JOINT
CYBERSECURITY
ADVISORY

TLP:CLEAR

Co-Authored by:

Product ID: AA23-136A

May 16, 2023

#StopRansomware: BianLian Data Extortion Group

Summary

Note: This joint Cybersecurity Advisory is part of an ongoing #StopRansomware effort to publish advisories for network defenders that detail various ransomware variants and ransomware threat actors. These #StopRansomware advisories include recently and historically observed tactics, techniques, and procedures (TTPs) and indicators of compromise (IOCs) to help organizations protect against ransomware. Visit stopransomware.gov to see all #StopRansomware advisories and to learn more about other ransomware threats and no-cost resources.

Note: This advisory, originally published May 2023, was updated November 20, 2024, with additional TTPs obtained as of June 2024 through FBI and ASD'S ACSC investigations and industry threat intelligence.

Actions to take today to mitigate cyber threats from BianLian data extortion:

- Strictly limit the use of RDP and other remote desktop services.
- Disable command-line and scripting activities and permissions.
- Restrict usage of PowerShell and update Windows PowerShell or PowerShell Core to the latest version.

The Federal Bureau of Investigation (FBI), Cybersecurity and Infrastructure Security Agency (CISA), and the Australian Signals Directorate's Australian Cyber Security Centre (ASD's ACSC) are releasing this joint Cybersecurity Advisory to disseminate known BianLian ransomware and data extortion group IOCs and TTPs identified through FBI and ASD'S ACSC investigations.

(New, November 20, 2024) The reporting agencies are aware of multiple ransomware groups, like BianLian, that seek to misattribute location and nationality by choosing foreign-language names, almost

---

U.S. Organizations: *To report suspicious or criminal activity related to information found in this joint Cybersecurity Advisory, contact your local FBI field office or CISA's 24/7 Operations Center at Report@cisa.gov or (888) 282-0870. 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.* ***Australian organizations:*** *Visit cyber.gov.au or call 1300 292 371 (1300 CYBER1) to report cybersecurity incidents and access alerts and advisories.*

certainly to complicate attribution efforts. BianLian is a ransomware developer, deployer, and data extortion cybercriminal group, likely based in Russia, with multiple Russia-based affiliates.

(Updated, November 20, 2024) BianLian group actors have affected organizations in multiple U.S. critical infrastructure sectors since June 2022. They have also targeted Australian critical infrastructure sectors in addition to professional services and property development. The group gains access to victim systems through valid Remote Desktop Protocol (RDP) credentials, uses open-source tools and command-line scripting for discovery and credential harvesting, and exfiltrates victim data via File Transfer Protocol (FTP), Rclone, or Mega. BianLian then extorts money by threatening to release data if payment is not made. BianLian group originally employed a double-extortion model in which they encrypted victims' systems after exfiltrating the data; however, they shifted primarily to exfiltration-based extortion around January 2023 and shifted to exclusively exfiltration-based extortion around January 2024.

FBI, CISA, and ASD'S ACSC encourage critical infrastructure organizations and small- and medium-sized organizations to implement the recommendations in the **Mitigations** section of this advisory to reduce the likelihood and impact of BianLian and other ransomware and data extortion incidents.

For a downloadable copy of IOCs, see AA23-136A STIX XML (XML, 35 KB)

Technical Details

Note: This advisory uses the MITRE ATT&CK® Matrix for Enterprise framework, version 16. See 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.

BianLian is a ransomware developer, deployer, and data extortion cybercriminal group. Since June 2022, FBI has observed BianLian group affecting organizations in multiple U.S. critical infrastructure sectors. In Australia, ASD'S ACSC has observed BianLian group predominately targeting private enterprises, including one critical infrastructure organization. BianLian group originally employed a double-extortion model in which they exfiltrated financial, client, business, technical, and personal files for leverage and encrypted victims' systems. In 2023, FBI observed BianLian shift primarily to exfiltration-based extortion with victims' systems left intact, and ASD'S ACSC observed BianLian shift exclusively to exfiltration-based extortion. BianLian actors warn of financial, business, and legal ramifications if payment is not made.

Initial Access

BianLian group actors gain initial access to networks by leveraging compromised Remote Desktop Protocol (RDP) credentials likely acquired from initial access brokers [T1078][T1133] or via phishing [T1566].

(New, November 20, 2024) BianLian group actors target public-facing applications of both Windows and ESXi infrastructure, possibly leveraging the ProxyShell (CVE-2021-34473, CVE-2021-34523, and CVE-2021-31207) exploit chain to gain initial access [T1190].

Command and Control

BianLian group actors implant a custom backdoor specific to each victim written in Go (see the **Indicators of Compromise** Section for an example) [T1587.001] and install remote management and access software for persistence and command and control [T1105][T1219].

FBI also observed BianLian group actors create and/or activate local administrator accounts [T1136.001] and change those account passwords [T1098].

(New, November 20, 2024) BianLian group actors may be using the reverse proxy tool Ngrok and/or a modified version of the open-source Rsocks utility [T1090]. The group may have used external proxy Rsocks to establish SOCKS5 network tunnels from victim networks and to mask the destination of C2 traffic [T1090.002].

Privilege Escalation

(New, November 20, 2024) BianLian group actors have exploited CVE-2022-37969, which affects Windows 10 and 11 systems, to escalate privileges [T1068].

Defense Evasion

BianLian group actors use PowerShell [T1059.001] and Windows Command Shell [T1059.003] to disable antivirus tools [T1562.001], specifically Windows defender and Anti-Malware Scan Interface (AMSI). BianLian actors modify the Windows Registry [T1112] to disable tamper protection for Sophos SAVEnabled, SEDEenabled, and SAVService services, which enables them to uninstall these services. See **Appendix: Windows PowerShell and Command Shell Activity** for additional information, including specific commands.

(New, November 20, 2024) BianLian group actors rename binaries and scheduled tasks after legitimate Windows services or security products [T1036.004]. BianLian group actors may pack executables using UPX to conceal their code in an attempt to bypass heuristic and signature-based detection methods [T1027.002].

Discovery

BianLian group actors use a combination of compiled tools, which they first download to the victim environment, to learn about the victim's environment. BianLian group actors have used:

- Advanced Port Scanner, a network scanner used to find open ports on network computers and retrieve versions of programs running on the detected ports [T1046].
- SoftPerfect Network Scanner (netscan.exe), a network scanner that can ping computers, scan ports, and discover shared folders [T1135].
- SharpShares to enumerate accessible network shares in a domain.
- PingCastle to enumerate Active Directory (AD) [T1482].
    - PingCastle provides an AD map to visualize the hierarchy of trust relationships.

BianLian actors also use native Windows tools and Windows Command Shell to:

- Query currently logged-in users [T1033].
- Query the domain controller to identify:
    - All groups [T1069.002].
    - Accounts in the Domain Admins and Domain Computers groups [T1087.002].
    - All users in the domain.
- Retrieve a list of all domain controllers and domain trusts.

- Identify accessible devices on the network [T1018].

See **Appendix: Windows PowerShell and Command Shell Activity** for additional information, including specific commands.

(New, November 20, 2024) BianLian group actors use PowerShell for discovery, using PowerShell scripts to list all running processes [T1057], list all software installed [T1518], and list all local drives [T1082].

Credential Access

BianLian group uses valid accounts for lateral movement through the network and to pursue other follow-on activity. To obtain the credentials, BianLian group actors use Windows Command Shell to find unsecured credentials on the local machine [T1552.001]. FBI also observed BianLian harvest credentials from the Local Security Authority Subsystem Service (LSASS) memory [T1003.001], download RDP Recognizer (a tool that could be used to brute force RDP passwords or check for RDP vulnerabilities) to the victim system, and attempt to access an AD domain database (NTDS.dit) [T1003.003].

In one case, FBI observed BianLian actors use a portable executable version of an Impacket tool (secretsdump.py) to move laterally to a domain controller and harvest credential hashes from it. **Note:** Impacket is a Python toolkit for programmatically constructing and manipulating network protocols. Through the Command Shell, an Impacket user with credentials can run commands on a remote device using the Windows management protocols required to support an enterprise network. Threat actors can run portable executable files on victim systems using local user rights, assuming the executable is not blocked by an application allowlist or antivirus solution.

See **Appendix: Windows PowerShell and Command Shell Activity** for additional information.

(New, November 20, 2024) BianLian group actors use SessionGopher, likely to extract session information for remote access tools (RATs) [T1552.004].

Persistence and Lateral Movement

BianLian group actors use PsExec and RDP with valid accounts for lateral movement [T1021.001]. Prior to using RDP, BianLian actors used Command Shell and native Windows tools to add user accounts to the local Remote Desktop Users group, modified the added account's password, and modified Windows firewall rules to allow incoming RDP traffic [T1562.004]. See **Appendix: Windows PowerShell and Command Shell Activity** for additional information.

In one case, FBI found a forensic artifact (exp.exe) on a compromised system that likely exploits the Netlogon vulnerability (CVE-2020-1472) and connects to a domain controller.

(New, November 20, 2024) In another instance, ASD'S ACSC found that BianLian group actors established network login type 3 connections to systems via Server Message Block (SMB) [T1021.002].

(New, November 20, 2024) BianLian group actors have created accounts and used them for lateral movement and persistence. In one confirmed compromise, BianLian actors created multiple domain admin accounts [T1136.002] for use in lateral movement to the domain controller. In the same compromise, the actors also created multiple Azure AD accounts [T1136.003] to maintain access to the victim systems.

(New, November 20, 2024) BianLian group actors also installed webshells [T1505.003] for persistence on a victim's Exchange server.

Collection

FBI observed BianLian group actors using malware (system.exe) that enumerates registry values [T1012] and files [T1083] and copies clipboard data from users [T1115].

(New, November 20, 2024) BianLian group actors ran PowerShell scripts to compress and/or encrypt data [T1560] that is collected prior to exfiltration.

Exfiltration and Impact

BianLian group actors search for sensitive files using PowerShell scripts (See **Appendix: Windows PowerShell and Command Shell Activity**) and exfiltrate them for data extortion. Prior to January 2023, BianLian actors encrypted files [T1486] after exfiltration for double extortion.

BianLian group uses File Transfer Protocol (FTP) [T1048] and Rclone, a tool used to sync files to cloud storage, to exfiltrate data [T1537]. FBI observed BianLian group actors install Rclone and other files in generic and typically unchecked folders such as programdata\vmware and music folders. ASD'S ACSC observed BianLian group actors use Mega file-sharing service to exfiltrate victim data [T1567.002].

(New, November 20, 2024) Prior to January 2024, BianLian used an encryptor (`encryptor.exe`) that modified all encrypted files to have the `.bianlian` extension. The encryptor created a ransom note in each affected directory. According to the ransom note, BianLian group specifically looked for, encrypted, and exfiltrated financial, client, business, technical, and personal files. (See **Figure 1** for a legacy ransomware note).

```
Your network systems were attacked and encrypted. Contact us in order to restore
your data. Don't make any changes in your file structure: touch no files, don't
try to recover by yourself, that may lead to it's complete loss.


To contact us you have to download "tox" messenger: https://qtox.github[.]io/


Add user with the following ID to get your instructions:

A4B3B0845DA242A64BF17E0DB4278EDF4BF17E0DB4278EDF85855739667D3E2AE8B89D5439015F07
E81D12D767FC


Alternative way: swikipedia@onionmail[.]org


Your ID: [Unique ID Assigned to Victim]
```

```
You should know that we have been downloading data from your network for a
significant time before the attack: financial, client, business, post, technical
and personal files.

In 10 days - it will be posted at our site
http://bianlianlbc5an4kgnay3opdemgcryg2
gnay3opdemgcryg2kpfcbgczopmm3dnbz3uaunad[.]onion with links send to your
clients, partners, competitors and news agencies, that will lead to a negative
impact on your company: potential financial, business and reputational loses.
```

Figure 1: BianLian Sample Legacy Ransom Note (Look at this `instruction.txt`)

(New, November 20, 2024) Newer ransomware notes state BianLian group has exfiltrated data and threaten to leak the exfiltrated data if the ransom is not paid. The ransom notes provide the Tox ID `88A612B3887D57A7FA3D48F5E3EDF952E4BE48E0972FC6456FBBCFF198CC8620E5609ED2D598`, which directs the victim organization to a Tox chat via https[:]//github.com/qTox/qTox/ and includes an alternative contact email addresses n0torious@onionmail[.]org and xwikipedia@onionmail[.]org. See **Figure 2** for a sample ransom note.

```
This report is left in <redacted>  internal network.

Just by quickly reviewing your files we found confidential data. The files on
your desktop are of that kind.

Leaking of folders like "Personal Data" is a disclosure of personal and medical
information of people that intrusted you to keep it. If this leak will take
place they will have to monitor their credit history and identity theft for next
3 years.

Folders like "Business files" discloses detailed financial information, supply
chain and other business information. Company competitors would be interested to
get it.

Spreading files like 'SQL' discloses all the company information exfiltrated
from SQL data bases.

Files <redacted> is screenshot made while operating in your network. It's only
an example of one among many others that we have made as proof of our job, and
as a proof of vulnerability of your network.

File <redacted> is a screen shot made from opened email archive.

Those are just examples for you to understand your near prospect.

FAQ.

- Who are you?

- BianLian team. Financial motivation only.

Our website:
http://bianlianlbc5an4kgnay3opdemgcryg2kpfcbgczopmm3dnbz3uaunad[.]onion (access
through tor browser)
```

Mirror: http://bianlivemqbawcco4cx4a672k2fip3guyxudzurfqvdszafam3ofqgqd[.]onion

- What will happen next?

Path number 1:

In 3 days we will start emailing and calling your partners and employees with notes of your company's breach and announce this data leak at our website.

During this time your data will be sorted and prepared to be published.

After that your data will be uploaded, your competitors, partners, clients, authorities, lawyer and tax agenesis would be able to access it. We will start mailing and calling your clients.

Or that will not happen, If we will close this deal in time!!!

- What should i do?

Embrace it and pay us. After that your data will be erased from our systems, with proof's provided to you. Also you might request your network improvement report.

- What should i NOT do?

1. Don't do any silly things, don't treat it lightly too. We got proofs that your data was kept with a number of data security violations of data breach laws. The penalty payments would be huge if we will anonymously sent our briefs and notes about your network structure to the regulators.

2. Based on your position in the company call your management to speak. DO NOT try to speak speak instead of your superiors, based on our experience, that may lead to disaster.

- Why this happened?

- Your network and data were not secure enough. We took advantage of it.

- What else should i know:

Our business depends on the reputation even more than many others. If we will take money and spread your information- we will have issues with payments in future. So, we will stick to our promises and reputation. That works in both ways: if we said that we will email all your staff and publicly spread all your data- we will.

Contact us using "Tox" messenger.

The contact of the user that you should add for further instructions:
88A612B3887D57A7FA3D48F5E3EDF952E4BE48E0972FC6456FBBCFF198CC8620E5609ED2D598

Link to download "Tox" messenger:
https://github.com/qTox/qTox/releases/download/v1.17.6/setup-qtox-x86_64-release.exe

Alternative way: N0torious@onionmail.org

```
Your ID: <redacted>

Now you should contact us.
```

Figure 2: BianLian Sample Ransom Note (New November 20, 2024)

(New, November 20, 2024) BianLian group engages in additional techniques to pressure the victim into paying the ransom; for example, printing the ransom note to printers on the compromised network. Employees of victim companies have also reported receiving threatening telephone calls from individuals associated with BianLian group.

Indicators of Compromise (IOC)

See **Table 1** for IOCs obtained from FBI investigations as of March 2023.

Table 1: BianLian Ransomware and Data Extortion Group IOCs

Name	SHA-256 Hash	Description
def.exe	7b15f570a23a5c5ce8ff942da60834a9d0549ea3ea9f34f900a09331325df893	Malware associated with BianLian intrusions, which is an example of a possible backdoor developed by BianLian group.
encryptor.exe	1fd07b8d1728e416f897bef4f1471126f9b18ef108eb952f4b75050da22e8e43	Example of a BianLian encryptor.
exp.exe	0c1eb11de3a533689267ba075e49d93d55308525c04d6aff0d2c54d1f52f5500	Possible NetLogon vulnerability (CVE-2020-1472) exploitation.
system.exe	40126ae71b857dd22db39611c25d3d5dd0e60316b72830e930fba9baf23973ce	Enumerates registry and files. Reads clipboard data.

MITRE ATT&CK Techniques

See **Table 2** to **Table 14** for all referenced threat actor tactics and techniques in this advisory.

Table 2: Resource Development

Technique Title	ID	Use
Develop Capabilities: Malware	T1587.001	BianLian group actors developed a custom backdoor used in their intrusions.

Table 3: Initial Access

Technique Title	ID	Use
External Remote Services	T1133	BianLian group actors used RDP with valid accounts as a means of gaining initial access and for lateral movement.
Phishing	T1566	BianLian group actors used phishing to obtain valid user credentials for initial access.
Valid Accounts	T1078	BianLian group actors used RDP with valid accounts as a means of gaining initial access and for lateral movement.
(New, November 20, 2024) Exploit Public-Facing Application	T1190	BianLian group actors are targeting public-facing applications of both Windows and ESXi infrastructure, possibly leveraging the ProxyShell exploit chain to gain initial access.

Table 4: Execution

Technique Title	ID	Use
Command and Scripting Interpreter: PowerShell	T1059.001	BianLian group actors used PowerShell to disable AMSI on Windows. See **Appendix: Windows PowerShell and Command Shell Activity** for additional information.
Command and Scripting Interpreter: Windows Command Shell	T1059.003	BianLian group actors used Windows Command Shell to disable antivirus tools, for discovery, and to execute their tools on victim networks. See **Appendix: Windows PowerShell and Command Shell Activity** for additional information.
Scheduled Task/Job: Scheduled Task	T1053.005	BianLian group actors used a Scheduled Task run as SYSTEM (the highest privilege Windows accounts) to execute a Dynamic Link Library (DLL) file daily. See **Appendix: Windows PowerShell and Command Shell Activity** for additional information.

Table 5: Persistence

Technique Title	ID	Use
Account Manipulation	T1098	BianLian group actors changed the password of an account they created. BianLian actors modified the password of an account they added to the local Remote Desktop Users group.
Create Account: Local Account	T1136.001	BianLian group actors created/activated a local administrator account. BianLian group actors used net.exe to add a user account to the local Remote Desktop Users group. (See **Appendix: Windows PowerShell and Command Shell Activity** for more information.)
(New, November 20, 2024) Create Account: Domain Account	T1136.002	BianLian actors created multiple domain admin accounts that were used for lateral movement.
(New, November 20, 2024) Create Account: Cloud Account	T1136.003	BianLian actors created multiple Azure AD accounts to maintain access to the victim systems.
(New, November 20, 2024) Server Software Component: Web Shell	T1505.003	BianLian group actors installed a webshell on a victim Exchange server.

Table 6: Privilege Escalation

Technique Title	ID	Use
(New, November 20, 2024) Exploitation for Privilege Escalation	T1068	BianLian group actors exploited CVE-2022-37969, which affects Windows 10 and 11 systems.

Table 7: Defense Evasion

Technique Title	ID	Use
Modify Registry	T1112	BianLian group actors modified the registry to disable user authentication for RDP connections, allow a user to receive help from Remote Assistance, and disable tamper protection for Sophos SAVEnabled, SEDEenabled, and SAVService services, which enables them to uninstall these services.

Technique Title	ID	Use
Impair Defenses: Disable or Modify Tools	T1562.001	BianLian group actors disabled Windows defender, AMSI, and Sophos SAVEnabled and SEDEenabled tamper protection services. See **Appendix: Windows PowerShell and Command Shell Activity** for additional information.
Impair Defenses: Disable or Modify System Firewall	T1562.004	BianLian group actors added modified firewalls to allow RDP traffic by adding new rules to the Windows firewall that allow incoming RDP traffic and enable a pre-existing Windows firewall rule group named Remote Desktop.
(New, November 20, 2024) Obfuscated Files or Information: Software Packing	T1027.002	BianLian group actors may pack executables using UPX, to conceal their code in an attempt to bypass heuristic and signature-based detection methods.
(New, November 20, 2024) Masquerading: Masquerade Task or Service	T1036.004	BianLian group actors rename binaries and scheduled tasks after legitimate Windows services or security products.

Table 8: Credential Access

Technique Title	ID	Use
OS Credential Dumping: LSASS Memory	T1003.001	BianLian group actors accessed credential material stored in the process memory of the LSASS. See **Appendix:Windows PowerShell and Command Shell Activity** for additional information.
OS Credential Dumping: NTDS	T1003.003	BianLian group actors attempted to access or create a copy of the Active Directory domain database in order to steal credential information and to obtain other information about domain members such as devices, users, and access rights.
Unsecured Credentials: Credentials In Files	T1552.001	BianLian group actors searched local file systems and remote file shares for files containing insecurely stored credentials.
(New, November 20, 2024) Unsecured Credentials: Private Keys	T1552.004	BianLian group actors uses SessionGopher, likely to extract session information for RATs.

Table 9: Discovery

Technique Title	ID	Use
Account Discovery: Domain Account	T1087.002	BianLian group actors queried the domain controller to identify accounts in the Domain Admins and Domain Computers groups. This information can help adversaries determine which domain accounts exist to aid in follow-on activity.
Domain Trust Discovery	T1482	BianLian group actors used PingCastle to enumerate the AD and map trust relationships. BianLian group actors retrieved a list of domain trust relationships used to identify lateral movement opportunities in Windows multi-domain/forest environments.
File and Directory Discovery	T1083	BianLian group used malware (system.exe) that enumerates files.
Network Service Discovery	T1046	BianLian actors used Advanced Port Scanner and SoftPerfect Network Scanner to ping computers, scan ports, and identify program versions running on ports.
Network Share Discovery	T1135	BianLian actors used SoftPerfect Network Scanner, which can discover shared folders. BianLian group actors used SharpShares to enumerate accessible network shares in a domain.
Permission Groups Discovery: Domain Groups	T1069.002	BianLian group actors queried the domain controller to identify groups.
Query Registry	T1012	BianLian group used malware (system.exe) that enumerates registry.
Remote System Discovery	T1018	BianLian group actors attempted to get a listing of other systems by IP address, hostname, or other logical identifier on a network that may be used for lateral movement. BianLian group actors retrieved a list of domain controllers.

Technique Title	ID	Use
System Owner User Discovery	T1033	BianLian group actors queried currently logged-in users on a machine.
(New, November 20, 2024) Process Discovery	T1057	BianLian group actors run PowerShell scripts to list all running processes.
(New, November 20, 2024) Software Discovery	T1518	BianLian group actors run PowerShell scripts to list all software installed.
(New, November 20, 2024) System Information Discovery	T1082	BianLian group actors run PowerShell scripts to list all local drives.

Table 10: Lateral Movement

Technique Title	ID	Use
Remote Services: Remote Desktop Protocol	T1021.001	BianLian group actors used RDP with valid accounts for lateral movement.
(New, November 20, 2024) Remote Services: SMB/Windows Admin Shares	T1021.002	BianLian group actors used SMB to establish network login connections for lateral movement.

Table 11: Collection

Technique Title	ID	Use
Clipboard Data	T1115	BianLian group actors' malware collects data stored in the clipboard from users copying information within or between applications.
(New, November 20, 2024) Archive Collected Data	T1560	BianLian group actors run PowerShell scripts to compress and/or encrypt data that is collected prior to exfiltration.

Table 12: Command and Control

Technique Title	ID	Use
Ingress Tool Transfer	T1105	BianLian group actors transferred tools or other files from an external system into a compromised environment.

Technique Title	ID	Use
Remote Access Software	T1219	BianLian group actors used legitimate desktop support and remote access software to establish an interactive command and control channel to target systems within networks.
(New, November 20, 2024) Proxy	T1090	BianLian group actors may be using the reverse proxy tool Ngrok and/or a modified version of the open-source Rsocks utility.
(New, November 20, 2024) Proxy: External Proxy	T1090.002	BianLian group actors may have used external proxy rsocks to establish SOCKS5 network tunnels from victim networks and to mask the destination of C2 traffic.

Table 13: Exfiltration

Technique Title	ID	Use
Transfer Data to Cloud Account	T1537	BianLian group actors used Rclone to exfiltrate data to a cloud account they control on the same service to avoid typical file transfers/downloads and network-based exfiltration detection.
Exfiltration Over Alternative Protocol	T1048	BianLian group actors exfiltrated data via FTP.
Exfiltration Over Web Service: Exfiltration to Cloud Storage	T1567.002	BianLian group actors exfiltrated data via Mega public file-sharing service.

Table 14: Impact

Technique Title	ID	Use
Data Encrypted for Impact	T1486	*(Updated, November 20, 2024)* Prior to January 2024, BianLian group actors encrypted data on target systems.

Mitigations

FBI, CISA, and ASD'S ACSC recommend 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 Cross-Sector Cybersecurity Performance Goals for more information on the CPGs, including additional recommended baseline protections.

- Reduce threat of malicious actors using remote access tools by:
  - **Auditing remote access tools** on your network to identify currently used and/or authorized software.
  - **Reviewing logs for execution of remote access software** to detect abnormal use of programs running as a portable executable [CPG 2.T].
  - **Using security software to detect instances of remote access** software only being loaded in memory.
  - **Requiring authorized remote access solutions only be used from within your network over approved remote access solutions**, such as virtual private networks (VPNs) or virtual desktop interfaces (VDIs).
  - **Blocking both inbound and outbound connections on common remote access software ports and protocols** at the network perimeter.
- **Implement application controls to manage and control execution of software**, including allowlisting remote access programs.
  - Application controls should prevent installation and execution of portable versions of unauthorized remote access and other software. A properly configured application allowlisting solution will block any unlisted application execution. Allowlisting is important because antivirus solutions may fail to detect the execution of malicious portable executables when the files use any combination of compression, encryption, or obfuscation.
    - See NSA Cybersecurity Information sheet Enforce Signed Software Execution Policies for additional guidance.
- **Strictly limit the use of RDP and other remote desktop services.** If RDP is necessary, rigorously apply best practices, for example [CPG 2.W]:
  - Audit the network for systems using RDP.
  - Close unused RDP ports.
  - Enforce account lockouts after a specified number of attempts.
  - Apply phishing-resistant multifactor authentication (MFA).
  - Log RDP login attempts.
- **Disable command-line and scripting activities and permissions** [CPG 2.N].
- **Restrict the use of PowerShell**, using Group Policy, and only grant to specific users on a case-by-case basis. Typically, only those users or administrators who manage the network or Windows operating systems (OSs) should be permitted to use PowerShell [CPG 2.E].
- **Update Windows PowerShell or PowerShell Core** to the latest version and uninstall all earlier PowerShell versions. Logs from Windows PowerShell prior to version 5.0 are either non-existent or do not record enough detail to aid in enterprise monitoring and incident response activities [CPG 1.E, 2.S, 2.T].

- **Enable enhanced PowerShell logging** [CPG 2.T, 2.U].
  - PowerShell logs contain valuable data, including historical OS and registry interaction and possible TTPs of a threat actor's PowerShell use.
  - Ensure PowerShell instances, using the latest version, have module, script block, and transcription logging enabled (enhanced logging).
  - The two logs that record PowerShell activity are the PowerShell Windows Event Log and the PowerShell Operational Log. FBI and CISA recommend turning on these two Windows Event Logs with a retention period of at least 180 days. These logs should be checked on a regular basis to confirm whether the log data has been deleted or logging has been turned off. Set the storage size permitted for both logs to as large as possible.
- **Configure the Windows Registry to require User Account Control (UAC) approval for any PsExec operations** requiring administrator privileges to reduce the risk of lateral movement by PsExec.
- **Review domain controllers, servers, workstations, and active directories** for new and/or unrecognized accounts [CPG 4.C].
- **Audit user accounts** with administrative privileges and configure access controls according to the principle of least privilege [CPG 2.E].
- Reduce the threat of credential compromise via the following:
  - **Place domain admin accounts in the protected users' group** to prevent caching of password hashes locally.
  - **Implement Credential Guard for Windows 10 and Server 2016** (Refer to Microsoft: Manage Windows Defender Credential Guard for more information). For Windows Server 2012R2, enable Protected Process Light for Local Security Authority (LSA).
  - **Refrain from storing plaintext credentials in scripts.**
- **Implement time-based access for accounts set at the admin level and higher** [CPG 2.A, 2.E]. For example, the Just-in-Time (JIT) access method provisions privileged access when needed and can support enforcement of the principle of least privilege (as well as the Zero Trust model). This is a process where a network-wide policy is set in place to automatically disable admin accounts at the AD level when the account is not in direct need. Individual users may submit their requests through an automated process that grants them access to a specified system for a set timeframe when they need to support the completion of a certain task.

In addition, FBI, CISA, and ASD'S ACSC recommend network defenders apply the following mitigations to limit potential adversarial use of common system and network discovery techniques and to reduce the impact and risk of compromise by ransomware or data extortion actors:

- **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 (e.g., hard drive, storage device, or the cloud).
- **Maintain offline backups of data**, and regularly maintain backup and restoration (daily or weekly at minimum). By instituting this practice, an organization minimizes the impact of disruption to business practices as they will not be as severe and/or only have irretrievable data [CPG 2.R].

ASD'S ACSC recommends organizations follow the 3-2-1 backup strategy in which organizations have three copies of data (one copy of production data and two backup copies) on two different media such as disk and tape, with one copy kept off-site for disaster recovery.

- **Require all accounts with password logins** (e.g., service account, admin accounts, and domain admin accounts) **to comply with** National Institute for Standards and Technology (NIST) standards for developing and managing password policies.
  - Use longer passwords consisting of at least 15 characters [CPG 2.B].
  - Store passwords in hashed format using industry-recognized password managers.
  - Add password user "salts" to shared login credentials.
  - Avoid reusing passwords [CPG 2.C].
  - Implement multiple failed login attempt account lockouts [CPG 2.G].
  - Disable password "hints."
  - Refrain from requiring password changes more frequently than once per year.
    Note: NIST guidance suggests favoring longer passwords instead of requiring regular and frequent password resets. Frequent password resets are more likely to result in users developing password "patterns" cyber criminals can easily decipher.
  - Require administrator credentials to install software.
- **Require phishing-resistant multifactor authentication** for all services to the extent possible, particularly for webmail, virtual private networks, and accounts that access critical systems [CPG 2.H].
- **Keep all operating systems, software, and firmware up to date.** Timely patching is one of the most efficient and cost-effective steps an organization can take to minimize its exposure to cybersecurity threats. Organizations should patch vulnerable software and hardware systems within 24 to 48 hours from vulnerability disclosure. Prioritize patching known exploited vulnerabilities in internet-facing systems [CPG 1.E].
- **Segment networks** to prevent the spread of ransomware. Network segmentation can help prevent the spread of ransomware by controlling traffic flows between—and access to—various subnetworks, restricting further lateral movement [CPG 2.F].
- **Identify, detect, and investigate abnormal activity and potential traversal of the indicated ransomware with a networking monitoring tool.** To aid in detecting ransomware, implement a tool that logs and reports all network traffic, including lateral movement activity on a network. Endpoint detection and response (EDR) tools are particularly useful for detecting lateral connections, as they have insight into common and uncommon network connections for each host [CPG 3.A].
- **Install, regularly update, and enable real time detection for antivirus software** on all hosts.
- **Disable unused ports** [CPG 2.V].
- **Consider adding an email banner to emails** received from outside your organization [CPG 2.M].

- **Ensure all backup data is encrypted, immutable** (i.e., cannot be altered or deleted), and covers the entire organization's data infrastructure [CPG 2.K, 2.L, 2.R].

Validate Security Controls

In addition to applying mitigations, FBI, CISA, and ASD'S ACSC 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. FBI, CISA, and ASD'S ACSC 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 14**).
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.

FBI, CISA, and ASD'S ACSC 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

- Stopransomware.gov, a whole-of-government approach with one central location for U.S. ransomware resources and alerts.
- cyber.gov.au for the Australian Government's central location to report cyber incidents, including ransomware, and to see advice and alerts. The site also provides ransomware advisories for businesses and organizations to help mitigate cyber threats.
- CISA-Multi-State Information Sharing and Analysis Center (MS-ISAC) Joint Ransomware Guide for guidance on mitigating and responding to a ransomware attack.
- For no-cost cyber hygiene services for U.S. organizations, Cyber Hygiene Services and Ransomware Readiness Assessment.

Reporting

The FBI is seeking any information that can be shared, including boundary logs showing communication to and from foreign IP addresses, a sample ransom note, communications with BianLian actors, Bitcoin wallet information, decryptor files, and/or a benign sample of an encrypted file. The FBI and CISA do not encourage paying ransom, as payment does not guarantee victim files will be recovered. Furthermore,

payment may also embolden adversaries to target additional organizations, encourage other criminal actors to engage in the distribution of ransomware, and/or fund illicit activities. Regardless of whether you or your organization have decided to pay the ransom, the FBI and CISA urge you to promptly report ransomware incidents to a local FBI Field Office or CISA at cisa.gov/report. Australian organizations that have been impacted or require assistance in regard to a ransomware incident can contact ASD'S ACSC via 1300 CYBER1 (1300 292 371) or by submitting a report cyber.gov.au.

Disclaimer

The information in this report is being provided "as is" for informational purposes only. FBI, CISA, and ASD'S ACSC do not endorse any commercial product or service, including any subjects of analysis. Any reference to specific commercial products, processes, or services by service mark, trademark, manufacturer, or otherwise, does not constitute or imply endorsement, recommendation, or favoring by FBI, CISA, or ASD'S ACSC.

Acknowledgements

CrowdStrike, Microsoft, and Sophos contributed to this advisory.

Version History

May 16, 2023: Initial version

November 20, 2024: Updates noted throughout

Appendix: Windows Powershell and Command Shell Activity

Through FBI investigations as of March 2023, FBI has observed BianLian actors use the commands in Table 15. ASD'S ACSC has observed BianLian actors use some of the same commands.

Table 15: PowerShell and Windows Command Shell Activity

Command	Use
[Ref].Assembly.GetType('System.Management.Automation.AmsiUtils').GetField('amsiInitFailed','NonPublic,* Static').SetValue($null,$true)	Disables the AMSI on Windows. AMSI is a built-in feature on Windows 10 and newer that provides an interface for anti-malware scanners to inspect scripts prior to execution. When AMSI is disabled, malicious scripts may bypass antivirus solutions and execute undetected.
cmd.exe /Q /c for /f "tokens=1,2 delims= " ^%A in ('"tasklist /fi "Imagename eq lsass.exe" | find "lsass""') do rundll32.exe C:\windows\System32\comsvcs.dll, MiniDump ^%B \Windows\Temp\<file>.csv full	Creates a memory dump `lsass.exe` process and saves it as a CSV file. BianLian actors used it to harvest credentials from `lsass.exe`.
cmd.exe /Q /c net user <admin> /active:yes 1> \\127.0.0.1\C$\Windows\Temp\<folder> 2>&1	Activates the local Administrator account.
cmd.exe /Q /c net user "<admin>"<password> 1> \\127.0.0.1\C$\Windows\Temp\<folder> 2>&1	Changes the password of the newly activated local Administrator account.
cmd.exe /Q /c quser 1> \\127.0.0.1\C$\Windows\Temp\<folder> 2>&1	Executes `quser.exe` to query the currently logged-in users on a machine. The command is provided arguments to run quietly and exit upon completion, and the output is directed to the `\Windows\Temp` directory.
dism.exe /online /Disable-Feature /FeatureName:Windows-Defender /Remove /NoRestart	Using the Deployment Image Servicing and Management (DISM) executable file, removes the Windows Defender feature.
dump.exe -no-pass -just-dc user.local/<fileserver.local>\@<local_ip>	Executes `secretsdump.py`, a Portable Executable version of an Impacket tool. Used to dump password hashes from domain controllers.

Command	Use
exp.exe -n <fileserver.local> -t <local_ip>	Possibly attempted exploitation of the NetLogon vulnerability (CVE-2020-1472).
findstr /spin "password" *.* >C:\Users\training\Music\<file>.txt	Searches for the string `password` in all files in the current directory and its subdirectories and puts the output to a file.
ldap.exe -u user\<user> -p <password> ldap://<local_ip>	Connects to the organization's Lightweight Directory Access Protocol (LDAP) server.
logoff	Logs off the current user from a Windows session. Can be used to log off multiple users at once.
mstsc	Launches Microsoft Remote Desktop Connection client application in Windows.
net group /domain	Retrieves a list of all groups from the domain controller.
net group 'Domain Admins' /domain	Queries the domain controller to retrieve a list of all accounts from `Domain Admins` group.
net group 'Domain Computers' /domain	Queries the domain controller to retrieve a list of all accounts from `Domain Computers` group.
net user /domain	Queries the domain controller to retrieve a list of all users in the domain.
net.exe localgroup "Remote Desktop Users" <user> /add	Adds a user account to the `local Remote Desktop Users` group.
net.exe user <admin> <password> /domain	Modifies the password for the specified account.
netsh.exe advfirewall firewall add rule "name=allow RemoteDesktop" dir=in * protocol=TCP localport=<port num> action=allow	Adds a new rule to the Windows firewall that allows incoming RDP traffic.
netsh.exe advfirewall firewall set rule "group=remote desktop" new enable=Yes	Enables the pre-existing Windows firewall rule group named `Remote Desktop`. This rule group allows incoming RDP traffic.
nltest /dclist	Retrieves a list of domain controllers.
nltest /domain_trusts	Retrieves a list of domain trusts.

Command	Use
ping.exe -4 -n 1 *	Sends a single ICMP echo request packet to all devices on the local network using the IPv4 protocol. The output of the command will show if the device is reachable or not.
quser; ([adsisearcher]"(ObjectClass=computer)").FindAll().count;([adsisearcher]"(ObjectClass=user)").FindAll().count;[Security.Principal.WindowsIdentity]::GetCurrent() | select name;net user "$env:USERNAME" /domain; (Get-WmiObject -class Win32_OperatingSystem).Caption; Get-WmiObject -Namespace root\cimv2 -Class Win32_ComputerSystem; net group "domain admins" /domain; nltest /dclist:; nltest /DOMAIN_TRUSTS	Lists the current Windows identity for the logged-in user and displays the user's name. Uses the Active Directory Services Interface (ADSI) to search for all computer and user objects in the domain and returns counts of the quantities found. Lists information about the current user account from the domain, such as the user's name, description, and group memberships. Lists information about the operating system installed on the local computer. Lists information about the "Domain Admins" group from the domain. Lists all domain controllers in the domain. Displays information about domain trusts.
reg.exe add "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server\WinStations\RDP-Tcp" /v UserAuthentication /t REG_DWORD /d 0 /f	Adds/overwrites a new Registry value to disable user authentication for RDP connections.
reg.exe add "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server" /* v fAllowToGetHelp /t REG_DWORD /d 1 /f	Adds/overwrites a new Registry value to allow a user to receive help from Remote Assistance.
reg.exe add "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Sophos Endpoint Defense\TamperProtection\Config" /t REG_DWORD /v SAVEnabled /d 0 /f	Adds/overwrites a new Registry value to disable tamper protection for Sophos antivirus named SAVEnabled.
reg.exe add "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Sophos Endpoint Defense\TamperProtection\Config" /t REG_DWORD /v SEDEnabled /d 0 /f	Adds/overwrites a new Registry value to disable tamper protection for Sophos antivirus named SEDEnabled.

Command	Use
reg.exe ADD * HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Sophos\SAVService\TamperProtection /t REG_DWORD /v Enabled /d 0 /f	Adds/overwrites a new registry value to disable tamper protection for a Sophos antivirus service called SAVService.
reg.exe copy hklm\system\CurrentControlSet\services\tvnserver * hklm\system\CurrentControlSet\control\safeboot\network\tvnserver /s /f	Copies the configuration settings for the `tvnserver` service to a new location in the registry that will be used when the computer boots into Safe Mode with Networking. This allows the service to run with the same settings in Safe Mode as it does in normal mode.
s.exe /threads:50 /ldap:all /verbose /outfile:c:\users\<user>\desktop\1.txt	Executes SharpShares.
schtasks.exe /RU SYSTEM /create /sc ONCE /<user> /tr "cmd.exe /crundll32.exe c:\programdata\netsh.dll,Entry" /ST 04:43	Creates a Scheduled Task run as `SYSTEM` at 0443 AM. When the task is run, `cmd.exe` uses `crundll32.exe` to run the DLL file `netsh.dll`. (It is likely that `netsh.dll` is a malware file and not associated with `netsh`.)
start-process PowerShell.exe -arg C:\Users\Public\Music\<file>.ps1 -WindowStyle Hidden	Executes a PowerShell script, while keeping the PowerShell window hidden from the user.