S. Army, U.S. Air Force, U.S. Navy, U.S. 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 U.S. weapons platforms development and deployment timelines, plans for communications infrastructure, and specific technologies employed by the U.S. 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. See figures 1 and 2 for information on targeted customers, industries, and information.

Figure 1. Targeted Industries

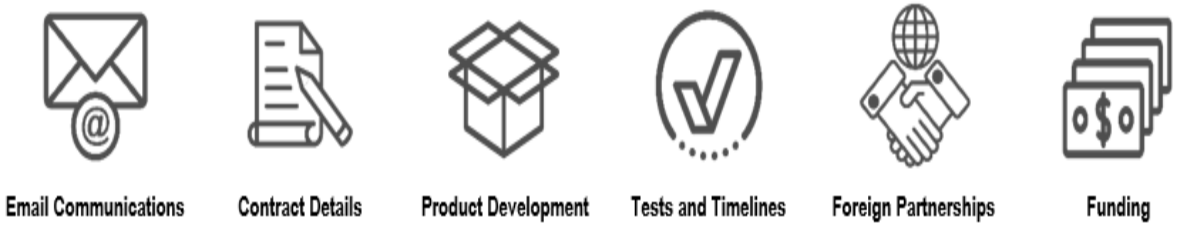

Figure 2. Exfiltrated Information

Threat Actor Activity

Note: *This advisory uses the MITRE ATT&CK® for Enterprise framework, version 10. See the ATT&CK for Enterprise for all referenced threat actor tactics and techniques. See the Tactics, Techniques, and Procedures (TTPs) section for a table of the threat actors' activity mapped to MITRE ATT&CK tactics and techniques.*

Initial Access

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

- Threat actors use brute force techniques [T1110] to identify valid account credentials [T1589.001] 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 [T1566.002] and use publicly available URL shortening services to mask the link [T1027]. 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 [T1078, T1190], 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` [T1003.003]. 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 [T1213.002], user profiles, and user emails [T1114.002].

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 [T1090.003].

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 [T1078], enabling them to pivot to other accounts, as needed, to maintain access to the compromised environments.

Tactics, Techniques, and Procedures

The following table maps observed Russian state-sponsored cyber activity to the MITRE ATT&CK for Enterprise framework. Several of the techniques listed in the table are based on observed procedures in contextual order. Therefore, some of the tactics and techniques listed in their respective columns appear more than once. See Appendix A for a functional

breakdown of TTPs. ***Note:*** *for specific countermeasures related to each ATT&CK technique, see the Enterprise Mitigations section and MITRE D3FEND™.*

Table 1: Observed Tactics, Techniques, and Procedures (TTPs)

Tactic	Technique	Procedure
Reconnaissance [TA0043] **Credential Access [TA0006]**	Gather Victim Identity Information: Credentials [T1589.001] Brute Force [T1110]	Threat actors used brute force to identify valid account credentials for domain and M365 accounts. After obtaining domain credentials, the actors used them to gain initial access.
Initial Access [TA0001]	External Remote Services [T1133]	Threat actors continue to research vulnerabilities in Fortinet's FortiGate VPN devices, conducting brute force attacks and leveraging CVE-2018-13379 to gain credentials to access victim networks. [2]
Initial Access [TA0001] **Privilege Escalation [TA0004]**	Valid Accounts [T1078] Exploit Public-Facing Application [T1190]	Threat actors used credentials in conjunction with known vulnerabilities on public-facing applications, such as virtual private networks (VPNs)—CVE-2020-0688 and CVE-2020-17144—to escalate privileges and gain remote code execution (RCE) on the exposed applications. [3]
Initial Access [TA0001] **Defense Evasion [TA0005]**	Phishing: Spearphishing Link [T1566.002] Obfuscated Files or Information [T1027]	Threat actors sent spearphishing emails using publicly available URL shortening services. Embedding shortened URLs instead of the actor-controlled malicious domain is an obfuscation technique meant to bypass virus and spam scanning tools. The technique often promotes a false legitimacy to the email recipient and thereby increases the possibility that a victim clicks on the link.

Tactic	Technique	Procedure
Initial Access [TA0001] **Credential Access [TA0006]**	OS Credential Dumping: NTDS [T1003.003] Valid Accounts: Domain Accounts [T1078.002]	Threat actors logged into a victim's VPN server and connected to the domain controllers, from which they exfiltrated credentials and exported copies of the AD database `ntds.dit`.
Initial Access [TA0001] **Privilege Escalation [TA0004]** **Collection [TA0009]**	Valid Accounts: Cloud Accounts [T1078.004] Data from Information Repositories: SharePoint [T1213.002]	In one case, the actors used valid credentials of a global admin account within the M365 tenant to log into the administrative portal and change permissions of an existing enterprise application to give read access to all SharePoint pages in the environment, as well as tenant user profiles and email inboxes.
Initial Access [TA0001] **Collection [TA0009]**	Valid Accounts: Domain Accounts [T1078.002] Email Collection [T1114]	In one case, the threat actors used legitimate credentials to exfiltrate emails from the victim's enterprise email system.

Tactic	Technique	Procedure
Persistence [TA0003] **Lateral Movement [TA0008]**	Valid Accounts [T1078]	Threat actors used valid accounts for persistence. After some victims reset passwords for individually compromised accounts, the actors pivoted to other accounts, as needed, to maintain access.
Discovery [TA0007]	File and Network Discovery [T1083]	After gaining access to networks, the threat actors used BloodHound to map the Active Directory.
Discovery [TA0007]	Domain Trust Discovery [T1482]	Threat actors gathered information on domain trust relationships that were used to identify lateral movement opportunities.
Command and Control [TA0011]	Proxy: Multi-hop Proxy [T1090.003]	Threat actors used multiple disparate nodes, such as VPSs, to route traffic to the target.

Detection

The FBI, NSA, and CISA urge all CDCs to investigate suspicious activity in their enterprise and cloud environments. ***Note:*** *for additional approaches on uncovering malicious cyber activity, see joint advisory Technical Approaches to Uncovering and Remediating Malicious Activity, authored by CISA and the cybersecurity authorities of Australia, Canada, New Zealand, and the United Kingdom.*

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 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.

Incident Response and Remediation

Organizations with evidence of compromise should assume full identity compromise and initiate a full identity reset.

- **Reset passwords for all local accounts.** These accounts should include Guest, HelpAssistant, DefaultAccount, System, Administrator, and krbtgt. It is essential to reset the password for the krbtgt account, as this account is responsible for handling Kerberos ticket requests as well as encrypting and signing them. ***Note:*** *reset the krbtgt account twice and consecutively with a 10-hour waiting period between resets (i.e., perform the first krbtgt password reset, wait 10 hours, and then follow with a second krbtgt password reset). The krbtgt password resets may take a long time to propagate fully on large AD environments. Refer to Microsoft's AD Forest Recovery - Resetting the krbtgt password guidance and automation script for additional information. [4][5]*
- **Reset all domain user, admin, and service account passwords.**

Note: *for guidance on evicting advanced persistent threat (APT) actors from cloud and enterprise environments, refer to CISA Analysis Report Eviction Guidance for Networks Affected by the SolarWinds and Active Directory/Microsoft 365 (M365) Compromise. Although this guidance was drafted for federal agencies compromised by the Russian*

Foreign Intelligence Service (SVR) via the SolarWinds Orion supply chain compromise, the steps provided in the Eviction Phase are applicable for all organizations crafting eviction plans for suspected APT actors.

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

- **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.[6] 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.[7]

Enforce Strong, Unique Passwords

- **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.

Introduce Account Lockout and Time-Based Access Features

- **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.

Reduce Credential Exposure

- **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).[8] Protecting domain credentials with CredGuard requires configuration and has limitations in protecting other types of credentials (e.g., WDigest and local accounts).[9][10] 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.[11] Disabling WDigest and rolling expiring NTLM secrets in smartcards will further protect other credentials not protected by CredGuard.[12][13]

Establish Centralized Log Management

- **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.

In addition to setting up centralized logging, organizations should:

- **Ensure PowerShell logging is turned on.** Threat actors often use PowerShell to hide their malicious activities.[14]
- **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.[15]
  - If an organization is unable to update all software shortly after a patch is released, **prioritize patches for CVEs that are already known** to be exploited or that would be

accessible to the largest number of potential adversaries (such as internet-facing systems).
    - **Subscribe to CISA cybersecurity notifications and advisories** to keep up with known exploited vulnerabilities, security updates, and threats. This will assist organizations in maintaining situational awareness of critical software vulnerabilities and, if applicable, associated exploitation.
- **Sign up for CISA's cyber hygiene services**, including vulnerability scanning, to help reduce exposure to threats. CISA's vulnerability scanning service evaluates external network presence by executing continuous scans of public, static IPs for accessible services and vulnerabilities.

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.**

Use Endpoint Detection and Response Tools

- **Utilize endpoint detection and response (EDR) tools.** These tools allow a high degree of visibility into the security status of endpoints and can be an effective defense against threat actors. EDR tools are particularly useful for detecting lateral movement, as they have insight into common and uncommon network connections for each host.

Maintain Rigorous Configuration Management Programs

- **Audit configuration management programs** to ensure they can track and mitigate emerging threats. Review system configurations for misconfigurations and security weaknesses. Having a robust configuration program hinders sophisticated threat operations by limiting the effectiveness of opportunistic attacks.[16]

Enforce the Principle of Least Privilege

- **Apply the principle of least privilege.** Administrator accounts should have the minimum permissions they need to do their tasks. This can reduce the impact if an administrator account is compromised.
- **For M365, assign administrator roles to role-based access control (RBAC)** to implement the principle of least privilege. Given its high level of default privilege, you should only use the Global Administrator account when absolutely necessary. Using Azure AD's numerous other built-in administrator roles instead of the Global Administrator account can limit assigning unnecessary privileges. ***Note:*** *refer to the Microsoft documentation, Azure AD built-in roles, for more information about Azure AD.*
- **Remove privileges not expressly required by an account's function or role.**
- **Ensure there are unique and distinct administrative accounts** for each set of administrative tasks.

- **Create non-privileged accounts for privileged users,** and ensure they use the non-privileged accounts for all non-privileged access (e.g., web browsing, email access).
- **Reduce the number of domain and enterprise administrator accounts,** and remove all accounts that are unnecessary.
- **Regularly audit administrative user accounts.**
- **Regularly audit logs to ensure new accounts are legitimate users.**
- **Institute a group policy that disables remote interactive logins,** and use Domain Protected Users Group.

To assist with identifying suspicious behavior with administrative accounts:

- **Create privileged role tracking.**
- **Create a change control process** for all privilege escalations and role changes on user accounts.
- **Enable alerts on privilege escalations and role changes.**
- **Log privileged user changes** in the network environment, and create an alert for unusual events.

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.

Note: *review CISA's page on APTs Targeting IT Service Provider Customers and CISA Insights: Mitigations and Hardening Guidance for MSPs and Small and Mid-sized Businesses for additional recommendations for MSP and CSP customers.*

Encourage Remote Work Environment Best Practices

With the increase in remote work and 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. ***Note:*** *for additional information, see joint NSA-CISA Cybersecurity Information Sheet: Selecting and Hardening Remote Access VPN Solutions.*

- **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.

Rewards for Justice Program

If you have information on state-sponsored Russian cyber operations targeting U.S. critical infrastructure, contact the Department of State's Rewards for Justice Program. You may be eligible for a reward of up to $10 million, which the Department is offering for information leading to the identification or location of any person who, while acting under the direction or control of a foreign government, participates in malicious cyber activity against U.S. critical infrastructure in violation of the Computer Fraud and Abuse Act (CFAA). Contact (202) 702-7843 on WhatsApp, Signal, or Telegram, or send information via the Rewards for Justice secure Tor-based tips line located on the Dark Web. For more details, refer to rewardsforjustice.net.

Caveats

The information you have accessed or received is being provided “as is” for informational purposes only. The FBI, NSA, and CISA do not endorse any commercial product or service, including any subjects of analysis. Any reference to specific commercial products, processes, or services by service mark, trademark, manufacturer, or otherwise, does not constitute or imply their endorsement, recommendation, or favoring by the FBI, NSA, or CISA.

Contact Information

To report suspicious activity related to information found in this Joint Cybersecurity Advisory, contact your local FBI field office at www.fbi.gov/contact-us/field-offices or the FBI’s 24/7 Cyber Watch (CyWatch) at (855) 292-3937 or by email at CyWatch@fbi.gov. When available, please include the following information regarding the incident: date, time, and location of the incident; type of activity; number of people affected; type of equipment used for the activity; the name of the submitting company or organization; and a designated point of contact. To request incident response resources or technical assistance related to these threats, contact CISA at Central@cisa.gov. For NSA client requirements or general cybersecurity inquiries, contact the NSA Cybersecurity Requirements Center at (410) 854-4200 or Cybersecurity_Requests@nsa.gov. Defense Industrial Base companies may additionally sign up for NSA’s free cybersecurity services, including Protective DNS, vulnerability scanning, and threat intelligence collaboration at dib_defense@cyber.nsa.gov.

Appendix: Detailed Tactics, Techniques, and Procedures

Reconnaissance [TA0043]

Reconnaissance consists of techniques that involve adversaries actively or passively gathering information that can be used to support targeting. The adversary is known for harvesting login credentials [T1589.001].[17]

ID	Name	Description
T1589.001	Gather Victim Identity Information: Credentials	Adversaries may gather credentials that can be used during targeting.

Initial Access [TA0001]

Initial Access consists of techniques that use various entry vectors to gain their initial foothold within a network. For example, the adversary may obtain and abuse credentials of existing accounts as a means of gaining Initial Access, Persistence, Privilege Escalation, or Defense Evasion [T1078].[18] These specific actors obtained and abused credentials of domain [T1078.002] and cloud accounts [T1078.004].[19] The actors also used external remote services to gain access to systems [T1133].[20] The adversary took advantage of

weaknesses in internet-facing servers and conducted SQL injection attacks against organizations' external websites [T1190].[21] Finally, they sent spearphishing emails with a malicious link in an attempt to gain access [T1566.002].[22]

ID	Name	Description
T1078	Valid Accounts	Adversaries may obtain and abuse credentials of existing accounts as a means of gaining Initial Access.
T1078.002	Valid Accounts: Domain Accounts	Adversaries may obtain and abuse credentials of a domain account as a means of gaining Initial Access, Persistence, Privilege Escalation, or Defense Evasion.
T1078.004	Valid Accounts: Cloud Accounts	Adversaries may obtain and abuse credentials of a cloud account as a means of gaining Initial Access, Persistence, Privilege Escalation, or Defense Evasion.
T1133	External Remote Services	Adversaries may leverage external-facing remote services to initially access and/or persist within a network.
T1190	Exploit Public-Facing Application	Adversaries may attempt to take advantage of a weakness in an internet-facing computer or program using software, data, or commands in order to cause unintended or unanticipated behavior.
T1566.002	Phishing: Spearphishing Link	Adversaries may send spearphishing emails with a malicious link in an attempt to gain access to victim systems.

Persistence [TA0003]

Persistence consists of techniques that adversaries use to keep access to systems across restarts, changed credentials, and other interruptions that could cut off their access. The adversary obtains and abuses credentials of existing accounts as a means of gaining Initial Access, Persistence, Privilege Escalation, or Defense Evasion [T1078].[23]

ID	Name	Description
T1078	Valid Accounts	Adversaries may obtain and abuse credentials of existing accounts as a means of gaining Initial Access, Persistence, Privilege Escalation, or Defense Evasion.

Privilege Escalation [TA0004]

Privilege Escalation consists of techniques that adversaries use to gain higher-level permissions on a system or network. The adversary obtains and abuses credentials of existing accounts as a means of gaining Initial Access, Persistence, Privilege Escalation, or Defense Evasion [T1078].[24] Specifically in this case, credentials of cloud accounts [T1078.004] were obtained and abused.[25]

ID	Name	Description
T1078	Valid Accounts	Adversaries may obtain and abuse credentials of existing accounts as a means of gaining Initial Access.
T1078.004	Valid Accounts: Cloud Accounts	Adversaries may obtain and abuse credentials of a cloud account as a means of gaining Initial Access, Persistence, Privilege Escalation, or Defense Evasion.

Defense Evasion [TA0005]

Defense Evasion consists of techniques that adversaries use to avoid detection throughout their compromise. The adversary made its executables and files difficult to discover or analyze by encrypting, encoding, or otherwise obfuscating its contents on the system or in transit [T1027].[26]

ID	Name	Description
T1027	Obfuscated Files or Information	Adversaries may attempt to make an executable or file difficult to discover or analyze by encrypting, encoding, or otherwise obfuscating its contents on the system or in transit.

Credential Access [TA0006]

Credential Access consists of techniques for stealing credentials like account names and passwords. The adversary attempted to access or create a copy of the Active Directory (AD) domain database to steal credential information, as well as obtain other information about domain members such as devices, users, and access rights [T1003.003].[27] The adversary also used a single or small list of commonly used passwords against many different accounts to attempt to acquire valid account credentials [T1110.003].[28]

ID	Name	Description
T1003.003	OS Credential Dumping: NTDS	Adversaries may attempt to access or create a copy of the Active Directory domain database to steal credential information, as well as obtain other information about domain members such as devices, users, and access rights.
T1110.003	Brute Force: Password Spraying	Adversaries may use a single or small list of commonly used passwords against many different accounts to attempt to acquire valid account credentials.

Discovery [TA0007]

Discovery consists of techniques an adversary may use to gain knowledge about the system and internal network. The adversary enumerated files and directories or searched in specific locations of a host or network share for certain information within a file system [T1083].[29] In addition, the adversary attempted to gather information on domain trust relationships that may be used to identify lateral movement opportunities in Windows multi-domain or forest environments [T1482].[30]

ID	Name	Description
T1083	File and Directory Discovery	Adversaries may enumerate files and directories or may search in specific locations of a host or network share for certain information within a file system.
T1482	Domain Trust Discovery	Adversaries may attempt to gather information on domain trust relationships that may be used to identify lateral movement opportunities in Windows multi-domain/forest environments.

Collection [TA0009]

Collection consists of both the techniques adversaries may use to gather information and the sources that information is collected from that are relevant to the adversary's objectives. The adversary leverages information repositories, such as SharePoint, to mine

valuable information [T1213.002].[31]

ID	Name	Description
T1213.002	Data from Information Repositories: SharePoint	Adversaries may leverage the SharePoint repository as a source to mine valuable information.

Command and Control [TA0011]

Command and Control (C2) consists of techniques that adversaries may use to communicate with systems under their control within a victim network. The adversary chained together multiple proxies to disguise the source of malicious traffic. In this case, TOR and VPN servers are used as multi-hop proxies to route C2 traffic and obfuscate their activities [T1090.003].[32]

ID	Name	Description
T1090.003	Proxy: Multi-hop Proxy	To disguise the source of malicious traffic, adversaries may chain together multiple proxies.

Additional Resources

[1] NSA, CISA, FBI, NCSC Cybersecurity Advisory: Russian GRU Conducting Global Brute Force Campaign to Compromise Enterprise and Cloud Environments, 1 July 2021.
[2] NSA Cybersecurity Advisory: Mitigating Recent VPN Vulnerabilities, 7 October 2019.
[3] NSA, CISA, FBI, NCSC Cybersecurity Advisory: Russian GRU Conducting Global Brute Force Campaign to Compromise Enterprise and Cloud Environments, 1 July 2021.
[4] Microsoft Article: AD Forest Recovery – Resetting the krbtgt password, 29 July 2021.
[5] Microsoft GitHub: New-KrbtgtKeys.ps1, 14 May 2020.
[6] NSA Cybersecurity Information: Defend Privileges and Accounts, August 2019.
[7] Microsoft Article: Group Managed Service Accounts Overview, 29 July 2021.
[8] NSA Cybersecurity Information: Leverage Modern Hardware Security Features, August 2019.
[9] Microsoft Article: Protect derived domain credentials with Windows Defender Credential Guard, 3 December 2021.
[10] Microsoft Article: Windows Defender Credential Guard protection limits, 3 December 2021.
[11] Microsoft Article: Windows 11 requirements, 30 November 2021.
[12] Microsoft Blog Post: The Importance of KB2871997 and KB2928120 for Credential Protection, 20 September 2021.
[13] Microsoft Article: What's New in Credential Protection, 7 January 2022.
[14] NSA Cybersecurity Factsheet: PowerShell: Security Risks and Defenses, 1 December 2016.
[15] NSA Cybersecurity Information: Update and Upgrade Software Immediately, August 2019.
[16] NSA Cybersecurity Information: Actively Manage Systems and Configurations, August 2019.
[17] MITRE Groups: APT28, 18 October 2021.
[18] MITRE Groups: APT28, 18 October 2021.
[19] MITRE Software: Cobalt Strike, 18 October 2021.
[20] Based on technical information shared by Mandiant.
[21] MITRE Groups: APT28, 18 October 2021.
[22] Based on technical information shared by Mandiant.
[23] MITRE Groups: APT28, 18 October 2021.
[24] MITRE Groups: APT28, 18 October 2021.
[25] MITRE Software: Cobalt Strike, 18 October 2021.
[26] MITRE Software: Fysbis, 6 November 2020.
[27] MITRE Software: Koadic, 30 March 2020.
[28] MITRE Groups: APT28, 18 October 2021.
[29] Based on technical information shared by Mandiant.
[30] Based on technical information shared by Mandiant.
[31] MITRE Groups: APT28, 18 October 2021.
[32] MITRE Groups: APT28, 18 October 2021.

Revisions

TLP:WHITE

February 16, 2022: Initial Version

This product is provided subject to this Notification and this Privacy & Use policy.