White Paper

# Corelight coverage for TTPs documented in CISA Alert AA21-200B

**Introduction**

President Biden has aggressively focused on addressing cybersecurity threats to the U.S. since he took office in January 2021. His three-prong approach includes the modernization of our cyber defenses across the U.S. Government, Critical Infrastructure Providers (CIP), the Defense Industrial Base (DIB), and private industry; creating cyber-specific policies to direct government resources to build up a stronger overall defensive posture and to build an international coalition to deter and stop nation-sponsored threat actors.

The Executive Order on Improving the Nation's Cybersecurity, the National Cyber Director Act, and the memorandum on Improving Critical Infrastructure Cybersecurity are just some of the administration's steps to focus the nation on the need for cybersecurity improvement. The departments and agencies in the U.S. Government with delegated authorities for cybersecurity are following suit.

In unprecedented fashion, on July 19, 2021, the National Security Agency, Cybersecurity, and Infrastructure Security Agency, and the Federal Bureau of Investigations released a joint Cybersecurity Advisory (CSA) titled "Alert (AA21-200B): Chinese State-Sponsored Cyber Operations: Observed TTPs" which details specific tactics, techniques, and procedures used by Chinese cyber actors. Rather than safeguarding this information through traditional classification protections, this publicly released information equips the whole of the U.S. Government, CIP, DIB, and private industry organizations with specifics on what network defenders should look for and how to mitigate these threats.

This CSA is unique in that it provides a comprehensive and unique mapping to the MITRE ATT&CK® and D3FEND™ frameworks that inventory a globally accessible knowledge base of adversary tactics and techniques based on real-world observations. Network-oriented defenders can use the described TTPs to understand the precise mitigation technique to implement and counter these ongoing cyber-attacks. We believe that this is the first of many follow-on CSA's that will provide this level of detail about adversarial cyber actors, but to identify these TTPs presumes that organizations and entities have visibility into their IT infrastructure in both the network and endpoints. Strong visibility comes from implementing the SOC Visibility Triad, a term coined by Gartner that describes a high-level architecture design consisting of a SIEM, EDR, and NDR.

Data streamed to a SIEM in this architecture should be:

- **In a uniform data format**—security analysts, automation tools, and machine learning algorithms need clean, consistent data formats to make quick judgment calls, convict and remediate threats with confidence, and train detection models.
- **Purpose-built for security**—the data should be designed for security use cases to avoid the pitfalls of familiar telemetry sources intended for IT and compliance. Their data collection biases leave gaping security visibility holes behind.
- **Resistant to compromise**—adversaries will attempt to muddle the "operational picture" by compromising upstream telemetry, up to and including generating false information from hijacked sources.
- **Designed for interoperability**—information collected should interoperate with tools and complementary data sources to facilitate fast correlations for analysis and investigation tasks.

While endpoints provide a critical source of information to form this picture, organizations who single thread their operational awareness on EDR technology do so at their peril. Endpoints offer an excellent depth of information, but that depth does not reach where EDR agents cannot (e.g., BYOD, Cloud, etc.). That depth is also rendered meaningless when adversaries succeed in evading or compromising the endpoints or EDR agents themselves.

Comprehensive network monitoring can address these security gaps left by EDR with complementary coverage that excels in the aforementioned information collection requirements, notably in its "resistance to compromise." No matter the environment, nearly all cyberattacks must communicate over networks and organizations that can silently capture, analyze, and store those communications to gain an immutable record of malicious activity. Unlike endpoints, the network cannot lie.

Corelight's data-first approach to security continuously collects evidence from network traffic across on-prem, cloud, and virtual environments. This fine-grained, actionable data that Corelight extracts from network traffic can be integrated into your SIEM, data lake, or XDR platforms as part of your current cybersecurity ecosystem. Notably, Corelight's network visibility enables proactive threat hunting for a wide array of adversarial techniques, tactics, and procedures documented in MITRE ATT&CK®, and analysts can download Corelight's free hunting guide for detailed technical guidance on this matter.

Regarding "Alert (AA21-200B) Chinese State-Sponsored Cyber Operations: Observed TTPs," the table that follows in this document demonstrates Corelight's coverage capabilities for the specific TTPs cited in this alert.

## Table 1: Corelight TTP coverage for alert (AA21-200B)

| Tactic | Technique | Sub technique | Threat actor procedure(s) | Corelight coverage |
|---|---|---|---|---|
| Reconnaissance | Active Scanning [T1595] | NA | 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. | When activity goes beyond scanning of O365, detecting active scans at the port level is easy with Corelight's conn.log that documents all connections on the network. This can also be done via other Corelight network logs such as http.log (e.g., looking for large numbers of accesses from a single client) and can be supported via Corelight's Suricata IDS functionality (if known bad user-agent strings are used). |
| Resource Development | Acquire Infrastructure [T1583]<br><br>Stage Capabilities [T1608] | NA | Chinese state-sponsored cyber actors have been observed using VPSs from cloud service providers that are physically distributed worldwide to host malware and function as C2 nodes. | Discovering this technique involves correlating what service providers' outbound connections are going to via MaxMind. You can combine this information with Corelight protocol analysis for those with smaller/less common VPSes to find anomalous activity. For example, RDP or SSH going to a low-prevalence VPS is a huge red flag. |
| Resource Development | Obtain Capabilities | 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 leveraging Corelight's network visibility and:<br>• 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.<br>• Looking for the default Cobalt Strike TLS certificate.<br>• Look at the user agent that generates the TLS traffic for discrepancies that may indicate faked and malicious traffic.<br>• Review the traffic destination domain, which may be malicious and an indicator of compromise.<br>• 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.<br>• 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. |

| Tactic | Technique | Sub technique | Threat actor procedure(s) | Corelight coverage |
|---|---|---|---|---|
| Initial Access | Drive-by Compromise [T1189] | NA | Chinese state-sponsored cyber actors have been observed gaining access to victim networks through watering hole campaigns of typo-squatted domains. | Suricata, supported in Corelight's platform, will detect some client-side exploits used in these campaigns. Corelight can detect distinct character sets within a given domain name and support URL analysis as well. |
| Initial Access | Exploit Public-Facing Application [T1190] | | Chinese state-sponsored cyber actors have exploited known vulnerabilities in Internet-facing systems.[1]<br>Chinese state-sponsored cyber actors have also been observed:<br>• Using short-term VPS devices to scan and exploit vulnerable Microsoft Exchange® Outlook Web Access (OWA®) and plant web shells.<br>• Targeting on-premises Identity and Access Management (IdAM) and federation services in hybrid cloud environments to gain access to cloud resources.<br>• Deploying a public proof of concept (POC) exploit targeting a public-facing appliance vulnerability. | Corelight covers more than three dozen CVEs associated with this technique via Suricata rules supported on the platform. |
| Initial Access | Phishing [T1566]: | Spearphishing Attachment [T1566.001] | 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.<br>These compromise attempts use the cyber actors' dynamic collection of VPSs, previously compromised accounts, or other infrastructure 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. | Phishing attachments that contain exploits or malicious attachments are popular and effective tools in attack campaigns. These attachments, once opened, may beacon to a second stage system for additional instructions or malicious files.<br>Corelight can monitor outbound HTTP connections to known-suspicious sites. Further, HTTP user-agent headers may indicate the use of suspect processes, such as Microsoft Office beaconing to external resources. These indicators are excellent indicators for defenders to begin an investigation.<br>For organizations that decrypt email, Corelight's file extraction can store attachments and log file hashes. Defenders can store this data for later analysis, or use automated tools to submit them for third-party testing. |

| Tactic | Technique | Sub technique | Threat actor procedure(s) | Corelight coverage |
|---|---|---|---|---|
| Initial Access | Phishing [T1566]: | 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.<br><br>These compromise attempts use the cyber actors' dynamic collection of VPSs, previously compromised accounts, or other infrastructure 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. | Attackers use spearphishing emails to target users with malicious links to externally-hosted malicious files. These links might trigger a browser exploit or the download of a malicious document.<br><br>For organizations that decrypt email, Corelight currently supports parsing the SMTP protocol, and Corelight scripts can be used to extract URIs from clear-text emails. Corelight can then also be used to monitor for outbound HTTP connections to those URIs. |
| Initial Access | External Remote Services [T1133] | | Chinese state-sponsored cyber actors have been observed:<br>• 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 to exploit vulnerable systems.<br>• Targeting Microsoft Exchange offline address book (OAB) virtual directories (VDs).<br>• Exploiting Internet-accessible web servers using web shell small code injections against multiple code languages, including net, asp, apsx, PHP, japx, and cfm.<br>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. | Corelight can cover this technique via Suricata rules supported on the platform. |

| Tactic | Technique | Sub technique | Threat actor procedure(s) | Corelight coverage |
|---|---|---|---|---|
| Initial Access | Valid Accounts [T1078]: | Default Accounts [T1078.001] | 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. | Attackers with knowledge of known-good credentials may acquire them through social engineering or specially-crafted lookalike websites that trick a user into divulging their username and password. Once captured, an attacker will be eager to try these credentials on a variety of resources, often attempting access to systems outside the users' normal usage during hours outside that employee's regular work schedule.<br><br>Corelight can identify suspicious account behavior across systems that share user accounts (either user, admin, or service accounts). Attempts to log in to multiple systems simultaneously, attempts to login at odd times, or outside of business hours warrant prompt investigation. Remote attempts to log in interactively or to spawn processes are solid indicators and can be reflected in the dce_rpc.log.<br><br>In some cases, Corelight may detect the leak of credentials before an attacker has a chance to use them. Attackers often lure victims to phishing websites, prompting users to enter valid credentials to be collected by the attacker. The victim may even be redirected to the legitimate service so as not to raise suspicion. These attempts generate DNS, HTTP, and SSL traffic and can be investigated in their respective log files. |
| Initial Access | Valid Accounts [T1078]: | 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. | Attackers with knowledge of known-good credentials may acquire them through social engineering or specially-crafted lookalike websites that trick a user into divulging their username and password. Once captured, an attacker will be eager to try these credentials on a variety of resources, often attempting access to systems outside the users' normal usage during hours outside that employee's regular work schedule.<br><br>Corelight can identify suspicious account behavior across systems that share user accounts (either user, admin, or service accounts). Attempts to log in to multiple systems simultaneously, attempts to login at odd times, or outside of business hours warrant prompt investigation. Remote attempts to log in interactively or to spawn processes are solid indicators and can be reflected in the dce_rpc.log.<br><br>In some cases, Corelight may detect the leak of credentials before an attacker has a chance to use them. Attackers often lure victims to phishing websites, prompting users to enter valid credentials to be collected by the attacker. The victim |

| Tactic | Technique | Sub technique | Threat actor procedure(s) | Corelight coverage |
|---|---|---|---|---|
| | | | | may even be redirected to the legitimate service so as not to raise suspicion. These attempts generate DNS, HTTP, and SSL traffic and can be investigated in their respective log files. |
| Execution | Command and Scripting Interpreter [T1059]: | PowerShell® [T1059.001] | Chinese state-sponsored cyber actors have been observed:<br>Using PowerShell to conduct reconnaissance, enumeration, and discovery of the victim network. | Attackers increasingly turn to "live off the land" techniques, such as using built-in PowerShell functionality when attacking Microsoft Windows workstations and servers. Commands, known as cmdlets ("command-lets"), can download and execute files locally or remotely.<br>Corelight detects the use of cmdlets between hosts by monitoring RPC traffic between Windows hosts. Additionally, if PowerShell is used to download files, telltale user-agent strings can help defenders quickly pinpoint suspicious activity. |
| Execution | User Execution [T1204] | Malicious Link [T1204.001]<br>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 provides the cyber actor access to the victim's device after the user clicks on the malicious link or opens the attachment. | Corelight's DNS.log and files.log can be used to investigate and monitor suspicious links. |
| Persistence | 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. | Corelight can cover this technique via Suricata rules supported on the platform and via visibility from Corelight's http.log. |
| Credential Access | Exploitation for Credential Access [T1212] | N/A | 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. | Corelight can cover this technique via Suricata rules supported on the platform for vulnerability detection. |

| Tactic | Technique | Sub technique | Threat actor procedure(s) | Corelight coverage |
|---|---|---|---|---|
| Discovery | Network Service Scanning [T1046] | N/A | Chinese state-sponsored cyber actors have been observed using Nbtscan and Nmap to scan and enumerate target network information. | Attackers must profile and fingerprint the target network to determine paths for further exploitation. In doing so, they leave behind fingerprints that may provide insight into the tools they have chosen, the parameters they provided, and their intent. For example, an attacker may begin host discovery using a tool like Nmap with a TCP SYN scan.<br><br>Corelight neatly summarizes connections within conn.log and uses the history field to identify the state of the connection. For example, many events within conn.log, from a single source and with incomplete connections may indicate that a host is performing service reconnaissance. If a burst of connections have occurred to numerous hosts and ports, with only the history field showing S0 and S1, Corelight has identified the fingerprints of a typical SYN scan. |
| Discovery | Remote System Discovery [T1018] | N/A | To enumerate target network information, Chinese state-sponsored cyber actors have been observed using Base-64 encoded commands, including ping, net group, and net user. | Attackers will sometimes use a custom toolset, or the built-in net command on a Windows host, to survey a network for Windows hosts. These tools generate RPC traffic to attempt to connect, authenticate, and profile Microsoft Windows workstations and servers. This traffic will often originate from a compromised host inside the network perimeter.<br><br>Corelight can identify this technique and log attempts within dce_rpc.log. A large amount of these events would be a strong indicator for defenders to begin investigating. Fusing Corelight's Zeek-based network data with other data via Community_ID, allows for simplified monitoring of processes and command-line arguments for actions that could be taken to gather system and network information. |

| Tactic | Technique | Sub technique | Threat actor procedure(s) | Corelight coverage |
|---|---|---|---|---|
| Lateral Movement | Exploitation of Remote Services [T1210] | N/A | 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.<br><br>Chinese state-sponsored cyber actors also used on-premises Identity and Access Management (IdAM) and federation services in hybrid cloud environments to pivot to cloud resources. | Given the complexity of today's enterprise networks, various third-party and external services are often in use. These services may allow attackers to gain initial access or to move laterally.<br><br>All connections are logged within conn.log. However, more details may be available within protocol-specific logs, depending on the nature of the remote service under attack. For example, the http.log file can be monitored for suspicious and unexpected requests (such as OPTIONS requests).<br><br>Additionally, Corelight extracts information about specific software versions into the software.log file. This file provides defenders valuable data to monitor for unexpected or unauthorized servers, vulnerable or out-of-date services, and unpatched client software. |
| Collection | Data Staged [T1074] | N/A | 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 web shell prior to compressing and exfiltrating the data from the target network. | Attackers use common protocols to stage data on a centralized host before beginning exfiltration. If attackers are making use of existing infrastructure, they will need to use common protocols like SMB, FTP, and HTTP.<br><br>Corelight monitors SMB, FTP, and HTTP traffic. Still, even if an attacker chooses a less common protocol, Corelight can detect a change in the producer-consumer ratio (e.g., greater than 40% traffic in conn.log between two hosts) or sizeable unexpected data transfers between hosts. |

| Tactic | Technique | Sub technique | Threat actor procedure(s) | Corelight coverage |
|---|---|---|---|---|
| C2 | Application Layer Protocol [T1071] | N/A | Chinese state-sponsored cyber actors have been observed:<br>• Using commercial cloud storage services for command and control.<br>• Using malware implants that use the Dropbox® API for C2 and a downloader that downloads and executes a payload using the Microsoft OneDrive® API. | Attackers use common ports to blend in with expected traffic on an enterprise network such as DNS and HTTP. Corelight detects known malware that communicates over HTTP, known DNS tunneling tools, and DNS tunneling behaviors to find unknown threats.<br>Corelight's Dynamic Protocol Detection (DPD) framework is a unique capability, allowing defenders to monitor large traffic volumes for connections while searching for mismatched protocol and port mappings. For example, an attacker sending HTTPS traffic over SSH port 22 will be detected by Corelight's protocol parsers, allowing Corelight to parse the traffic and log the relevant protocol details. Corelight summarizes each TCP, UDP, and ICMP connection in a detailed log, providing statistics for in-depth analysis. These connection events are provided in the conn.log file; defenders can identify these mismatched connections within this log. Further, protocols like DNS and HTTP will be, analyzed and stored in a protocol-specific log file. |
| C2 | Ingress Tool Transfer [T1105] | N/A | 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. | Corelight's ftp.log and smb.logs can provide visibility around this technique. |
| C2 | Non-Standard Port [T1571] | N/A | Chinese state-sponsored cyber actors have been observed using a non-standard SSH port to establish covert communication channels with VPS infrastructure. | Corelight's unique Dynamic Protocol Detection (DPD) capability allows defenders to monitor large traffic volumes for connections while searching for mismatched protocol and port mappings. For example, an attacker sending HTTPS traffic over SSH port 22 will be detected by Corelight's protocol parsers, allowing Corelight to parse the traffic and log the relevant protocol details. Corelight summarizes each TCP, UDP, and ICMP connection in a detailed log, providing statistics for in-depth analysis. These connection events are provided in the conn.log file; defenders can identify these mismatched connections within this log. Further, protocols like DNS and HTTP will be analyzed and stored in a protocol-specific log file. |

| Tactic | Technique | Sub technique | Threat actor procedure(s) | Corelight coverage |
|---|---|---|---|---|
| C2 | Protocol Tunneling [T1572] | N/A | Chinese state-sponsored cyber actors have been observed using tools like dog-tunnel and dns2tcp.exe to conceal C2 traffic with existing network activity. | The Corelight C2 Collection helps organizations find command and control activity with over 50 unique insights and detections. Battle-tested by some of the world's most sophisticated organizations, this collection covers both known C2 toolkits and MITRE ATT&CK C2 techniques to find novel attacks, covering:<br>• HTTP C2<br>• DNS tunneling<br>• ICMP tunneling<br>• Domain Generation Algorithms<br>• Meterpreter<br>• And more... |
| C2 | 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. | Malware can be designed to reroute and encapsulate traffic through custom protocols and purpose-built networks like The Onion Router (TOR). These protocols will make use of common ports and encryption mechanisms but "bounce" C2 traffic between an ever-changing number of hosts in an attempt to obfuscate the source of the attacker's actual C2 infrastructure.<br>Corelight's protocol analysis can identify TOR and other SSL-based traffic through the use of the JA3 and JA3S hash. These hashes help correlate fingerprints associated with TOR-based malware and are stored within the ssl.log file. Additionally, malware communications, such as WannaCry, make use of TOR and are identifiable through the use of temporary SSL certificates with random domain names.<br>Additionally, the conn.log captures timestamp information for each connection for defenders to scrutinize. Alternatively, purpose-built Corelight scripts can be written to correlate data exchanges between hosts and help pinpoint the source of a proxied connection. |

Defenders have always sought the high ground in order to see farther and turn back attacks. Corelight delivers a commanding view of your network so you can outsmart and outlast adversaries. We capture, interpret, and connect the data that means everything to defenders.

**info@corelight.com | 888-547-9497**