

JOINT CYBERSECURITY ADVISORY

TLP:CLEAR

Co-Authored by:

Product ID: AA26-281A



National Cyber
Security Centre
a part of GCHQ



ASD AUSTRALIAN
SIGNALS
DIRECTORATE
ACSC Australian
Cyber Security
Centre



Communications Security
Establishment Canada
**Canadian Centre
for Cyber Security**

Centre de la sécurité des
télécommunications Canada
**Centre canadien
pour la cybersécurité**



警察庁
National Police Agency



国家サイバー統括室
National Cybersecurity Office



Te Tira Tiaki
Government Communications
Security Bureau



**National Cyber
Security Centre**
NEW ZEALAND



Chinese Government-linked Cyber Threat Actors Combine Automated and Hands- on Hacking Tools to Steal Sensitive Data

Publication: October 8, 2026

US Federal Bureau of Investigation
US Cybersecurity and Infrastructure Security Agency
US National Security Agency
United Kingdom National Cyber Security Centre
Australian Signals Directorate's Australian Cyber
Security Centre

Canadian Centre for Cybersecurity
Japan's National Police Agency
Japan's National Cybersecurity Office
New Zealand National Cyber Security Centre
Spain's Centro Nacional de Inteligencia

To report suspicious or criminal activity related to information found in this joint Cybersecurity Advisory, contact the FBI's [Internet Crime Complaint Center \(IC3\)](#), your [local FBI field office](#), and/or CISA's 24/7 Operations Center at contact@cisa.dhs.gov or 1-844-Say-CISA (1-844-729-2472). 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. For NSA-client requirements or cybersecurity inquiries, contact CybersecurityReports@nsa.gov.

This document is distributed as TLP:CLEAR. Disclosure is not limited. Sources may use TLP:CLEAR 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:CLEAR information may be distributed without restriction. For more information on the Traffic Light Protocol, see [Traffic Light Protocol \(TLP\) Definitions and Usage](#).

TLP:CLEAR

Advisory at a Glance

Title	Chinese Government-linked Cyber Threat Actors Combine Automated and Hands-on Hacking Tools to Steal Sensitive Data
Original Publication	October 8, 2026
Executive Summary	Chinese government-linked cyber threat actors, enabled by the Integrity Technology Group, are combining automated scanning tools, large-scale botnets, and hands-on exploitation techniques to target and steal sensitive data from organizations worldwide, including US critical infrastructure sectors. These actors exploit vulnerabilities by using scanning tools, cross-site scripting attacks, and password spraying on Microsoft Exchange servers, while establishing persistence through VPN software and exfiltrating emails and credentials using scripts. To help mitigate against this activity, organizations should prioritize disabling unused services and ports, sanitizing web application inputs to prevent injection attacks, implementing multifactor authentication for all services, and applying timely patches to reduce risks of compromise.
Affected Products	CVE-2014-6278 , CVE-2015-3306 , CVE-2015-5477 , CVE-2016-3081 , CVE-2019-11510 , CVE-2021-22205 , CVE-2021-3199 , CVE-2023-22894
Key Actions	▪ Disable unused services and ports, such as automatic configuration, remote access, or file sharing protocols. ▪ Sanitize user input in web applications to prevent possible cross-site scripting (XSS) payload injection. ▪ Implement identity, credential, and access management (ICAM) policies, and then require multifactor authentication (MFA) for services (to the extent possible).
Indicators of Compromise	For a downloadable copy of indicators of compromise, see: ▪ AA26-281A STIX XML ▪ AA26-281A STIX JSON
Intended Audience	Organizations: Government; Federal Civilian Executive Branch (FCEB); State, Local, Tribal, and Territorial (SLTT); Critical Infrastructure. Sectors: Government Services and Facilities, Critical Manufacturing, Healthcare and Public Health, and Information Technology. Roles: Defensive Cybersecurity Analysts, Vulnerability Analysts, Security Systems Managers, Incident Response Analysts.

Table of Contents

Advisory at a Glance	2
Introduction	4
Threat Actor Background	5
Technical Details	5
Reconnaissance	5
MicroScan	5
Initial Access and Execution	6
EBurst	7
Persistence	8
Collection and Exfiltration	8
Curlc4.txt	9
DC.exe	10
Data Exfiltration	11
Office-cli Program	11
Indicators of Compromise	11
MITRE ATT&CK Tactics and Techniques	11
Incident Response	13
Mitigations	14
Validate Security Controls	16
Resources	16
Contact Information	17
Disclaimer	18
Version History	18
Appendix A: Indicators of Compromise	19
Appendix B: Observed Common Vulnerabilities and Exposures	58

Introduction

Integrity Technology Group, a China-based company with links to the Chinese government, enables China-linked threat actors to exploit US and foreign organization networks across multiple sectors using various tools and techniques. This advisory provides an analysis of tactics, techniques, and procedures (TTPs) and indicators of compromise (IOCs) from Integrity Technology Group and the threat actors they enable (hereafter referred to as “the threat actors”). The analysis in this advisory provides network defenders with detection and mitigation guidance to reduce the risk of threat actors compromising critical data.

The threat actors use a unique combination of large-scale botnets, virtual private network (VPN) infrastructure, living-off-the-land (LOTL) techniques, and repositories of computer network exploitation (CNE) tools. Although these techniques are not unique to Chinese threat actors, this advisory details how the threat actors use them to support CNE activity.

The threat actors targeted victims across multiple US critical infrastructure sectors, including: [Government Services and Facilities](#), [Critical Manufacturing](#), [Healthcare and Public Health](#), and [Information Technology](#). The actors also targeted victims in US law enforcement, education, and religious organizations, as well as organizations across Southeast Asia, Africa, and North America.

The information in this advisory originates from technical evidence recovered from, and observed during, multiple Federal Bureau of Investigation (FBI) investigations related to Integrity Technology Group.

The FBI, Cybersecurity and Infrastructure Security Agency (CISA), National Security Agency (NSA), United Kingdom National Cyber Security Centre (NCSC-UK), Australian Signals Directorate’s Australian Cyber Security Centre (ASD’s ACSC), the Canadian Centre for Cyber Security (Cyber Centre), Japan’s National Police Agency (NPA) and National Cybersecurity Office (NCO), New Zealand’s National Cyber Security Centre (NCSC-NZ), and Spain’s Centro Nacional de Inteligencia (CNI), hereafter referred to as “the authoring organizations”—are releasing this joint cybersecurity advisory to urge network defenders from government and relevant organizations to:

- Hunt for potential compromises from this activity.
- Better protect against this threat activity and other Chinese government-linked cyber targeting.

This advisory also provides our US federal, state, local, territorial, and tribal (FSLTT) government agencies, and international and industry partners, with the indicators and details necessary to proactively defend their networks against this threat and protect critical data.

For more information on People’s Republic of China (PRC) state-sponsored malicious cyber activity in general, see the FBI’s [Cyber Threat Overview: China](#) webpage. For more information on China-linked malicious cyber activity, see CISA’s People’s Republic of [China Threat Overview and Advisories](#) webpage.

The authoring organizations encourage network defenders to implement the recommendations in the **Mitigations** section of this advisory to reduce the likelihood and impact of these incidents.

For a downloadable copy of IOCs, see:

- [AA26-281A STIX XML](#)
- [AA26-281A STIX JSON](#)

Threat Actor Background

Integrity Technology Group (Integrity Tech) is a China-based for-profit company with links to the Chinese government. Integrity Tech employs individuals who support malicious cyber activity in different ways, including acquiring or building cyber tools for use and sale, acquiring and hosting infrastructure, and compromising networks across global victims, which the authoring organizations track as China-based malicious cyber activity. The services provided by Integrity Tech also contribute to the larger Chinese cyber ecosystem, which aims to exfiltrate sensitive data from victims around the world.

Notably, the threat actors enabled by Integrity Tech use TTPs consistent with the cyber activity publicly known as Flax Typhoon, Ethereal Panda, and Red Juliett, among others. However, these threat actors may also perform activity not associated with Integrity Tech.

Note: Cybersecurity companies have different methods of tracking and attributing cyber actors and these may not be a 1:1 correlation to the US Government's methodology and understanding for all activity related to these groupings.

Technical Details

Note: This advisory uses the [MITRE ATT&CK® Matrix for Enterprise](#) framework, version 19. See **Appendix A: Indicators of Compromise** and the **MITRE ATT&CK Tactics and Techniques** section of this advisory for a table of the threat actors' activity mapped to MITRE ATT&CK tactics and techniques.

Reconnaissance

The threat actors use a variety of open source scanning tools to find vulnerabilities in networks and web-based applications, including: BBScan, dirsearch, Fscan, ksubdomain, masscan, NMAP, OneForAll, ShuiZe, and wpscan [[T1595.002](#)]. See **Appendix A: Indicators of Compromise** for a complete list of scanning tools.

Some of these tools contain features useful for fingerprinting remote applications, testing remote authentication protocols, or enumerating the pages of a website. The use of open source tools typically found on GitHub suggests the threat actors tend to look for more vulnerable targets. In general, the threat actors focus on scanning ports **21** (file transfer protocol [FTP]), **22** (SSH), **53** (domain name system [DNS]), **80** (HTTP), **443** (HTTPS), and **1080** (SOCKS). When scanning websites with dirsearch, the threat actors attempt to enumerate PHP and ASP (**.NET**) pages.

MicroScan

As early as 2017, these threat actors have also used a malicious application known as "MicroScan." This Python-based web application contains over 1,300 penetration testing scripts written to scan websites for specific vulnerabilities. The threat actors used these scripts to target services including OpenSSL, Oracle WebLogic, Rejetto, WordPress, Juniper ScreenOS, Jenkins, and Apache Struts. See **Appendix B: Observed Common Vulnerabilities and Exposures** for a list of successfully exploited common vulnerabilities and exposures (CVEs) recovered from penetration testing scripts. **Figure 1** shows a MicroScan account dashboard displaying detected vulnerabilities.

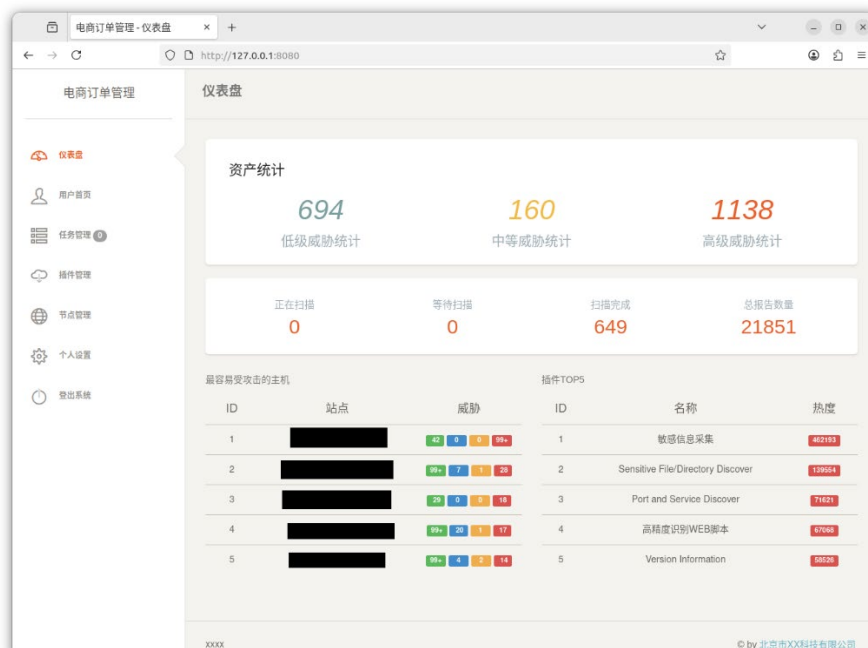


Figure 1. MicroScan Account Dashboard Showing Detected Vulnerabilities

Initial Access and Execution

Since at least mid-January 2021, the threat actors have gained access to victim networks and cloud-based services primarily through command line utilities built on exploit codes written in popular programming languages, such as Python and Go [T1059.006]. Additionally, the threat actors have used JavaScript [T1059.007] and HTML code to execute cross-site scripting (XSS) attacks. XSS vulnerabilities allow malicious actors to use unwitting third-party applications vulnerable to XSS to modify content on a webpage [T1189] and target other victims.

During the investigations, the FBI recovered an XSS payload used by the threat actors. When executed on a vulnerable website running JavaScript, this payload modifies webpage content to display username and password fields, facilitating user credential harvesting (see Figure 2).

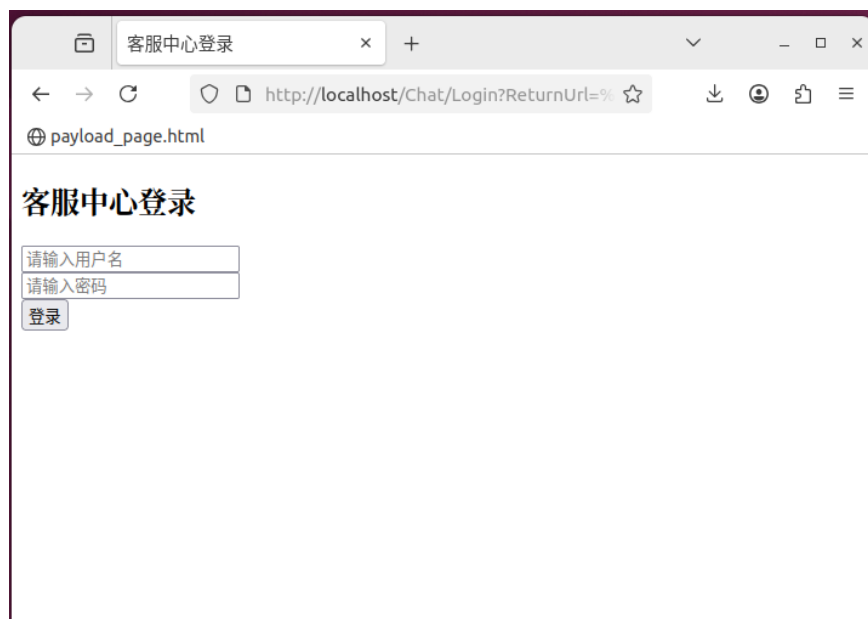


Figure 2. Executed XSS Payload

After a user enters any username and password, the executed XSS payload page generates a link to download a password-protected `.zip` file. The `.zip` file's contents originate from encoded bytes within the XSS payload and contain the executable file `live700_v1.exe`.

Analysis of `live700_v1.exe` demonstrated the executable begins a process named `DiagTrack.exe`, which shares its name with legitimate Windows software [T1036.003]. `DiagTrack.exe` then establishes encrypted communications over the HTTP protocol with the domain `dns.studiocloud.xyz`, which the FBI attributes to Integrity Tech. Given that the executable also contains functions designed to query data from user mailboxes, the FBI assesses the malware likely targets user email data for exfiltration.

EBurst

The threat actors use EBurst, an open source Python-based tool, to target accounts in the Microsoft Office365 Cloud environment. The tool compromises email accounts on Microsoft Exchange servers using multiple interfaces for password spraying [T1110.003] and password guessing [T1110.001] against each supplied email address. Based on the open source EBurst `ReadMe` file, these interfaces include:

- Exchange Control Panel (ECP);
- Exchange Web Services (EWS);
- Offline Address Book (OAB);
- Outlook Web Access (OWA);
- Remote Procedure Call (RPC);
- Application Programming Interface (API);
- Messaging Application Programming Interface (MAPI);
- PowerShell;
- Autodiscover; and
- Microsoft-Server-ActiveSync.

Network defenders should include these interfaces when defending against EBurst.

Persistence

To establish persistence, the threat actors install virtual private network (VPN) software clients on victim devices [T1133] to obfuscate command and control (C2) communications or other actions, further preventing victims from attributing malicious network activity.

The threat actors typically download SoftEther installers onto victim devices from threat actor-controlled infrastructure using PowerShell or LOTL binaries for Windows Systems [T1059.001]. For Linux/Unix distributions, the threat actors download SoftEther installers via `curl` or `wget`. For either operating system, the actors configure the SoftEther client to automatically reconnect on startup. They often name the installers `conhost.exe` or `dllhost.exe` to appear as common Windows executables [T1036.003]. Additionally, endpoint detection software is less likely to flag SoftEther because it is a legitimate VPN software.

In some observed cases, the threat actors stored the SoftEther program directly on the server. Analysis of these servers revealed victim domains and subdomains that hosted the SoftEther connections:

- 98aiblog[.]com;
- hmbcloud[.]com;
- hmbcloud[.]net;
- hmbiplc-01[.]com;
- iepl.node[.]cm;
- javacheck.ooguy[.]com;
- javaupdate.giize[.]com;
- sexytube0[.]com; and
- twimg.co[.]uk.

The threat actors use SoftEther to maintain persistent remote access to victim devices to enable data exfiltration. The FBI observed the threat actors installing the client on the end-user's system, which connected to the C2 server using one of the identified domains, subdomains, or the server's IP address. The threat actors also accessed other targets, including cybersecurity websites, connected to these hubs.

Collection and Exfiltration

The FBI observed the threat actors downloading databases or manually pulling data from the victim emails and staging the exfiltration data with discreet file names to minimize detection of the MySQL email dump. Some of these names include:

- 001.gif;
- All_scanner_vXX.pl.gz (XX represents either a one- or two-digit number);
- Css.js;
- Include.png;
- M2k.js;
- M2k_list.js; and
- M2k_ui_adm.js.

Curlc4.txt

The FBI observed that the threat actors created a bot using the PHP script Curlc4.txt to obtain emails from victims. The script is specifically designed to interface with the Microsoft EWS API, which allows the threat actors to access email and content items, such as calendars and contacts [T1114.002].

Based on observations, the script appears to be stand-alone rather than installed on a compromised device. The script uploaded emails to a remote server [T1020], obfuscating many of the directories and files it created, and changed the name of the child process to **crypto**.

The script downloaded the original file from [https://upl.natcloudservice\[.\]com](https://upl.natcloudservice[.]com) using IP address **149.28.132[.]137**. The main C2 domain for the bot was natcloudservice[.]com, and the domain communicated with [https://natcloudservice\[.\]com/ews](https://natcloudservice[.]com/ews) and [upl.natcloudservice\[.\]com/ews](https://upl.natcloudservice[.]com/ews). Before exfiltration, the bot compressed emails. In some instances, the threat actor also used a password to encrypt emails using RC4 or AES-128-CBC [T1560.003].

The PHP script took up to two command-line arguments. The first argument appeared to be the root directory where the scripts execute. If the first argument was not supplied, then the script searched for a writeable directory [T1074.001] to use as its directory. The script searched the directories listed in **Table 1** until it found a writeable one. The script stored the second command-line argument in a variable saved to the targeted system.

*Table 1. Directories Searched by **Curlc4***

Directory to Search	Subdirectories to Skip
/	/bin, /boot, /dev, /etc, /run, /proc, /sys, /var, /tmp, /usr
/home	
/var/www	
/usr	
/var/tmp	

The following is a list of unique strings found in the script:

- \$dir/storage/fm/.run;
- \$dir/.run;
- public \$password='jh4jnryw76ikmh';
- public \$file='/var/tmp/.sess.zip';
- [https://upl.natcloudservice\[.\]com/ews](https://upl.natcloudservice[.]com/ews);
- public \$key='rhnr5m54pk65wertc';
- \$this->enc="r";this->cipher="rc4";this->iv="";

- `$this->enc="a";this->cipher="aes-128-cbc";this->iv="1111111111111111";`
- `https://natcloudservice[.]com/ews;` and
- `curl_setopt($this->ch, CURLOPT_HTTPHEADER,array("X-Id: $clientid")).`

Other directories and files that indicate this script may be executed on a system include:

- `RUNNING_DIRECTORY/storage/fm;`
- `RUNNING_DIRECTORY /storage/fm.run` (file);
- `RUNNING_DIRECTORY /.run;`
- `RUNNING_DIRECTORY/clientid` (file); and
- `RUNNING_DIRECTORY/cp` (file).

DC.exe

The threat actors used `DC.exe` to execute the DCSync replication technique [T1003.006] to copy sensitive information from the Active Directory (AD), including account credentials, group membership details, and trust relationships. `DC.exe` used a Remote Procedure Call (RPC) binding to the victim's domain controller. The file then used the Directory Replication Service to retrieve data from the victim's AD. Specifically, it retrieved a handle to the local security policy object, which is used to query the domain controller for the DNS domain name, domain security identifier (SID), and domain replication epoch. The file also used the following object IDs to retrieve information about Active Directory attributes and configurations:

- | | |
|---------------------------|------------------------------|
| ▪ 1.2.840.113556.1.2.48; | ▪ 1.2.840.113556.1.4.27; |
| ▪ 1.2.840.113556.1.4.1; | ▪ 1.2.840.113556.1.4.302; |
| ▪ 1.2.840.113556.1.4.125; | ▪ 1.2.840.113556.1.4.55; |
| ▪ 1.2.840.113556.1.4.129; | ▪ 1.2.840.113556.1.4.609; |
| ▪ 1.2.840.113556.1.4.133; | ▪ 1.2.840.113556.1.4.656; |
| ▪ 1.2.840.113556.1.4.135; | ▪ 1.2.840.113556.1.4.8; |
| ▪ 1.2.840.113556.1.4.146; | ▪ 1.2.840.113556.1.4.90; |
| ▪ 1.2.840.113556.1.4.159; | ▪ 1.2.840.113556.1.4.94; and |
| ▪ 1.2.840.113556.1.4.160; | ▪ 1.2.840.113556.1.4.96. |
| ▪ 1.2.840.113556.1.4.221; | |

Data Exfiltration

The FBI recovered an archived email database the threat actors used to target email accounts of victim organizations. The threat actors collect account credentials and exfiltrate victim email data from on-premise systems and cloud-based services. Observed victims of email data theft included government organizations, law enforcement agencies, healthcare systems, and religious institutions located in Southeast Asia. In some instances, the threat actors restricted access to the exfiltrated data to only IP addresses from Xiamen, China.

Office-cli Program

The threat actors use a command-line utility `office-cli` [T1059.004] to continuously target and access Microsoft Outlook 365 email accounts to exfiltrate emails across different time periods. The threat actors occasionally update these accounts and swap them for the most recent accounts. The threat actors use `office-cli` to automate access and exfiltration of mail content using configuration files, such as `client_id`, `tenant_id`, and `secret`.

The FBI observed the threat actors executing `office-cli` from the command line or by running it from a Bash script. In both instances, the threat actors place the JSON files required to access the mailboxes in the config directory. Additionally, `office-cli` saves data gathered from the victims in a subdirectory of the dump directory. The threat actors evade detection when using this program by using legitimate access methods.

The threat actors maintain a custom web application that provides third-party access to stolen email content. Users of this application can pass specific arguments in URLs to see email content for specific accounts.

Indicators of Compromise

See **Appendix A: Indicators of Compromise** for a list of all observed indicators.

MITRE ATT&CK Tactics and Techniques

See **Table 2** to **Table 9** for all referenced threat actor tactics and techniques in this advisory. For assistance with mapping malicious cyber activity to the MITRE ATT&CK framework, see CISA and MITRE ATT&CK's [Best Practices for MITRE ATT&CK Mapping](#) and CISA's [Decider Tool](#).

Table 2. Reconnaissance

Technique Title	ID	Use
Active Scanning: Vulnerability Scanning	T1595.002	The threat actors leverage several scanning tools to find vulnerabilities in networks and web-based applications.

Table 3. Initial Access

Technique Title	ID	Use
Drive-by Compromise	T1189	The threat actors execute XSS attacks to leverage an unwitting third-party application to modify content on a webpage.

Table 4. Execution

Technique Title	ID	Use
Command and Scripting Interpreter: PowerShell	T1059.001	The threat actors typically download SoftEther installers onto victim devices from threat actor controlled infrastructure using PowerShell.
Command and Scripting Interpreter: Unix Shell	T1059.004	The threat actors use <code>office-cli</code> , a Linux-based binary, to continuously target and access Microsoft Outlook 365 accounts. <code>Office-cli</code> automates exfiltration of mail content using configuration files, including account credentials.
Command and Scripting Interpreter: Python	T1059.006	The threat actors gain access to victim networks and cloud-based services primary through command-line utility tools based on exploit codes written in Python.
Command and Scripting Interpreter: JavaScript	T1059.007	The threat actors use JavaScript to execute XSS attacks.

Table 5. Persistence

Technique Title	ID	Use
External Remote Services	T1133	The threat actors install VPN software clients on victim devices to establish persistence and obfuscate C2 communications.

Table 6. Defense Evasion

Technique Title	ID	Use
Masquerading: Rename Legitimate Utilities	T1036.003	The threat actors run executables with the same name of a known, legitimate Windows software and installers to evade detection.

Table 7. Credential Access

Technique Title	ID	Use
OS Credential Dumping: DCSync	T1003.006	The threat actors use <code>DC.exe</code> to execute the DCSync replication technique to copy sensitive information from the Active Directory.
Brute Force: Password Guessing	T1110.001	The threat actors use <code>eburst.py</code> to conduct password guessing to compromise email accounts on Microsoft Exchange servers.

Technique Title	ID	Use
Brute Force: Password Spraying	T1110.003	The threat actors use <code>eburst.py</code> to conduct password spraying to compromise email accounts on Microsoft Exchange servers.

Table 8. Collection

Technique Title	ID	Use
Email Collection: Remote Email	T1114.002	The threat actors use the PHP script to interface with the Microsoft EWS API, enabling them to access email and content items.
Archive Collection Data: Archive via Custom Method	T1560.003	The threat actors use a custom bot to compress, and in some cases encrypt, files prior to exfiltration.
Data Staged: Local Data Staging	T1074.001	The PHP script searches for a writeable directory to use as its directory.

Table 9. Exfiltration

Technique Title	ID	Use
Automated Exfiltration	T1020	The threat actors leverage the PHP script to automatically upload emails to a remote server.

Incident Response

If a potential compromise is detected, organizations should take the following actions:

1. **Determine which hosts were compromised and isolate them** by quarantining or taking them offline.
2. **Initiate threat hunting activities to scope the intrusion.**
 - a. Collect and review relevant artifacts, logs, and other data to identify threat actor TTPs, compromised devices and accounts, a timeline of activity, etc.
3. **Follow national guidelines and requirements in your country on reporting cyber incidents** (see **Contact Information**).
4. **Apply eviction countermeasures** to contain the incident and eradicate the threat actor from the network.
 - a. Start applying countermeasures after collecting enough threat hunting data to inform effective countermeasure selection; this will likely overlap with threat hunting activities):
 - b. Use CISA's [Eviction Strategies Tool](#) to assemble countermeasures for a systematic eviction plan—the tool comprises **Playbook-NG** (a web application) and **COUN7ER** (a database of post-compromise countermeasures mapped to adversary TTPs).

- i. Use Playbook-NG and COUN7ER together to assemble a systematic eviction plan, or playbook, that leverages distinct countermeasures to contain and evict cyber threat actors.
- ii. The playbook features a list of recommended response actions based on threat actor TTPs and includes each action's intended outcome, preparatory steps, and associated risks. For more information, see CISA's [Eviction Strategies Tool Fact Sheet](#).

5. Harden the network to prevent additional malicious activity (see **Mitigations** for guidance).

Mitigations

The authoring organizations recommend network defenders and organizations implement the mitigations below to improve your organization's cybersecurity posture on the basis of the threat actors' activity. These mitigations align with the [Cross-Sector Cybersecurity Performance Goals \(CPGs\)](#) developed by CISA and the National Institute of Standards and Technology (NIST). The CPGs provide a minimum set of practices and protections that CISA and NIST recommend all organizations implement. CISA and NIST based the CPGs on existing cybersecurity frameworks and guidance to protect against the most common and impactful threats and TTPs. Visit CISA's [CPGs webpage](#) for more information on the CPGs, including additional recommended baseline protections.

The authoring organizations recommend network defenders and organizations implement these mitigations:

- **Disable unused services and ports**, such as automatic configuration, remote access, or file sharing protocols.
 - Configure applications to reveal as little information as possible when serving login pages or banner information in response to external requests.
 - Consider using an attack surface management service or web-based search platforms that search the internet to identify exposed services or ports [\[CPG 3.S\]](#). For additional support, follow CISA's [Internet Exposure Reduction Guidance](#) and NSA's [Attack Surface Management](#).
- **Sanitize user input in web applications** to prevent possible XSS payload injection.
- **Implement identity, credential, and access management (ICAM) policies across the organization and then require multifactor authentication (MFA)** [\[CPG 3.F\]](#) for all services (to the extent possible), particularly for webmail, VPNs, and accounts that access critical systems.
- **Replace default passwords with strong passwords** [\[CPG 3.A\]](#).
 - Limit and audit user accounts with administrative privileges and configure access controls with least privilege in mind.
 - Ensure only users that need administrator privileges are granted these privileges, and regularly review access to assess whether it is still required [\[CPG 3.G\]](#).
- **Enable download and domain reputation screening** in web browsers, along with protective DNS resolution, to block downloads of known malware and connections to websites and domains with unsafe reputations.
- **Monitor for signs of unauthorized use of LOTL tools** and unexpected Active Directory replication [\[CPG 4.B\]](#).

- **Implement network segmentation** to ensure a compromised device has no access to sensitive resources of another organizational unit [\[CPG 3.I\]](#).
 - Use the principle of least privilege to provide just enough connectivity for devices to perform their intended functions [\[CPG 3.H\]](#).
 - For a less resource constrictive mitigation, organizations may segment edge devices internally.
- **Monitor cloud accounts** for connected applications that can access sensitive data in file systems and email data.
- **Review web application access logs for signs of exploitation attempts**, such as malicious directory traversal attempts, command injection attempts, or enumeration attempts [\[CPG 3.Q\]](#).
- **Apply patches and updates**, including software and firmware updates (regular patching mitigates many high-risk security vulnerabilities) [\[CPG 2.B\]](#).
 - If available, use automatic update channels from trusted network locations.
 - Do not trust email messages claiming to provide software updates as attachments or via links to untrusted websites.
- **Install and regularly update antivirus software** on all hosts and enable real time detection.
- **Monitor for abnormal and high volumes of unexpected traffic** (scanning) using firewalls and/or intrusion detection systems [\[CPG 4.B\]](#).
 - Since an attempted compromise using a distributed denial of service (DDoS) technique may appear as normal traffic, it is critical for organizations to define, monitor, and prepare for abnormal traffic volumes.
- **Monitor for high volumes of outbound or upload traffic from workstations** or other devices that usually have low volumes of uploads compared to downloads.
- **Monitor logs and investigate unusual IP addresses and ports** in command lines, registry entries, and firewall logs to identify other hosts that are potentially involved in actor actions [\[CPG 3.Q\]](#).
 - Review perimeter firewall configurations for unauthorized changes and/or entries that may permit external connections to internal hosts.
- **Monitor for abnormal account activity**, such as logons outside of normal working hours and impossible time and distance logons (e.g., a user logging on from two geographically separated locations at the same time) [\[CPG 4.B\]](#).
- **Implement a recovery plan to maintain and retain multiple copies** of sensitive or proprietary data and servers in a physically separate, segmented, and secure location (i.e., hard drive, storage device, or the cloud) [\[CPG 1.C\]](#).
- **Regularly back up data and password protect backup copies offline** [\[CPG 3.O\]](#).
 - Ensure copies of critical data are not accessible for modification or deletion from the system where data resides.
- **Replace end-of-life products** with supported alternatives that are included in vendor support plans.
- **Ensure systems use the strongest feasible form of authentication** [\[CPG 3.B\]](#); [\[CPG 3.F\]](#).
- **Harden authentication protocols and access lists** [\[CPG 3.H\]](#).

- Regularly rotate keys for your service accounts, use strong key lengths to enhance security and minimize the risk of key compromise, and implement role-based access control (RBAC) to avoid granting excess privileges.
- **Provide cyber security awareness and training** [[CPG 3.J](#)].
 - Regularly train users on information security principles and techniques, as well as overall emerging cybersecurity risks and vulnerabilities (e.g., ransomware and phishing scams).
- **Regularly engage reputable and skilled penetration testing services** to evaluate your public attack surface and remediate the most commonly exploited vulnerabilities used by these actors.

Validate Security Controls

In addition to applying mitigations, the authoring organizations recommend exercising, testing, and validating your organization's security program against the threat behaviors mapped to the MITRE ATT&CK for Enterprise framework in this advisory. The authoring organizations recommend testing your existing security controls inventory to assess how they perform against the ATT&CK techniques described in this advisory.

To get started:

1. Select an ATT&CK technique described in this advisory (see **Table 2** to **Table 9**).
2. Align your security technologies against the technique.
3. Test your technologies against the technique.
4. Analyze your detection and prevention technologies' performance.
5. Repeat the process for all security technologies to obtain a set of comprehensive performance data.
6. Tune your security program, including people, processes, and technologies, based on the data generated by this process.

The authoring organizations recommend continually testing your security program, at scale, in a production environment to ensure optimal performance against the MITRE ATT&CK techniques identified in this advisory.

Resources

- For more information on attack surface management, see:
 - CISA's [Internet Exposure Reduction Guidance](#);
 - CISA's [Cyber Hygiene Services](#) for US critical infrastructure; and
 - NSA's [Attack Surface Management](#) for the US Defense Industrial Base (DIB).
- For additional information on the UK's National Cyber Security Centre's (NCSC-UK's) resources see:
 - [Network Security Fundamentals](#);
 - [Protective DNS Service](#);
 - Guidance [Selecting Right Methods to Authenticate Customers](#);

- Guidance [Ransomware-Resistant Backups](#); and
- Penetration testing guidance, see [Penetration Testing](#).
- For more information on sanitizing user input, see:
 - CISA's [Secure by Design Alert: Eliminating Cross Site Scripting Vulnerabilities](#);
 - The Open Worldwide Application Security Project's (OWASP) [Input Validation Cheat Sheet](#); and
 - OWASP's [Cross-Site Scripting Prevention Cheat Sheet](#).
- For more information on protective DNS (PDNS), see:
 - NSA and CISA's guidance [Selecting a Protective DNS Service](#); and
 - NSA's [Protective DNS Service](#) offerings for the US Defense Industrial Base.
- For more information on LOTL, see ASD's ACSC and CISA's joint guidance [Identifying and Mitigating Living Off the Land Techniques](#).
- For more information on defending Active Directory, see ASD's ACSC's joint guidance [Detecting and Mitigating Active Directory Compromises](#).
- For more information on Canadian Cyber Centre resources, see:
 - [Phishing-resistant MFA](#);
 - [Top 10 security actions on network segmentation](#);
 - [Top 10 security actions for patching OS and applications](#);
 - [Obsolete products](#) (end-of-life);
 - [Preventative security tools](#); and
 - [Best practices with passphrases and passwords](#).

Contact Information

US organizations are encouraged to report suspicious or criminal activity related to information in this advisory to the FBI, CISA, and/or NSA:

- File a claim with FBI's [Internet Crime Complaint Center \(IC3\)](#) or contact your local [FBI field office](#), or contact CISA via CISA's 24/7 Operations Center at contact@cisa.dhs.gov or 1-844-Say-CISA (1-844-729-2472). 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; and
 - Name of the submitting company or organization, and a designated point of contact.
- For NSA cybersecurity guidance inquiries, contact CybersecurityReports@nsa.gov.

United Kingdom organizations: Report a significant cyber security incident at ncsc.gov.uk/report-an-incident (monitored 24 hours) or, for urgent assistance, call 03000 200 973.

Australian organizations: Visit cyber.gov.au or call 1300 292 371 (1300 CYBER 1) to report cybersecurity incidents and access alerts and advisories.

Canadian organizations: Report incidents by emailing the Canadian Centre for Cyber Security (Cyber Centre) at contact@cyber.gc.ca, (613) 949-7048, or 1-833-CYBER-88.

Japan organizations: Report an incident to the National Cybersecurity Office (NCO) via email at first-team@cyber.go.jp or the National Police Agency's (NPAs) web portal at <https://www.npa.go.jp/bureau/cyber/soudan.html>.

New Zealand organizations: Visit ncsc.govt.nz or call 0800 114 115 to report cyber security incidents.

Disclaimer

The information in this report is being provided “as is” for informational purposes only. The authoring organizations do not endorse any commercial entity, product, company, or service, including any entities, products, or services linked within this document. Any reference to specific commercial entities, products, processes, or services by service mark, trademark, manufacturer, or otherwise, does not constitute or imply endorsement, recommendation, or favoring by the authoring organizations.

Version History

October 8, 2026: Initial version.

Appendix A: Indicators of Compromise

See **Table 10** to **Table 15** for a list of observed IOCs. The IOCs listed in the appendices may or may not be addressed in detail in the body of this document; however, endpoint detection systems can ingest all of these IOCs to help mitigate threat activity.

Disclaimer: Several of the observed IOCs date back to as early as 2016. The authoring organizations recommend investigating or vetting these IOCs prior to taking action, such as blocking.

Note: The first and last dates are included in this table, with an asterisk (*) denoting the WHOIS registry expiration date specified within.

Table 10. Domain Names

Domain	First Seen	Last Seen
_msdcs.cktime.ooguy[.]com	12/26/2023	7/30/2024
067[.]cz	12/6/2018	1/16/2021
1421.client.96html[.]com	1/18/2019	1/18/2027*
1421.cloud.96html[.]com	1/18/2019	1/18/2027*
1421.support.96html[.]com	1/18/2019	1/18/2027*
154-119-131-252-103-58-216-162-36.m.secshow[.]net	6/26/2023	6/26/2026*
20656.hus1.ptps[.]tk	12/5/2019	7/24/2021
20656.hus3.ptps[.]tk	12/5/2019	7/24/2021
2-12-44-140-78-81-211-109-241.h.secshow[.]net	6/26/2023	6/26/2026*
22852.careers.96html[.]com	1/18/2019	1/18/2027*
22852.careers.trendmicro.96html[.]com	1/18/2019	1/18/2027*
22852.trendmicro.96html[.]com	1/18/2019	1/18/2027*
23175.careers.96html[.]com	1/18/2019	1/18/2027*
23175.careers.trendmicro.96html[.]com	1/18/2019	1/18/2027*
24280.hus1.ptps[.]tk	12/5/2019	7/24/2021
2637596418.softether[.]net	9/22/2023	6/22/2024

Domain	First Seen	Last Seen
28394.careers.96html[.]com	1/18/2019	1/18/2027*
28394.careers.trendmicro.96html[.]com	1/18/2019	1/18/2027*
28394.trendmicro.96html[.]com	1/18/2019	1/18/2027*
28733.careers.trendmicro.96html[.]com	1/18/2019	1/18/2027*
28733.trendmicro.96html[.]com	1/18/2019	1/18/2027*
30773.hus2.ptps[.]tk	12/5/2019	7/24/2021
30773.hus3.ptps[.]tk	12/5/2019	7/24/2021
35584.careers.96html[.]com	1/18/2019	1/18/2027*
35584.careers.trendmicro.96html[.]com	1/18/2019	1/18/2027*
35584.trendmicro.96html[.]com	1/18/2019	1/18/2027*
39583.b.alitagotest[.]cf	1/27/2020	12/7/2021
3w.feeee[.]jio	2/8/2024	2/8/2025
44673.careers.96html[.]com	1/18/2019	1/18/2027*
44673.trendmicro.96html[.]com	1/18/2019	1/18/2027*
47298.96html[.]com	1/18/2019	1/18/2027*
47298.client.96html[.]com	1/18/2019	1/18/2027*
47298.cloud.96html[.]com	1/18/2019	1/18/2027*
47298.support.96html[.]com	1/18/2019	1/18/2027*
50669.careers.trendmicro.96html[.]com	1/18/2019	1/18/2027*
51640.careers.trendmicro.96html[.]com	1/18/2019	1/18/2027*
51943.hus1.ptps[.]tk	12/5/2019	7/24/2021
51943.hus3.ptps[.]tk	12/5/2019	7/24/2021

Domain	First Seen	Last Seen
54-2-32-236-208-2-40-107-38.h.secshow[.]net	6/26/2023	6/26/2026*
60928.hus1.ptps[.]tk	12/5/2019	7/24/2021
66-37-178-96-110-2-40-107-38.h.secshow[.]net	6/26/2023	6/26/2026*
74788.careers.96html[.]com	1/18/2019	1/18/2027*
74788.trendmicro.96html[.]com	1/18/2019	1/18/2027*
77692.careers.96html[.]com	1/18/2019	1/18/2027*
77692.careers.trendmicro.96html[.]com	1/18/2019	1/18/2027*
77692.trendmicro.96html[.]com	1/18/2019	1/18/2027*
82262.careers.96html[.]com	1/18/2019	1/18/2027*
82262.careers.trendmicro.96html[.]com	1/18/2019	1/18/2027*
85005.careers.96html[.]com	1/18/2019	1/18/2027*
85005.careers.trendmicro.96html[.]com	1/18/2019	1/18/2027*
85005.trendmicro.96html[.]com	1/18/2019	1/18/2027*
88783.hus1.ptps[.]tk	12/5/2019	7/24/2021
90174.careers.96html[.]com	1/18/2019	1/18/2027*
90174.careers.trendmicro.96html[.]com	1/18/2019	1/18/2027*
96976.careers.96html[.]com	1/18/2019	1/18/2027*
96976.trendmicro.96html[.]com	1/18/2019	1/18/2027*
96cee[.]com	1/7/2016	5/9/2024
96html[.]com	1/18/2019	9/3/2024
98aiblog[.]com	3/11/2024	3/12/2026*
a.alitagotest[.]cf	1/27/2020	12/7/2021

Domain	First Seen	Last Seen
a.studiocloud[.]xyz	12/31/2021	12/3/2024
admin.dellme[.]ml	3/20/2020	8/8/2020
alitagotest[.]cf	1/27/2020	12/7/2021
arforcex[.]com	3/5/2019	5/11/2021
asean.twimg.co[.]uk	9/21/2024	12/15/2024
az.studiocloud[.]xyz	12/31/2021	12/3/2024
b.alitagotest[.]cf	1/27/2020	12/7/2021
bailbonding[.]info	1/3/2020	1/3/2022
bbs.sunmoon[.]website	9/20/2023	9/20/2024
bj-hk.hmbcloud[.]net	3/29/2021	3/29/2021
bj-jp.hmbcloud[.]net	4/10/2021	5/7/2021
blog.98aiblog[.]com	7/12/2024	8/14/2024
bsnl.twimg.co[.]uk	6/17/2024	7/7/2024
careers.96html[.]com	1/18/2019	1/18/2027*
careers.trendmicro.96html[.]com	1/18/2019	1/18/2027*
cch.ooguy[.]com	10/11/2024	10/11/2024
check.96html[.]com	1/18/2019	1/18/2027*
checkapi[.]tk	1/6/2022	4/10/2023
checkinfo[.]tk	9/22/2012	12/14/2022
chr0mail[.]com	6/23/2021	6/23/2026*
cktime.ooguy[.]com	12/26/2023	7/30/2024
client.96html[.]com	1/18/2019	1/18/2027*

Domain	First Seen	Last Seen
cloud.96html[.]com	1/18/2019	1/18/2027*
csrfproxy.studiocloud[.]xyz	12/31/2021	12/3/2024
dasxcyb[.]ga	1/29/2021	1/29/2021
dc-29465b27aa45.96html[.]com	1/18/2019	1/18/2027*
dc-4fe9871cb224.96html[.]com	1/18/2019	1/18/2027*
dc-582fc0f46da9.96html[.]com	1/18/2019	1/18/2027*
dc-843d98722400.96html[.]com	1/18/2019	1/18/2027*
dc-bb503834b7dc.96html[.]com	1/18/2019	1/18/2027*
dc-c11a983d7f83.96html[.]com	1/18/2019	1/18/2027*
dellme[.]ml	3/20/2020	8/8/2020
dns.studiocloud[.]xyz	12/10/2021	5/9/2024
dns361[.]tk	2/7/2022	11/19/2023
dsdsei[.]com	4/10/2018	4/10/2025
eck.giize[.]com	9/28/2024	9/30/2024
eg.twimg.co[.]uk	9/22/2024	12/14/2024
etechhosting.twimg.co[.]uk	9/21/2024	12/16/2024
fcchk.twimg.co[.]uk	9/21/2024	12/14/2024
feeee[.]io	2/8/2024	2/8/2025
findfindx[.]com	1/6/2022	8/10/2023
fukua[.]org	11/24/2017	11/24/2027*
gate.sinica.edu.tw.checkapi[.]cf	1/6/2022	4/10/2023
googles.ddns[.]net	10/22/2021	10/22/2021

Domain	First Seen	Last Seen
gz-hk.hmbcloud[.]net	12/28/2020	1/22/2021
h.secshow[.]net	6/26/2023	6/26/2026*
h5.feeee[.]io	2/8/2024	2/8/2025
halloween.checkapi[.]cf	1/6/2022	4/10/2023
helpuself.ptps[.]tk	12/5/2019	7/24/2021
hgiga.96html[.]com	1/18/2019	1/18/2027*
honey1314520[.]com	11/23/2020	11/23/2022
hook.studiocloud[.]xyz	12/31/2021	12/3/2024
hus1.ptps[.]tk	12/5/2019	7/24/2021
hus3.ptps[.]tk	12/5/2019	7/24/2021
hw1.ptps[.]tk	12/5/2019	7/24/2021
ica.96html[.]com	1/18/2019	1/18/2027*
im.arforcex[.]com	3/4/2019	3/5/2026*
imap.sunmoon[.]website	9/20/2023	9/20/2024
info.96html[.]com	1/18/2019	1/18/2027*
integritytoch[.]com	12/11/2020	12/11/2022
iplc-hk.hmbcloud[.]com	11/30/2020	12/8/2020
javacheck.ooguy[.]com	12/22/2023	6/25/2024
javaupdate.giize[.]com	12/22/2023	6/15/2024
just.checkapi[.]cf	1/6/2022	4/10/2023
kk.dasxcyb[.]ga	1/29/2021	1/29/2021
leicc009[.]ga	5/24/2020	4/24/2021

Domain	First Seen	Last Seen
live.studiocloud[.]xyz	12/31/2021	12/3/2024
ls.twimg.co[.]uk	9/21/2024	12/14/2024
m.secshow[.]net	6/26/2023	6/26/2026*
ma.studiocloud[.]xyz	12/31/2021	12/3/2024
mail.bailbonding[.]info	1/3/2020	1/3/2022
mail.sunmoon[.]website	9/20/2023	9/20/2024
masaplus[.]club	7/22/2021	7/22/2024
microscan[.]me	12/10/2017	12/10/2018
mitt.96html[.]com	1/18/2019	1/18/2027*
ms.studiocloud[.]xyz	12/31/2021	12/3/2024
msedge[.]store	11/9/2023	11/9/2025
mx.sunmoon[.]website	9/20/2023	9/20/2024
natcloudservice[.]com	9/8/2023	9/8/2024
nikoes[.]gq	6/15/2021	3/22/2023
np.twimg.co[.]uk	9/21/2024	11/25/2024
ns1.alitagotest[.]cf	1/27/2020	12/7/2021
ns1.honey1314520[.]com	11/23/2020	11/23/2022
ns1.nikoes[.]gq	6/15/2021	3/22/2023
ns2.nikoes[.]gq	6/15/2021	3/22/2023
one.hmbiplc-01[.]com	4/2/2022	4/2/2022
payment.feeee[.]io	2/8/2024	2/8/2025
pdc._msdcs.cktime.ooguy[.]com	12/26/2023	7/30/2024

Domain	First Seen	Last Seen
ptps[.]tk	12/5/2019	7/24/2021
puc.checkapi[.]tk	1/6/2022	4/10/2023
purple76[.]com	11/11/2021	11/11/2026*
pw.sexytube0[.]com	8/6/2021	4/18/2024
pw2.sexytube0[.]com	10/7/2017	10/8/2027*
random.cktime.ooguy[.]com	12/26/2023	7/30/2024
s3crts.softether[.]net	3/25/2021	7/27/2022
scallpay[.]com	7/3/2023	7/3/2024
search.96html[.]com	1/18/2019	1/18/2027*
secretr.feieee[.]io	2/8/2024	2/8/2025
secshow[.]net	6/26/2023	6/26/2026*
senate.twimg.co[.]uk	9/21/2024	12/14/2024
server.feieee[.]io	2/8/2024	2/8/2025
sexytube0[.]com	10/7/2017	10/8/2027*
shifuj[.]com	6/3/2019	6/5/2019
sh-jp.hmbcloud[.]net	4/10/2021	4/25/2021
shop.96html[.]com	1/18/2019	1/18/2027*
shopify.feieee[.]io	2/8/2024	2/8/2025
smtp.sunmoon[.]website	9/20/2023	9/20/2024
streescans[.]com	5/10/2022	3/4/2025
studiocloud[.]xyz	12/10/2021	5/9/2024
sunmoon[.]website	9/20/2023	9/20/2024

Domain	First Seen	Last Seen
supper.feeeee[.]io	2/8/2024	2/8/2025
support.96html[.]com	1/18/2019	1/18/2027*
szxcm-hkg01.iepl.node[.]cm	12/7/2020	1/8/2021
t.checkinfo[.]tk	9/22/2012	12/14/2022
teyan.microscan[.]me	12/10/2017	12/10/2018
tj.twimg.co[.]uk	9/21/2024	12/14/2024
traffic.96html[.]com	1/18/2019	1/18/2027*
trendmicro.96html[.]com	1/18/2019	1/18/2027*
trust[.]feeee	2/8/2024	2/8/2025
tsedws[.]com	6/1/2020	6/1/2026*
txt.studiocloud[.]xyz	12/31/2021	12/3/2024
update.96html[.]com	1/18/2019	1/18/2027*
upgrate.checkapi[.]cf	1/6/2022	4/10/2023
upl.natcloudservice[.]com	9/8/2023	9/8/2024
v3.streescans[.]com	5/10/2022	3/4/2025
vnpt.sexytube0[.]com	10/7/2017	10/8/2027*
vpn21.arforcex[.]com	3/4/2019	3/5/2026*
vpn328433596.softether[.]net	3/28/2023	10/17/2024
vpn614174689.softether[.]net	9/2/2023	9/2/2023
vpn677190427.softether[.]net	4/17/2024	4/30/2024
vpn718535264.softether[.]net	3/11/2022	3/11/2022
vpn823494147.softether[.]net	6/26/2023	6/26/2023

Domain	First Seen	Last Seen
wanfang.accesscam[.]org	9/18/2024	9/26/2024
webdisk.bailbonding[.]info	1/3/2020	1/3/2022
webmail.studiocloud[.]xyz	12/31/2021	12/3/2024
well.96html[.]com	1/18/2019	1/18/2027*
ws.studiocloud[.]xyz	12/31/2021	12/3/2024
wss.studiocloud[.]xyz	12/31/2021	12/3/2024
www.96html[.]com	1/18/2019	1/18/2027*
www.alitagotest[.]cf	1/27/2020	12/7/2021
www.chr0mail[.]com	6/23/2021	6/23/2026*
www.cktime.ooguy[.]com	12/26/2023	7/30/2024
www.dns361[.]tk	2/7/2022	11/19/2023
www.feeee[.]io	2/8/2024	2/8/2025
www.javacheck.ooguy[.]com	6/17/2024	7/25/2024
www.leicc009[.]ga	5/24/2020	4/24/2021
www.msedge[.]store	11/9/2023	11/9/2025
www.mx.sunmoon[.]website	9/20/2023	9/20/2024
www.purple76[.]com	11/11/2021	11/11/2026*
www.smtp.sunmoon[.]website	9/20/2023	9/20/2024
www.sofeter[.]ml	3/13/2023	3/13/2023
www.studiocloud[.]xyz	12/31/2021	12/3/2024
www.sunmoon[.]website	9/20/2023	9/20/2024
www.www.smtp.sunmoon[.]website	9/20/2023	9/20/2024

Domain	First Seen	Last Seen
www.www.sunmoon[.]website	9/20/2023	9/20/2024
xassxxdns.alitagotest[.]cf	1/27/2020	12/7/2021
ximmd.sexytube0[.]com	7/14/2020	10/31/2020
zerogravity1986.softether[.]net	12/9/2023	12/9/2023

Table 11. IP Addresses

IP Address	First Seen	Last Seen
1.34.140[.]5	3/15/2023	3/20/2023
2.58.242[.]74	12/2/2024	12/2/2024
5.188.34[.]134	8/30/2024	9/12/2024
5.188.230[.]69	8/7/2023	4/19/2024
8.219.119[.]5	9/12/2024	9/12/2024
14.1.98[.]160	3/22/2024	4/28/2024
14.128.33[.]8	12/4/2023	1/9/2024
14.1.98[.]223	6/20/2023	10/9/2023
27.154.215[.]126	7/11/2023	7/11/2023
27.154.105[.]36	2/3/2024	2/3/2024
27.149.115[.]78	3/22/2023	3/22/2023
27.149.79[.]35	3/23/2023	3/23/2023
31.232.221[.]35	5/14/2024	5/17/2024
36.112.10[.]102	9/4/2023	9/12/2024
36.112.188[.]119	8/13/2023	8/13/2023
36.112.186[.]135	8/14/2023	8/14/2023

IP Address	First Seen	Last Seen
36.112.206[.]121	8/12/2023	8/13/2023
36.249.156[.]117	11/29/2023	11/29/2023
36.249.156[.]122	11/15/2023	11/18/2023
36.249.156[.]159	5/31/2023	6/5/2023
36.249.156[.]178	5/22/2023	12/6/2023
36.249.156[.]205	11/13/2023	11/13/2023
36.249.156[.]206	11/23/2023	11/24/2023
36.249.156[.]220	6/7/2022	6/7/2022
36.249.156[.]226	5/8/2023	5/13/2023
36.112.200[.]35	8/9/2023	8/10/2023
36.249.156[.]51	11/20/2023	11/22/2023
36.112.198[.]68	8/13/2023	8/13/2023
36.249.156[.]69	5/31/2023	5/31/2023
36.112.10[.]99	9/19/2024	9/19/2024
39.72.220[.]221	3/20/2023	3/20/2023
42.73.98[.]232	5/13/2024	5/13/2024
45.123.189[.]19	11/16/2021	2/14/2022
45.32.140[.]182	1/8/2021	1/8/2021
45.32.232[.]146	12/18/2020	12/25/2020
45.63.123[.]142	6/4/2021	7/25/2024
45.63.116[.]190	11/20/2019	11/20/2019
45.131.69[.]197	3/31/2023	3/31/2023

IP Address	First Seen	Last Seen
45.76.169[.]12	5/11/2020	5/13/2020
45.77.195[.]169	6/12/2020	6/16/2020
45.32.61[.]246	11/11/2024	12/16/2024
45.77.231[.]209	1/25/2024	6/5/2024
45.76.37[.]168	12/20/2019	12/20/2019
45.63.59[.]121	3/19/2020	3/19/2020
45.77.11[.]47	9/29/2020	9/29/2020
45.32.84[.]223	4/23/2020	5/9/2020
45.63.62[.]217	10/28/2020	11/4/2020
45.63.48[.]36	1/10/2020	1/10/2020
45.76.43[.]37	2/17/2020	2/27/2020
45.76.66[.]19	4/16/2024	5/6/2024
45.76.243[.]67	7/1/2020	7/9/2020
45.63.17[.]9	5/9/2024	6/19/2024
45.77.28[.]77	12/5/2021	4/3/2023
45.76.194[.]89	11/22/2021	9/25/2023
45.76.37[.]85	2/10/2020	2/10/2020
45.63.95[.]62	4/10/2020	4/13/2020
45.63.94[.]71	9/30/2019	12/16/2024
45.77.86[.]70	12/21/2019	12/23/2019
49.93.136[.]14	3/25/2024	3/25/2024
49.93.184[.]194	3/25/2024	3/25/2024

IP Address	First Seen	Last Seen
59.120.144[.]153	5/24/2023	5/25/2023
59.124.120[.]178	2/20/2023	9/27/2023
59.120.167[.]25	1/15/2024	1/15/2024
59.125.128[.]54	3/30/2023	10/7/2023
59.120.58[.]176	3/8/2022	3/8/2022
60.250.199[.]112	11/15/2022	12/1/2022
60.250.146[.]19	11/17/2022	12/18/2023
60.251.155[.]19	1/4/2023	9/23/2023
60.248.152[.]204	5/11/2023	5/16/2023
59.120.82[.]67	11/22/2023	1/8/2024
60.184.242[.]224	3/23/2023	3/23/2023
60.251.205[.]37	12/20/2021	12/23/2021
60.220.43[.]193	10/3/2023	10/3/2023
60.251.58[.]145	6/8/2023	1/22/2024
60.248.1[.]64	12/8/2022	4/23/2023
60.251.201[.]8	5/16/2023	3/5/2024
60.248.88[.]151	6/8/2023	2/26/2024
60.248.110[.]97	3/31/2023	1/4/2024
60.249.239[.]86	9/18/2021	1/5/2022
61.220.112[.]137	5/25/2023	5/26/2023
60.220.84[.]41	2/9/2024	2/9/2024
61.247.165[.]27	4/8/2022	4/11/2022

IP Address	First Seen	Last Seen
60.220.84[.]63	10/1/2023	10/1/2023
61.220.35[.]15	5/24/2023	9/7/2023
61.221.55[.]4	5/24/2024	11/13/2024
61.222.245[.]73	4/11/2023	7/25/2023
61.219.118[.]99	12/1/2022	11/23/2023
61.216.74[.]97	1/29/2024	1/29/2024
64.176.38[.]35	8/30/2024	12/16/2024
65.20.97[.]251	1/25/2024	6/5/2024
66.42.103[.]188	11/26/2019	11/26/2019
66.42.42[.]109	7/11/2024	8/20/2024
66.42.40[.]189	9/4/2024	12/16/2024
66.42.36[.]236	2/28/2024	7/25/2024
66.42.60[.]242	2/23/2024	12/16/2024
66.42.77[.]138	2/9/2022	6/19/2024
77.111.226[.]5	4/19/2023	4/19/2023
78.141.221[.]241	2/29/2020	3/10/2020
78.141.238[.]97	1/25/2024	6/5/2024
84.17.57[.]40	4/4/2023	4/4/2023
89.187.163[.]216	9/19/2024	9/19/2024
95.179.189[.]106	6/4/2020	6/4/2020
95.179.235[.]135	1/27/2021	1/27/2021
95.179.186[.]251	2/2/2021	2/2/2021

IP Address	First Seen	Last Seen
98.159.37[.]4	7/4/2024	7/4/2024
103.107.198[.]117	9/26/2023	9/26/2023
103.16.231[.]220	3/7/2022	7/4/2024
103.16.231[.]254	11/9/2022	2/10/2023
103.233.253[.]197	3/19/2023	9/6/2023
103.25.254[.]210	10/28/2019	11/26/2019
103.149.200[.]44	4/25/2023	10/11/2023
103.179.45[.]203	9/23/2024	12/16/2024
103.73.160[.]232	3/17/2023	3/17/2023
103.77.211[.]193	5/8/2024	5/8/2024
103.106.230[.]88	6/25/2024	6/25/2024
103.172.80[.]35	11/26/2022	11/30/2022
104.238.149[.]146	3/6/2020	7/8/2024
104.238.182[.]153	6/24/2020	7/1/2020
104.238.152[.]209	2/24/2022	4/2/2022
103.51.145[.]98	4/26/2023	5/28/2023
103.73.162[.]99	3/17/2023	11/20/2023
104.156.231[.]98	5/29/2020	6/2/2020
106.53.181[.]231	5/31/2024	5/31/2024
106.122.171[.]92	1/31/2024	1/31/2024
108.61.181[.]104	7/11/2024	12/12/2024
108.61.177[.]81	1/25/2024	6/5/2024

IP Address	First Seen	Last Seen
110.42.10[.]148	4/10/2021	5/5/2021
110.85.170[.]125	2/10/2020	2/10/2020
111.203.153[.]245	11/5/2023	11/5/2023
110.74.172[.]80	10/29/2021	2/17/2022
111.55.138[.]141	7/4/2024	7/4/2024
111.55.137[.]40	7/5/2024	7/5/2024
111.203.153[.]95	11/5/2023	11/5/2023
112.5.168[.]102	2/21/2022	2/21/2022
112.5.168[.]104	3/29/2021	3/29/2021
112.5.145[.]154	6/29/2023	6/29/2023
112.5.143[.]161	6/27/2023	6/27/2023
112.5.168[.]138	4/24/2022	4/24/2022
112.5.168[.]151	7/20/2023	8/4/2023
112.5.168[.]160	10/31/2023	11/9/2023
112.54.132[.]162	7/3/2023	7/5/2023
112.5.168[.]187	8/27/2021	8/27/2021
112.5.168[.]218	8/31/2023	9/1/2023
112.5.168[.]231	8/16/2023	8/17/2023
112.5.168[.]234	6/5/2023	6/16/2023
112.5.168[.]238	4/6/2023	5/18/2023
112.51.26[.]151	6/26/2023	6/29/2023
112.66.108[.]16	8/14/2023	8/14/2023

IP Address	First Seen	Last Seen
112.5.168[.]29	11/11/2021	11/11/2021
112.51.44[.]102	7/10/2023	7/18/2023
112.51.44[.]142	6/16/2023	6/16/2023
112.51.44[.]143	11/21/2023	11/21/2023
112.51.44[.]188	12/15/2022	12/20/2022
112.51.44[.]189	12/4/2023	12/4/2023
112.51.44[.]20	11/27/2023	11/29/2023
112.51.44[.]206	9/6/2023	9/22/2023
112.51.44[.]217	8/6/2022	8/6/2022
112.51.44[.]234	4/24/2022	5/5/2022
112.5.168[.]65	3/18/2022	3/21/2022
112.51.44[.]37	7/21/2023	8/2/2023
112.80.50[.]138	6/5/2024	6/5/2024
112.51.44[.]57	7/4/2023	7/5/2023
112.5.168[.]93	3/26/2020	3/26/2020
113.76.136[.]171	3/23/2023	3/23/2023
114.246.237[.]111	6/4/2024	6/4/2024
114.255.70[.]18	6/30/2022	9/1/2023
114.255.70[.]20	9/24/2023	7/16/2024
114.255.70[.]30	5/26/2023	7/14/2023
114.246.93[.]103	4/18/2023	4/18/2023
114.246.94[.]102	11/19/2023	1/11/2024

IP Address	First Seen	Last Seen
114.35.122[.]83	3/28/2024	12/13/2024
114.246.94[.]154	6/9/2024	6/10/2024
114.246.92[.]58	6/8/2023	6/8/2023
114.246.92[.]71	8/23/2023	9/11/2023
117.133.51[.]176	3/21/2024	3/21/2024
117.61.244[.]135	10/15/2020	10/15/2020
117.56.214[.]246	6/8/2023	7/4/2023
117.132.198[.]70	7/5/2024	7/5/2024
117.92.127[.]132	3/24/2023	3/24/2023
117.130.201[.]90	3/21/2024	3/21/2024
118.163.217[.]199	3/12/2024	4/17/2024
118.163.197[.]241	5/12/2023	10/16/2023
118.163.31[.]226	5/16/2024	5/28/2024
118.163.104[.]67	3/11/2024	12/6/2024
118.163.142[.]80	3/20/2024	3/22/2024
118.163.3[.]76	3/18/2024	10/29/2024
119.116.159[.]217	3/24/2023	3/24/2023
119.13.79[.]145	3/20/2023	3/21/2023
120.233.10[.]212	4/2/2022	4/2/2022
120.36.251[.]100	12/21/2023	12/21/2023
120.36.248[.]104	1/2/2024	1/2/2024
120.42.128[.]165	3/19/2023	3/19/2023

IP Address	First Seen	Last Seen
120.36.250[.]103	10/20/2023	5/31/2024
120.36.254[.]100	8/19/2021	8/19/2021
120.36.248[.]109	5/11/2021	5/11/2021
120.36.253[.]106	1/12/2023	1/12/2023
120.36.255[.]105	10/29/2021	11/1/2021
120.36.251[.]110	3/7/2024	3/7/2024
120.36.251[.]11	6/12/2024	6/13/2024
120.36.249[.]114	3/7/2022	3/10/2022
120.36.251[.]114	1/4/2024	1/8/2024
120.36.254[.]112	12/26/2022	12/26/2022
120.36.249[.]121	6/19/2024	6/19/2024
120.36.249[.]122	9/28/2022	9/28/2022
120.36.254[.]119	8/19/2021	8/19/2021
120.36.254[.]120	10/25/2023	10/27/2023
120.36.249[.]127	2/10/2023	2/14/2023
120.36.251[.]130	10/18/2021	10/21/2021
120.36.255[.]127	8/5/2022	8/6/2022
120.36.252[.]13	3/31/2023	3/31/2023
120.36.250[.]133	7/11/2022	7/14/2022
120.36.250[.]134	7/15/2021	7/15/2021
120.36.250[.]135	2/25/2022	3/3/2022
120.36.254[.]131	6/30/2023	6/30/2023

IP Address	First Seen	Last Seen
120.36.254[.]135	8/27/2021	8/27/2021
120.36.251[.]141	12/13/2022	12/13/2022
120.36.250[.]142	1/12/2024	1/12/2024
120.41.125[.]225	7/11/2023	7/11/2023
120.36.253[.]148	8/5/2021	8/11/2021
120.36.250[.]152	5/23/2024	5/24/2024
120.36.252[.]151	11/15/2023	11/15/2023
120.36.253[.]152	4/12/2021	5/19/2023
120.36.254[.]151	3/21/2024	3/22/2024
120.36.255[.]153	9/25/2023	9/26/2023
120.36.252[.]157	1/28/2023	1/28/2023
120.37.162[.]246	3/21/2023	3/21/2023
120.36.252[.]166	9/6/2024	9/6/2024
120.36.249[.]172	10/17/2022	10/21/2022
120.36.253[.]169	12/10/2021	12/10/2021
120.36.252[.]175	2/23/2023	2/23/2023
120.36.254[.]175	5/31/2022	5/31/2022
120.36.251[.]179	5/17/2021	5/24/2021
120.36.253[.]178	4/28/2021	4/29/2021
120.36.252[.]18	5/9/2024	5/9/2024
120.36.252[.]181	4/21/2021	4/27/2021
120.36.248[.]185	2/26/2024	2/26/2024

IP Address	First Seen	Last Seen
120.36.253[.]180	5/15/2024	5/17/2024
120.36.255[.]179	3/19/2024	3/20/2024
120.36.253[.]186	2/27/2024	3/4/2024
120.36.253[.]187	9/24/2021	9/24/2021
120.36.250[.]19	10/9/2021	10/9/2021
120.36.251[.]19	5/24/2021	5/24/2021
120.36.251[.]190	8/29/2023	8/31/2023
120.36.255[.]189	6/21/2023	6/27/2023
120.41.244[.]15	1/25/2024	1/25/2024
120.36.254[.]192	7/6/2021	7/7/2021
120.36.249[.]197	8/13/2021	8/16/2021
120.36.248[.]200	11/17/2022	11/17/2022
120.36.253[.]195	11/22/2023	11/24/2023
120.36.251[.]2	3/4/2022	3/4/2022
120.36.251[.]20	4/25/2022	4/25/2022
120.36.255[.]196	6/3/2024	6/3/2024
120.36.251[.]202	12/24/2021	12/24/2021
120.36.254[.]202	8/23/2021	8/25/2021
120.36.250[.]207	7/14/2023	7/19/2023
120.36.250[.]210	12/15/2023	12/15/2023
120.36.249[.]213	5/9/2022	5/13/2022
120.36.251[.]213	10/13/2023	10/16/2023

IP Address	First Seen	Last Seen
120.36.253[.]212	4/24/2022	4/24/2022
120.36.251[.]215	4/19/2023	4/19/2023
120.36.252[.]215	9/8/2022	9/8/2022
120.36.255[.]214	10/7/2023	10/7/2023
120.36.250[.]221	11/2/2023	11/2/2023
120.36.255[.]22	3/26/2024	3/28/2024
120.36.251[.]230	12/4/2023	12/4/2023
120.36.255[.]228	11/8/2021	11/11/2021
120.36.253[.]23	11/7/2023	11/7/2023
120.36.253[.]231	12/1/2022	12/1/2022
120.36.251[.]234	10/12/2021	10/12/2021
120.36.248[.]237	12/28/2021	12/28/2021
120.36.253[.]232	3/31/2023	3/31/2023
120.36.253[.]233	4/15/2024	4/20/2024
120.36.249[.]238	9/20/2022	9/22/2022
120.36.251[.]237	2/18/2022	2/24/2022
120.36.255[.]233	2/6/2024	2/6/2024
120.36.255[.]237	6/15/2022	6/21/2022
120.36.249[.]245	5/24/2022	5/25/2022
120.36.252[.]242	3/5/2024	3/6/2024
120.36.255[.]24	9/8/2023	9/8/2023
120.36.249[.]248	7/23/2021	7/23/2021

IP Address	First Seen	Last Seen
120.36.250[.]247	11/25/2021	11/30/2021
120.36.253[.]247	5/6/2021	5/6/2021
120.36.253[.]248	4/19/2021	4/20/2021
120.36.251[.]25	6/7/2024	6/11/2024
120.36.251[.]254	3/22/2021	3/28/2021
120.36.249[.]28	10/24/2022	10/28/2022
120.36.251[.]3	12/8/2021	12/8/2021
120.36.251[.]30	1/19/2022	1/21/2022
120.36.254[.]3	6/30/2021	7/5/2021
120.36.254[.]32	7/30/2024	7/30/2024
120.36.249[.]33	11/7/2022	11/7/2022
120.36.250[.]4	3/31/2021	3/31/2021
120.36.250[.]43	6/8/2021	6/8/2021
120.36.249[.]47	1/3/2023	1/3/2023
120.36.248[.]48	3/15/2021	3/18/2021
120.36.250[.]48	5/25/2023	5/25/2023
120.36.249[.]52	5/16/2022	5/20/2022
120.36.250[.]53	1/22/2024	1/22/2024
120.36.249[.]54	9/13/2022	9/15/2022
120.36.251[.]54	7/8/2021	7/9/2021
120.36.249[.]55	4/7/2024	4/7/2024
120.36.251[.]56	11/16/2022	11/17/2022

IP Address	First Seen	Last Seen
120.36.248[.]57	6/5/2023	6/5/2023
120.36.250[.]58	3/22/2022	3/25/2022
120.36.250[.]6	1/14/2022	1/19/2022
120.36.253[.]6	8/11/2021	8/12/2021
120.36.254[.]63	3/30/2023	6/11/2024
120.36.250[.]65	9/5/2023	9/6/2023
120.36.251[.]65	6/22/2022	6/23/2022
120.36.250[.]67	5/27/2021	5/27/2021
120.36.252[.]69	4/8/2024	4/12/2024
120.36.248[.]73	8/17/2021	8/17/2021
120.36.255[.]74	11/19/2021	11/25/2021
120.36.250[.]76	6/5/2024	6/6/2024
120.41.222[.]74	11/4/2023	11/4/2023
120.36.248[.]80	10/11/2022	10/12/2022
120.36.251[.]80	7/27/2021	7/28/2021
120.36.251[.]84	7/5/2022	7/5/2022
120.36.252[.]90	4/24/2024	4/25/2024
120.36.249[.]91	4/6/2021	4/9/2021
120.36.251[.]91	9/29/2022	9/29/2022
120.36.252[.]91	6/24/2022	6/27/2022
120.36.254[.]92	9/15/2023	9/20/2023
120.36.254[.]94	11/12/2021	11/18/2021

IP Address	First Seen	Last Seen
120.36.248[.]97	3/14/2022	3/18/2022
120.36.251[.]97	8/19/2021	8/19/2021
120.36.249[.]98	2/1/2023	2/3/2023
120.36.252[.]98	4/13/2022	4/15/2022
121.207.60[.]123	3/19/2023	3/19/2023
122.116.33[.]118	5/12/2023	3/5/2024
122.232.149[.]231	3/23/2023	3/23/2023
122.201.241[.]230	5/23/2023	8/3/2023
122.116.159[.]52	5/22/2023	9/25/2023
122.116.102[.]93	5/21/2024	5/21/2024
123.121.157[.]240	4/12/2022	4/12/2022
123.51.237[.]194	4/8/2024	11/4/2024
123.252.121[.]7	2/26/2024	3/4/2024
123.252.122[.]7	2/28/2024	3/4/2024
123.12.90[.]227	1/26/2023	1/26/2023
123.60.61[.]104	9/12/2024	9/12/2024
124.126.158[.]130	2/21/2024	2/21/2024
124.126.139[.]199	5/31/2023	5/31/2023
124.127.17[.]171	8/10/2023	8/11/2023
124.127.220[.]223	8/21/2023	8/21/2023
124.150.135[.]3	9/7/2023	9/7/2023
123.51.223[.]96	3/14/2023	4/18/2023

IP Address	First Seen	Last Seen
124.64.22[.]13	12/11/2023	12/11/2023
124.126.141[.]74	4/23/2023	4/23/2023
124.127.78[.]22	8/15/2023	8/16/2023
124.127.72[.]52	8/12/2023	8/12/2023
125.227.147[.]106	11/1/2023	12/5/2023
125.227.140[.]168	3/18/2024	11/12/2024
125.227.1[.]220	5/25/2023	11/14/2023
125.227.196[.]157	1/19/2024	1/29/2024
125.227.219[.]145	3/6/2024	7/1/2024
125.228.239[.]13	4/2/2024	12/2/2024
125.227.218[.]2	5/16/2024	5/16/2024
124.64.23[.]80	7/7/2023	7/7/2023
125.229.172[.]48	5/23/2024	5/23/2024
125.227.136[.]60	5/11/2023	2/28/2024
137.220.34[.]137	12/16/2020	12/17/2020
137.220.39[.]222	1/21/2021	1/25/2021
137.220.43[.]47	7/17/2020	7/24/2020
137.220.36[.]87	3/16/2023	7/7/2024
138.199.62[.]148	12/5/2024	12/14/2024
139.180.137[.]219	1/25/2024	6/5/2024
139.180.217[.]19	6/5/2024	6/19/2024
139.180.158[.]51	12/13/2021	7/8/2024

IP Address	First Seen	Last Seen
139.84.174[.]129	6/17/2024	12/16/2024
140.82.27[.]163	1/2/2020	1/8/2020
140.82.50[.]151	3/5/2021	3/17/2021
141.164.41[.]128	4/11/2023	7/8/2024
140.82.48[.]6	7/13/2020	7/17/2020
141.164.55[.]227	9/4/2024	12/16/2024
141.164.56[.]93	6/20/2025	6/20/2025
144.202.26[.]205	5/14/2020	5/14/2020
144.34.171[.]162	3/29/2023	11/28/2023
144.202.33[.]164	9/17/2020	9/27/2020
144.202.62[.]109	10/16/2019	10/28/2019
144.202.91[.]107	10/19/2020	10/27/2020
144.202.94[.]216	8/17/2020	8/18/2020
144.202.98[.]41	11/18/2020	11/18/2020
147.139.133[.]246	5/26/2023	6/6/2023
149.28.132[.]137	2/23/2024	7/5/2024
149.28.132[.]161	5/17/2024	7/4/2024
149.28.201[.]146	11/20/2020	12/11/2020
149.28.188[.]184	11/21/2019	11/21/2019
149.248.34[.]100	6/5/2020	6/5/2020
149.28.149[.]29	4/30/2024	4/30/2024
149.28.252[.]19	11/18/2019	11/18/2019

IP Address	First Seen	Last Seen
149.248.38[.]179	6/3/2020	6/3/2020
149.248.39[.]202	6/8/2023	2/29/2024
149.248.44[.]191	2/23/2024	5/10/2024
149.248.51[.]22	1/25/2024	6/5/2024
149.28.72[.]106	2/24/2023	3/2/2023
155.138.155[.]170	2/4/2021	2/4/2021
155.138.136[.]190	12/5/2019	12/16/2019
155.138.151[.]225	6/5/2024	6/5/2024
155.138.133[.]56	1/25/2024	6/5/2024
156.146.45[.]152	9/21/2024	9/21/2024
156.146.45[.]194	9/19/2024	9/19/2024
158.247.197[.]28	6/25/2023	9/26/2023
159.138.152[.]61	3/16/2023	3/22/2023
162.14.178[.]86	3/29/2021	5/7/2021
167.172.33[.]16	4/14/2023	4/14/2023
167.179.87[.]215	11/21/2022	6/20/2025
167.179.97[.]121	12/14/2022	3/20/2023
171.120.88[.]137	9/27/2023	9/27/2023
178.62.208[.]162	4/14/2023	4/14/2023
180.122.149[.]177	3/22/2023	3/22/2023
182.34.19[.]234	3/23/2023	3/23/2023
183.240.139[.]216	12/7/2020	1/8/2021

IP Address	First Seen	Last Seen
183.253.28[.]104	2/27/2024	2/27/2024
183.253.29[.]110	5/6/2024	5/10/2024
183.253.28[.]121	12/6/2023	12/14/2023
183.250.213[.]20	4/3/2023	4/3/2023
183.253.29[.]189	8/9/2024	8/9/2024
183.250.213[.]55	9/26/2023	10/11/2023
183.253.29[.]66	3/25/2024	3/28/2024
183.253.28[.]67	10/12/2024	10/12/2024
183.250.213[.]80	3/3/2023	3/31/2023
183.250.213[.]83	3/24/2023	3/24/2023
183.166.90[.]97	3/20/2023	3/20/2023
185.216.118[.]71	6/7/2024	7/2/2024
185.135.73[.]192	1/4/2022	1/5/2022
185.213.82[.]239	6/27/2024	7/3/2024
185.213.82[.]243	6/28/2024	6/28/2024
185.213.82[.]55	10/16/2024	10/16/2024
185.213.82[.]65	9/21/2023	9/21/2023
190.92.241[.]15	3/20/2023	3/27/2023
191.232.188[.]144	6/23/2022	6/23/2022
193.42.24[.]68	11/28/2024	11/28/2024
193.42.25[.]73	3/24/2024	7/11/2024
198.13.38[.]211	7/5/2024	7/5/2024

IP Address	First Seen	Last Seen
202.182.109[.]151	6/1/2024	9/13/2024
202.101.145[.]22	3/23/2023	3/23/2023
202.182.106[.]31	1/25/2024	7/2/2024
202.39.151[.]239	3/8/2024	12/5/2024
202.99.19[.]250	7/10/2023	7/10/2023
202.99.19[.]254	7/13/2023	7/13/2023
203.74.126[.]20	3/28/2023	3/31/2023
203.69.36[.]122	4/1/2024	12/12/2024
207.246.118[.]144	10/21/2022	12/15/2022
207.246.117[.]149	3/24/2020	3/27/2020
207.246.114[.]173	10/30/2019	10/30/2019
207.148.68[.]131	1/25/2024	6/5/2024
207.148.122[.]69	1/25/2024	6/5/2024
207.148.67[.]146	1/6/2021	1/20/2021
207.246.108[.]64	1/16/2020	1/16/2020
207.246.127[.]64	9/12/2019	9/6/2024
207.148.73[.]238	6/14/2023	9/13/2024
207.148.92[.]220	4/25/2024	7/5/2024
207.148.4[.]96	9/30/2019	5/18/2023
208.72.154[.]55	4/24/2022	5/17/2022
210.242.152[.]155	3/26/2024	12/12/2024
210.242.38[.]241	3/14/2023	1/15/2024

IP Address	First Seen	Last Seen
210.243.225[.]41	5/14/2024	11/29/2024
210.66.220[.]39	10/18/2021	10/21/2021
210.242.76[.]32	5/23/2024	5/23/2024
210.71.166[.]50	6/3/2024	6/11/2024
211.20.144[.]116	5/16/2024	5/19/2024
211.20.104[.]187	5/21/2024	5/21/2024
211.21.19[.]11	3/6/2024	4/2/2024
211.22.143[.]228	7/27/2023	7/27/2023
211.20.115[.]60	2/27/2023	3/5/2024
211.20.154[.]60	3/18/2024	4/1/2024
211.20.100[.]78	12/21/2023	12/22/2023
211.20.100[.]79	12/22/2023	12/22/2023
211.99.103[.]102	12/1/2020	12/8/2020
211.21.61[.]46	4/2/2024	4/29/2024
211.75.185[.]37	10/30/2023	1/4/2024
211.99.103[.]243	12/28/2020	1/22/2021
212.107.28[.]16	9/9/2022	9/9/2022
212.107.28[.]22	9/9/2022	9/9/2022
212.107.28[.]23	9/9/2022	9/9/2022
211.78.84[.]17	12/27/2023	12/27/2023
211.20.91[.]77	4/17/2024	4/18/2024
211.99.100[.]90	4/8/2021	4/8/2021

IP Address	First Seen	Last Seen
211.99.100[.]91	4/9/2021	4/9/2021
211.99.98[.]197	11/30/2020	11/30/2020
216.128.149[.]106	12/15/2022	2/22/2023
216.128.128[.]238	2/21/2021	2/21/2021
218.26.159[.]254	10/5/2023	10/5/2023
218.5.173[.]137	3/22/2023	3/22/2023
218.5.157[.]171	3/20/2023	3/20/2023
218.66.163.188	3/24/2023	3/24/2023
219.143.179[.]250	7/10/2023	7/13/2023
220.128.108[.]164	10/28/2022	7/19/2023
220.130.153[.]127	4/3/2023	12/18/2023
220.130.176[.]23	12/18/2023	3/1/2024
220.128.125[.]3	3/8/2023	5/9/2023
220.130.254[.]251	12/13/2023	12/13/2023
219.92.229[.]53	5/15/2023	5/15/2023
220.162.9[.]150	3/20/2023	3/23/2023
220.250.44[.]62	6/28/2023	6/29/2023
221.218.143[.]112	2/29/2024	3/11/2024
221.218.136[.]12	7/16/2023	8/9/2023
221.218.138[.]123	5/23/2024	5/23/2024
221.218.143[.]122	6/4/2023	7/3/2023
221.218.143[.]184	7/5/2023	7/12/2023

IP Address	First Seen	Last Seen
221.218.136[.]192	10/8/2023	11/15/2023
221.216.116[.]238	4/24/2024	4/24/2024
221.218.137[.]229	6/4/2024	6/4/2024
221.218.139[.]248	1/18/2024	1/24/2024
221.216.208[.]188	6/19/2023	6/19/2023
221.218.142[.]26	5/9/2024	5/13/2024
221.218.141[.]96	4/2/2024	4/3/2024
222.92.153[.]125	6/6/2024	6/6/2024
223.104.40[.]128	4/16/2024	4/16/2024
223.104.41[.]13	4/18/2024	4/18/2024
223.104.40[.]142	4/17/2024	4/17/2024
223.104.40[.]204	4/19/2024	4/19/2024
223.27.34[.]132	4/10/2024	12/13/2024
223.104.55[.]183	7/3/2024	7/3/2024
223.104.39[.]82	7/11/2023	7/11/2023

Table 12 shows observed domain names attributed to this threat activity and obfuscation network hosts.

Table 12. Domain Names Attributed to Threat Activity and Obfuscation Network Hosts

Name	Type	First Seen	Last Seen
96cee[.]com	Infrastructure	6/29/2020	5/9/2024
asean.twimg.co[.]uk	SoftEther Host	9/21/2024	12/15/2024
bj-hk.hmbcloud[.]net	SoftEther Host	3/29/2021	3/29/2021
bj-jp.hmbcloud[.]net	SoftEther Host	4/10/2021	5/7/2021

Name	Type	First Seen	Last Seen
blog.98aiblog[.]com	SoftEther Host	7/12/2024	8/14/2024
bsnl.twimg.co[.]uk	SoftEther Host	6/17/2024	7/7/2024
dns.studiocloud[.]xyz	Infrastructure	12/10/2021	5/9/2024
eg.twimg.co[.]uk	SoftEther Host	9/22/2024	12/14/2024
etechhosting.twimg.co[.]uk	SoftEther Host	9/21/2024	12/16/2024
fcchk.twimg.co[.]uk	SoftEther Host	9/21/2024	12/14/2024
gz-hk.hmbcloud[.]net	SoftEther Host	12/28/2020	1/22/2021
iplc-hk.hmbcloud[.]com	SoftEther Host	11/30/2020	12/8/2020
javacheck.ooguy[.]com	SoftEther Host	12/22/2023	6/25/2024
javaupdate.giize[.]com	SoftEther Host	12/22/2023	6/15/2024
ls.twimg.co[.]uk	SoftEther Host	9/21/2024	12/14/2024
np.twimg.co[.]uk	SoftEther Host	9/21/2024	11/25/2024
one.hmbiplc-01[.]com	SoftEther Host	4/2/2022	4/2/2022
pw.sexytube0[.]com	SoftEther Host	8/6/2021	4/18/2024
senate.twimg.co[.]uk	SoftEther Host	9/21/2024	12/14/2024
sh-jp.hmbcloud[.]net	SoftEther Host	4/10/2021	4/25/2021
studiocloud[.]xyz	Infrastructure	12/10/2021	5/9/2024
szxcm-hkg01.iepl.node[.]cm	SoftEther Host	12/7/2020	1/8/2021
tj.twimg.co[.]uk	SoftEther Host	9/21/2024	12/14/2024
ximmd.sexytube0[.]com	SoftEther Host	7/14/2020	10/31/2020

Table 13 contains known webshells from the threat actor's repository of CNE tooling, which may appear on a compromised system. The threat actors have used these webshell files for unauthorized access to victim environments.

Table 13. Leveraged Webshells

Name	Hashes
b374.php	MD5: 48ca18a25424a0f52276290b619a7a83 SHA-256: 72c6af6a4be99e31c4a7a0aa4f01750792788e7f6f9749243a9f2c47c14a708f
back.pl	MD5: 38f5ff8169423e2c756848c02e8cac3b SHA-256: 456586ababa08f70216c4459f4d6375676166ebfddd98a33b447ceb5099e8dc5
error.jsp	MD5: d61326c4e6d24aa9b67e2b7a3ef7cedf SHA-256: 2f5c406eb64ad8902c8e30610d43fd3efc05a14cdb8fb158818953eaf3dc6a81
file_back.aspx	MD5: f8de2e99dc7523d2c83d1a48e844c5ff SHA-256: 5782ff2c835c88cc1ee521d2e8c523cfad73db3f9a29c93b40c4223f0338ade9
gf.phtml	MD5: 5b5a2c7fa705d8b1eb04da5db900b0d7 SHA-256: 0e6fecb2d369b0eae63731616a3daada52036634885ab1b85b115af6bc5bcb86
yaml-payload.jar	MD5: 655cd134976d3e80c521708aa8be418b SHA-256: 36f3b7645609ef40444dbc68f01d26c543d67689eda4937272ea5cfa4df1b522

Table 14 contains known binaries and scripts from the threat actor's repository of CNE tooling. The threat actors used these utilities to perform various scanning or computer intrusion tasks.

Table 14. Leveraged Binaries and Scripts

Name	Category	Hashes
ksubdomain	Enumeration	MD5: dae8f50ea44225fae3ba1f160b42bfdc SHA-256: 670fa10a2ddde21fd594c4fef86b554d864089ed2de7153b472e921c623403ae
ksubdomain_linux	Enumeration	MD5: fdece34bc084f1e252aeae274650eb8d SHA-256: 645f6f2667af01a94d04a9d7a71916a13d9426835d636b4ceee2e25ccb34e525
oneforall.py	Enumeration	MD5: 596b990b0b389d906a8f4384837c1878 SHA-256: 4d488f21269b18e37aaca93ac2a61707c9b611e506cdb3b287277746e94636b5

Name	Category	Hashes
subDomainsBrute.py	Enumeration	MD5: a73eca669fe80628dbbd2c7d9bb14c8f SHA-256: a14844e982f172d0f23910558c3f390a9d4c45dc32db825c2af7cf0ed8631db2
office-cli	Information dump	MD5: be121e707f817aa9392c55af1e7ec2aa SHA-256: add7dd142e4f7e2873bc8f7b7fb6308063608e0b49a773dea93abad4047f1489
JuicyPotato.exe	Privilege escalation	MD5: 7ce68f0dd85355ba2897a68521167e56 SHA-256: e7e727458f573dded05537baddac2867d2801db1c3c74410398d063dfd6f6575
BBSan.py	Scanning	MD5: f82694de2f19e1bff333c27bb7eb7a56 SHA-256: 8e1b56ef51ba70aa4c4cfd4430820f20875b354588d5d723ba4d3940ea6c924b
dirmap.py	Scanning	MD5: 1933c314041415939331fce183939547 SHA-256: 46e59172c40c95d83c3a6f24f801fc2265653c8b575b66a726463e2a4eebd7f2
dirsearch.py	Scanning	MD5: 8829f6f1cc5fc0aab2f6e71bfd7dc53d SHA-256: 752b14c6e6936991d51fcd5ebf40d303e657c2372893604f96044848ad9a5f24
fscan.exe	Scanning	MD5: cf903e4a1629aa0582fd0363b5786676 SHA-256: 7b9efc7ef8957411cdd22582ce4bfb3a5f76d9c91cdb7e36bf85c9785a2480e9
nbtscan.exe	Scanning	MD5: f01a9a2d1e31332ed36c1a4d2839f412 SHA-256: c9d5dc956841e000bfd8762e2f0b48b66c79b79500e894b4efa7fb9ba17e4e9e
nbtscan_linux	Scanning	MD5: ef713447f18f5b7ee16af4ac37ec4133 SHA-256: 2fbcbb1995c458e5affd5fb8f1f979a08ddce21714a2e413aa3d5dc44f9f245fe
PackerFuzzer.py	Scanning	MD5: 8dcc4f9ccc6b6adf7eeeb3f51c95afad SHA-256: 33790218d5871af646feef5be29e0596d4703a45ce675c1eb2ca00140b3a1bde

Name	Category	Hashes
ShuiZe.py	Scanning	MD5: b04375cca637f0702bf27feaff22a92d SHA-256: c7f86a4623db5c90273cea041d43207849c5c6b0060c370b2095f13871b1366d
sqlmap.py	Scanning	MD5: bcacc7ca999980d26c186ef791242fb5 SHA-256: 2ecb51d7fa3bc3fa7ad7df64c6d0cd1f4ff2b37ed6839d3cff529fb08af49fb0
wpscan	Scanning	MD5: 1b8e29b6b7972fb124425aaa257f8f6d SHA-256: efb0437e6a6a0f07169952f1a8b734299ec9a8b1faadbed811fe017f2cf54976

Table 15 contains known files that the threat actors dropped onto victim systems and used to install unauthorized software, dump sensitive information, or enable other follow-on activity from within a victim's network.

Table 15. Potentially Dropped Files

Name	Category	Hashes
curlc4.txt	Malware	MD5: 4f61b9ab907f351bb40b37b10f4974d0 SHA-256: 8b869a5edaff74ff18bca3658a519a19771e66d00ff7849af7a142dd6fc8da85
DiagTrack.exe	Malware	MD5: 6d57c42dee8bd7789969e2dd28671162 SHA-256: 804a53be802378a8ec4c94602fd3d6584e0d472d83148e8a42c731950fec415d
live700_v1.exe	Malware	MD5: 776807750280daad05348f931a33e4ef SHA-256: c4503db6ece93eddf4511e787607cb14606a1df9f526f1e39992497119437cec
conhost.exe	SoftEther	MD5: a973c0ab904c1b74655a906b99b76850 SHA-256: b1552703ff0035f197c22cdb3a514bb6aa45ec98de3ef5409faab0978f18c35e

Name	Category	Hashes
dllhost.exe	SoftEther	MD5: f62cbbdbdf35c7790909c26c7c5fbce05 SHA-256: 8a592e22c51311d482272ec5aba0103c9cd0cfd78e5b5ba75dfa8f1c56926672
dllhost.exe	SoftEther	MD5: a05cdf6afcb107961307f59cbab5e4f SHA-256: 86f1cfa6a2e0a8cb6fc1fbee28472308e6467932f8658a6a4885e29ed8c34a67
b.exe	Information dump	MD5: 7d5a182f70bed0e4fa2f8615aba070de SHA-256: e93244080a749b521f63476343ce3c81cc8c1b672fa0d9e67359aee37544c784
dc.exe	Information dump	MD5: 1bcaef76b2063f1b80b0fa0d277ec9c5 SHA-256: 9dc85f9569a15eaf51c7d34254767ea30dd67b2178cec4cc7125288b9544fe00
secretsdump.exe	Information dump	MD5: 4d33bfb75e27fefaa72526899604d557 SHA-256: 644decabc6ce8c52382f4755fa6fc2cb4d89a0e7ec0e574c11b398a6f2eed04b1
secretsdump.py	Information dump	MD5: fc6e8ca41cf4f6100177352660e520b4 SHA-256: 67db57a1f957031b78f29aa91e2e87780eae3835290259eff846d8f14afb794b

Appendix B: Observed Common Vulnerabilities and Exposures

Table 16 displays successfully exploited common vulnerabilities and exposures (CVEs). The asterisk (*) indicates CVEs that were newly added to CISA's [Known Exploited Vulnerabilities \(KEV\) Catalog](#).

Table 16. Successfully Exploited CVEs

CVE	Vendor	Product	Versions Affected	Vulnerability Type
CVE-2014-6278 [Common Weakness Enumeration (CWE)-78: Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')]	GNU	Bash	Through 4.3 bash43-026	Remote code execution
CVE-2015-3306 * [CWE-284: Improper Access Control]	ProFTPD	Proftpd	1.3.5	Unauthorized read
CVE-2015-5477 * [CWE-19: Data Processing Errors]	ISC	BIND 9.x	Before 9.9.7-P2 and 9.10.x before 9.10.2-P3	Denial of service
CVE-2016-3081 * [CWE-77: Improper Neutralization of Special Elements used in a Command ('Command Injection')]	Apache	Struts	2.3.19 to 2.3.20.2, 2.3.21 to 2.3.24.1, and 2.3.25 to 2.3.28	Remote code execution
CVE-2019-11510 [CWE-22: Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')]	Pulse Secure	Pulse Connect Secure	8.2 before 8.2R12.1, 8.3 before 8.3R7.1, and 9.0 before 9.0R3.4	Unauthorized read
CVE-2021-22205 [CWE-94: Improper Control of Generation of Code ('Code Injection')]	GitLab	GitLab	All versions starting from 11.9	Remote code execution
CVE-2021-3199 * [CWE-22: Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')]	ONLYOFFICE	DocumentServer	5.1.5 through 5.6.2	Unauthorized write
CVE-2023-22894 * [CWE-312: Cleartext Storage of Sensitive Information]	Strapi	Strapi	Up to 4.5.5	Information disclosure