Advanced Persistent Threat Actors Targeting U.S. Think Tanks

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

The Cybersecurity and Infrastructure Security Agency (CISA) and the Federal Bureau of Investigation (FBI) have observed persistent continued cyber intrusions by advanced persistent threat (APT) actors targeting U.S. think tanks. This malicious activity is often, but not exclusively, directed at individuals and organizations that focus on international affairs or national security policy.[1] The following guidance may assist U.S. think tanks in developing network defense procedures to prevent or rapidly detect these attacks.

APT actors have relied on multiple avenues for initial access. These have included low-effort capabilities such as spearphishing emails and third-party message services directed at both corporate and personal accounts, as well as exploiting vulnerable web-facing devices and remote connection capabilities. Increased telework during the COVID-19 pandemic has expanded workforce reliance on remote connectivity, affording malicious actors more opportunities to exploit those connections and to blend in with increased traffic. Attackers may leverage virtual private networks (VPNs) and other remote work tools to gain initial access or persistence on a victim's network. When successful, these low-effort, high-reward approaches allow threat actors to steal sensitive information, acquire user credentials, and gain persistent access to victim networks.

Given the importance that think tanks can have in shaping U.S. policy, CISA and FBI urge individuals and organizations in the international affairs and national security sectors to immediately adopt a heightened state of awareness and implement the critical steps listed in the Mitigations section of this Advisory.

[1] CyberScoop | As Europe prepares to vote, Microsoft warns of Fancy Bear attacks on democratic think tanks | 20-FEB-2020 | URL: https://www.cyberscoop.com/european-think-tanks-hack-microsoft-fancy-bear-russia/

To report suspicious or criminal activity related to information found in this Joint Cybersecurity Advisory, contact your local FBI field office at www.fbi.gov/contact-us/field, or the FBI's 24/7 Cyber Watch (CyWatch) at (855) 292-3937 or by e-mail 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 CISAServiceDesk@cisa.dhs.gov.

This document is marked TLP:WHITE. Disclosure is not limited. Sources may use TLP:WHITE when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release. Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction. For more information on the Traffic Light Protocol, see http://www.us-cert.gov/tlp/.

TECHNICAL DETAILS

ATT&CK Profile

CISA created the following MITRE ATT&CK profile to provide a non-exhaustive list of tactics, techniques, and procedures (TTPs) employed by APT actors to break through think tanks' defenses, conduct reconnaissance in their environments, exfiltrate proprietary or confidential information, and execute effects on targets. These TTPs were included based upon closed reporting on APT actors that are known to target think tanks or based upon CISA incident response data.

- ***Initial Access*** [TA0001]
  - *Valid Accounts* [T1078]
  - *Valid Accounts: Cloud Accounts* [T1078.004]
  - *External Remote Services* [T1133]
  - *Drive-by Compromise* [T1189]
  - *Exploit Public-Facing Application* [T1190]
    - *Supply Chain Compromise: Compromise Software Supply Chain* [T1195.002]
    - *Trusted Relationship* [T1199]
    - *Phishing: Spearphishing Attachment* [T1566.001]
    - *Phishing: Spearphishing Link* [T1566.002]
    - *Phishing: Spearphishing via Service* [T1566.003]
- ***Execution*** [TA0002]
  - *Windows Management Instrumentation* [T1047]
  - *Scheduled Task/Job: Scheduled Task* [T1053.005]
  - *Command and Scripting Interpreter: PowerShell* [T1059.001]
  - *Command and Scripting Interpreter: Windows Command Shell* [T1059.003]
  - *Command and Scripting Interpreter: Unix Shell* [T1059.004]
  - *Command and Scripting Interpreter: Visual Basic* [T1059.005]
  - *Command and Scripting Interpreter: Python* [T1059.006]
  - *Native API* [T1106]
  - *Exploitation for Client Execution* [T1203]
  - *User Execution: Malicious Link* [T1204.001]
  - *User Execution: Malicious File* [T1204.002]
  - *Inter-Process Communication: Dynamic Data Exchange* [T1559.002]
  - *System Services: Service Execution* [T1569.002]
- ***Persistence*** [TA0003]
  - *Boot or Logon Initialization Scripts: Logon Script (Windows)* [T1037.001]
  - *Scheduled Task/Job: Scheduled Task* [T1053.005]
  - *Account Manipulation: Exchange Email Delegate Permissions* [T1098.002]
  - *Create Account: Local Account* [T1136.001]
  - *Office Application Startup: Office Test* [T1137.002]
  - *Office Application Startup: Outlook Home Page* [T1137.004]

- *Browser Extensions* [T1176]
- *BITS Jobs* [T1197]
- *Server Software Component: Web Shell* [T1505.003]
- *Pre-OS Boot: Bootkit* [T1542.003]
- *Create or Modify System Process: Windows Service* [T1543.003]
- *Event Triggered Execution: Change Default File Association* [T1546.001]
- *Event Triggered Execution: Windows Management Instrumentation Event Subscription* [T1546.003]
- *Event Triggered Execution: Accessibility Features* [T1546.008]
- *Event Triggered Execution: Component Object Model Hijacking* [T1546.015]
- *Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder* [T1547.001]
- *Boot or Logon Autostart Execution: Shortcut Modification* [T1547.009]

- ***Privilege Escalation*** [TA0004]
  - *Process Injection* [T1055]
  - *Process Injection: Process Hollowing* [T1055.012]
  - *Exploitation for Privilege Escalation* [T1068]
  - *Access Token Manipulation: Token Impersonation/Theft* [T1134.001]
  - *Event Triggered Execution: Accessibility Features* [T1546.008]
  - *Boot or Logon Autostart Execution: Shortcut Modification* [T1547.009]
  - *Abuse Elevation Control Mechanism: Bypass User Access Control* [T1548.002]
  - *Hijack Execution Flow: DLL Side-Loading* [T1574.002]

- ***Defense Evasion*** [TA0005]
  - *Rootkit* [T1014]
  - *Obfuscated Files or Information: Binary Padding* [T1027.001]
  - *Obfuscated Files or Information: Software Packing* [T1027.002]
  - *Obfuscated Files or Information: Steganography* [T1027.003]
  - *Obfuscated Files or Information: Indicator Removal from Tools* [T1027.005]
  - *Masquerading: Match Legitimate Name or Location* [T1036.005]
  - *Indicator Removal on Host: Clear Windows Event Logs* [T1070.001]
  - *Indicator Removal on Host: Clear Command History* [1070.003]
  - *Indicator Removal on Host: File Deletion* [T1070.004]
  - *Indicator Removal on Host: Timestomp* [T1070.006]
  - *Modify Registry* [T1112]
  - *Deobfuscate/Decode Files or Information* [T1140]
  - *Exploitation for Defense Evasion* [T1211]
  - *Signed Binary Proxy Execution: Compiled HTML File* [T1218.001]
  - *Signed Binary Proxy Execution: Mshta* [T1218.005]
  - *Signed Binary Proxy Execution: Rundll32* [T1218.011]
  - *Template Injection* [T1221]
  - *Execution Guardrails: Environmental Keying* [T1480.001]
  - *Abuse Elevation Control Mechanism: Bypass User Access Control* [T1548.002]

- *Use Alternate Authentication Material: Application Access Token* [T1550.001]
- *Subvert Trust Controls: Code Signing* [T1553.002]
- *Impair Defenses: Disable or Modify Tools* [T1562.001]
- *Impair Defenses: Disable or Modify System Firewall* [T1562.004]
- *Hide Artifacts: Hidden Files and Directories* [T1564.001]
- *Hide Artifacts: Hidden Window* [T1564.003]

- ***Credential Access*** [TA0006]
  - *OS Credential Dumping: LSASS Memory* [T1003.001]
  - *OS Credential Dumping: Security Account Manager* [T1003.002]
  - *OS Credential Dumping: NTDS* [T1003.003]
  - *OS Credential Dumping: LSA Secrets* [T1003.004]
  - *OS Credential Dumping: Cached Domain Credentials* [T1003.005]
  - *Network Sniffing* [T1040]
  - *Input Capture: Keylogging* [T1056.001]
  - *Brute Force: Password Cracking* [T1110.002]
  - *Brute Force: Password Spraying* [T1110.003]
  - *Forced Authentication* [T1187]
  - *Steal Application Access Token* [T1528]
  - *Unsecured Credentials: Credentials in Files* [T1552.001]
  - *Unsecured Credentials: Group Policy Preferences* [T1552.006]
  - *Credentials from Password Stores: Credentials from Web Browsers* [T1555.003]

- ***Discovery*** [TA0007]
  - *System Service Discovery* [T1007]
  - *Query Registry* [T1012]
  - *System Network Configuration Discovery* [T1016]
  - *Remote System Discovery* [T1018]
  - *System Owner/User Discovery* [T1033]
  - *Network Sniffing* [T1040]
  - *Network Service Scanning* [T1046]
  - *System Network Connections Discovery* [T1049]
  - *Process Discovery* [T1057]
  - *Permission Groups Discovery: Local Groups* [T1069.001]
  - *Permission Groups Discovery: Domain Groups* [T1069.002]
  - *System Information Discovery* [T1082]
  - *File and Directory Discovery* [T1083]
  - *Account Discovery: Local Account* [T1087.001]
  - *Account Discovery: Domain Account* [T1087.002]
  - *Peripheral Device Discovery* [T1120]
  - *Network Share Discovery* [T1135]
  - *Password Policy Discovery* [T1201]
  - *Software Discovery: Security Software Discovery* [T1518.001]

- ***Lateral Movement*** [TA0008]
  - *Remote Services: Remote Desktop Protocol* [T1021.001]
  - *Remote Services: SSH* [T1021.004]
  - *Taint Shared Content* [T1080]
  - *Replication Through Removable Media* [T1091]
  - *Exploitation of Remote Services* [T1210]
  - *Use Alternate Authentication Material: Pass the Hash* [T1550.002]
  - *Use Alternate Authentication Material: Pass the Ticket* [T1550.003]
- ***Collection*** [TA0009]
  - *Data from Local System* [T1005]
  - *Data from Removable Media* [T1025]
  - *Data Staged: Local Data Staging* [T1074.001]
  - *Screen Capture* [T1113]
  - *Email Collection: Local Email Collection* [T1114.001]
  - *Email Collection: Remote Email Collection* [T1114.002]
  - *Automated Collection* [T1119]
  - *Audio Capture* [T1123]
  - *Data from Information Repositories: SharePoint* [T1213.002]
  - *Archive Collected Data: Archive via Utility* [T1560.001]
  - *Archive Collected Data: Archive via Custom Method* [T1560.003]
- ***Command and Control*** [TA0011]
  - *Data Obfuscation: Junk Data* [T1001.001]
  - *Fallback Channels* [T1008]
  - *Application Layer Protocol: Web Protocols* [T1071.001]
  - *Application Layer Protocol: File Transfer Protocols* [T1071.002]
  - *Application Layer Protocol: Mail Protocols* [T1071.003]
  - *Application Layer Protocol: DNS* [T1071.004]
  - *Proxy: External Proxy* [T1090.002]
  - *Proxy: Multi-hop Proxy* [T1090.003]
  - *Proxy: Domain Fronting* [T1090.004]
  - *Communication Through Removable Media* [T1092]
  - *Non-Application Layer Protocol* [T1095]
  - *Web Service: Dead Drop Resolver* [T1102.001]
  - *Web Service: Bidirectional Communication* [T1102.002]
  - *Multi-Stage Channels* [T1104]
  - *Ingress Tool Transfer* [T1105]
  - *Data Encoding: Standard Encoding* [T1132.001]
  - *Remote Access Software* [T1219]
  - *Dynamic Resolution: Domain Generation Algorithms* [T1568.002]
  - *Non-Standard Port* [T1571]
  - *Protocol Tunneling* [T1572]

- *Encrypted Channel: Symmetric Cryptography* [T1573.001]
- *Encrypted Channel: Asymmetric Cryptography* [T1573.002]

- ***Exfiltration*** [TA0010]
  - *Exfiltration Over C2 Channel* [T1041]
  - *Exfiltration Over Alternative Protocol: Exfiltration Over Unencrypted/Obfuscated Non-C2 Protocol* [T1048.003]

- ***Impact*** [TA0040]
  - *Data Encrypted for Impact* [T1486]
  - *Resource Hijacking* [T1496]
  - *System Shutdown/Reboot* [T1529]
  - *Disk Wipe: Disk Structure Wipe* [T1561.002]

MITIGATIONS

CISA and FBI recommend think tank organizations apply the following critical practices to strengthen their security posture.

Leaders

- Implement a training program to familiarize users with identifying social engineering techniques and phishing emails.

Users/Staff

- Log off remote connections when not in use.
- Be vigilant against tailored spearphishing attacks targeting corporate and personal accounts (including both email and social media accounts).
- Use different passwords for corporate and personal accounts.
- Install antivirus software on personal devices to automatically scan and quarantine suspicious files.
- Employ strong multi-factor authentication for personal accounts, if available.
- Exercise caution when:
  - Opening email attachments, even if the attachment is expected and the sender appears to be known. See Using Caution with Email Attachments.
  - Using removable media (e.g., USB thumb drives, external drives, CDs).

IT Staff/Cybersecurity Personnel

- Segment and segregate networks and functions.
- Change the default username and password of applications and appliances.
- Employ strong multi-factor authentication for corporate accounts.
- Deploy antivirus software on organizational devices to automatically scan and quarantine suspicious files.

- Apply encryption to data at rest and data in transit.
- Use email security appliances to scan and remove malicious email attachments or links.
- Monitor key internal security tools and identify anomalous behavior. Flag any known indicators of compromise or threat actor behaviors for immediate response.
- Organizations can implement mitigations of varying complexity and restrictiveness to reduce the risk posed by threat actors who use Tor (The Onion Router) to carry out malicious activities. See the CISA-FBI Joint Cybersecurity Advisory on Defending Against Malicious Cyber Activity Originating from Tor for mitigation options and additional information.
- Prevent exploitation of known software vulnerabilities by routinely applying software patches and upgrades. Foreign cyber threat actors continue to exploit publicly known—and often dated—software vulnerabilities against broad target sets, including public and private sector organizations. If these vulnerabilities are left unpatched, exploitation often requires few resources and provides threat actors with easy access to victim networks. Review CISA and FBI's Top 10 Routinely Exploited Vulnerabilities and other CISA alerts that identify vulnerabilities exploited by foreign attackers.
- Implement an antivirus program and a formalized patch management process.
- Block certain websites and email attachments commonly associated with malware (e.g., .scr, .pif, .cpl, .dll, .exe).
- Block email attachments that cannot be scanned by antivirus software (e.g., .zip files).
- Implement Group Policy Object and firewall rules.
- Implement filters at the email gateway and block suspicious IP addresses at the firewall.
- Routinely audit domain and local accounts as well as their permission levels to look for situations that could allow an adversary to gain wide access by obtaining credentials of a privileged account.
- Follow best practices for design and administration of the network to limit privileged account use across administrative tiers.
- Implement a Domain-Based Message Authentication, Reporting & Conformance (DMARC) validation system.
- Disable or block unnecessary remote services.
- Limit access to remote services through centrally managed concentrators.
- Deny direct remote access to internal systems or resources by using network proxies, gateways, and firewalls.
- Limit unnecessary lateral communications.
- Disable file and printer sharing services. If these services are required, use strong passwords or Active Directory authentication.
- Ensure applications do not store sensitive data or credentials insecurely.
- Enable a firewall on agency workstations, configured to deny unsolicited connection requests.
- Disable unnecessary services on agency workstations and servers.
- Scan for and remove suspicious email attachments; ensure any scanned attachment is its "true file type" (i.e., the extension matches the file header).

- Monitor users' web browsing habits; restrict access to suspicious or risky sites. Contact law enforcement or CISA immediately regarding any unauthorized network access identified.
- Visit the MITRE ATT&CK techniques and tactics pages linked in the ATT&CK Profile section above for additional mitigation and detection strategies for this malicious activity targeting think tanks.

CONTACT INFORMATION

Recipients of this report are encouraged to contribute any additional information that they may have related to this threat. To report suspicious or criminal activity related to information found in this Joint Cybersecurity Advisory, contact your local FBI field office at www.fbi.gov/contact-us/field, 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.

REFERENCES

- CISA Alert: Microsoft Office 365 Security Recommendations
- CISA Alert: Technical Approaches to Uncovering and Remediating Malicious Activity
- CISA Webpage: Telework Guidance
- CISA Webpage: VPN-Related Guidance
- FBI Private Industry Notification: PIN 20200409-001

DISCLAIMER

This document is marked TLP:WHITE. Disclosure is not limited. Sources may use TLP:WHITE when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release. Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction. For more information on the Traffic Light Protocol, see https://cisa.gov/tlp.