Chinese Ministry of State Security-Affiliated Cyber Threat Actor Activity

SUMMARY

The Cybersecurity and Infrastructure Security Agency (CISA) has consistently observed Chinese Ministry of State Security (MSS)-affiliated cyber threat actors using publicly available information sources and common, well-known tactics, techniques, and procedures (TTPs) to target U.S. Government agencies. CISA has observed these—and other threat actors with varying degrees of skill—routinely using open-source information to plan and execute cyber operations. CISA leveraged the MITRE Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK®) and Pre-ATT&CK frameworks to characterize the TTPs used by Chinese MSS-affiliated actors. This product was written by CISA with contributions by the Federal Bureau of Investigation (FBI).

KEY TAKEAWAYS

- Chinese MSS-affiliated cyber threat actors use open-source information to plan and conduct cyber operations.
- Chinese MSS-affiliated cyber threat actors use readily available exploits and exploit toolkits to quickly engage target networks.
- Maintaining a rigorous patching cycle continues to be the best defense against the most frequently used attacks.
- If critical vulnerabilities remain unpatched, cyber threat actors can carry out attacks without the need to develop custom malware and exploits or use previously unknown vulnerabilities to target a network.
- This Advisory identifies some of the more common—yet most effective—TTPs employed by cyber threat actors, including Chinese MSS-affiliated cyber threat actors.

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.

TECHNICAL DETAILS

Through the operation of the National Cybersecurity Protection System (NCPS) and by fulfilling its mission as the national risk advisor, CISA has observed Chinese MSS-affiliated cyber threat actors operating from the People's Republic of China using commercially available information sources and open-source exploitation tools to target U.S. Government agency networks.

According to a recent U.S. Department of Justice indictment, MSS-affiliated actors have targeted various industries across the United States and other countries—including high-tech manufacturing; medical device, civil, and industrial engineering; business, educational, and gaming software; solar energy; pharmaceuticals; and defense—in a campaign that lasted over ten years.[1] These hackers acted for both their own personal gain and the benefit of the Chinese MSS.[2]

According to the indictment,

> *To conceal the theft of information from victim networks and otherwise evade detection, the defendants typically packaged victim data in encrypted Roshal Archive Compressed files (RAR files), changed RAR file and victim documents' names and extensions (e.g., from ".rar" to ".jpg") and system timestamps, and concealed programs and documents at innocuous-seeming locations on victim networks and in victim networks' "recycle bins." The defendants frequently returned to re-victimize companies, government entities, and organizations from which they had previously stolen data, in some cases years after the initial successful data theft. In several instances, however, the defendants were unsuccessful in this regard, due to the efforts of the FBI and network defenders.*

The continued use of open-source tools by Chinese MSS-affiliated cyber threat actors highlights that adversaries can use relatively low-complexity capabilities to identify and exploit target networks. In most cases, cyber operations are successful because misconfigurations and immature patch management programs allow actors to plan and execute attacks using existing vulnerabilities and known exploits. Widespread implementation of robust configuration and patch management programs would greatly increase network security. It would also reduce the speed and frequency of opportunistic attacks by forcing threat actors to dedicate time and funding to research unknown vulnerabilities and develop custom exploitation tools.

MITRE PRE-ATT&CK® Framework for Analysis

In the last 12 months, CISA analysts have routinely observed Chinese MSS-affiliated actors using the following PRE-ATT&CK® Framework TTPs.

[1] https://www.justice.gov/opa/pr/two-chinese-hackers-working-ministry-state-security-charged-global-computer-intrusion

[2] https://www.justice.gov/opa/pr/two-chinese-hackers-working-ministry-state-security-charged-global-computer-intrusion

Target Selection and Technical Information Gathering

Target Selection [TA0014] is a critical part of cyber operations. While cyber threat actors' motivations and intents are often unknown, they often make their selections based on the target network's security posture. Threat actors can use information sources such as Shodan, the Common Vulnerabilities and Exposure (CVE) database, and the National Vulnerabilities Database (NVD).[3,4,5]

- Shodan is an internet search engine that can be used to identify vulnerable devices connected to the internet. Shodan queries can also be customized to discover specific vulnerabilities on devices, which enables sophisticated cyber threat actors to use relatively unsophisticated techniques to execute opportunistic attacks on susceptible targets.
- The CVE database and the NVD contain detailed information about vulnerabilities in applications, appliances, and operating systems that can be exploited by cyber threat actors if they remain unpatched. These sources also provide risk assessments if any of the recorded vulnerabilities are successfully exploited.

These information sources have legitimate uses for network defense. CISA analysts are able to identify Federal Government systems that may be susceptible to exploitation attempts by using Shodan, the CVE database, and the NVD to enrich NCPS information. Unlike threat actors, CISA takes the necessary actions to notify network owners of their exposure in order to prevent an impending intrusion or quickly identify intrusions as they occur.

While using these data sources, CISA analysts have observed a correlation between the public release of a vulnerability and targeted scanning of systems identified as being vulnerable. This correlation suggests that cyber threat actors also rely on Shodan, the CVE database, the NVD, and other open-source information to identify targets of opportunity and plan cyber operations. Together, these data sources provide users with the understanding of a specific vulnerability, as well as a list of systems that may be vulnerable to attempted exploits. These information sources therefore contain invaluable information that can lead cyber threat actors to implement highly effective attacks.

CISA has observed Chinese MSS-affiliated actors using the techniques in table 1 to gather technical information to enable cyber operations against Federal Government networks (*Technical Information Gathering* [TA0015]).

Table 1: Technical information gathering techniques observed by CISA

MITRE ID	Name	Observation
T1245	Determine Approach/Attack Vector	The threat actors narrowed the attack vectors to relatively recent vulnerability disclosures with open-source exploits.

[3] https://www.shodan.io

[4] https://cve.mitre.org

[5] https://nvd.nist.gov/

T1247	Acquire Open Source Intelligence (OSINT) Data Sets and Information	CISA observed activity from network proxy service Internet Protocol (IP) addresses to three Federal Government webpages. This activity appeared to enable information gathering activities.
T1254	Conduct Active Scanning	CISA analysts reviewed the network activity of known threat actor IP addresses and found evidence of reconnaissance activity involving virtual security devices.

Technical Weakness Identification

CISA analysts consistently observe targeting, scanning, and probing of significant vulnerabilities within days of their emergence and disclosure. This targeting, scanning, and probing frequently leads to compromises at the hands of sophisticated cyber threat actors. In some cases, cyber threat actors have used the same vulnerabilities to compromise multiple organizations across many sectors. Organizations do not appear to be mitigating known vulnerabilities as quickly as cyber threat actors are exploiting them. CISA recently released an alert that highlighted the top 10 vulnerabilities routinely exploited by sophisticated foreign cyber threat actors from 2016 to 2019.[6]

Additionally, table 2 provides a list of notable compromises by Chinese MSS-affiliated actors within the past 12 months.

Table 2: Significant CVEs targeted by Chinese MSS-affiliated actors in the last 12 months

Vulnerability	Observations
CVE-2020-5902: F5 Big-IP vulnerability	CISA has conducted incident response engagements at Federal Government and commercial entities where the threat actors exploited CVE-2020-5902. This is a vulnerability in F5's Big-IP Traffic Management User Interface that allows cyber threat actors to execute arbitrary system commands, create or delete files, disable services, and/or execute Java code.[7]
CVE-2019-19781: Citrix Virtual Private Network (VPN) Appliances	CISA has observed the threat actors attempting to discover vulnerable Citrix VPN Appliances. CVE-2019-19781 enabled the actors to execute directory traversal attacks.[8]

[6] https://us-cert.cisa.gov/ncas/alerts/aa20-133a

[7] https://us-cert.cisa.gov/ncas/alerts/aa20-206a

[8] https://us-cert.cisa.gov/ncas/alerts/aa20-031a

CVE-2019-11510: Pulse Secure VPN Servers	CISA has conducted multiple incident response engagements at Federal Government and commercial entities where the threat actors exploited CVE-2019-11510—an arbitrary file reading vulnerability affecting Pulse Secure VPN appliances—to gain access to victim networks. Although Pulse Secure released patches for CVE-2019-11510 in April 2019, CISA observed incidents where compromised Active Directory credentials were used months after the victim organization patched their VPN appliance.[9]
CVE-2020-0688: Microsoft Exchange Server	CISA has observed the actors exploiting CVE-2020-0688 for remote code execution to enable email collection of targeted networks.

Additionally, CISA has observed Chinese MSS-affiliated actors using the techniques listed in table 3 to identify technical weaknesses in Federal Government networks (*Technical Weakness Identification* [TA0018]).

Table 3: Technical weakness identification techniques observed by CISA

MITRE ID	Name	Observation
T1288	Analyze Architecture and Configuration Posture	CISA observed the cyber actors scanning a Federal Government agency for vulnerable web servers. CISA also observed the threat actors scanning for known vulnerable network appliance CVE-2019-11510.
T1291	Research Relevant Vulnerabilities	CISA has observed the threat actors scanning and reconnaissance of Federal Government internet-facing systems shortly after the disclosure of significant CVEs.

Build Capabilities

CISA analysts have observed cyber threat actors using command and control (C2) infrastructure as part of their cyber operations. These observations also provide evidence that threat actors can build and maintain relatively low-complexity capabilities, such as C2, to enable cyber operations against Federal Government networks (*Build Capabilities* [TA0024]). CISA has observed Chinese MSS-affiliated actors using the build capabilities summarized in table 4.

Table 4: Build capabilities observed by CISA

MITRE ID	Name	Observation
T1352	C2 Protocol Development	CISA observed beaconing from a Federal Government entity to the threat actors' C2 server.

[9] https://us-cert.cisa.gov/ncas/alerts/aa20-107a

T1328	Buy Domain Name	CISA has observed the use of domains purchased by the threat actors.
T1329	Acquire and / or use of 3rd Party Infrastructure	CISA has observed the threat actors using virtual private servers to conduct cyber operations.
T1346	Obtain/Re-use Payloads	CISA has observed the threat actors use and reuse existing capabilities.
T1349	Build or Acquire Exploit	CISA has observed the threat actors using a variety of open-source and publicly available exploits and exploit code to compromise Federal Government networks.

MITRE ATT&CK Framework for Analysis

CISA has observed sophisticated cyber threat actors, including Chinese MSS-affiliated actors, using commercial and open-source tools to conduct their operations. For example, threat actors often leverage internet software repositories such as GitHub and Exploit-DB.[10,11] Both repositories are commonly used for legitimate development and penetration testing and developing open-source code, but cyber threat actors can also use them to find code to enable nefarious actions.

During incident response activities, CISA frequently observed Chinese government-affiliated actors using the open-source tools outlined in table 5.

Table 5: Common exploit tools CISA observed used by Chinese MSS-affiliated actors

Tool	Observations
Cobalt Strike	CISA has observed the threat actors using Cobalt Strike to target commercial and Federal Government networks. Cobalt Strike is a commercial penetration testing tool used to conduct red team operations. It contains a number of tools that complement the cyber threat actor's exploitation efforts, such as a keystroke logger, file injection capability, and network services scanners. CISA observed connections from a Federal Government agency to multiple IP addresses possibly hosting Cobalt Strike team servers.
China Chopper Web Shell	CISA has observed the actors successfully deploying China Chopper against organizations' networks. This open-source tool can be downloaded from internet software repositories such GitHub and Exploit-DB. China Chopper is a web shell hosted on a web server. It is mainly used for web application attacks, and it is configured in a client/server relationship. China Chopper contains security scanners and can be used to upload files and brute-force passwords.

[10] https://www.GitHub.com

[11] https://exploit-db.com

Mimikatz	CISA has observed the actors using Mimikatz during their operations. This open-source tool is used to capture account credentials and perform privilege escalation with pass-the-hash attacks that allow an attacker to pass captured password hashes and authenticate to network devices.[12]

The following sections list the ATT&CK Framework TTPs routinely employed by Chinese government-affiliated actors to conduct cyber operations as observed by CISA analysts.

Initial Access

In the last 12 months, CISA has observed Chinese MSS-affiliated actors use spearphishing emails with embedded links to actor-owned infrastructure and, in some cases, compromise or poison legitimate sites to enable cyber operations.

CISA has observed the threat actors using the *Initial Access* [TA0001] techniques identified in table 6.

Table 6: Initial access techniques observed by CISA

MITRE ID	Name	Observation
T1204.001	User Execution: Malicious Link	CISA has observed indications that users have clicked malicious links embedded in spearphishing emails that the threat actors sent
T1566.002	Phishing: Spearphishing Link	CISA analyzed network activity of a Federal Government entity and concluded that the threat actors sent a malicious email weaponized with links.
T1190	Exploit Public-Facing Application	CISA has observed the actors leveraging CVE-2019-19781 to compromise Citrix Application Delivery Controllers.

Cyber threat actors can continue to successfully launch these types of low-complexity attacks—as long as misconfigurations in operational environments and immature patch management programs remain in place—by taking advantage of common vulnerabilities and using readily available exploits and information.

Execution

CISA analysts continue to observe beaconing activity indicative of compromise or ongoing access to Federal Government networks. This beaconing is a result of cyber threat actors successfully completing cyber operations that are often designed around emergent vulnerabilities and reliant on existing exploitation tools, as mentioned in this document.

[12] https://www.varonis.com/blog/what-is-mimikatz/

CISA has observed Chinese MSS-affiliated actors using the *Execution* [TA0002] technique identified in table 7.

Table 7: Execution technique observed by CISA

MITRE ID	Name	Observation
T1072	Software Deployment Tools	CISA observed activity from a Federal Government IP address beaconing out to the threat actors' C2 server, which is usually an indication of compromise.

Credential Access

Cyber threat actors also continue to identify large repositories of credentials that are available on the internet to enable brute-force attacks. While this sort of activity is not a direct result of the exploitation of emergent vulnerabilities, it demonstrates that cyber threat actors can effectively use available open-source information to accomplish their goals. Further, a threat actor does not require a high degree of competence or sophistication to successfully carry out this kind of opportunistic attack.

CISA has observed Chinese MSS-affiliated actors using the *Credential Access* [TA0006] techniques highlighted in table 8.

Table 8: Credential access techniques observed by CISA

MITRE ID	Name	Observation
T1003.001	Operating System (OS) Credential Dumping: Local Security Authority Subsystem Service (LSASS) Memory	CISA observed the threat actors using Mimikatz in conjunction with coin miner protocols and software. The actors used Mimikatz to dump credentials from the OS using a variety of capabilities resident within the tool.
T1110.004	Brute Force: Credential Stuffing	CISA observed what was likely a brute-force attack of a Remote Desktop Protocol on a public-facing server.

Discovery

As with any cyber operation, cyber threat actors must be able to confirm that their target is online and vulnerable—there are a multitude of open-source scanning and reconnaissance tools available to them to use for this purpose. CISA consistently observes scanning activity across federal agencies that is indicative of discovery techniques. CISA has observed Chinese MSS-affiliated actors scanning Federal Government traffic using the discovery technique highlighted in table 9 (*Discovery* [TA0007]).

Table 9: Discovery technique observed by CISA

MITRE ID	Name	Observation
T1046	Network Service Scanning	CISA has observed suspicious network scanning activity for various ports at Federal Government entities.

Collection

Within weeks of public disclosure of CVE-2020-0688, CISA analysts identified traffic that was indicative of Chinese MSS-affiliated threat actors attempting to exploit this vulnerability using the *Collection* [TA0009] technique listed in table 10.

Table 10: Collection technique observed by CISA

MITRE ID	Name	Observation
T1114	Email Collection	CISA observed the actors targeting CVE-2020-0688 to collect emails from the exchange servers found in Federal Government environments.

Command and Control

CISA analysts often observe cyber threat actors using external proxy tools or hop points to enable their cyber operations while remaining anonymous. These proxy tools may be commercially available infrastructure as a service (IaaS) or software as a service (SaaS) in the form of a web browser promising anonymity on the internet. For example, “The Onion Router” (Tor) is often used by cyber threat actors for anonymity and C2. Actor’s carefully choose proxy tools depending on their intended use. These techniques are relatively low in complexity and enabled by commercially available tools, yet they are highly effective and often reliant upon existing vulnerabilities and readily available exploits.

CISA has observed Chinese MSS-affiliated actors using the *Command and Control* [TA0011] techniques listed in table 11.

Table 11: Command and control techniques observed by CISA

MITRE ID	Name	Observation
T1090.002	Proxy: External Proxy	CISA observed activity from a network proxy tool to 221 unique Federal Government agency IP addresses.
T1090.003	Proxy: Multi-hop Proxy	CISA observed activity from Tor that has resulted in confirmed compromises of internet-facing Federal Government agency systems.
T1573.002	Encrypted Channel: Asymmetric Cryptography	CISA observed activity from Tor that has resulted in confirmed compromises of internet-facing Federal Government agency systems.

MITIGATIONS

CISA asserts with high confidence that sophisticated cyber threat actors will continue to use open-source resources and tools to target networks with a low security posture. When sophisticated cyber threat actors conduct operations against soft targets, it can negatively impact critical infrastructure, federal, and state, local, tribal, territorial government networks, possibly resulting in loss of critical data or personally identifiable information.

CISA and the FBI recommend that organizations place an increased priority on patching the vulnerabilities routinely exploited by MSS-affiliated cyber actors. See table 12 for patch information on the CVEs mentioned in this report. For more information on vulnerabilities routinely exploited by sophisticated cyber actors, see CISA Alert: Top 10 Routinely Exploited Vulnerabilities.

Table 12: Patch information for vulnerabilities routinely exploited by MSS-affiliated cyber actors

Vulnerability	Vulnerable Products	Patch Information
CVE-2020-5902	• Big-IP devices (LTM, AAM, Advanced WAF, AFM, Analytics, APM, ASM, DDHD, DNS, FPS, GTM, Link Controller, PEM, SSLO, CGNAT)	• F5 Security Advisory: K52145254: TMUI RCE vulnerability CVE-2020-5902
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
CVE-2019-11510	• Pulse Connect Secure 9.0R1 - 9.0R3.3, 8.3R1 - 8.3R7, 8.2R1 - 8.2R12, 8.1R1 - 8.1R15 • Pulse Policy Secure 9.0R1 - 9.0R3.1, 5.4R1 - 5.4R7, 5.3R1 - 5.3R12, 5.2R1 - 5.2R12, 5.1R1 - 5.1R15	• Pulse Secure Out-of-Cycle Advisory: Multiple vulnerabilities resolved in Pulse Connect Secure / Pulse Policy Secure 9.0RX

CVE-2020-0688	• Microsoft Exchange Servers	• Microsoft Security Advisory: CVE-2020-0688: Microsoft Exchange Validation Key Remote Code Execution Vulnerability

CISA and the FBI also recommend that organizations routinely audit their configuration and patch management programs to ensure they can track and mitigate emerging threats. Implementing a rigorous configuration and patch management program will hamper sophisticated cyber threat actors' operations and protect organizations' resources and information systems.