Chinese State-Sponsored Cyber Operations: Observed TTPs

us-cert.cisa.gov/ncas/alerts/aa21-200b

Summary

This advisory uses the MITRE Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK®) framework, Version 9, and MITRE D3FEND™ framework, version 0.9.2-BETA-3. See the ATT&CK for Enterprise for all referenced threat actor tactics and techniques and the D3FEND framework for referenced defensive tactics and techniques.

The National Security Agency, Cybersecurity and Infrastructure Security Agency (CISA), and Federal Bureau of Investigation (FBI) assess that People's Republic of China state-sponsored malicious cyber activity is a major threat to U.S. and Allied cyberspace assets. Chinese state-sponsored cyber actors aggressively target U.S. and allied political, economic, military, educational, and critical infrastructure (CI) personnel and organizations to steal sensitive data, critical and emerging key technologies, intellectual property, and personally identifiable information (PII). Some target sectors include managed service providers, semiconductor companies, the Defense Industrial Base (DIB), universities, and medical institutions. These cyber operations support China's long-term economic and military development objectives.

This Joint Cybersecurity Advisory (CSA) provides information on tactics, techniques, and procedures (TTPs) used by Chinese state-sponsored cyber actors. This advisory builds on previous NSA, CISA, and FBI reporting to inform federal, state, local, tribal, and territorial (SLTT) government, CI, DIB, and private industry organizations about notable trends and persistent TTPs through collaborative, proactive, and retrospective analysis.

To increase the defensive posture of their critical networks and reduce the risk of Chinese malicious cyber activity, NSA, CISA, and FBI urge government, CI, DIB, and private industry organizations to apply the recommendations listed in the Mitigations section of this advisory and in Appendix A: Chinese State-sponsored Cyber Actors' Observed Procedures. **Note:** NSA, CISA, and FBI encourage organization leaders to review CISA Joint Insights: Chinese Malicious Cyber Activity: Threat Overview for Leaders for information on this threat to their organization.

Click here for a PDF version of this report.

Technical Details

Trends in Chinese State-Sponsored Cyber Operations

NSA, CISA, and FBI have observed increasingly sophisticated Chinese state-sponsored cyber activity targeting U.S. political, economic, military, educational, and CI personnel and organizations. NSA, CISA, and FBI have identified the following trends in Chinese state-sponsored malicious cyber operations through proactive and retrospective analysis:

- **Acquisition of Infrastructure and Capabilities**. Chinese state-sponsored cyber actors remain agile and cognizant of the information security community's practices. These actors take effort to mask their activities by using a revolving series of virtual private servers (VPSs) and common open-source or commercial penetration tools.

- **Exploitation of Public Vulnerabilities.** Chinese state-sponsored cyber actors consistently scan target networks for critical and high vulnerabilities within days of the vulnerability's public disclosure. In many cases, these cyber actors seek to exploit vulnerabilities in major applications, such as Pulse Secure, Apache, F5 Big-IP, and Microsoft products. For information on Common Vulnerabilities and Exposures (CVE) known to be exploited by malicious Chinese state-sponsored cyber actors, see:
    - CISA-FBI Joint CSA AA20-133A: Top 10 Routinely Exploited Vulnerabilities,
    - CISA Activity Alert: AA20-275A: Potential for China Cyber Response to Heightened U.S.-China Tensions, and
    - NSA CSA U/OO/179811-20: Chinese State-Sponsored Actors Exploit Publicly Known Vulnerabilities.
- **Encrypted Multi-Hop Proxies.** Chinese state-sponsored cyber actors have been routinely observed using a VPS as an encrypted proxy. The cyber actors use the VPS as well as small office and home office (SOHO) devices as operational nodes to evade detection.

Observed Tactics and Techniques

Chinese state-sponsored cyber actors use a full array of tactics and techniques to exploit computer networks of interest worldwide and to acquire sensitive intellectual property, economic, political, and military information. Appendix B: MITRE ATT&CK Framework lists the tactics and techniques used by Chinese state-sponsored cyber actors. A downloadable JSON file is also available on the NSA Cybersecurity GitHub page.

Refer to Appendix A: Chinese State-Sponsored Cyber Actors' Observed Procedures for information on procedures affiliated with these tactics and techniques as well as applicable mitigations.

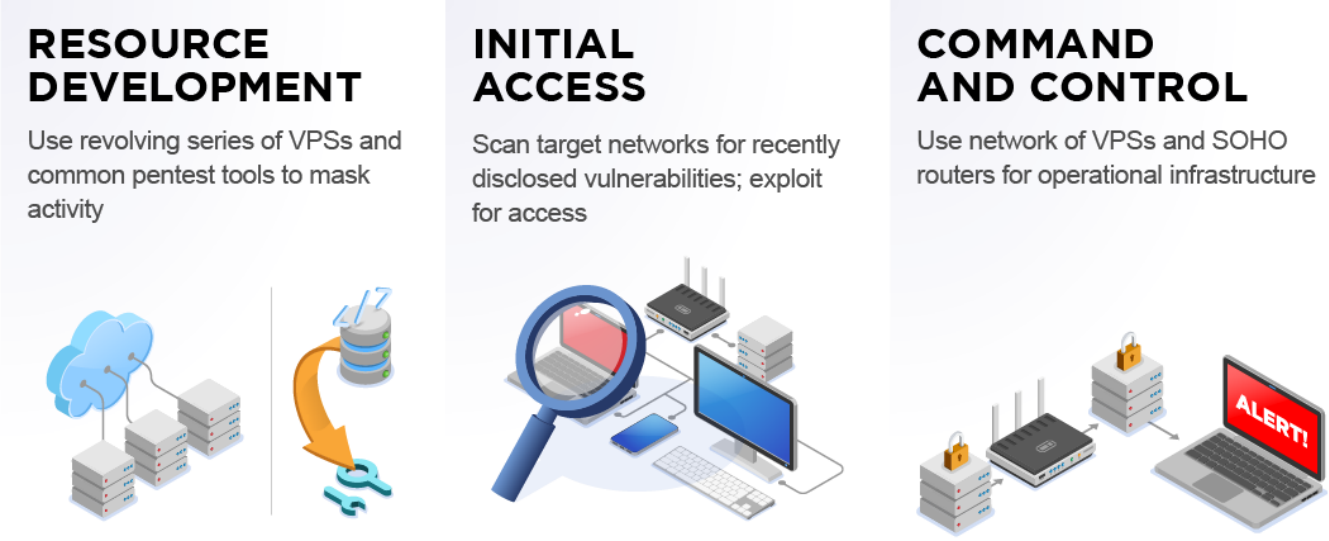

Figure 1: Example of tactics and techniques used in various cyber operations.

Mitigations

NSA, CISA, and FBI urge federal and SLTT government, CI, DIB, and private industry organizations to apply the following recommendations as well as the detection and mitigation recommendations in Appendix A, which are tailored to observed tactics and techniques:

- **Patch systems and equipment promptly and diligently.** Focus on patching critical and high vulnerabilities that allow for remote code execution or denial-of-service on externally facing equipment and CVEs known to be exploited by Chinese state-sponsored cyber actors. Consider implementing a patch management program that enables a timely and thorough patching cycle.
  Note: for more information on CVEs routinely exploited by Chinese state-sponsored cyber actors refer to the resources listed in the Trends in Chinese State-Sponsored Cyber Operations section.

- **Enhance monitoring of network traffic, email, and endpoint systems.** Review network signatures and indicators for focused activities, monitor for new phishing themes, and adjust email rules accordingly. Follow the best practices of restricting attachments via email and blocking URLs and domains based upon reputation. Ensure that log information is aggregated and correlated to enable maximum detection capabilities, with a focus on monitoring for account misuse. Monitor common ports and protocols for command and control (C2) activity. SSL/TLS inspection can be used to see the contents of encrypted sessions to look for network-based indicators of malware communication protocols. Implement and enhance network and endpoint event analysis and detection capabilities to identify initial infections, compromised credentials, and the manipulation of endpoint processes and files.
- **Use protection capabilities to stop malicious activity.** Implement anti-virus software and other endpoint protection capabilities to automatically detect and prevent malicious files from executing. Use a network intrusion detection and prevention system to identify and prevent commonly employed adversarial malware and limit nefarious data transfers. Use a domain reputation service to detect suspicious or malicious domains. Use strong credentials for service accounts and multi-factor authentication (MFA) for remote access to mitigate an adversary's ability to leverage stolen credentials, but be aware of MFA interception techniques for some MFA implementations.▪

Resources

Refer to us-cert.cisa.gov/china, https://www.ic3.gov/Home/IndustryAlerts, and https://www.nsa.gov/What-We-Do/Cybersecurity/Advisories-Technical-Guidance/ for previous reporting on Chinese state-sponsored malicious cyber activity.

Disclaimer of Endorsement

The information and opinions contained in this document are provided "as is" and without any warranties or guarantees. Reference herein to any specific commercial products, process, or service by trade name, trademark, manufacturer, or otherwise, does not constitute or imply its endorsement, recommendation, or favoring by the United States Government, and this guidance shall not be used for advertising or product endorsement purposes.

Purpose

This document was developed by NSA, CISA, and FBI in furtherance of their respective cybersecurity missions, including their responsibilities to develop and issue cybersecurity specifications and mitigations. This information may be shared broadly to reach all appropriate stakeholders.
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/.

Trademark Recognition

MITRE and ATT&CK are registered trademarks of The MITRE Corporation. • D3FEND is a trademark of The MITRE Corporation. • Microsoft, Microsoft Exchange, Office 365, Microsoft Office, OneDrive, Outlook, OWA, PowerShell, Windows Defender, and Windows are registered trademarks of Microsoft Corporation. • Pulse Secure is a registered trademark of Pulse Secure, LLC. • Apache is a registered trademark of Apache Software Foundation. • F5 and BIG-IP are registered trademarks of F5 Networks. • Cobalt Strike is a registered trademark of Strategic Cyber LLC. • GitHub is a registered trademark of GitHub, Inc. • JavaScript is a registered trademark of Oracle Corporation. • Python is a registered trademark of Python Software Foundation. • Unix is a registered trademark of The Open Group. • Linux is a registered trademark of Linus Torvalds. • Dropbox is a registered trademark of Dropbox, Inc.

APPENDIX A: Chinese State-Sponsored Cyber Actors' Observed Procedures

Note: D3FEND techniques are based on the Threat Actor Procedure(s) and may not match automated mappings to ATT&CK techniques and sub-techniques.

Tactics: *Reconnaissance* [TA0043]

Table 1: Chinese state-sponsored cyber actors' Reconnaissance TTPs with detection and mitigation recommendations

Threat Actor Technique / Sub-Techniques	Threat Actor Procedure(s)	Detection and Mitigation Recommendations	Defensive Tactics and Techniques

Threat Actor Technique / Sub-Techniques	Threat Actor Procedure(s)	Detection and Mitigation Recommendations	Defensive Tactics and Techniques
Active Scanning [T1595]	Chinese state-sponsored cyber actors have been assessed to perform reconnaissance on Microsoft® 365 (M365), formerly Office® 365, resources with the intent of further gaining information about the networks. These scans can be automated, through Python® scripts, to locate certain files, paths, or vulnerabilities. The cyber actors can gain valuable information on the victim network, such as the allocated resources, an organization's fully qualified domain name, IP address space, and open ports to target or exploit.	Minimize the amount and sensitivity of data available to external parties, for example: • Scrub user email addresses and contact lists from public websites, which can be used for social engineering, • Share only necessary data and information with third parties, and • Monitor and limit third-party access to the network. Active scanning from cyber actors may be identified by monitoring network traffic for sources associated with botnets, adversaries, and known bad IPs based on threat intelligence.	Detect: Network Traffic Analysis Connection Attempt Analysis [D3-CAA] Isolate: Network Isolation Inbound Traffic Filtering [D3-ITF]
Gather Victim Network Information [T1590]			

Tactics: *Resource Development* [TA0042]

Table II: Chinese state-sponsored cyber actors' Resource Development TTPs with detection and mitigation recommendations

Threat Actor Technique / Sub-Techniques	Threat Actor Procedure(s)	Detection and Mitigation Recommendations	Defensive Tactics and Techniques
Acquire Infrastructure [T1583]	Chinese state-sponsored cyber actors have been observed using VPSs from cloud service providers that are physically distributed around the world to host malware and function as C2 nodes.	Adversary activities occurring outside the organization's boundary of control and view makes mitigation difficult. Organizations can monitor for unexpected network traffic and data flows to and from VPSs and correlate other suspicious activity that may indicate an active threat.	N/A
Stage Capabilities [T1608]			
Obtain Capabilities [T1588]: Tools [T1588.002]	Chinese state-sponsored cyber actors have been observed using Cobalt Strike® and tools from GitHub® on victim networks.	Organizations may be able to identify malicious use of Cobalt Strike by: • Examining network traffic using Transport Layer Security (TLS) inspection to identify Cobalt Strike. Look for human generated vice machine-generated traffic, which will be more uniformly distributed. • Looking for the default Cobalt Strike TLS certificate. • Look at the user agent that generates the TLS traffic for discrepancies that may indicate faked and malicious traffic. • Review the traffic destination domain, which may be malicious and an indicator of compromise. • Look at the packet's HTTP host header. If it does not match with the destination domain, it may indicate a fake Cobalt Strike header and profile. • Check the Uniform Resource Identifier (URI) of the flow to see if it matches one associated with Cobalt Strike's malleable C2 language. If discovered, additional recovery and investigation will be required.	N/A

Tactics: *Initial Access* [TA0001]

Table III: Chinese state-sponsored cyber actors' Initial Access TTPs with detection and mitigation recommendations

Threat Actor Technique / Sub-Techniques	Threat Actor Procedure(s)	Detection and Mitigation Recommendations	Detection and Mitigation Recommendations

Drive By Compromise [T1189]	Chinese state-sponsored cyber actors have been observed gaining access to victim networks through watering hole campaigns of typo-squatted domains.	• Ensure all browsers and plugins are kept up to date.
		• Use modern browsers with security features turned on.
		• Restrict the use of unneeded websites, block unneeded downloads/attachments, block unneeded JavaScript®, restrict browser extensions, etc.
		• Use adblockers to help prevent malicious code served through advertisements from executing.
		• Use script blocking extensions to help prevent the execution of unneeded JavaScript, which may be used during exploitation processes.
		• Use browser sandboxes or remote virtual environments to mitigate browser exploitation.
		• Use security applications that look for behavior used during exploitation, such as Windows Defender® Exploit Guard (WDEG).
			Detect:
			• Identifier Analysis
			  ◦ Homoglyph Detection [D3-HD]
			  ◦ URL Analysis [D3-UA]
			• File Analysis
			  Dynamic Analysis [D3-DA]
			
			Isolate:
			• Execution Isolation
			  ◦ Hardware-based Process Isolation [D3-HBPI]
			  ◦ Executable Allowlisting [D3-EAL]
			• Network Isolation
			  ◦ DNS Denylisting [D3-DNSDL]
			  ◦ Outbound Traffic Filtering [D3-OTF]

Exploit Public-Facing Application [T1190]	Chinese state-sponsored cyber actors have exploited known vulnerabilities in Internet-facing systems.[1] For information on vulnerabilities known to be exploited by Chinese state-sponsored cyber actors, refer to the Trends in Chinese State-Sponsored Cyber Operations section for a list of resources.
	Chinese state-sponsored cyber actors have also been observed:
		Review previously published alerts and advisories from NSA, CISA, and FBI, and diligently patch vulnerable applications known to be exploited by cyber actors. Refer to the Trends in Chinese State-Sponsored Cyber Operations section for a non-inclusive list of resources.
		
		Additional mitigations include:
		• Consider implementing Web Application Firewalls (WAF), which can prevent exploit traffic from reaching an application.
			Harden:
			• Application Hardening [D3-AH]
			• Platform Hardening
			  Software Update [D3-SU]
			
			Detect:
			• File Analysis [D3-FA]
			• Network Traffic Analysis
			  Client-server Payload Profiling [D3-CSPP]

Threat Actor Technique / Sub-Techniques	Threat Actor Procedure(s)	Detection and Mitigation Recommendations	Detection and Mitigation Recommendations

	• Using short-term VPS devices to scan and exploit vulnerable Microsoft Exchange® Outlook Web Access (OWA®) and plant webshells.
	• Targeting on-premises Identity and Access Management (IdAM) and federation services in hybrid cloud environments to gain access to cloud resources.
	• Deploying a public proof of concept (POC) exploit targeting a public-facing appliance vulnerability.
		• Segment externally facing servers and services from the rest of the network with a demilitarized zone (DMZ).
		• Use multi-factor authentication (MFA) with strong factors and require regular re-authentication.
		• Disable protocols using weak authentication.
		• Limit access to and between cloud resources with the desired state being a Zero Trust model. For more information refer to NSA Cybersecurity Information Sheet: [Embracing a Zero Trust Security Model].
		• When possible, use cloud-based access controls on cloud resources (e.g., cloud service provider (CSP)-managed authentication between virtual machines).
		• Use automated tools to audit access logs for security concerns.
		• Where possible, enforce MFA for password resets.
		• Do not include Application Programing Interface (API) keys in software version control systems where they can be unintentionally leaked.
			• Process Analysis
			  ◦ Process Spawn Analysis
			  ◦ Process Lineage Analysis [D3-PLA]
			Isolate:
			Network Isolation
			Inbound Traffic Filtering [D3-ITF]

Phishing [T1566]:
• Spearphishing Attachment [T1566.001]
• Spearphishing Link [T1566.002]
	Chinese state-sponsored cyber actors have been observed conducting spearphishing campaigns. These email compromise attempts range from generic emails with mass targeted phishing attempts to specifically crafted emails in targeted social engineering lures.
	These compromise attempts use the cyber
		• Implement a user training program and simulated spearphishing emails to discourage users from visiting malicious websites or opening malicious attachments and re-enforce the appropriate user responses to spearphishing emails.
		Quarantine suspicious files with antivirus solutions.
			Harden:
			Message Hardening
			  ◦ Message Authentication [D3-MAN]
			  ◦ Transfer Agent Authentication [D3-TAAN]
			Detect:

Threat Actor Technique / Sub-Techniques	Threat Actor Procedure(s)	Detection and Mitigation Recommendations	Detection and Mitigation Recommendations
	actors' dynamic collection of VPSs, previously compromised accounts, or other infrastructure in order to encourage engagement from the target audience through domain typo-squatting and masquerading. These emails may contain a malicious link or files that will provide the cyber actor access to the victim's device after the user clicks on the malicious link or opens the attachment.	• Use a network intrusion prevention system (IPS) to scan and remove malicious email attachments. • Block uncommon file types in emails that are not needed by general users (`.exe` , `.jar` , `.vbs`) • Use anti-spoofing and email authentication mechanisms to filter messages based on validity checks of the sender domain (using Sender Policy Framework [SPF]) and integrity of messages (using Domain Keys Identified Mail [DKIM]). Enabling these mechanisms within an organization (through policies such as Domain-based Message Authentication, Reporting, and Conformance [DMARC]) may enable recipients (intra-org and cross domain) to perform similar message filtering and validation. • Determine if certain websites that can be used for spearphishing are necessary for business operations and consider blocking access if activity cannot be monitored well or if it poses a significant risk. • Prevent users from clicking on malicious links by stripping hyperlinks or implementing "URL defanging" at the Email Security Gateway or other email security tools. • Add external sender banners to emails to alert users that the email came from an external sender.	• File Analysis ◦ Dynamic Analysis [D3-DA] • Identifier Analysis ◦ Homoglyph Detection [D3-HD] ◦ URL Analysis [D3-UA] • Message Analysis ◦ Sender MTA Reputation Analysis [D3-SMRA] ◦ Sender Reputation Analysis [D3-SRA]
External Remote Services [T1133]	Chinese state-sponsored cyber actors have been	• Many exploits can be mitigated by applying available patches for	Harden:

Threat Actor Technique / Sub-Techniques	Threat Actor Procedure(s)	Detection and Mitigation Recommendations	Detection and Mitigation Recommendations
	observed: • Exploiting vulnerable devices immediately after conducting scans for critical zero-day or publicly disclosed vulnerabilities. The cyber actors used or modified public proof of concept code in order to exploit vulnerable systems. • Targeting Microsoft Exchange offline address book (OAB) virtual directories (VDs). • Exploiting Internet accessible webservers using webshell small code injections against multiple code languages, including `net`, `asp`, `apsx`, `php`, `japx`, and `cfm`. **Note:** refer to the references listed above in Exploit Public-Facing Application [T1190] for information on CVEs known to be exploited by malicious Chinese cyber actors. **Note:** this technique also applies to Persistence [TA0003].	vulnerabilities (such as CVE-2019-11510, CVE-2019-19781, and CVE-2020-5902) affecting external remote services. • Reset credentials after virtual private network (VPN) devices are upgraded and reconnected to the external network. • Revoke and generate new VPN server keys and certificates (this may require redistributing VPN connection information to users). • Disable Remote Desktop Protocol (RDP) if not required for legitimate business functions. • Restrict VPN traffic to and from managed service providers (MSPs) using a dedicated VPN connection. • Review and verify all connections between customer systems, service provider systems, and other client enclaves.	Software Update [D3-SU] Detect: • Network Traffic Analysis Connection Attempt Analysis [D3-CAA] • Platform Monitoring [D3-PM] • Process Analysis Process Spawn Analysis [D3-SPA] Process Lineage Analysis [D3-PLA]

Threat Actor Technique / Sub-Techniques	Threat Actor Procedure(s)	Detection and Mitigation Recommendations	Detection and Mitigation Recommendations
Valid Accounts [T1078]: • Default Accounts [T1078.001] • Domain Accounts [T1078.002]	Chinese state-sponsored cyber actors have been observed: gaining credential access into victim networks by using legitimate, but compromised credentials to access OWA servers, corporate login portals, and victim networks. **Note:** this technique also applies to Persistence [TA0003], Privilege Escalation [TA0004], and Defense Evasion [TA0005].	• Adhere to best practices for password and permission management. • Ensure that MSP accounts are not assigned to administrator groups and restrict those accounts to only systems they manage • Do not store credentials or sensitive data in plaintext. • Change all default usernames and passwords. • Routinely update and secure applications using Secure Shell (SSH). • Update SSH keys regularly and keep private keys secure. • Routinely audit privileged accounts to identify malicious use.	Harden: Credential Hardening Multi-factor Authentication [D3-MFA] Detect: User Behavior Analysis [D3-UBA] ◦ Authentication Event Thresholding [D3-ANET] ◦ Job Function Access Pattern Analysis [D3-JFAPA]

Tactics: *Execution* [TA0002]

Table IV: Chinese state-sponsored cyber actors' Execution TTPs with detection and mitigation recommendations

Threat Actor Technique / Sub-Techniques	Threat Actor Procedure(s)	Detection and Mitigation Recommendations	Defensive Tactics and Techniques
Command and Scripting Interpreter [T1059]: • PowerShell® [T1059.001] • Windows® Command Shell [T1059.003] • Unix® Shell [T1059.004] • Python [T1059.006]	Chinese state-sponsored cyber actors have been observed: • Using cmd.exe, JavaScript/Jscript Interpreter, and network device command line interpreters (CLI). • Using PowerShell to conduct reconnaissance, enumeration, and discovery of the victim network.	PowerShell • Turn on PowerShell logging. (**Note:** this works better in newer versions of PowerShell. NSA, CISA, and FBI recommend using version 5 or higher.) • Push Powershell logs into a security information and event management (SIEM) tool. • Monitor for suspicious behavior and commands. Regularly evaluate and update blocklists and allowlists.	Harden: Platform Hardening [D3-PH] Detect: Process Analysis Script Execution Analysis [D3-SEA] Isolate:

Threat Actor Technique / Sub-Techniques	Threat Actor Procedure(s)	Detection and Mitigation Recommendations	Defensive Tactics and Techniques
• JavaScript [T1059.007] • Network Device CLI [T1059.008]	• Employing Python scripts to exploit vulnerable servers. • Using a UNIX shell in order to conduct discovery, enumeration, and lateral movement on Linux® servers in the victim network.	• Use an antivirus program, which may stop malicious code execution that cyber actors attempt to execute via PowerShell. • Remove PowerShell if it is not necessary for operations. • Restrict which commands can be used. Windows Command Shell • Restrict use to administrator, developer, or power user systems. Consider its use suspicious and investigate, especially if average users run scripts. • Investigate scripts running out of cycle from patching or other administrator functions if scripts are not commonly used on a system, but enabled. • Monitor for and investigate other unusual or suspicious scripting behavior. Unix • Use application controls to prevent execution. • Monitor for and investigate unusual scripting behavior. Use of the Unix shell may be common on administrator, developer, or power user systems. In this scenario, normal users running scripts should be considered suspicious. • If scripts are not commonly used on a system, but enabled, scripts running out of cycle from patching or other administrator functions should be considered suspicious. Python • Audit inventory systems for unauthorized Python installations.	Execution Isolation Executable Allowlisting [D3-EAL]

Threat Actor Technique / Sub-Techniques	Threat Actor Procedure(s)	Detection and Mitigation Recommendations	Defensive Tactics and Techniques
		• Blocklist Python where not required. • Prevent users from installing Python where not required. JavaScript • Turn off or restrict access to unneeded scripting components. • Blocklist scripting where appropriate. • For malicious code served up through ads, adblockers can help prevent that code from executing. Network Device Command Line Interface (CLI) • Use TACACS+ to keep control over which commands administrators are permitted to use through the configuration of authentication and command authorization. • Use an authentication, authorization, and accounting (AAA) systems to limit actions administrators can perform and provide a history of user actions to detect unauthorized use and abuse. • Ensure least privilege principles are applied to user accounts and groups.	

Threat Actor Technique / Sub-Techniques	Threat Actor Procedure(s)	Detection and Mitigation Recommendations	Defensive Tactics and Techniques
Scheduled Task/Job [T1053] • Cron [T1053.003] • Scheduled Task [T1053.005]	Chinese state-sponsored cyber actors have been observed using Cobalt Strike, webshells, or command line interface tools, such as `schtask` or `crontab` to create and schedule tasks that enumerate victim devices and networks. **Note:** this technique also applies to Persistence [TA0003] and Privilege Escalation [TA0004].	• Monitor scheduled task creation from common utilities using command-line invocation and compare for any changes that do not correlate with known software, patch cycles, or other administrative activity. • Configure event logging for scheduled task creation and monitor process execution from `svchost.exe` (Windows 10) and Windows Task Scheduler (Older version of Windows) to look for changes in `%systemroot%\System32\Tasks` that do not correlate with known software, patch cycles, or other administrative activity. Additionally monitor for any scheduled tasks created via command line utilities —such as PowerShell or Windows Management Instrumentation (WMI)—that do not conform to typical administrator or user actions.	Detect: Platform Monitoring Operating System Monitoring [D3-OSM] ▪ Scheduled Job Analysis [D3-SJA] ▪ System Daemon Monitoring [D3-SDM] ▪ System File Analysis [D3-SFA] Isolate: Execution Isolation Executable Allowlisting [D3-EAL]

Threat Actor Technique / Sub-Techniques	Threat Actor Procedure(s)	Detection and Mitigation Recommendations	Defensive Tactics and Techniques
User Execution [T1204] • Malicious Link [T1204.001] • Malicious File [T1204.002]	Chinese state-sponsored cyber actors have been observed conducting spearphishing campaigns that encourage engagement from the target audience. These emails may contain a malicious link or file that provide the cyber actor access to the victim's device after the user clicks on the malicious link or opens the attachment.	• Use an antivirus program, which may stop malicious code execution that cyber actors convince users to attempt to execute. • Prevent unauthorized execution by disabling macro scripts from Microsoft Office files transmitted via email. Consider using Office Viewer software to open Microsoft Office files transmitted via email instead of full Microsoft Office suite applications. • Use a domain reputation service to detect and block suspicious or malicious domains. • Determine if certain categories of websites are necessary for business operations and consider blocking access if activity cannot be monitored well or if it poses a significant risk. • Ensure all browsers and plugins are kept up to date. • Use modern browsers with security features turned on. • Use browser and application sandboxes or remote virtual environments to mitigate browser or other application exploitation.	Detect: • File Analysis ◦ Dynamic Analysis [D3-DA] ◦ File Content Rules [D3-FCR] • Identifier Analysis ◦ Homoglyph Detection [D3-HD] ◦ URL Analysis [D3-UA] • Network Traffic Analysis DNS Traffic Analysis [D3-DNSTA] Isolate: • Execution Isolation ◦ Hardware-based Process Isolation [D3-HBPI] ◦ Executable Allowlisting [D3-EAL] • Network Isolation ◦ DNS Denylisting [D3-DNSDL] ◦ Outbound Traffic Filtering [D3-OTF]

Tactics: *Persistence* [TA0003]

Table V: Chinese state-sponsored cyber actors' Persistence TTPs with detection and mitigation recommendations

Threat Actor Technique / Sub-Techniques	Threat Actor Procedure(s)	Detection and Mitigation Recommendations	Defensive Tactics and Techniques

Threat Actor Technique / Sub-Techniques	Threat Actor Procedure(s)	Detection and Mitigation Recommendations	Defensive Tactics and Techniques
Hijack Execution Flow [T1574]: DLL Search Order Hijacking [T1574.001]	Chinese state-sponsored cyber actors have been observed using benign executables which used Dynamic Link Library (DLL) load-order hijacking to activate the malware installation process. **Note:** this technique also applies to Privilege Escalation [TA0004] and Defense Evasion [TA0005].	• Disallow loading of remote DLLs. • Enable safe DLL search mode. • Implement tools for detecting search order hijacking opportunities. • Use application allowlisting to block unknown DLLs. • Monitor the file system for created, moved, and renamed DLLs. • Monitor for changes in system DLLs not associated with updates or patches. • Monitor DLLs loaded by processes (e.g., legitimate name, but abnormal path).	Detect: • Platform Monitoring Operating System Monitoring Service Binary Verification [D3-SBV] • Process Analysis File Access Pattern Analysis [D3-FAPA] Isolate: Execution Isolation Executable Allowlisting [D3-EAL]

Threat Actor Technique / Sub-Techniques	Threat Actor Procedure(s)	Detection and Mitigation Recommendations	Defensive Tactics and Techniques
Modify Authentication Process [T1556] Domain Controller Authentication [T1556.001]	Chinese state-sponsored cyber actors were observed creating a new sign-in policy to bypass MFA requirements to maintain access to the victim network. Note: this technique also applies to Defense Evasion [TA0005] and Credential Access [TA0006].	• Monitor for policy changes to authentication mechanisms used by the domain controller. • Monitor for modifications to functions exported from authentication DLLs (such as `cryptdll.dll` and `samsrv.dll`). • Configure robust, consistent account activity audit policies across the enterprise and with externally accessible services. • Look for suspicious account behavior across systems that share accounts, either user, admin, or service accounts (for example, one account logged into multiple systems simultaneously, multiple accounts logged into the same machine simultaneously, accounts logged in at odd times or outside of business hours). • Correlate other security systems with login information (e.g., a user has an active login session but has not entered the building or does not have VPN access). • Monitor for new, unfamiliar DLL files written to a domain controller and/or local computer. Monitor for and correlate changes to Registry entries.	Detect: • Process Analysis [D3-PA] • User Behavior Analysis ◦ Authentication Event Thresholding [D3-ANET] ◦ User Geolocation Logon Pattern Analysis [D3-UGLPA]
Server Software Component [T1505]: Web Shell [T1505.003]	Chinese state-sponsored cyber actors have been observed planting web shells on exploited servers and using them to provide the cyber actors with access to the victim networks.	• Use Intrusion Detection Systems (IDS) to monitor for and identify China Chopper traffic using IDS signatures. • Monitor and search for predictable China Chopper shell syntax to identify infected files on hosts. • Perform integrity checks on critical servers to identify and investigate unexpected changes.	Detect: • Network Traffic Analysis ◦ Client-server Payload Profiling [D3-CSPP] ◦ Per Host Download-Upload Ratio Analysis [D3-PHDURA]

Threat Actor Technique / Sub-Techniques	Threat Actor Procedure(s)	Detection and Mitigation Recommendations	Defensive Tactics and Techniques
		• Have application developers sign their code using digital signatures to verify their identity. • Identify and remediate web application vulnerabilities or configuration weaknesses. Employ regular updates to applications and host operating systems. • Implement a least-privilege policy on web servers to reduce adversaries' ability to escalate privileges or pivot laterally to other hosts and control creation and execution of files in particular directories. • If not already present, consider deploying a DMZ between web-facing systems and the corporate network. Limiting the interaction and logging traffic between the two provides a method to identify possible malicious activity. • Ensure secure configuration of web servers. All unnecessary services and ports should be disabled or blocked. Access to necessary services and ports should be restricted, where feasible. This can include allowlisting or blocking external access to administration panels and not using default login credentials. • Use a reverse proxy or alternative service, such as mod_security, to restrict accessible URL paths to known legitimate ones. • Establish, and backup offline, a "known good" version of the relevant server and a regular change management policy to enable monitoring for changes to servable content with a file integrity system.	• Process Analysis Process Spawn Analysis Process Lineage Analysis [D3-PLA] Isolate: Network Isolation Inbound Traffic Filtering [D3-ITF]

Threat Actor Technique / Sub-Techniques	Threat Actor Procedure(s)	Detection and Mitigation Recommendations	Defensive Tactics and Techniques
		• Employ user input validation to restrict exploitation of vulnerabilities. • Conduct regular system and application vulnerability scans to establish areas of risk. While this method does not protect against zero-day exploits, it will highlight possible areas of concern. • Deploy a web application firewall and conduct regular virus signature checks, application fuzzing, code reviews, and server network analysis.	
Create or Modify System Process [T1543]: Windows Service [T1543.003]	Chinese state-sponsored cyber actors have been observed executing malware shellcode and batch files to establish new services to enable persistence. **Note:** this technique also applies to Privilege Escalation [TA0004].	• Only allow authorized administrators to make service changes and modify service configurations. • Monitor processes and command-line arguments for actions that could create or modify services, especially if such modifications are unusual in your environment. • Monitor WMI and PowerShell for service modifications.	Detect: Process Analysis Process Spawn Analysis [D3-PSA]

Tactics: *Privilege Escalation* [TA0004]

Table VI: Chinese state-sponsored cyber actors' Privilege Escalation TTPs with detection and mitigation recommendations

Threat Actor Technique / Sub-Techniques	Threat Actor Procedure(s)	Detection and Mitigation Recommendations	Defensive Tactics and Techniques

Threat Actor Technique / Sub-Techniques	Threat Actor Procedure(s)	Detection and Mitigation Recommendations	Defensive Tactics and Techniques
Domain Policy Modification [T1484] Group Policy Modification [T1484.001]	Chinese state-sponsored cyber actors have also been observed modifying group policies for password exploitation. **Note:** this technique also applies to Defense Evasion [TA0005].	• Identify and correct Group Policy Object (GPO) permissions abuse opportunities (e.g., GPO modification privileges) using auditing tools. • Monitor directory service changes using Windows event logs to detect GPO modifications. Several events may be logged for such GPO modifications. • Consider implementing WMI and security filtering to further tailor which users and computers a GPO will apply to.	Detect: • Network Traffic Analysis Administrative Network Activity Analysis [D3-ANAA] • Platform Monitoring Operating System Monitoring System File Analysis [D3-SFA]

Threat Actor Technique / Sub-Techniques	Threat Actor Procedure(s)	Detection and Mitigation Recommendations	Defensive Tactics and Techniques
Process Injection [T1055]: • Dynamic Link Library Injection [T1055.001] • Portable Executable Injection [T1055.002]	Chinese state-sponsored cyber actors have been observed: • Injecting into the `rundll32.exe` process to hide usage of Mimikatz, as well as injecting into a running legitimate `explorer.exe` process for lateral movement. • Using shellcode that injects implants into newly created instances of the Service Host process (`svchost`) **Note:** this technique also applies to Defense Evasion [TA0005].	• Use endpoint protection software to block process injection based on behavior of the injection process. • Monitor DLL/Portable Executable (PE) file events, specifically creation of these binary files as well as the loading of DLLs into processes. Look for DLLs that are not recognized or not normally loaded into a process. • Monitor for suspicious sequences of Windows API calls such as `CreateRemoteThread` , `VirtualAllocEx` , or `WriteProcessMemory` and analyze processes for unexpected or atypical behavior such as opening network connections or reading files. • To minimize the probable impact of a threat actor using Mimikatz, always limit administrative privileges to only users who actually need it; upgrade Windows to at least version 8.1 or 10; run Local Security Authority Subsystem Service (LSASS) in protected mode on Windows 8.1 and higher; harden the local security authority (LSA) to prevent code injection.	Execution Isolation ◦ Hardware-based Process Isolation [D3-HBPI] ◦ Mandatory Access Control [D3-MAC]

Tactics: *Defense Evasion* [TA0005]

Table VII: Chinese state-sponsored cyber actors' Defensive Evasion TTPs with detection and mitigation recommendations

Threat Actor Technique / Sub-Techniques	Threat Actor Procedure(s)	Detection and Mitigation Recommendations	Defensive Tactics and Techniques

Threat Actor Technique / Sub-Techniques	Threat Actor Procedure(s)	Detection and Mitigation Recommendations	Defensive Tactics and Techniques
Deobfuscate/Decode Files or Information [T1140]	Chinese state-sponsored cyber actors were observed using the 7-Zip utility to unzip imported tools and malware files onto the victim device.	• Monitor the execution file paths and command-line arguments for common archive file applications and extensions, such as those for Zip and RAR archive tools, and correlate with other suspicious behavior to reduce false positives from normal user and administrator behavior. • Consider blocking, disabling, or monitoring use of 7-Zip.	Detect: Process Analysis Process Spawn Analysis [D3-PSA] Isolate: Execution Isolation Executable Denylisting [D3-EDL]
Hide Artifacts [T1564]	Chinese state-sponsored cyber actors were observed using benign executables which used DLL load-order hijacking to activate the malware installation process.	• Monitor files, processes, and command-line arguments for actions indicative of hidden artifacts, such as executables using DLL load-order hijacking that can activate malware. • Monitor event and authentication logs for records of hidden artifacts being used. • Monitor the file system and shell commands for hidden attribute usage.	Detect: Process Analysis File Access Pattern Analysis [D3-FAPA] Isolate: Execution Isolation Executable Allowlisting [D3-EAL]

Threat Actor Technique / Sub-Techniques	Threat Actor Procedure(s)	Detection and Mitigation Recommendations	Defensive Tactics and Techniques
Indicator Removal from Host [T1070]	Chinese state-sponsored cyber actors have been observed deleting files using `rm` or `del` commands. Several files that the cyber actors target would be timestomped, in order to show different times compared to when those files were created/used.	• Make the environment variables associated with command history read only to ensure that the history is preserved. • Recognize timestomping by monitoring the contents of important directories and the attributes of the files. • Prevent users from deleting or writing to certain files to stop adversaries from maliciously altering their `~/.bash_history` or `ConsoleHost_history.txt` files. • Monitor for command-line deletion functions to correlate with binaries or other files that an adversary may create and later remove. Monitor for known deletion and secure deletion tools that are not already on systems within an enterprise network that an adversary could introduce. • Monitor and record file access requests and file handles. An original file handle can be correlated to a compromise and inconsistencies between file timestamps and previous handles opened to them can be a detection rule.	Detect: • Platform Monitoring Operating System Monitoring System File Analysis [D3-SFA] • Process Analysis File Access Pattern Analysis [D3-FAPA] Isolate: Execution Isolation Executable Allowlisting [D3-EAL]
Obfuscated Files or Information [T1027]	Chinese state-sponsored cyber actors were observed Base64 encoding files and command strings to evade security measures.	Consider utilizing the Antimalware Scan Interface (AMSI) on Windows 10 to analyze commands after being processed/interpreted.	Detect: Process Analysis File Access Pattern Analysis [D3-FAPA]

Threat Actor Technique / Sub-Techniques	Threat Actor Procedure(s)	Detection and Mitigation Recommendations	Defensive Tactics and Techniques
Signed Binary Proxy Execution [T1218] • `Mshta` [T1218.005] • `Rundll32` [T1218.011]	Chinese state-sponsored cyber actors were observed using Microsoft signed binaries, such as `Rundll32`, as a proxy to execute malicious payloads.	Monitor processes for the execution of known proxy binaries (e.g., r `undll32.exe`) and look for anomalous activity that does not follow historically good arguments and loaded DLLs associated with the invocation of the binary.	Detect: Process Analysis ◦ File Access Pattern Analysis [D3-FAPA] ◦ Process Spawn Analysis [D3-PSA]

Tactics: *Credential Access* [TA0006]

Table VIII: Chinese state-sponsored cyber actors' Credential Access TTPs with detection and mitigation recommendations

Threat Actor Technique / Sub-Techniques	Threat Actor Procedure(s)	Detection and Mitigation Recommendations	Defensive Tactics and Techniques
Exploitation for Credential Access [T1212]	Chinese state-sponsored cyber actors have been observed exploiting Pulse Secure VPN appliances to view and extract valid user credentials and network information from the servers.	• Update and patch software regularly. • Use cyber threat intelligence and open-source reporting to determine vulnerabilities that threat actors may be actively targeting and exploiting; patch those vulnerabilities immediately.	Harden: • Platform Hardening Software Update [D3-SU] • Credential Hardening Multi-factor Authentication [D3-MFA]

Threat Actor Technique / Sub-Techniques	Threat Actor Procedure(s)	Detection and Mitigation Recommendations	Defensive Tactics and Techniques
OS Credential Dumping [T1003] • LSASS Memory [T1003.001] • NTDS [T1003.003]	Chinese state-sponsored cyber actors were observed targeting the LSASS process or Active directory (`NDST.DIT)` for credential dumping.	• Monitor process and command-line arguments for program execution that may be indicative of credential dumping, especially attempts to access or copy the `NDST.DIT` . • Ensure that local administrator accounts have complex, unique passwords across all systems on the network. • Limit credential overlap across accounts and systems by training users and administrators not to use the same passwords for multiple accounts. • Consider disabling or restricting NTLM. • Consider disabling `WDigest` authentication. • Ensure that domain controllers are backed up and properly secured (e.g., encrypt backups). • Implement Credential Guard to protect the LSA secrets from credential dumping on Windows 10. This is not configured by default and requires hardware and firmware system requirements. • Enable Protected Process Light for LSA on Windows 8.1 and Windows Server 2012 R2.	Harden: Credential Hardening [D3-CH] Detect: Process Analysis ◦ File Access Pattern Analysis [D3-FAPA] ◦ System Call Analysis [D3-SCA] Isolate: Execution Isolation ◦ Hardware-based Process Isolation [D3-HBPI] ◦ Mandatory Access Control [D3-MAC]

Tactics: *Discovery* [TA0007]

Table IX: Chinese state-sponsored cyber actors' Discovery TTPs with detection and mitigation recommendations

Threat Actor Technique / Sub-Techniques	Threat Actor Procedure(s)	Detection and Mitigation Recommendations	Defensive Tactics and Techniques

File and Directory Discovery [T1083]	Chinese state-sponsored cyber actors have been observed using multiple implants with file system enumeration and traversal capabilities.	Monitor processes and command-line arguments for actions that could be taken to gather system and network information. WMI and PowerShell should also be monitored.	Detect:
			• User Behavior Analysis
			  ◦ Job Function Access Pattern Analysis [D3-JFAPA]
			• Process Analysis
			  ◦ Database Query String Analysis [D3-DQSA]
			  ◦ File Access Pattern Analysis [D3-FAPA]
			  ◦ Process Spawn Analysis [D3-PSA]

Permission Group Discovery [T1069]	Chinese state-sponsored cyber actors have been observed using commands, including `net group` and `net localgroup`, to enumerate the different user groups on the target network.	Monitor processes and command-line arguments for actions that could be taken to gather system and network information. Remote access tools with built-in features may interact directly with the Windows API to gather information. Information may also be acquired through Windows system management tools such as Windows Management Instrumentation and PowerShell.	Detect: • Process Analysis • Process Spawn Analysis [D3-PSA] ◦ System Call Analysis [D3-SCA] • User Behavior Analysis [D3-UBA]

Threat Actor Technique / Sub-Techniques	Threat Actor Procedure(s)	Detection and Mitigation Recommendations	Defensive Tactics and Techniques
Process Discovery [T1057]	Chinese state-sponsored cyber actors have been observed using commands, including `tasklist`, `jobs`, `ps`, or `taskmgr`, to reveal the running processes on victim devices.	Normal, benign system and network events that look like process discovery may be uncommon, depending on the environment and how they are used. Monitor processes and command-line arguments for actions that could be taken to gather system and network information. Remote access tools with built-in features may interact directly with the Windows API to gather information. Information may also be acquired through Windows system management tools such as Windows Management Instrumentation and PowerShell.	Detect: • Process Analysis ◦ Process Spawn Analysis [D3-PSA] ◦ System Call Analysis [D3-SCA] • User Behavior Analysis [D3-UBA]
Network Service Scanning [T1046]	Chinese state-sponsored cyber actors have been observed using `Nbtscan` and `nmap` to scan and enumerate target network information.	• Ensure that unnecessary ports and services are closed to prevent discovery and potential exploitation. • Use network intrusion detection and prevention systems to detect and prevent remote service scans such as `Nbtscan` or `nmap`. • Ensure proper network segmentation is followed to protect critical servers and devices to help mitigate potential exploitation.	Detect: Network Traffic Analysis Connection Attempt Analysis [D3-CAA] Isolate: Network Isolation Inbound Traffic Filtering [D3-ITF]

Threat Actor Technique / Sub-Techniques	Threat Actor Procedure(s)	Detection and Mitigation Recommendations	Defensive Tactics and Techniques

Remote System Discovery [T1018]	Chinese state-sponsored cyber actors have been observed using Base-64 encoded commands, including `ping`, `net group`, and `net user` to enumerate target network information.	Monitor for processes that can be used to discover remote systems, such as `ping.exe` and `tracert.exe`, especially when executed in quick succession.	Detect:
			• Process Analysis
			  Process Spawn Analysis [D3-PSA]
			• User Behavior Analysis
			  Job Function Access Pattern Analysis [D3-JFAPA]

Tactics: *Lateral Movement* [TA0008]

Table X: Chinese state-sponsored cyber actors' Lateral Movement TTPs with detection and mitigation recommendations

Threat Actor Technique / Sub-Techniques	Threat Actor Procedure(s)	Detection and Mitigation Recommendations	Defensive Tactics and Techniques

Threat Actor Technique / Sub-Techniques	Threat Actor Procedure(s)	Detection and Mitigation Recommendations	Defensive Tactics and Techniques
Exploitation of Remote Services [T1210]	Chinese state-sponsored cyber actors used valid accounts to log into a service specifically designed to accept remote connections, such as telnet, SSH, RDP, and Virtual Network Computing (VNC). The actor may then perform actions as the logged-on user. Chinese state-sponsored cyber actors also used on-premises Identity and Access Management (IdAM) and federation services in hybrid cloud environments in order to pivot to cloud resources.	Chinese state-sponsored cyber actors used valid accounts to log into a service specifically designed to accept remote connections, such as telnet, SSH, RDP, and Virtual Network Computing (VNC). The actor may then perform actions as the logged-on user. Chinese state-sponsored cyber actors also used on-premises Identity and Access Management (IdAM) and federation services in hybrid cloud environments in order to pivot to cloud resources. • Disable or remove unnecessary services. • Minimize permissions and access for service accounts. • Perform vulnerability scanning and update software regularly. • Use threat intelligence and open-source exploitation databases to determine services that are targets for exploitation.	Detect: • Network Traffic Analysis Remote Terminal Session Detection [D3-RTSD] • User Behavior Analysis [D3-UBA] Isolate: Execution Isolation Mandatory Access Control [D3-MAC]

Tactics: *Collection* [TA0009]

Table XI: Chinese state-sponsored cyber actors' Collection TTPs with detection and mitigation recommendations

Threat Actor Technique / Sub-Techniques	Threat Actor Procedure(s)	Detection and Mitigation Recommendations	Defensive Tactics and Techniques

Threat Actor Technique / Sub-Techniques	Threat Actor Procedure(s)	Detection and Mitigation Recommendations	Defensive Tactics and Techniques
Archive Collected Data [T1560]	Chinese state-sponsored cyber actors used compression and encryption of exfiltration files into RAR archives, and subsequently utilizing cloud storage services for storage.	• Scan systems to identify unauthorized archival utilities or methods unusual for the environment. • Monitor command-line arguments for known archival utilities that are not common in the organization's environment.	Detect: Process Analysis ◦ File Access Pattern Analysis [D3-FAPA] ◦ Process Spawn Analysis [D3-PSA] Isolate: Execution Isolation Executable Denylisting [D3-EDL]
Clipboard Data [T1115]	Chinese state-sponsored cyber actors used RDP and execute `rdpclip.exe` to exfiltrate information from the clipboard.	• Access to the clipboard is a legitimate function of many applications on an operating system. If an organization chooses to monitor for this behavior, then the data will likely need to be correlated against other suspicious or non-user-driven activity (e.g. excessive use of `pbcopy/pbpaste` (Linux) or `clip.exe` (Windows) run by general users through command line). • If possible, disable use of RDP and other file sharing protocols to minimize a malicious actor's ability to exfiltrate data.	Detect: Network Traffic Analysis Remote Terminal Session Detection [D3-RTSD] Isolate: Network Isolation ◦ Inbound Traffic Filtering [D3-ITF] ◦ Outbound Traffic Filtering [D3-OTF]

Threat Actor Technique / Sub-Techniques	Threat Actor Procedure(s)	Detection and Mitigation Recommendations	Defensive Tactics and Techniques
Data Staged [T1074]	Chinese state-sponsored cyber actors have been observed using the `mv` command to export files into a location, like a compromised Microsoft Exchange, IIS, or emplaced webshell prior to compressing and exfiltrating the data from the target network.	Processes that appear to be reading files from disparate locations and writing them to the same directory or file may be an indication of data being staged, especially if they are suspected of performing encryption or compression on the files, such as using 7-Zip, RAR, ZIP, or zlib. Monitor publicly writeable directories, central locations, and commonly used staging directories (recycle bin, temp folders, etc.) to regularly check for compressed or encrypted data that may be indicative of staging.	Detect: Process Analysis File Access Pattern Analysis [D3-FAPA]
Email Collection [T1114]	Chinese state-sponsored cyber actors have been observed using the `New-MailboxExportReques t` PowerShell cmdlet to export target email boxes.	• Audit email auto-forwarding rules for suspicious or unrecognized rulesets. • Encrypt email using public key cryptography, where feasible. • Use MFA on public-facing mail servers.	Harden: • Credential Hardening Multi-factor Authentication [D3-MFA] • Message Hardening Message Encryption [D3-MENCR] Detect: Process Analysis [D3-PA]

Tactics: *Command and Control* [TA0011]

Table XII: Chinese state-sponsored cyber actors' Command and Control TTPs with detection and mitigation recommendations

Threat Actor Technique / Sub-Techniques	Threat Actor Procedure(s)	Detection and Mitigation Recommendations	Defensive Tactics and Techniques

Threat Actor Technique / Sub-Techniques	Threat Actor Procedure(s)	Detection and Mitigation Recommendations	Defensive Tactics and Techniques
Application Layer Protocol [T1071]	Chinese state-sponsored cyber actors have been observed: • Using commercial cloud storage services for command and control. • Using malware implants that use the Dropbox® API for C2 and a downloader that downloads and executes a payload using the Microsoft OneDrive® API.	Use network intrusion detection and prevention systems with network signatures to identify traffic for specific adversary malware.	Detect: Network Traffic Analysis ◦ Client-server Payload Profiling [D3-CSPP] ◦ File Carving [D3-FC] Isolate: Network Isolation DNS Denylisting [D3-DNSDL]
Ingress Tool Transfer [T1105]	Chinese state-sponsored cyber actors have been observed importing tools from GitHub or infected domains to victim networks. In some instances. Chinese state-sponsored cyber actors used the Server Message Block (SMB) protocol to import tools into victim networks.	• Perform ingress traffic analysis to identify transmissions that are outside of normal network behavior. • Do not expose services and protocols (such as File Transfer Protocol [FTP]) to the Internet without strong business justification. • Use signature-based network intrusion detection and prevention systems to identify adversary malware coming into the network.	Isolate: Network Isolation Inbound Traffic Filtering [D3-ITF]

Threat Actor Technique / Sub-Techniques	Threat Actor Procedure(s)	Detection and Mitigation Recommendations	Defensive Tactics and Techniques
Non-Standard Port [T1571]	Chinese state-sponsored cyber actors have been observed using a non-standard SSH port to establish covert communication channels with VPS infrastructure.	• Use signature-based network intrusion detection and prevention systems to identify adversary malware calling back to C2. • Configure firewalls to limit outgoing traffic to only required ports based on the functions of that network segment. • Analyze packet contents to detect communications that do not follow the expected protocol behavior for the port.	Detect: Network Traffic Analysis ◦ Client-server Payload Profiling [D3-CSPP] ◦ Protocol Metadata Anomaly Detection [D3-PMAD] Isolate: Network Isolation ◦ Inbound Traffic Filtering [D3-ITF] ◦ Outbound Traffic Filtering [D3-OTF]

Threat Actor Technique / Sub-Techniques	Threat Actor Procedure(s)	Detection and Mitigation Recommendations	Defensive Tactics and Techniques
Protocol Tunneling [T1572]	Chinese state-sponsored cyber actors have been observed using tools like dog-tunnel and `dns2tcp.exe` to conceal C2 traffic with existing network activity.	• Monitor systems for connections using ports/protocols commonly associated with tunneling, such as SSH (port 22). Also monitor for processes commonly associated with tunneling, such as Plink and the OpenSSH client. • Analyze packet contents to detect application layer protocols that do not follow the expected protocol standards. • Analyze network data for uncommon data flows (e.g., a client sending significantly more data than it receives from a server)	Detect: Network Traffic Analysis Protocol Metadata Anomaly Detection [D3-PMAD]
Proxy [T1090]: Multi-Hop Proxy [T1090.003]	Chinese state-sponsored cyber actors have been observed using a network of VPSs and small office and home office (SOHO) routers as part of their operational infrastructure to evade detection and host C2 activity. Some of these nodes operate as part of an encrypted proxy service to prevent attribution by concealing their country of origin and TTPs.	Monitor traffic for encrypted communications originating from potentially breached routers to other routers within the organization. Compare the source and destination with the configuration of the device to determine if these channels are authorized VPN connections or other encrypted modes of communication. • Alert on traffic to known anonymity networks (such as Tor) or known adversary infrastructure that uses this technique. • Use network allow and blocklists to block traffic to known anonymity networks and C2 infrastructure.	Detect: Network Traffic Analysis ◦ Protocol Metadata Anomaly Detection [D3-PMAD] ◦ Relay Pattern Analysis [D3-RPA] Isolate: Network Isolation Outbound Traffic Filtering [D3-OTF]

Appendix B: MITRE ATT&CK Framework

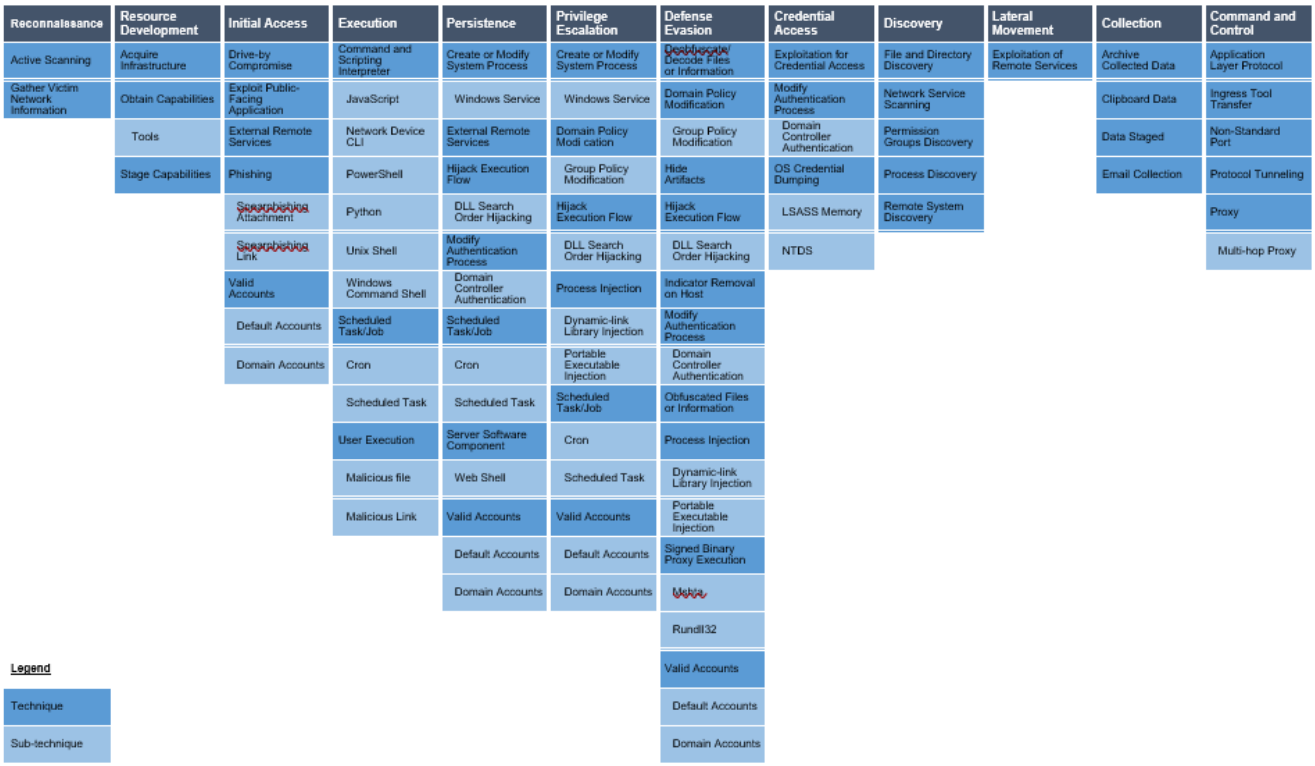

Figure 2: MITRE ATT&CK Enterprise tactics and techniques used by Chinese state-sponsored cyber actors (Click here for the downloadable JSON file.)

Contact Information

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 Central@cisa.dhs.gov.

For NSA client requirements or general cybersecurity inquiries, contact the NSA Cybersecurity Requirements Center at 410-854-4200 or Cybersecurity_Requests@nsa.gov.

Media Inquiries / Press Desk:

- NSA Media Relations, 443-634-0721, MediaRelations@nsa.gov
- CISA Media Relations, 703-235-2010, CISAMedia@cisa.dhs.gov
- FBI National Press Office, 202-324-3691, npo@fbi.gov

References

[1] FireEye: This is Not a Test: APT41 Initiates Global Intrusion Campaign Usin…

Revisions

July 19, 2021: Initial Version

Please share your thoughts.

We recently updated our anonymous product survey; we'd welcome your feedback.