# How INC Ransom and BianLian Use Remote Access to Infiltrate Networks

***C-Suite level threat review by applicable business area addressing active threats.***

INC Ransom and BianLian, two prominent ransomware groups, are leveraging Remote Desktop Protocol (RDP) as a primary entry point to networks. While RDP-based attacks are not new, they remain one of the most common methods cybercriminals use to breach networks, mainly because organizations still have weak or stolen credentials in play. Even though there has been significant effort to secure remote access, RDP is still an easy target for these groups.

## INC Ransom:

INC Ransom is suspected to be a Russian-based cybercrime group that has operated since mid-2023. The group primarily targets the Professional Services, Manufacturing, and Healthcare industries, particularly in North America, Europe, and Australia. So far in 2025, there have been at least fifteen ransomware attacks attributed to INC Ransom. Lynx Ransomware, popular today, is an established and rebranded version of INC Ransom. Despite different variants, INC Ransom remains a major player in the cybercriminal landscape.

## BianLian:

BianLian first appeared in 2022 and is likely operating out of Russia, even though its name suggests a Chinese origin. The group has mainly targeted the United States, with Healthcare and Manufacturing being their primary focus. The group recently moved away from traditional encryption-based extortion tactics and now focuses solely on exfiltrating data.

### INC Ransom:

Threat Level: Medium

**Attack:**

INC Ransom gains initial access to networks primarily by exploiting RDP with stolen or purchased credentials, often acquired from initial access brokers or phishing campaigns (MITRE T1555 and MITRE T1566). In some cases, they exploit vulnerabilities in public-facing applications, such as the Citrix NetScaler vulnerability (CVE-2023-3519) (MITRE T1190). Once inside, they use the RDP sessions to conduct further reconnaissance, which helps them identify high-value targets such as domain admin accounts (MITRE T1591). Access to these accounts allows them to steal sensitive data, create or modify user accounts, and move through the network freely. After gaining complete control, INC Ransom encrypts critical files using the AES encryption algorithm and demands a ransom for the decryption key. In addition to encrypting files, the group attempts to delete shadow copies in the system to hinder system recovery (MITRE T1490).

**Remediation:**

- Enforce the principle of least privilege to limit admin access, which helps reduce the risk of attackers gaining elevated control over the network.
- Restrict RDP access to trusted IPs to prevent unauthorized logins from stolen or purchased credentials.
- Review logs to detect unusual remote access activities.

### BianLian:

Threat Level: Low

**Attack:**

Similarly, BianLian relies on RDP as a primary entry point, using credentials obtained from initial access brokers or phishing campaigns (MITRE T1555 and MITRE T1566). Once inside the network, the group exploits vulnerabilities in services such as Windows 10 and 11 (CVE-2022-37969) to elevate their privileges and deepen their foothold in the network (MITRE T1068). The group uses a variety of tools to turn off antivirus software, which enables them to remain undetected (MITRE T1562). To further evade detection, they rename tasks to resemble legitimate Windows Services (MITRE T1036). BianLian recently showcased their advanced evasion tactics in an attack where they remained undetected in a manufacturing company's network for about two months. Unlike typical ransomware groups, BianLian has shifted to an exfiltration-only method, focusing on stealing sensitive data rather than encrypting files. However, they still pressure victims by printing ransom notes on compromised network printers and directly contacting employees (MITRE T1491).

**Remediation:**

- Regularly patch vulnerabilities in public-facing applications to keep systems up-to-date and secure.
- Implement multifactor authentication to prevent attackers from accessing accounts, even if they have obtained credentials.
- Isolate critical systems to limit lateral movement and reduce attack surface in the event of a network breach.

## INC Ransom:

- **INC Ransom Tactics:** https://www.trendmicro.com/vinfo/us/security/news/ransomware-spotlight/ransomware-spotlight-inc
- **INC Ransom Background:** https://www.vectra.ai/threat-actors/inc-ransom#background

## BianLian:

- **BianLian Tactics Explained:** https://www.picussecurity.com/resource/blog/bianlians-shape-shifting-tactics-from-encryption-to-pure-extortion
- **BianLian Persistence and Ability to Evade Detection:** https://www.bleepingcomputer.com/news/security/mizuno-usa-says-hackers-stayed-in-its-network-for-two-months/

## How K logix Can Help

Technology Advisory

- Email Security
- Endpoint Detection and Response (EDR)
- Identity and Access Management (IAM)
- Managed Security Service Provider (MSSP)
- Security Information and Event Management (SIEM)
- Cloud Security Posture Management (CSPM)
- SaaS Security Posture Management (SaaS)

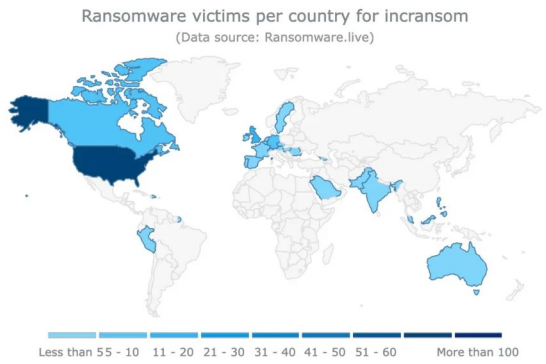
Program Advisory

- Advanced Risk Assessment (i.e., HIPAA, NIST, PCI, etc.)
- Cloud Security Maturity
- Identity and Access Management Program Maturity

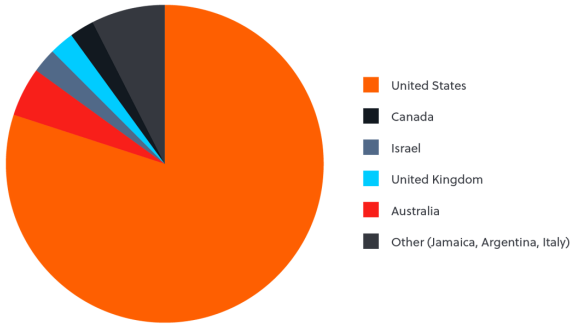
Threat Intelligence

- Notification to customers of threats
- On-demand briefings
- Threat exposure workshops
- User awareness training seminars
- Monthly and quarterly threat intelligence reports

**INC Ransom Attacks by Country:**




**BianLian Attacks by Country:**




## ABOUT K LOGIX

Cybersecurity Advisory and Consulting Services

Our white-glove approach empowers leaders to advance their security programs and strategically align with the business to reduce risk.