JOINT
CYBERSECURITY
ADVISORY

Co-Authored by:

TLP:AMBER

Product ID: AA22-066A

March 7, 2022

Chinese APT Activity in State Government Departments, Agencies, and Programs

SUMMARY

The Federal Bureau of Investigation (FBI), the Cybersecurity and Infrastructure Security Agency (CISA), and the Multi-State Information Sharing and Analysis Center (MS-ISAC) are observing a Chinese advanced persistent threat (APT) group leveraging customized attack tooling (e.g., KEYPLUG Remote Access Trojan, DEADEYE launcher, LOWKEY backdoor, and BADPOTATO family of post-exploitation tools) in attacks against state government agencies and services from at least 2021 to present. Successful attacks enabled actors to establish command and control (C2), move laterally through networks, and gain privileged domain access.

Actions to Take Today:

- Search for indicators of compromise, and report newly identified activity.
- Keep software updated, prioritizing known exploited vulnerabilities.
- Secure public-facing web applications to ensure validation and decryption keys are dynamically generated at runtime.
- Enforce the principle of least privilege.
- Implement multifactor authentication.

The FBI, CISA, and MS-ISAC have associated intrusion activity related to this APT group with the targeting of states more broadly, as well as various types of state government departments and agencies, including health, transportation, labor (including unemployment benefit systems), higher education, agriculture, and court networks and systems. This series of intrusions is believed to be part

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 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 888-282-0870 or Central@cisa.gov. Organizations can reach the MS-ISAC at 866-787-4722 or SOC@cisecurity.org.

Disclaimer: the information in this joint Cybersecurity Advisory is provided "as is" for informational purposes only. FBI, CISA, and MS-ISAC do not provide any warranties of any kind regarding this information or endorse any commercial product or service, including any subjects of analysis. This document is distributed as TLP:AMBER: Limited disclosure, restricted to participants' organizations. Recipients may only share TLP:AMBER information with members of their own organization, and with clients or customers who need to know the information to protect themselves or prevent further harm. Sources are at liberty to specify additional intended limits of the sharing: these must be adhered to. For more information on the Traffic Light Protocol, see https://www.cisa.gov/tlp.

of a broader set of activity also involving exploitation of the USAHERDS application.[1] These attacks have been enabled by the following observed initial intrusion vectors.[2]

- Exploitation of Umbraco Content Management System[3]
- Exploitation of web applications, including USAHERDS
- SQL injection
- Password spray attack

In some known intrusions related to this activity, the threat actor was able to move laterally from initially compromised infrastructure to other portions of a larger state network.

The FBI, CISA, and MS-ISAC encourage recipients of this advisory to review the indicators and recommendations contained throughout and provide notification of any newly identified activity via the contact information in the Contact section below.

TECHNICAL DETAILS

The FBI, CISA, and MS-ISAC are observing a Chinese APT group penetrating state networks using a variety of different initial intrusion vectors, including a vulnerability in a content management system as well as various vulnerabilities in web applications in use by state governments, Structured Query Language (SQL) injection, and password sprays. In one intrusion occurring in late 2021, actors leveraged a vulnerability in an unemployment application to upload a China Chopper webshell.[4] Once the intrusion progressed beyond that initial compromised system, the actors used a number of different tools and techniques for persistence and lateral movement within the compromised network. Actors were able to gain access to domain controllers by dumping credentials, which led to admin access for several hours.

[1] The U.S. Animal Health Emergency Response and Diagnostic System (USAHERDS) application is used by multiple U.S. state government organizations to track and manage livestock data, including information about livestock disease outbreaks and animal incidents related to natural disasters. See the CISA-MS-ISAC-FBI Cybersecurity Advisory: APT Actors Exploiting Static Machine Keys in Public-Facing Web Applications (TLP:AMBER) for additional information.

[2] Given the diverse nature of state network architectures, this list may not be exhaustive.

[3] Umbraco is an open-source content management system platform for publishing content on the web and intranets. It is written in C# and deployed on Microsoft-based infrastructure.

[4] China Chopper is a web shell hosted on a web server and is mainly used for web application attacks; it is configured in a client/server relationship. China Chopper contains a “security scan” feature that can give an attacker the ability to upload files and brute-force passwords.

In addition, these APT actors commonly use KEYPLUG,[5] DEADEYE,[6] and LOWKEY[7] malware, and the BADPOTATO[8] family of post-exploitation tools as part of their tactics, techniques, and procedures (TTPs).

In recently reported intrusions, KEYPLUG malware used Command and Control Dead Drop (C2DD) webpages to facilitate C2 functionality. The malware can be configured to visit a preconfigured C2DD webpage, which may contain an encoded string that the malware decodes. Once the malware decodes the C2DD information, it communicates with the decoded IP address and port. Specific posts on several commonly used web forums were used as C2DD domains to mask and complicate identification of illegitimate network communications, including posts on `communities[.]vmware[.]com`, `www[.]dell[.]com/community`, and `social[.]msdn[.]microsoft[.]com`.

The APT actors using C2DD can quickly recover access to an affected network if an organization decides to block malicious IP addresses without understanding adversary TTPs and without locating adversary tools on affected systems. The actors can accomplish this by changing the content on C2DD websites (e.g., posts at the websites listed above) with the effect of changing the IP address the malware uses for C2. This makes blocking known C2 IP addresses alone an ineffective measure for network defense, as it is trivial for the actor to pivot to a potentially unknown alternate C2 IP. Accordingly, initial blocking of known C2 IPs without understanding the extent of a related intrusion will not effectively address the ability of the adversary to maintain access to an affected network. Relatedly, multiple victims reported lapses in observed APT activity after initial compromise and during initial lateral movement stages, suggesting access maintenance and persistence are focuses.

Finally, KEYPLUG malware samples typically use a complex encryption key which includes the victim's Active Directory (AD) domain name as a part of the key; as a result, tracking the KEYPLUG malware by hash values alone may not be helpful across impacted organizations.

In at least two intrusions, the APT actors used infrastructure (IP address `118.192.48[.]48`) associated with domain name `ceye[.]io`. Recent open-source articles describe a technique of data retrieval over DNS using domain name `ceye[.]io` as part of a blind SQL injection attack technique.

During an active intrusion, the APT actors also sent password reset messages via popup notification bubbles. The messages included the following syntax:

[5] KEYPLUG is a backdoor written in C/C++ that communicates via HTTP. KEYPLUG's core functionality involves expanding its capabilities by retrieving plugins from a C2 server. Downloaded plugins are mapped directly into memory and executed.

[6] DEADEYE is a launcher written in C/C++ that decrypts a file in its current directory and executes the result in memory.

[7] LOWKEY is a passive backdoor that supports commands for a reverse shell.

[8] BADPOTATO is an open-source tool used to impersonate another user to gain privilege escalation.

```
> C:\Windows\System32\wlrmdr.exe -s 60000 -f 1 -t Consider changing your
password -m Your password will expire in 8 days.\u000aTo change your
password, press CTRL+ALT+END and then click "Change a password". -a 0
```

Although the intent of the actors in resetting the password is unknown, it likely involved using the `CTR+ALT+END` text to target users coming in over RDP, using a keylogger to record keystrokes when users changed the password, or pulling credentials from memory with Mimikatz after the user authenticated to Local Security Authority Subsystem Service (LSASS).

In one intrusion, the APT actors installed the FASTPACE malware on a Microsoft SQL Server database. FASTPACE facilitates unauthenticated database access by implementing a backdoor password, which the actor can use to access privileged accounts including the System Administrator account on the Microsoft SQL Server database.

Tactics, Techniques, and Procedures

The APT actors leveraged the following intrusion vectors for initial access as part of attacks on state governments.

- Exploitation of Umbraco Content Management System
- Exploitation of web applications, including USAHERDS
- SQL injection
- Password spray attack

The APT actors also used the following techniques:

- Leveraged ACUNETIX web vulnerability scanner to perform web application vulnerability scans
- Dropped China Chopper webshell during exploitation of an internet-accessible web server
- Deployed FASTPACE malware against Microsoft SQL database for privileged access
- Exploited static machine key vulnerabilities in web applications (see the Mitigations section below for specific actions to take to address this)
- Uploaded BADPOTATO to impersonate a local user for privilege escalation
- Performed credential dumping using Mimikatz to gain account and password information
- Cleaned up tools after usage
- Ran processes from legitimate hollowed memory space
- Established persistence via functions added to a legitimate VMWare tools dynamic link library (DLL) – See CISA's Malware Analysis Report MAR-10372979.r1.v1
- Used naming conventions that blended in with existing naming to avoid alerting analysts
- Timestomped files to alter/obfuscate creation timestamps and complicate investigation of malicious activity
- Modified `hosts` files to modify DNS lookups with malicious IP addresses

Detection

Organizations should conduct a thorough search of their networks and investigate potential suspicious activity. Organizations should:

- **Search for IOCs,** beginning with those in the Appendix section of this report, including network and host-based artifacts. In addition to the IOCs listed in the Appendix, see CISA's Malware Analysis Report MAR-10372979.r1.v1 (TLP:AMBER).
- **Log evidence,** including behavioral, network, and host-based artifacts from known TTPs associated with this activity. Based on observed activity, this should include taking a live memory (RAM) capture from systems with signs of compromise.
- **Search for modifications to `hosts` files,** which an actor can use to modify DNS lookups with malicious IP addresses.[9] This activity was observed in conjunction with other attacks on authentication systems in previous intrusions related to this group. On modern Microsoft Windows operating systems, the `hosts` file is located at: `\Windows\System32\drivers\etc\hosts`. In Linux, `/etc/hosts` is a file used by the operating system to translate hostnames to IP addresses. By adding lines to this file, arbitrary hostnames can be mapped to arbitrary IPs.
- **Look for service host (svchost.exe) processes initiating DNS requests for the known C2DD domains.**
    - Search memory of service host process IDs (PIDs) for the C2DD domain names.
    - See CISA's Malware Analysis Report MAR-10372979.r1.v1

Affected organizations should take the following recommended actions:

- Build a remediation plan that includes understanding the initial intrusion vector and eviction of the threat actor based on subsequent activity, including identification of established persistence mechanisms. **Note:** based on observed activity involving the compromise of domain controllers, see CISA's Analysis Report, Eviction Guidance for Networks Affected by the SolarWinds and Active Directory/M365 Compromise as a guide for crafting eviction plans.
- Based on the threat actor's demonstrated ability to establish persistence and re-compromise affected entities, it is recommended that potentially affected partners seek out the services of a trusted third party with experience evicting APT actors from compromised networks.
- Report suspected and confirmed incidents to the FBI, CISA, or MS-ISAC. See the Contact section below for more information on reporting. This reporting will help determine the full scope of these intrusions and uncover additional IOCs and TTPs to support the network defense of all states.

MITIGATIONS

The FBI, CISA, and MS-ISAC urge organizations to:

- Log DNS queries and consider blocking all outbound DNS requests that do not originate from approved DNS servers. Monitor DNS queries for C2 over DNS or other data exfiltration over DNS. **Reminder:** based on the TTPs employed by the actor to maintain persistence (e.g., C2DD), initial, outright blocking of IOCs is likely not an effective way to address this activity. Organizations should consider taking steps to understand the full extent of an ongoing compromise before blocking associated malicious infrastructure.
- Enforce the principle of least privilege.

[9] A "host" file is a plain text file used to map host names to IP addresses. In most operating systems, the "host" file is owned by the "System" account and therefore requires access to that privilege before the file can be changed.

- Strengthen credential requirements and implement multifactor authentication to protect individual accounts, particularly for webmail and VPN access and for accounts that access critical systems.
- Keep systems updated. Prioritize patching known exploited vulnerabilities.
- Implement network segmentation to restrict an adversary's lateral movement.
- Review any public-facing web applications to ensure validation and decryption keys are dynamically generated at runtime. If keys must be static, encrypt the machine key and other sensitive content within the `web.config` file.
- Implement input validation on websites/webforms to guard against SQL injection attempts.
- For defense-in-depth, implement and configure a web application firewall (WAF) in front of critical applications to help mitigate potential underlying vulnerabilities in those applications as well as the use of observed techniques like SQL injection.
- Use endpoint detection and response (EDR) tools. Many of these tools go beyond signature-based detection mechanisms, allow a high degree of visibility into the security status of endpoints, and can be an effective defense against threat actors. EDR tools are particularly useful for detecting lateral movement, as they have insight into common and uncommon network connections for each host.

CONTACT

Recipients of this report are encouraged to contribute any additional information that they may have related to this threat.

For any questions related to this report or to report an intrusion and request resources for incident response or technical assistance, please contact:

- The FBI through the FBI Cyber Division (855-292-3937 or CyWatch@fbi.gov) or a local field office
- CISA (888-282-0870 or Central@cisa.gov)
- MS-ISAC (866-787-4722 or SOC@cisecurity.org)

APPENDIX: INDICATORS OF COMPROMISE

Files

Table 1: Hash Values

MD5Sum Hash	SHA256Sum hash
0FCD7A8B37EDAD2F9090B44096D27FC8	003F9BD021FA9B54C1FD81DA0C4184B89F7DF5ECAE6ACBB3F1F618BA513D6498
8FDFD9D1D62D4B8CC863F24BBD96FD8A	10D09EE353A3365056252499498B5BC3A005C302D308A5A611E7B232CB0030B4
2AA991C7B8DE2DBABA3962263DD6E6BE	2642D61EA68340FB07708D610E95021B898385664924EB8E41629FAD20A9AB72
BFE8D5AA5831D7C7C1A9DBF4323DAE5E	3497A3F68D1D60DFD88F88872096E37DFC6B5D20AFAA4C67ADF7AB41F12277B0
7C33DB81BF7D0DA056364A3A8E38D9C3	37C53A58DC97ECD684822E815A3296924B2E08C28269C0D82CCEB46A78C263CF
D5757F377A22EFF6A1925D3D459350B0	4739C9E8B93D0F007EA4D3EA7185A834FE62D415EDC38F0ACDCB94E510ADC709
759589512A2A31342C5BA13C61F9909D	4C139DEC35B155B0C7E116D0A58F5059042107385CF5CCB94AEAB87A1978115F
34C4856BB61EFAF9E7920A03AE368930	58628AA5C4D5DAD567E7673C327E5908F1DEE1AFC2D2AC5B3F211ACB40916CB0
66572D37219C1F03ACDB9F03D6CD0338	74567F93030612A5F7262FF928CB0F139A24FBB767731BDEBC7166EFA2B5FD87
CF284ED3720A35E97FC528B23184E8D8	85C69A03792CAC7C00602468F0752DB5F33F01D1FFC9727A16B0A4728B5C32A6
BF831B3916EF19E0BC74F4C783B7A368	9A52799F6C938BC97D9474A21D17A550DC174B7C38E3CC84C9A0473176168947
8C7B2A428F1BFA6038FA4B3DE6CAF938	C0346A4097D17006D9F25D27E1B8263582930867E43C53E7EB3A17500D07D97C
4804FB66406240617B0ED0B47DAE2F2F	DF97E0733197DE3F2F65408F044028EFE2D09794A773DEA2E32FACA40527555C
63fb821cc4310b8bdb5d77fe24df92b1	12d5b55e9524e5a6a1fb68fcacf90c4b2c9c30c543e2ec165bd96ad8d86409ea
d85a48ba367efe2781531900a9b8dbbc	317f30bad387e64e673c188ff4ebdaf0bc8c42faf218eb6436efd14c7e105940
a1630a4d9b423268a10ac87f47dd8de6	46271777072815b82b85fc35feafced9b9036b3b1427a7ac17993d01e72724c0
bdd6c0902d419de4c8e1770cccab47f2	4e14267bcc3bc2b4b1226921bcf8d1e71311fae8070a0db5af64e8de6824cea4
be900dddd36e4408df232bbd941cef78	5a476787cf193679b24d03a631e10107d1e517d883463bdce2051c1bf1b45704
50e35c62bf9f6de275f60a98a6e79cfa	6caacfd6e49e5453bed951aebcaccf5fc11f46f4c73db6437d791fd62bf653dc
8cabad1a8968358ac58ce6afdc30f9dc	909a7e023cd8ce44445f9f7a28c8aa239cc05d5b4bab508c6d4c215374add116
844096c0aecef82c29dda3e0fad440d7	93df473d23aaadca8dd6e5579ef1457a73e93ab51583ccf60bd9e5a9c42e7701
a693834690a432389811ceed601bbfb6	a5abaa278ad33bfdb82751be586795acaf8877f85d734874a0939b902f89f6f4
d8949ba3fa463607d3938f424c1cf8cd	eea77d0a74b229ec2add7c7d9e030c9735e13eddd5effa03ffd853d92962e924

Network

The IP addresses associated with this activity are listed in Table 2. **Note:** the date ranges associated with these IPs are based on observed activity. However, these IPs may also have been in use by the threat actors outside of the specified date ranges.

Table 2: IP Addresses

Observed Date Range	IP Address
12/29/2021 – 01/31/2022	104.149.140[.]182
12/29/2021 – 01/02/2022	18.118.56[.]237
12/29/2021 – 01/31/2022	35.87.250[.]69
12/29/2021 – 01/31/2022	20.121.42[.]11
12/14/2021 – 12/14/2021	104.149.134[.]38
12/22/2021 – 01/30/2022	104.149.140[.]180/30
11/19/2021 – 02/01/2022	118.192.48[.]48
11/19/2021 – 02/01/2022	122.10.117[.]202
11/19/2021 – 02/01/2022	144.202.112[.]250
11/19/2021 – 02/01/2022	149.248.7[.]127
11/19/2021 – 02/01/2022	158.69.253[.]64
11/25/2021 – 12/14/2021	54.144.37[.]217
	54.248.110[.]45
	54.199.117[.]45
	107.172.210[.]69
	172.104.206[.]48
	108.138.19[.]129

Domain Names

- `ceye[.]io`
  - `fln9co.ceye[.]io`
- `subnet.milli-seconds[.]com`
- `microsofttranslator[.]com`
- `time12[.]cf`
- `wbsdv95928.lithium[.]com`
- `d3n16yao9o6z9d.cloudfront[.]net`

KEYPLUG C2 Dead Drop Domains

Note: changes to encoded C2 IPs at the following C2DD domains associated with KEYPLUG malware have been observed over time. In addition, as it is trivial for the adversary to deploy new versions of KEYPLUG malware and associated C2DD domains, this list may not be exhaustive.

- `https://communities[.]vmware[.]com/t5/VMware-vCenter-Discussions/vCenter-6-0-0-patch-upgrade/m-p/510281`
- `https://communities[.]vmware[.]com/t5/VMware-vCenter-Discussions/VCENTER-upgrade-from-5-5-windows-to-6-5-Appliance/m-p/452517`
- `https://communities[.]vmware[.]com/t5/vSphere-Hypervisor-Discussions/Unable-to-update-after-7-0U3-upgrade/m-p/2881567#M6905`
- `https://www[.]dell[.]com/community/Networking-General/PowerConnect-6224-Won-t-Boot/m-p/3293797`
- `https://social[.]msdn[.]microsoft.com/Profile/AzureOpenSource`