Russian State-Sponsored Advanced Persistent Threat Actor Compromises US Government Targets

SUMMARY

***Callout Box**: This joint cybersecurity advisory uses the MITRE Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK®) framework. See the ATT&CK for Enterprise framework for all referenced threat actor tactics and techniques.*

This joint cybersecurity advisory—written by the Federal Bureau of Investigation (FBI) and the Cybersecurity and Infrastructure Security Agency (CISA)—provides information on Russian state-sponsored advanced persistent threat (APT) actor activity targeting various US state, local, territorial, and tribal (SLTT) government networks, as well as aviation networks. This advisory updates joint CISA-FBI cybersecurity advisory AA20-283A: APT Actors Chaining Vulnerabilities Against SLTT, Critical Infrastructure, and Elections Organizations.

Since at least September 2020, a Russian state-sponsored APT actor—known variously as Berserk Bear, Energetic Bear, TeamSpy, Dragonfly, Havex, Crouching Yeti, and Koala in open-source reporting—has conducted a campaign against a wide variety of US targets. The Russian state-sponsored APT actor has targeted dozens of SLTT government and aviation networks, attempted intrusions at several SLTT organizations, successfully compromised network infrastructure, and as of 1 October 2020, exfiltrated data from at least two victim servers.

The Russian-sponsored APT actor is obtaining user and administrator credentials to establish initial access, enable lateral movement once inside the network, and locate high value assets in order to exfiltrate data. In at least one compromise, the APT actor laterally traversed an SLTT victim network and accessed documents related to:

- Sensitive network configurations and passwords.
- Standard operating procedures (SOP), such as enrolling in multi-factor authentication (MFA).
- IT instructions, such as requesting password resets.
- Vendors and purchasing information.
- Printing access badges.

To date, the FBI and CISA have no information to indicate this APT actor has intentionally disrupted any aviation, education, or government operations. However, the actor may be seeking access to

obtain future disruption options, to influence US policies and actions, or to delegitimize SLTT government entities.

As this recent malicious activity has been directed at SLTT government networks, there may be some risk to elections information housed on SLTT government networks. However, the FBI and CISA have no evidence to date that integrity of elections data has been compromised. Due to the heightened awareness surrounding elections infrastructure and the targeting of SLTT government networks, the FBI and CISA will continue to monitor this activity and its proximity to elections infrastructure.

TECHNICAL DETAILS

The FBI and CISA have observed Russian state-sponsored APT actor activity targeting US SLTT government networks, as well as aviation networks. The APT actor is using Turkish IP addresses `213.74.101[.]65`, `213.74.139[.]196`, and `212.252.30[.]170` to connect to victim web servers (*Exploit Public Facing Application* [T1190]).

The actor is using `213.74.101[.]65` and `213.74.139[.]196` to attempt brute force logins and, in several instances, attempted Structured Query Language (SQL) injections on victim websites (*Brute Force* [T1110]; *Exploit Public Facing Application* [T1190]). The APT actor also hosted malicious domains, including possible aviation sector target `columbusairports.microsoftonline[.]host`, which resolved to `108.177.235[.]92` and `[cityname].westus2.cloudapp.azure.com`; these domains are US registered and are likely SLTT government targets (*Drive-By Compromise* [T1189]).

The APT actor scanned for vulnerable Citrix and Microsoft Exchange services and identified vulnerable systems, likely for future exploitation. This actor continues to exploit a Citrix Directory Traversal Bug (CVE-2019-19781), and a Microsoft Exchange remote code execution flaw (CVE-2020-0688).

The APT actor has been observed using Cisco AnyConnect Secure Socket Layer (SSL) virtual private network (VPN) connections to enable remote logins on at least one victim network, possibly enabled by an Exim Simple Mail Transfer Protocol (SMTP) vulnerability (CVE 2019-10149) (*External Remote Services* [T1133]). More recently, the APT actor enumerated and exploited a Fortinet VPN vulnerability (CVE-2018-13379) for *Initial Access* [TA0001] and a Windows Netlogon vulnerability (CVE-2020-1472) to obtain access to Windows Active Directory (AD) servers for *Privilege Escalation* [TA004] within the network (*Valid Accounts* [T1078]). These vulnerabilities can also be leveraged to compromise other devices on the network (*Lateral Movement* [TA0008]) and to maintain *Persistence* [TA0003]).

Between early February and mid-September, these APT actors used `213.74.101[.]65`, `212.252.30[.]170`, `5.196.167[.]184`, `37.139.7[.]16`, `149.56.20[.]55`, `91.227.68[.]97`, and `5.45.119[.]124` to target US SLTT government networks. Successful authentications—including the compromise of Microsoft Office 365 (O365) accounts—have been observed on at least one victim network (*Valid Accounts* [T1078]).

MITIGATIONS

Indicators of Compromise

The APT actor used the following IP addresses and domains to carry out its objectives:

- `213.74.101[.]65`
- `213.74.139[.]196`
- `212.252.30[.]170`
- `5.196.167[.]184`
- `37.139.7[.]16`
- `149.56.20[.]55`
- `91.227.68[.]97`
- `138.201.186[.]43`
- `5.45.119[.]124`
- `193.37.212[.]43`
- `146.0.77[.]60`
- `51.159.28[.]101`
- `columbusairports.microsoftonline[.]host`
- `microsoftonline[.]host`
- `email.microsoftonline[.]services`
- `microsoftonline[.]services`
- `[cityname].westus2.cloudapp.azure.com`

IP address `51.159.28[.]101` appears to have been configured to receive stolen Windows New Technology Local Area Network Manager (NTLM) credentials. FBI and CISA recommend organizations take defensive actions to mitigate the risk of leaking NTLM credentials; specifically, organizations should disable NTLM or restrict outgoing NTLM. Organizations should consider blocking IP address `51.159.28[.]101` (although this action alone may not mitigate the threat, as the APT actor has likely established, or will establish, additional infrastructure points).

Organizations should check available logs for traffic to/from IP address `51.159.28[.]101` for indications of credential-harvesting activity. As the APT actors likely have—or will—establish additional infrastructure points, organizations should also monitor for Server Message Block (SMB) or WebDAV activity leaving the network to other IP addresses.

Refer to AA20-296A.stix for a downloadable copy of IOCs.

Network Defense-in-Depth

Proper network defense-in-depth and adherence to information security best practices can assist in mitigating the threat and reducing the risk to critical infrastructure. The following guidance may assist organizations in developing network defense procedures.

- Keep all applications updated according to vendor recommendations, and especially prioritize updates for external facing applications and remote access services to address CVE-2019-19781, CVE-2020-0688, CVE 2019-10149, CVE-2018-13379, and CVE-2020-1472. Refer to Table 1 for patch information on these CVEs.

Table 1: Patch information for CVEs

Vulnerability	Vulnerable Products	Patch Information
CVE-2019-19781	• Citrix Application Delivery Controller • Citrix Gateway • Citrix SDWAN WANOP	Citrix blog post: firmware updates for Citrix ADC and Citrix Gateway versions 11.1 and 12.0 Citrix blog post: security updates for Citrix SD-WAN WANOP release 10.2.6 and 11.0.3 Citrix blog post: firmware updates for Citrix ADC and Citrix Gateway versions 12.1 and 13.0 Citrix blog post: firmware updates for Citrix ADC and Citrix Gateway version 10.5

Vulnerability	Vulnerable Products	Patch Information
CVE-2020-0688	• Microsoft Exchange Server 2010 Service Pack 3 Update Rollup 30 • Microsoft Exchange Server 2013 Cumulative Update 23 • Microsoft Exchange Server 2016 Cumulative Update 14 • Microsoft Exchange Server 2016 Cumulative Update 15 • Microsoft Exchange Server 2019 Cumulative Update 3 • Microsoft Exchange Server 2019 Cumulative Update 4	Microsoft Security Advisory for CVE-2020-0688
CVE-2019-10149	• Exim versions 4.87–4.91	Exim page for CVE-2019-10149
CVE-2018-13379	• FortiOS 6.0: 6.0.0 to 6.0.4 • FortiOS 5.6: 5.6.3 to 5.6.7 • FortiOS 5.4: 5.4.6 to 5.4.12	Fortinet Security Advisory: FG-IR-18-384
CVE-2020-1472	• Windows Server 2008 R2 for x64-based Systems Service Pack 1 • Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation) • Windows Server 2012 • Windows Server 2012 (Server Core installation) • Windows Server 2012 R2 • Windows Server 2016 • Windows Server 2019 • Windows Server 2019 (Server Core installation) • Windows Server, version 1903 (Server Core installation) • Windows Server, version 1909 (Server Core installation) • Windows Server, version 2004 (Server Core installation)	Microsoft Security Advisory for CVE-2020-1472

- Follow Microsoft's guidance on monitoring logs for activity related to the Netlogon vulnerability, CVE-2020-1472.
- If appropriate for your organization's network, prevent external communication of all versions of SMB and related protocols at the network boundary by blocking Transmission Control Protocol (TCP) ports 139 and 445 and User Datagram Protocol (UDP) port 137. See the CISA publication on SMB Security Best Practices for more information.
- Implement the prevention, detection, and mitigation strategies outlined in:
    - CISA Alert TA15-314A – Compromised Web Servers and Web Shells – Threat Awareness and Guidance
    - National Security Agency Cybersecurity Information Sheet U/OO/134094-20 – Detect and Prevent Web Shells Malware.
- Isolate external facing services in a network demilitarized zone (DMZ) since they are more exposed to malicious activity; enable robust logging, and monitor the logs for signs of compromise.
- Establish a training mechanism to inform end users on proper email and web usage, highlighting current information and analysis and including common indicators of phishing. End users should have clear instructions on how to report unusual or suspicious emails.
- Implement application controls to only allow execution from specified application directories. System administrators may implement this through Microsoft Software Restriction Policy, AppLocker, or similar software. Safe defaults allow applications to run from `PROGRAMFILES`, `PROGRAMFILES(X86)`, and `WINDOWS` folders. All other locations should be disallowed unless an exception is granted.
- Block Remote Desktop Protocol (RDP) connections originating from untrusted external addresses unless an exception exists; routinely review exceptions on a regular basis for validity.

Comprehensive Account Resets

For accounts where NTLM password hashes or Kerberos tickets may have been compromised (e.g., through CVE-2020-1472), a *double-password-reset* may be required in order to prevent continued exploitation of those accounts. For domain-admin-level credentials, a reset of KRB-TGT "Golden Tickets" may be required and, for this, Microsoft has released specialized guidance. Such a reset should be performed very carefully if needed.

If there is an observation of CVE-2020-1472 Netlogon activity or other indications of valid credential abuse, it should be assumed the APT actors have compromised AD administrative accounts. In such cases, the AD forest should not be fully trusted, and, therefore, a new forest should be deployed. Existing hosts from the old compromised forest cannot be migrated in without being rebuilt and rejoined to the new domain, but migration may be done through "creative destruction," wherein, as endpoints in the legacy forest are decommissioned, new ones can be built in the new forest. This will need to be completed in on-premise—as well as in Azure-hosted—AD instances.

Note that fully resetting an AD forest is difficult and complex; it is best done with the assistance of personnel who have successfully completed the task previously.

It is critical to perform a full password reset on all user and computer accounts in the AD forest. Use the following steps as a guide.

1. Create a temporary administrator account, and use this account only for all administrative actions
2. Reset the Kerberos Ticket Granting Ticket (`krbtgt`) password;[1] this must be completed before any additional actions (a second reset will take place in step 5)
3. Wait for the `krbtgt` reset to propagate to all domain controllers (time may vary)
4. Reset all account passwords (passwords should be 15 characters or more and randomly assigned):
    a. User accounts (forced reset with no legacy password reuse)
    b. Local accounts on hosts (including local accounts not covered by Local Administrator Password Solution [LAPS])
    c. Service accounts
    d. Directory Services Restore Mode (DSRM) account
    e. Domain Controller machine account
    f. Application passwords
5. Reset the `krbtgt` password again
6. Wait for the `krbtgt` reset to propagate to all domain controllers (time may vary)
7. Reboot domain controllers
8. Reboot all endpoints

The following accounts should be reset:

- AD Kerberos Authentication Master (2x)
- All Active Directory Accounts
- All Active Directory Admin Accounts
- All Active Directory Service Accounts
- All Active Directory User Accounts
- DSRM Account on Domain Controllers
- Non-AD Privileged Application Accounts
- Non-AD Unprivileged Application Accounts
- Non-Windows Privileged Accounts
- Non-Windows User Accounts
- Windows Computer Accounts
- Windows Local Admin

[1] https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/manage/ad-forest-recovery-resetting-the-krbtgt-password

VPN Vulnerabilities

Implement the following recommendations to secure your organization's VPNs:

- **Update VPNs, network infrastructure devices, and devices** being used to remote into work environments with the latest software patches and security configurations. See CISA Tips Understanding Patches and Software Updates and Securing Network Infrastructure Devices. Wherever possible, enable automatic updates.
- **Implement MFA on all VPN connections to increase security**. Physical security tokens are the most secure form of MFA, followed by authenticator app-based MFA. SMS and email-based MFA should only be used when no other forms are available. If MFA is not implemented, require teleworkers to use strong passwords. See CISA Tips Choosing and Protecting Passwords and Supplementing Passwords for more information.

Discontinue unused VPN servers. Reduce your organization's attack surface by discontinuing unused VPN servers, which may act as a point of entry for attackers. To protect your organization against VPN vulnerabilities:

- **Audit** configuration and patch management programs.
- **Monitor** network traffic for unexpected and unapproved protocols, especially outbound to the Internet (e.g., Secure Shell [SSH], SMB, RDP).
- **Implement** MFA, especially for privileged accounts.
- **Use** separate administrative accounts on separate administration workstations.
- **Keep** software up to date. Enable automatic updates, if available.

REFERENCES

- APT Actors Chaining Vulnerabilities Against SLTT, Critical Infrastructure, and Elections Organizations – https://us-cert.cisa.gov/ncas/alerts/aa20-283a
- CISA Activity Alert CVE-2019-19781 – https://us-cert/cisa.gov/ncas/alerts/aa20-031a
- CISA Vulnerability Bulletin – https://us-cert/cisa.gov/ncas/bulletins/SB19-161
- CISA Current Activity – https://us-cert.cisa/ncas/current-activity/2020/03/10/unpatched-microsoft-exchange-servers-vulnerable-cve-2020-0688
- Citrix Directory Traversal Bug (CVE-2019-19781) – https://nvd.nist.gov/vuln/detail/CVE-2019-19781
- Microsoft Exchange remote code execution flaw (CVE-2020-0688) – https://nvd.nist.gov/vuln/detail/CVE-2020-0688
- CVE-2018-13379 – https://nvd.nist.gov/vuln/detail/CVE-2018-13379
- CVE-2020-1472 – https://nvd.nist.gov/vuln/detail/CVE-2020-1472
- CVE 2019-10149 – https://nvd.nist.gov/vuln/detail/CVE-2019-10149
- NCCIC/USCERT Alert TA15-314A – Compromised Web Servers and Web Shells – Threat Awareness and Guidance – https://us-cert.cisa.gov/ncas/alerts/TA15-314A
- NCCIC/US-CERT publication on SMB Security Best Practices – https://us-cert.cisa.gov/ncas/current-activity/2017/01/16/SMB-Security-Best-Practices