KPMG

KPMG Cyber Threat Intelligence Platform

Cyber Threat Notification | ‘BianLian’ Ransomware Variant on the Rise

Tracker ID: TN0907 **Date:** 07/Sep/2022 **Category:** Malware **Industry:** All **Region**: All

Background

Cybercriminals are aggressively distributing a novel ransomware strain known as "BianLian" due to its cross-platform capabilities, which makes reverse engineering more difficult. It has grown in popularity since it was originally introduced in mid-July. BianLian's operators use double-extortion tactics, threatening to publish key stolen documents online if ransom demands are not met within ten days. This data comprises financial, customer, company, technological, and personal information. Meanwhile, they also keep an onion leak site operational to leak the stolen data. Threat actors have so far targeted a wide range of businesses with the novel BianLian malware, with 25% of their victims being media and entertainment organizations, and 12.5% each being professional services, manufacturing, education, healthcare, and banking, financial services, and insurance (BFSI) organizations.

When the ransomware is executed, it checks the wine get version() function using the GetProcAddress() API to see if the file is operating in a WINE environment. The ransomware then uses the CreateThread() API call to launch multiple threads for file encryption, making it more difficult to reverse engineer the infection. The GetDriveTypeW() API method is then employed to identify the system drives (from A: to Z:) and encrypts all data on the corresponding drives. The malware leaves a ransom note in various locations with the filename "Look at this instruction.txt.“

In the dropped ransom note, victims are given instructions on how to contact the ransomware operators in order to restore their encrypted files. They threaten their victims by stating that critical information has been downloaded and will be uploaded on their leak site if the ransom is not paid within 10 days. The ransom note also includes the TOX Messenger ID for ransom conversations as well as the onion URL of the leak site page. The BianLian Leak website has a list of all firms impacted by the ransomware, as well as contact information for the TA for ransomware data recovery.

After dropping the ransom note, it lists files and directories and checks them for encryption using the FindFirstFileW() and FindNextFileW() API functions. On the victim's system, the ransomware use GoLang Packages such as "crypto/cipher," "crypto/aes," and "crypto/rsa." for file encryption. For encryption, the malware divides the file content into 10-byte chunks. It reads 10 bytes from the original file, encrypts those bytes, and then writes the encrypted data into the destination file. To avoid detection by anti-virus, the data is split into such small bits. The malware then renames the ".bianlian" extension-encrypted files and replaces them with the original files using the MoveFileExW() API call. It then erases itself via the command line, leaving just the encrypted files and the ransom message on the victim's PC.

Thus, the novel BianLian continues to infiltrate businesses and demand hefty ransoms, by upgrading its tools to evade detection and developing ransomware in Golang, which is compatible with most of the popular OS. Furthermore, if the ransom is not paid on time, it is triggering double extortion techniques by leaking critical files stolen from the victim's machine.

The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavour to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act on such information without appropriate professional advice after a thorough examination of the particular situation.

This document is for e-communication only.

Tracker ID: TN0907 **Date:** 07/Sep/2022 **Category:** Malware **Industry:** All **Region:** All

Detections

Identify and block below commands for any malicious utilizations in the network:

```
• "C:\Windows\system32\Dism.exe" /online /Disable-Feature /FeatureName:Windows-Defender /Remove /NoRestart
• "C:\Windows\system32\net.exe" localgroup "Remote Desktop Users" <similar name to existing admin> /add
• "C:\Windows\system32\net.exe" user <legitimate admin account> 3gDZNxtsQ9G029k7D6Ljxe /domain
• "C:\Windows\system32\netsh.exe" advfirewall firewall set rule "group=remote desktop" new enable=Yes
• "C:\Windows\system32\netsh.exe" advfirewall firewall add rule "name=allow RemoteDesktop" dir=in *
  protocol=TCP localport=3389 action=allow
• "C:\Windows\system32\reg.exe" add "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server"
  /* v fAllowToGetHelp /t REG_DWORD /d 1 /f
• "C:\Windows\system32\reg.exe" add "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal *
  Server\WinStations\RDP-Tcp" /v UserAuthentication /t REG_DWORD /d 0 /f
• "C:\Windows\system32\reg.exe" ADD "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Sophos
  Endpoint * Defense\TamperProtection\Config" /t REG_DWORD /v SAVEnabled /d 0 /f
• "C:\Windows\system32\reg.exe" ADD "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Sophos
  Endpoint * Defense\TamperProtection\Config" /t REG_DWORD /v SEDEnabled /d 0 /f
• "C:\Windows\system32\reg.exe" ADD *
  HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Sophos\SAVService\TamperProtection /t REG_DWORD /v
  Enabled /d 0 /* f
• "C:\Windows\system32\reg.exe" copy hklm\system\CurrentControlSet\services\tvnserver *
  hklm\system\CurrentControlSet\control\safeboot\network\tvnserver /s /f
• \cmd.exe /Q /c net user "Administrator" /active:yes 1> \\127.0.0.1\C$\Windows\Temp\abjAlC 2>&1
• cmd.exe /Q /c net user "Administrator" ChangeMe2morrow! 1> \\127.0.0.1\C$\Windows\Temp\OxNEcz 2>&1
• cmd.exe /Q /c quser 1> \\127.0.0.1\C$\Windows\Temp\VXPrvY 2>&1
• "C:\Windows\system32\PING.EXE" -4 -n 1 *
• [Ref].Assembly.GetType(‘System.Management.Automation.AmsiUtils’).GetField(‘amsiInitFailed’,’NonPublic,*
  Static’).SetValue($null,$true)
```

KPMG Assurance and Consulting Services LLP, Lodha Excelus, Apollo Mills Compound, NM Joshi Marg, Mahalaxmi, Mumbai - 400 011 Phone: +91 22 3989 6000, Fax: +91 22 3983 6000.

KPMG

KPMG Cyber Threat Intelligence Platform

Cyber Threat Notification | 'BianLian' Ransomware Variant on the Rise

Tracker ID: TN0907 **Date:** 07/Sep/2022 **Category:** Malware **Industry:** All **Region:** All

MITRE ATT&CK Tactics

Reconnaissance, Execution, Defense Evasion, Discovery, Impact, Lateral Movement, Credential Access and Execution.

Indicators of Compromise

Please refer to the attached sheet for IOCs

Recommendations

- Check with your existing AV/EDR vendor to validate the detection scope of identified samples. Validate the IOCs attached and implement the detection & prevention accordingly.
- Examine system logs for ominous occurrences. Remove infected devices from the same network and unplug external storage devices.
- Use anti-virus and internet security software on connected devices.
- Use strong passwords, change them frequently, and, when available, multi-factor authentication.
- Implement network segmentation to limit or block lateral movement. Follow multilayered defense solutions and active monitoring to detect and thwart threats.
- Use endpoint detection and response systems that can detect and remediate suspicious activity automatically
- Maintain consistent backup procedures and store those backups offline or on a different network.
- Wherever practical and possible, enable automatic software updates on your computer, and other linked devices.
- Avoid clicking on suspicious links and opening email attachments without first checking their legitimacy.

References

- BianLian: New Ransomware Variant On The Rise, 18th August 2022, Cyble, External Link (blog.cyble.com)
- Ben Armstrong, Lauren Pearce, Brad Pittack, Danny Quist, BianLian Ransomware Gang Gives It a Go!, 01st September 2022, Redacted, External Link (redacted.com)
- Elizabeth Montalbano, New 'BianLian' Ransomware Variant on the Rise, 22nd August 2022, Dark Reading, External Link (darkreading.com)

In case of a Security Incident, please report to IN-FM KPMG SOC.

For any query or feedback, feel free to reach us at IN-FM KPMG CTI.

KPMG in India Cyber Response Hotline : +91 9176471 471

The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavour to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act on such information without appropriate professional advice after a thorough examination of the particular situation.

KPMG Assurance and Consulting Services LLP, Lodha Excelus, Apollo Mills Compound, NM Joshi Marg, Mahalaxmi, Mumbai - 400 011 Phone: +91 22 3989 6000, Fax: +91 22 3983 6000.

This document is for e-communication only.

#KPMG josh

home.kpmg/in

Follow us on home.kpmg/in/socialmedia