Read more: Boosty | Sponsr | TG

Abstract – This document provides a analysis of the Bian Lian ransomware, a malicious software that has been increasingly targeting various sectors with a focus on data exfiltration-based extortion. The analysis delves into multiple aspects of ransomware, including its operational tactics, technical characteristics, and the implications of its activities on cybersecurity.

The analysis of BianLian ransomware is particularly useful for security professionals, IT personnel, and organizations across various industries. It equips them with the knowledge to understand the threat landscape, anticipate potential attack vectors, and implement robust security protocols to mitigate risks associated with ransomware attacks.

I. Introduction

BianLian is a ransomware group that has been active since June 2022, targeting organizations across multiple critical infrastructure sectors in the United States and Australia. The group is known for developing, deploying, and using ransomware for data extortion purposes.

The Cybersecurity and Infrastructure Security Agency (CISA), the Federal Bureau of Investigation (FBI), and the Australian Cyber Security Centre (ACSC) have issued advisories with recommendations to mitigate cyber threats from BianLian ransomware that include observed tactics, techniques, and procedures (TTPs), and indicators of compromise (IOCs) to help organizations protect against such ransomware attacks.

The average ransom demand made by the BianLian ransomware group varies significantly. According to a report by BeforeCrypt, the average BianLian ransom demand is somewhere between $100,000 – $350,000. However, a report by Halcyon suggests that ransom demands can average around $3 million dollars but have been reported to be as high as $20 million. Coveware, a security consulting firm, found that the average ransom payment for Q3 2023 was $850,700 USD

II. Profiling

The group has been known to target a wide range of industries, including financial institutions, healthcare, manufacturing, education, entertainment, and energy sectors.

BianLian usually attacks high-profile targets from a variety of fields. These include healthcare, finances, government, education, law, and professional services. The group has also targeted the education sector heavily.The group has targeted various industries, including but not limited to:

- Healthcare
- Education
- Government entities
- Professional services
- Manufacturing
- Media and entertainment
- Banking and financial services
- Energy sector

In the healthcare sector, common entry points for BianLian ransomware include servers, PCs, databases, and medical records. A growing concern is the targeting of medical devices, not just networks. This is due to the sensitive data these devices hold, including intellectual property, trade secrets, personal data, and medical records. The healthcare sector has seen over 630 ransomware incidents worldwide in 2023, with over 460 of these affecting the U.S.

In the education sector, cybercriminals often exploit obsolete software with known security problems as an entry point. This is due to inadequate patch management, which leaves systems vulnerable to attacks. The BianLian group has been known to target education institutions, exploiting these vulnerabilities to gain unauthorized access to school networks and systems.

For government entities, the entry points for BianLian are similar. They exploit vulnerabilities to move within breached networks undetected, utilizing custom malware. They also target Remote Desktop Protocol and other remote access tools.

For manufacturing organizations, BianLian ransomware commonly exploits known vulnerabilities in internet-facing systems. It's crucial for these organizations to prioritize patching these vulnerabilities to prevent ransomware attacks. BianLian also targets systems through the use of valid Remote Desktop Protocol (RDP) credentials

In professional services organizations, BianLian often gains initial access through professional services. The ransomware group has been known to use valid RDP credentials as a common entry point. Additionally, the group has been observed to use Business Email Compromise (BEC) as a vector to deliver their ransomware

In energy organizations, BianLian employs various tactics, including spear-phishing campaigns and exploiting vulnerabilities, to gain unauthorized access and encrypt files for ransom. The group has also been observed to exploit the Netlogon vulnerability (CVE-2020-1472) and connect to an Active Directory.

CYBERKIB SECURITY

III. How BianLian works

The group typically infiltrates victim systems using legitimate Remote Desktop Protocol (RDP) credentials. They also exploit known vulnerabilities and use open-source tools and command-line scripting for discovery and credential harvesting. Once inside, they disable antivirus software such as Windows Defender and modify the system's settings.

The ransomware encrypts files and appends the .bianlian extension to them, leaving a ransom note titled "Look at this instruction.txt" in each affected directory. The group initially followed a double-extortion model, where they would encrypt victims' systems after exfiltrating data (via File Transfer Protocol (FTP), Rclone, or Mega file-sharing services). However, since January 2023, they have shifted to a primarily exfiltration-based extortion model.

However, in January 2023, the group shifted its tactics. Instead of encrypting systems, they moved to a model of exfiltration-based extortion. This shift coincided with the release of a decryptor for the ransomware by Avast. In this new model, the group continues to steal data but no longer encrypts the victim's systems. They then threaten to release the stolen data unless a ransom is paid.

IV. Signs of a BianLian ransomware attack

- **Ransom Note**: Victims typically receive a message of data encryption or exfiltration, demanding a ransom. The ransom note is often named "Look at this instruction.txt"
- **File Extension Changes**: Files on the infected system may have their extensions changed to ".bianlian"
- **Threatening Calls**: Employees of victim companies have reported receiving threatening telephone calls from individuals associated with the BianLian group
- **Cryptocurrency Wallets**: The BianLian group receives payments in unique cryptocurrency wallets for each victim company
- **Rapid Encryption**: BianLian ransomware is known for its exceptional speed in encrypting files, which can make it difficult for defenders to respond in time
- **Data Exfiltration**: The group exfiltrates victim data via File Transfer Protocol (FTP), Rclone, or Mega, and then extorts money by threatening to release the data if payment is not made
- **Spearphishing Emails**: Initial access to the target system is often achieved through spearphishing emails containing malicious attachments or links
- **Use of Remote Desktop Protocol (RDP)**: The group often gains access to victim systems through valid RDP credentials
- **System Changes and Slow Performance**: Advanced ransomware like BianLian can cause noticeable system changes and slow down the performance of the infected system

V. Initial access vectors

BianLian ransomware group uses several initial access vectors to infiltrate target networks. These initial access vectors highlight the importance of robust security measures, including strong password policies, multi-factor authentication, regular patching and updating of software, and user education on phishing threats:

- **Reconnaissance**: To perform network reconnaissance, BianLian uses tools such as Advanced Port Scanner, SoftPerfect Network Scanner, SharpShares, and PingCastle. These tools help them identify network resources, open ports, and potential vulnerabilities that can be exploited.
- **Compromised Remote Desktop Protocol (RDP) Credentials**: The group often exploits compromised RDP credentials to gain initial access to networks. They use these valid accounts to access the targets' networks via RDP
- **Spearphishing Emails**: BianLian also uses spearphishing emails containing malicious attachments or links to gain initial access to the target system
- **Exploitation of Vulnerabilities**: There has been a shift in the threat landscape with ransomware operators, including BianLian, increasingly exploiting known vulnerabilities for initial access
- **External Remote Services**: BianLian exploits weaknesses in externally accessible remote services, such as RDP, to gain a foothold into targeted networks
- **Exploitation of ProxyShell Flaws**: The group has been known to exploit ProxyShell vulnerabilities to gain initial access to networks
- **Use of Initial Access Brokers (IABs)**: There have been instances where BianLian has used Initial Access Brokers, who specialize in gaining initial access to networks and then selling that access to other threat actors

VI. IoCs

Indicators of Compromise (IOCs) associated with BianLian ransomware attacks can provide valuable insights for detecting and responding to these threats. While specific IOCs may vary depending on the particular attack, some common IOCs associated with BianLian ransomware include:

- **SHA-256 Hashes**: Specific SHA-256 hashes associated with malware used by the BianLian group have been identified (like anabolic.exe (SHA256: 46d340eaf6b78207e24b6011422f1a5b4a566e493d72365c6a1cace11c36b28b that is a 64-bit executable file compiled with Golang version 1.18.3.)
- **IP Addresses**: Certain IP addresses have been linked to BianLian ransomware attacks. For example, the IP address 104.207.155[.]133 has been associated with the group's activities

Cyberkill Security

- **File Changes**: The ransomware modifies all encrypted files to have the .bianlian extension
- **Ransom Note**: The presence of a ransom note named "Look at this instruction.txt" in each affected directory is a clear indicator of a BianLian ransomware attack
- **Network Traffic**: Unusual network traffic to or from known malicious IP addresses or domains associated with BianLian ransomware can be an indicator of compromise like BianLian leveraged netsh to add a firewall rule to open 3389 to Remote Desktop
- **System Changes**: Changes in system settings or the disabling of antivirus software such as Windows Defender can be indicative of a BianLian ransomware attack

VII. C2C INFRASTRUCTURE

The BianLian ransomware group uses a variety of methods for establishing C2C infrastructure:

- **Use of Legitimate Remote Access Software**: The group has been observed using legitimate remote access software like TeamViewer, Atera, and AnyDesk to establish interactive command and control channels
- **Expanding Infrastructure**: The group has been rapidly expanding its C2 infrastructure, indicating an increase in its operational tempo
- **Custom Go-Based Backdoor**: After gaining access to a network, the group deploys a custom Go-based backdoor specific to each victim
- **Use of PowerShell Scripts**: The group uses PowerShell scripts for various activities, including data exfiltration
- **Use of Open-Source Tools and Command-Line Scripting**: The group uses open-source tools and command-line scripting for discovery and credential harvesting
- **Use of IP Addresses**: The group uses a variety of IP addresses for its C2 infrastructure. For example, the IP address 104.207.155[.]133 has been associated with the group's activities

VIII. BIANLIAN EXPLOIT VULNERABILITIES IN NETWORKS

BianLian ransomware exploits vulnerabilities in networks through a variety of methods. Initial access is often achieved through spearphishing emails containing malicious attachments, or by exploiting known vulnerabilities in systems and services. The group has been known to use valid Remote Desktop Protocol (RDP) credentials and exploits for vulnerabilities such as CVE-2020-1472. This is a critical vulnerability in Microsoft's Netlogon Remote Protocol, which is used for various tasks related to user and machine authentication. BianLian ransomware has been observed exploiting this vulnerability to gain unauthorized access to Windows domains. They also use reconnaissance malware and custom backdoors.

Once inside a network, BianLian employs tools like PsExec and RDP along with valid accounts for lateral movement. They utilize Command Shell and native Windows tools to add user accounts to the local Remote Desktop, modify the added account's password, and adjust Windows firewall rules to allow incoming RDP traffic.

The group also deploys a custom Go-based backdoor specific to each victim and installs remote management tools like AnyDesk, SplashTop, and TeamViewer. They use PowerShell scripts to harvest data, which is then exfiltrated over FTP and via tools such as Rclone.

BianLian initially employed a double-extortion model, encrypting systems after stealing private data from victim networks, and then threatening to publish the files. However, since January 2023, they have shifted their focus to data exfiltration and no longer deploy file-encrypting ransomwar

IX. REMOTE ACCESS SOFTWARE USED BY BIANLIAN

The BianLian ransomware group uses a variety of legitimate desktop support and remote access software to establish command and control (C2) infrastructure. These tools are typically used for legitimate purposes, such as providing remote technical support.

- **TeamViewer**: a widely used remote access and remote-control software that allows users to control computers remotely over the internet
- **Atera**: a remote IT management platform designed for managed service providers (MSPs) that provides remote monitoring and management (RMM), professional services automation (PSA), and remote access capabilities
- **SplashTop**: a remote access tool that allows users to connect to and control computers from any device
- **AnyDesk**: a remote desktop software that provides remote access to personal computers running the host application

Using RDP software allows the group to remotely control compromised systems, execute commands, and perform malicious activities. In both cases, the group deploys a custom Go-based backdoor specific to each victim after gaining access to a network. This backdoor enables the threat actor to install remote management tools to maintain persistence. The group also creates or activates administrator accounts and changes their passwords to further secure their access.

A. TeamViewer & AnyDesk

TeamViewer & AnyDesk is a popular choice for the BianLian ransomware group due to its robust features that facilitate remote access and control, which can be exploited for malicious purposes.

- **Widespread Use and Ease of Access**: TeamViewer & AnyDesk is installed on hundreds of millions of endpoints worldwide, with over 400 million devices running the software, of which 30 million are connected to TeamViewer at any given time.
- **Remote Support and Access**: TeamViewer enables remote support, collaboration, and access to endpoint

CYFIRMA SECURITY

devices. This feature allows attackers to gain control over victim environments remotely.

- **Asset Management**: TeamViewer & AnyDesk offers asset management capabilities, allowing for the management of software updates, system upgrades, and patch deployments remotely.
- **Integration with Other Remote Access Tools**: TeamViewer & AnyDesk integrates with other remote access tools like Splashtop and AnyDesk, providing additional pathways for attackers to access and control compromised systems.
- **Security Measures**: Despite TeamViewer's/AnyDesk's high encryption standards and security measures, attackers have found ways to exploit the tool. TeamViewer emphasizes the importance of complex passwords, two-factor authentication, allow-lists, and regular software updates to prevent unauthorized access.

B. Atera

Atera Agent is a popular choice for the BianLian ransomware group due to its robust features and capabilities that can be exploited for malicious purposes:

- **Remote Monitoring and Management (RMM)**: Atera provides real-time monitoring and alerts, IT automation, patch management, and advanced remote maintenance. This allows the BianLian group to monitor and control compromised systems in real-time.
- **Integrated Remote Access**: Atera integrates with Splashtop and AnyDesk, providing remote access capabilities. This allows the BianLian group to remotely access and control compromised systems.
- **Asset and Inventory Management**: Atera provides asset and inventory management capabilities. This can provide the BianLian group with valuable information about the compromised systems.
- **Professional Services Automation (PSA)**: Atera includes capabilities like ticketing, billing, and reporting. While these features are designed for legitimate IT professionals, they can be exploited by the BianLian group for malicious purposes.
- **AI Capabilities**: Atera Agent includes AI capabilities. While the specific use of these capabilities by the BianLian group is not clear, they could potentially be exploited for malicious purposes.
- **Scripting**: Atera allows for scripting, which can be very useful for the BianLian group to automate certain tasks on the compromised systems

C. Splashtop

Splashtop is a popular choice for BianLian ransomware due to its robust security features and ease of use:

- **Security Measures**: Splashtop employs a multilayered security approach, which includes encryption, user and device authentication, and numerous other security measures. All remote sessions are encrypted end-to-end via TLS and 256-bit AES. It also includes features like two-factor authentication, multi-level password security, blank screen, screen auto-lock, session idle timeout, and remote connection notification
- **Ease of Setup and Use**: Splashtop is easy to set up and use, which makes it a convenient tool for remote access. It works independently from your legacy IT infrastructure, taking only minutes to set up
- **Splashtop Connector**: This feature enables remote access to computers that are typically only accessible within LAN. It allows users to connect to computers that support the RDP protocol directly from Splashtop, without using VPN or installing any remote access agent
- **Granular Permissions**: Splashtop offers granular permissions, allowing IT teams to have full control over securing the data
- **Device Authentication**: This feature adds an extra layer of security by ensuring that only authenticated devices can access the network
- **Single Sign-On (SSO)**: This feature simplifies the login process, making it easier for users to access their systems securely
- **Scheduled Access Module**: This feature allows IT teams to manage schedules and policies for when users and groups of users can access certain endpoints

OVERALL SECURITY