IMPORTANT CYBERSECURITY NEWS: FAKE BIANLIAN RANSOM NOTES SENT VIA U.S. POSTAL SERVICE TO SCAM EXECUTIVES

Vairav Cyber Security News Report

Date: March 05, 2025

Vairav Cyber Threat Intelligence Team

Vairav Technology Security Pvt. Ltd.

Thirbam Sadak 148

Baluwatar, Kathmandu

Phone: +977 4541540

Mobile: +977-9820105900

Email: sales@vairavtech.com

EXECUTIVE SUMMARY

Cybercriminals are impersonating the BianLian ransomware gang, sending fraudulent ransom notes via U.S. mail to company executives to extort payments. These letters, claiming that company data has been stolen, demand a Bitcoin ransom between $250,000 and $500,000 to prevent leaks. Unlike real ransomware attacks, no actual breaches have been detected, making this a new extortion scam. Security teams must alert executives to avoid unnecessary panic and resource waste.

INCIDENT ANALYSIS

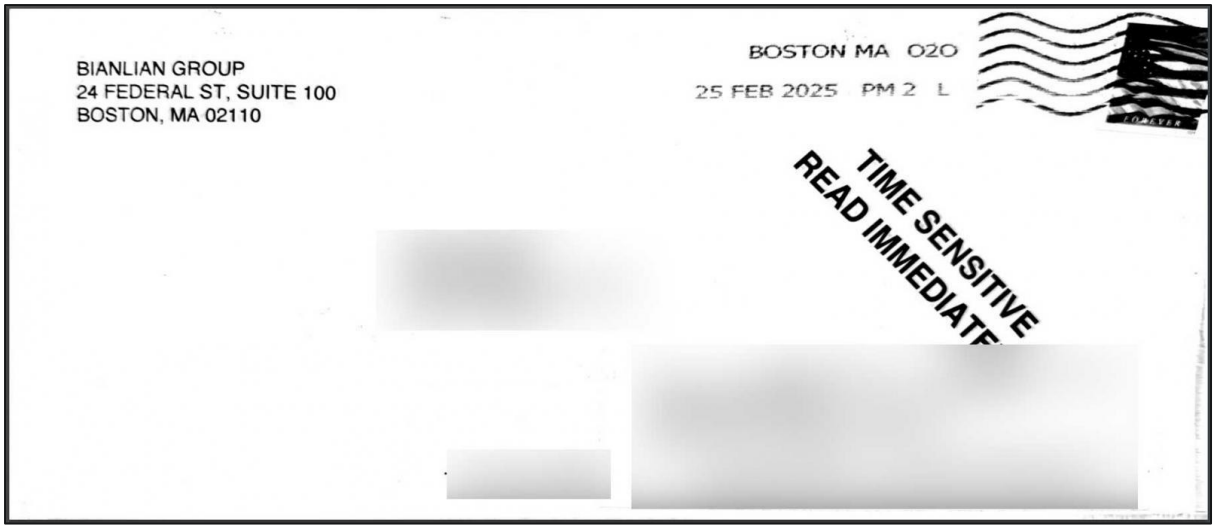

Figure 1: Envelope for fake BianLian ransom note

The scam was first reported by GuidePoint Security and later confirmed by multiple organizations, including Arctic Wolf and BleepingComputer. The letters, mailed from Boston, Massachusetts, are addressed to CEOs and high-level executives, marked as “Time Sensitive”, and claim that threat actors have stolen:

- Customer and employee information (including SSNs and payroll data)
- Financial records, tax documents, and invoices
- Legal and investor information

The ransom notes direct victims to real BianLian Tor leak sites to appear legitimate but falsely claim that the group does not negotiate, and that the recipient has 10 days to pay. Some letters include legitimate compromised passwords to add credibility. Each letter demands a ransom between $250,000 and $500,000, providing a unique Bitcoin address and a QR code for payment. According to Arctic Wolf, all healthcare organizations were

targeted with a fixed ransom demand of $350,000, consistent with the amount reported by a healthcare firm to BleepingComputer.

Dear [REDACTED]

I regret to inform you that we have gained access to [REDACTED] systems and over the past several weeks have exported thousands of data files, including customer order and contact information, employee information with IDs, SSNs, payroll reports, and other sensitive HR documents, company financial documents, legal documents, investor and shareholder information, invoices, and tax documents.

How did this happen?

Your network is insecure and we were able to gain access and intercept your network traffic, leverage your personal email address, passwords, online accounts and other information to social engineer our way into [REDACTED] systems via your home network with the help of another employee. If you follow our instructions below, we will provide you with the exact details of how we gained access, and how to protect your home network and company from falling prey to this kind of attack in the future.

What do we want?

We require [REDACTED] in Bitcoin paid to the address below within 10 days of receipt of this letter. If you do as we say, we will permanently destroy all data in our possession and will send you a follow-up letter detailing exactly how we were able to access your system, after which you will never hear from us again.

If you do not comply, all of [REDACTED] sensitive data will be published to our TOR darknet sites, sent to all interested supervisory organizations and the media, distributed via email to all your investors, partners, customers, employees, and other relevant parties, and you can expect collective lawsuits as we will invite various law firms to take up a group case.

What guarantees we will do what we say?

We are not a politically motivated group and we want nothing more than money. Our industry only works if we hold up our end of the bargain. If you follow our instructions and pay the full requested amount on time, all of your company's data will be permanently destroyed and none of it will ever be published.

As proof that we are serious, below is our website with published data from prior victims who did not comply with our demands. **If you do not pay us on time all of the data in our possession will be leaked to the public to abuse.**

Download and install Tor Browser from this website: https://www.torproject[.]org
Open one of the below links in Tor Browser
[REDACTED] (Main)
[REDACTED] (Backup)

What should you do now?

You or your company should pay the below amount to the following Bitcoin address within 10 days. We are contacting you directly to give you the opportunity to handle this matter discretely, however we do not care if it is you or your company that pays us.

Required Amount: 350,000
Bitcoin Payment Address: [REDACTED]
Bitcoin Payment QR Code: [REDACTED]

Important

Do not go to the police or the FBI for help. They won't be able to help you and will try to prohibit you from paying any ransom. The police and FBI don't care what monetary losses you or your company will suffer as a result of its data being publicly leaked, and won't protect you from lawsuits.

We no longer negotiate with victims: You have 10 days from the receipt of this letter to pay. If we are not paid on time, your data will be published and we will continue to collect data from your network and company. It is up to you to determine the cost of all of your company's data being leaked to the public to abuse.

Sincerely,

BIANLIAN GROUP

Figure 2: Fake BianLian ransom note sent via snail mail

Key Observations:

1. **Targeting Executives via Traditional Mail –** A shift from email extortion to physical mail scams.
2. **Tailored Messaging** – Different industries receive customized threats (e.g., healthcare firms are told patient data was stolen).
3. **No Actual Data Breach Detected –** Security firms confirm these ransom notes are fraudulent and not linked to BianLian.

These fake ransom notes represent a new twist on traditional cyber extortion, targeting corporate executives via physical mail instead of email. While no real breaches have been linked to these letters, organizations must remain vigilant, educate leadership, and report incidents to prevent financial losses and resource misallocation.

RECOMMENDED ACTIONS

- Inform leadership teams about this scam to prevent panic.
- Conduct internal security checks before responding to demands of extortion.
- No payments should be made, as these letters are fraudulent.
- Scammers may expand tactics to other industries.
- Companies receiving these letters should notify law enforcement and security agencies

RESOURCES

https://www.bleepingcomputer.com/news/security/fake-bianlian-ransom-notes-mailed-to-us-ceos-in-postal-mail-scam/

https://www.guidepointsecurity.com/blog/snail-mail-fail-fake-ransom-note-campaign-preys-on-fear/

https://arcticwolf.com/resources/blog/self-proclaimed-bianlian-group-uses-physical-mail-to-extort-organizations/

CONTACT US

Vairav Technology Security Pvt. Ltd.

Cyber Defender from the land of Gurkha

Thirbam Sadak 148, Baluwatar

Kathmandu, Nepal

Phone: +977-01-4541540

Mobile: +977-9820105900

Email: sales@vairavtech.com

Website: https://vairavtech.com