**ATT&CK Threat Intelligence Report using Cyber Threat Intelligence (CTI)**

**By:**

**Tevin Herath**

Contents

[Attack 1 : Ransome attack 1](#_Toc177894922)

[Summary: 1](#_Toc177894923)

[Scope: 1](#_Toc177894924)

[Techniques: 1](#_Toc177894925)

[Mitigations and Recommendations: 2](#_Toc177894926)

[Attack 2: Brute-Force 3](#_Toc177894927)

[Summary 3](#_Toc177894928)

[Scope: 3](#_Toc177894929)

[Techniques: 3](#_Toc177894930)

[Mitigations and Recommendations: 4](#_Toc177894931)

# Attack 1 : Ransome attack

## Summary:

In mid-2024, a major ransomware campaign linked to the "LockBit" group targeted financial institutions, healthcare organizations, and large enterprises worldwide. LockBit employed sophisticated evasion techniques and powerful encryption methods to lock victims' data, demanding ransom payments in cryptocurrency.

## Scope:

This report focuses on identifying the tactics and techniques used by attackers to exploit, encrypt, and extort victims by threatening to publish their sensitive data unless a ransom is paid. This analysis maps observed TTPs to the MITRE ATT&CK framework.

## Techniques:

|  |  |  |
| --- | --- | --- |
| **Tactic** | **Technique** | **Description** |
| Initial Access | T1133 External Remote Services (RDP) | The adversary exploited weak RDP credentials to gain initial access to the network. |

|  |  |  |
| --- | --- | --- |
| Initial Access | T1566.001 Phishing: phishing Attachment | Phishing emails containing malicious attachments were sent to employees. |

|  |  |  |
| --- | --- | --- |
| Execution | T1059.003 Command and Scripting Interpreter: Windows Command Shell | Execution of PowerShell scripts to download and run malicious payloads. |

|  |  |  |
| --- | --- | --- |
| Persistence | T1547.001 Boot or Logon Auto start Execution | The adversary modified startup files to persist across reboots. |

|  |  |  |
| --- | --- | --- |
| Privilege Escalation | T1068 Exploitation for Privilege Escalation | Exploiting vulnerabilities in Windows systems to escalate privileges. |

|  |  |  |
| --- | --- | --- |
| Defence Evasion | T1027 Obfuscated Files or Information | The ransomware binary was obfuscated to evade detection by antivirus solutions. |

|  |  |  |
| --- | --- | --- |
| Collection | T1119 Automated Collection | Automated scripts were used to gather sensitive data before encryption. |

|  |  |  |
| --- | --- | --- |
| Impact | T1486 Data Encrypted for Impact | Files across the victim's network were encrypted using LockBit's ransomware. |

|  |  |  |
| --- | --- | --- |
| Exfiltration | T1041 Exfiltration Over C2 Channel | Sensitive data was exfiltrated to external servers controlled by the adversary before encryption. |

## Mitigations and Recommendations:

To mitigate the risks associated with ransomware attacks, we should consider applying the following security measures:

* Disable or restrict RDP access and use multi-factor authentication (MFA) to protect remote access services (T1133)
* Implement endpoint detection and response (EDR) solutions to detect and respond to malicious behaviour like credential dumping (T1003.001).
* Maintain regular, encrypted backups of critical data and store them offline to mitigate the impact of data encryption (T1486)
* Segment critical business systems and restrict unnecessary access to limit lateral movement (T1021.002).
* Educate people about phishing awareness

# Attack 2: Brute-Force

## Summary

In 2024, several organizations experienced an increase in brute force attacks targeting their external-facing services and user accounts. These attacks aimed to compromise accounts by systematically guessing login credentials, leveraging weak passwords or misconfigurations to gain unauthorized access.

## Scope:

Brute force attacks involve repeatedly attempting to guess login credentials, such as passwords, until the correct combination is found. These attacks are often automated using tools or scripts to try large numbers of password combinations quickly. This report analyses the techniques used and provides actionable intelligence to prevent and mitigate such attacks.

## Techniques:

|  |  |  |
| --- | --- | --- |
| **Tactic** | **Technique** | **Description** |
| Initial Access | T1110.001 Brute Force: Password Guessing | Attackers systematically guessed login credentials to gain access to exposed RDP and VPN services. |

|  |  |  |
| --- | --- | --- |
| Persistence | T1078 Valid Accounts | Once valid credentials were obtained, attackers established persistence by using the compromised accounts. |

|  |  |  |
| --- | --- | --- |
| Privilege Escalation | T1068 Exploitation for Privilege Escalation | Attackers used the compromised accounts to attempt privilege escalation by exploiting system vulnerabilities. |

|  |  |  |
| --- | --- | --- |
| Defence Evasion | T1027 Obfuscated Files or Information | Some attackers obfuscated malicious scripts to evade detection while leveraging compromised credentials. |

|  |  |  |
| --- | --- | --- |
| Credential Access | T1110 Brute Force | Attackers used automated brute force tools to repeatedly attempt login attempts until success. |

|  |  |  |
| --- | --- | --- |
| Lateral Movement | T1021.001 Remote Services: RDP | Compromised credentials were used to move laterally within the victim's network by exploiting RDP. |

|  |  |  |
| --- | --- | --- |
| Collection | T1005 Data from Local System | Attackers accessed and collected sensitive files from compromised systems. |

## Mitigations and Recommendations:

To mitigate the risks associated with Brute-force attacks, we should consider applying the following security measures:

* Implement strict password policies requiring complex and unique passwords to minimize the success of brute force attacks (T1110.001).
* Use MFA across all external-facing services and sensitive accounts to add an extra layer of defense (T1078).
* Implement account lockout policies to disable user accounts after a predefined number of failed login attempts. This will prevent automated tools from continuously trying credentials (T1110).
* Set up alerts for multiple failed login attempts, especially from unusual geographic locations or IP addresses (T1005).