



Threat Intelligence Assessment report on Lockbit Group

This report provides a comprehensive overview of the threat landscape associated with LockBit 3.0 group, enabling organizations to better understand the risks posed by this threat actor and implement effective cybersecurity measures to mitigate potential impacts.

Submitted To: Black Perl

Submitted By: Lokesh Sundaramurthy [[LinkedIn](#)]

Published Date: 02-26-2024.

INDEX

1. Executive Summary
2. Analysis & Attribution
3. Threat Actor Attribution & Rating
4. Chain of Infection
5. IOCs or IOAs
6. Impact and Mitigation
7. References

1. Executive Summary:

Threat Group Background	The LockBit 3.0 group is a sophisticated cybercriminal organization known for its ransomware operations targeting organizations across various industries globally.
Country of Origin	Russia
Chronology of LockBit Ransomware Group's Activities and Impact	<p>2024:</p> <ul style="list-style-type: none"> February 24: Threat actors published few more companies leaked data on dark web with a caption Lockbit 4.0 February 23: Japan Interpol released a Decryptor for lockbit 3.0. February 20: Operation Cronos, led by global law enforcement agencies such as the FBI, NCA, and Europol, successfully disrupted the operations of the LockBit ransomware group. <p>2023:</p> <ul style="list-style-type: none"> August 31: LockBit faced operational struggles, issued empty threats, but experienced a sudden surge. July 03: LockBit claimed to hack TSMC, but only their supplier, Kinmax Technology, was breached. June 23: LockBit was reportedly developing ransomware targeting a broader range of systems, including Apple, Linux, and FreeBSD. June 15: LockBit was identified as the most active global ransomware group and RaaS provider based on the number of victims on their data leak site. <p>2022:</p> <ul style="list-style-type: none"> LockBit became the most active ransomware group after Conti's shutdown. <p>2021:</p> <ul style="list-style-type: none"> Atento, a CRM company, reported \$42.1 million in losses due to a LockBit attack in their financial performance report. This loss included \$34.8 million in revenue loss and \$7.3 million in mitigation expenses. <p>2019:</p> <ul style="list-style-type: none"> LockBit Ransomware Group was first observed in September.

Target Countries	<p>Thailand 4.0%</p> <p>Taiwan 4.0%</p> <p>Spain 4.0%</p> <p>Germany 4.2%</p> <p>Brazil 4.4%</p> <p>Italy 5.5%</p> <p>Canada 5.5%</p> <p>United Kingdom 7.3%</p> <p>France 11.7%</p> <p>United States 49.3%</p>
Target Sectors	<p>Targets by Industry</p> <p>Attack Counts</p> <p>Industries</p>
Impact	<p>LockBit 3.0 ransomware group includes significant financial losses, operational disruptions, and reputational damage for targeted organizations globally.</p>
Decryption Possibilities	<p>Leverage available decryption tools, such as the LockBit decryptor provided by No More Ransom, to recover encrypted files without paying the ransom.</p> <p>This can significantly reduce the impact of a ransomware attack and restore normal operations without incurring financial losses or data compromise.</p> <p>Reference Link: https://www.nomoreransom.org/</p>
Mitigation	<ul style="list-style-type: none"> Implement robust cybersecurity measures such as regular software patching, network segmentation, and access controls to prevent initial access by LockBit 3.0 ransomware group.

- Conduct regular employee training on phishing awareness and best cybersecurity practices to mitigate the risk of social engineering attacks, which are commonly used by LockBit 3.0 for initial compromise.
- Maintain comprehensive and regularly updated backups of critical data stored offline to ensure quick recovery in the event of a ransomware attack by LockBit 3.0, minimizing the impact of potential data encryption.

2. Analysis & Attribution:

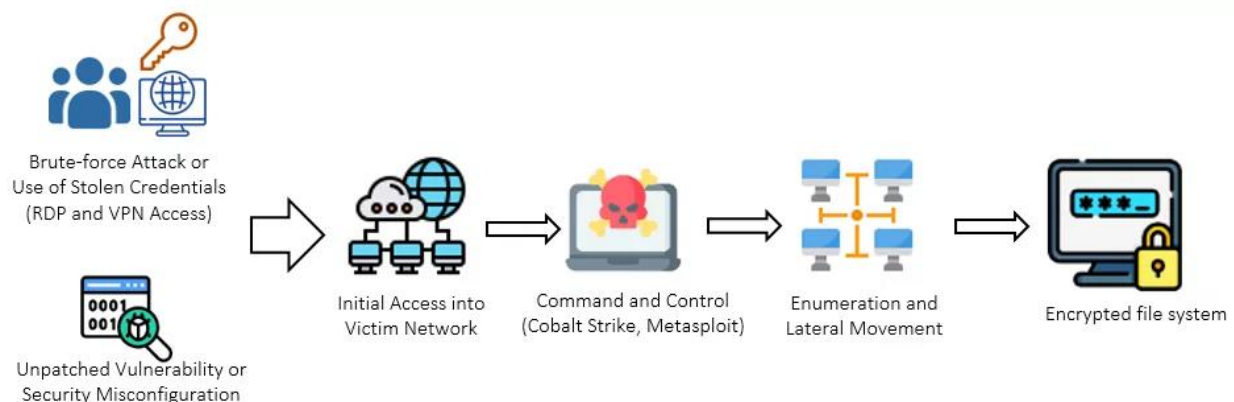
LockBit 3.0 group has been actively recruiting affiliates and sharing tips on evading detection, exploiting vulnerabilities, and negotiating ransom payments with victims.

Social media posts and advertisements by LockBit 3.0 group highlight their capabilities in encrypting sensitive data, exfiltrating information for leverage, and providing decryption tools upon ransom payment, showcasing their business-like approach to cybercrime.

LockBit ransomware deletes log files, files in the recycle bin, and volume shadow copies after encrypting the victim's files. The group also employs a hybrid [encryption](#) approach using AES and RSA encryption algorithms.

Sample Analysis:

Analysis of malware samples associated with LockBit 3.0 group reveals the use of custom-built ransomware variants with advanced encryption algorithms and anti-analysis techniques, indicating a high level of technical proficiency.



An overview of a typical LockBit operation. (Source: Australian Cyber Security Center)

Refer to [cybersecurity-advisories/aa23-165a](#), [Threat-Analysis-Assemble-LockBit-3](#) for more information.

Common CVEs Exploited by LockBit Affiliates

CISA notes that LockBit affiliates take advantage of both old and new exploits, including:

- [CVE-2021-22986](#): F5 iControl REST Unauthenticated Remote Code Execution Vulnerability
- [CVE-2023-0669](#): Fortra GoAnywhere Managed File Transfer (MFT) Remote Code Execution Vulnerability
- [CVE-2023-27350](#): PaperCut MF/NG Improper Access Control Vulnerability
- [CVE-2021-44228](#): Apache Log4j2 Remote Code Execution Vulnerability
- [CVE-2021-22986](#): F5 BIG-IP and BIG-IQ Centralized Management iControl REST Remote Code Execution Vulnerability
- [CVE-2020-1472](#): NetLogon Privilege Escalation Vulnerability
- [CVE-2019-0708](#): Microsoft Remote Desktop Services Remote Code Execution Vulnerability
- [CVE-2018-13379](#): Fortinet FortiOS Secure Sockets Layer (SSL) Virtual Private Network (VPN) Path Traversal Vulnerability

Tools Used by LockBit Affiliates:

LockBit has been identified to use the following tools, as CISA lists:

- **7-zip**: Compresses data to avoid detection before exfiltration.
- **AdFind**: Gathers Active Directory information for network exploitation.
- **Advanced Internet Protocol (IP) Scanner**: Maps victim networks for access vectors.
- **Advanced Port Scanner**: Identifies open ports for exploitation.
- **AdvancedRun**: Enables privilege escalation before software execution.
- **AnyDesk, Atera RMM, Splashtop, TeamViewer**: Remote access tools for network compromise.
- **Bat Armor, Backstab, Defender Control**: Bypasses security measures for execution.
- **Bloodhound, Impacket, LaZagne**: Exploits Active Directory for network infiltration.
- **Chocolatey, FileZilla, FreeFileSync, MEGA Ltd MegaSync, Rclone, WinSCP**: Facilitates data exfiltration.


- **GMER, PCHunter, PowerTool, Process Hacker, TDSSKiller:** Terminate and bypass endpoint detection.
- **Microsoft Sysinternals ProcDump, PsExec:** Extract credentials and execute commands remotely.
- **Mimikatz:** Extracts credentials for network access.
- **Ngrok:** Bypasses network protections via internet tunneling.
- **PasswordFox:** Extracts browser passwords for exploitation.
- **PuTTY Link (Plink):** Avoids detection during SSH actions.
- **Seatbelt, SoftPerfect Network Scanner:** Enumerates system and network information.
- **ScreenConnect, ThunderShell, Splashtop, TeamViewer:** Facilitates remote system access.
- **WinSCP:** Enables data exfiltration via SSH File Transfer Protocol.

3. Threat Actor Attribution & Rating:

LockBit 3.0 group operates as a ransomware-as-a-service (RaaS) organization, providing affiliates with access to their ransomware infrastructure in exchange for a percentage of the ransom payments. They are motivated by financial gain and have demonstrated a willingness to target organizations of all sizes and sectors.

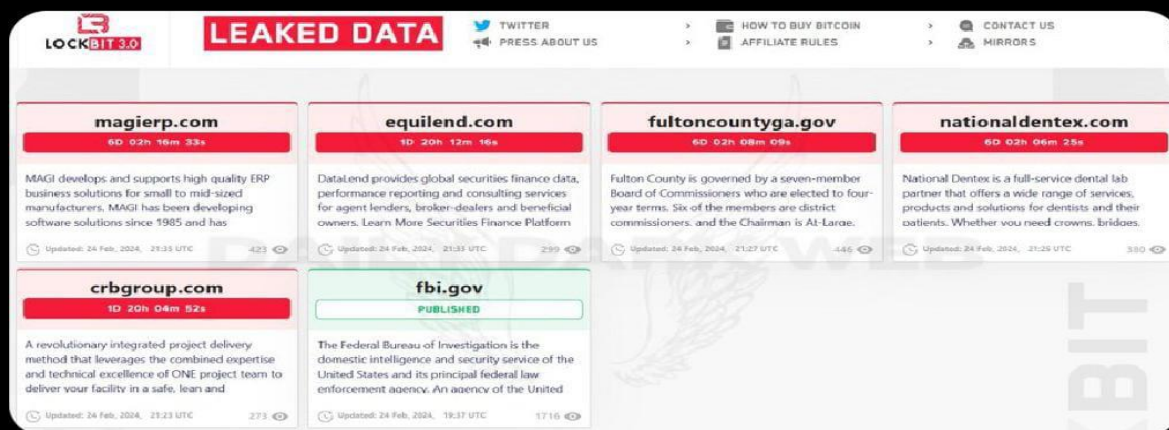
Threat Actor Rating: highly sophisticated

Lockbit 4.0 is Loading ...  Lockbit released a lengthy response for the FBI and others

"The only thing that motivates me to work is strong competitors and the FBI" 

You can read the full post here:
samples.vx-underground.org/tmp/Lockbit_St...
(via: @vxunderground)

#DarkWeb #LockBit



7:59 am · 25 Feb 24 · 5,353 Views

4. Chain of Infection:

MITRE ATT&CK:

LockBit 3.0 group employs a variety of techniques outlined in the MITRE ATT&CK framework, including initial access through phishing emails or exploiting remote desktop protocols (RDP), privilege escalation using stolen credentials or exploitation of misconfigurations, and lateral movement using tools like Mimikatz and PsExec.

MITRE ATT&CK Critical TTPs

Initial Access	Valid Accounts					
Execution	Windows Management Instrumentation					
Persistence	Boot or Logon AutoStart Execution	Create or Modify System Process	Valid Accounts			
Privilege Escalation	Boot or Logon AutoStart Execution	Abuse Elevation Control Mechanism	Create or Modify System Process	Process Injection	Valid Accounts	
Defense Evasion	Abuse Elevation Control Mechanism	Debugger Evasion	Indicator Removal on Host	Process Injection	System Binary Proxy Execution	Valid Accounts
Credential Access	OS Credential Dumping					
Discovery	Debugger Evasion					
Collection	Automated Collection					
Exfiltration	Exfiltration Over C2 Channel					
Impact	Data Destruction	Inhibit System Recovery	Service Stop			

Source: <https://controlcompass.github.io>

<u>Initial Access</u>		
Technique Title	ID	Use
Valid Accounts	T1078	LockBit 3.0 actors obtain and abuse credentials of existing accounts as a means of gaining initial access.
Exploit External Remote Services	T1133	LockBit 3.0 actors exploit RDP to gain access to victim networks.
Drive-by Compromise	T1189	LockBit 3.0 actors gain access to a system through a user visiting a website over the normal course of browsing.
Exploit Public-Facing Application	T1190	LockBit 3.0 actors exploit vulnerabilities in internet-facing systems to gain access to victims' systems.
Phishing	T1566	LockBit 3.0 actors use phishing and spearphishing to gain access to victims' networks.
<u>Execution</u>		
Technique Title	ID	Use
Execution	TA0002	LockBit 3.0 launches commands during its execution.
Software Deployment Tools	T1072	LockBit 3.0 uses Chocolatey, a command-line package manager for Windows.

<u>Persistence</u>		
Technique Title	ID	Use
Valid Accounts	T1078	LockBit 3.0 uses a compromised user account to maintain persistence on the target network.
Boot or Logo Autostart Execution	T1547	LockBit 3.0 enables automatic logon for persistence.
<u>Privilege Escalation</u>		
Technique Title	ID	Use
Privilege Escalation	TA0004	Lockbit 3.0 will attempt to escalate to the required privileges if current account privileges are insufficient.
Boot or Logo Autostart Execution	T1547	LockBit 3.0 enables automatic logon for privilege escalation.
<u>Defense Evasion</u>		
Technique Title	ID	Use
Obfuscated Files or Information	T1027	LockBit 3.0 will send encrypted host and bot information to its C2 servers.
Indicator Removal: File Deletion	T1070.004	LockBit 3.0 will delete itself from the disk.
Execution Guardrails: Environmental Keying	T1480.001	LockBit 3.0 will only decrypt the main component or continue to decrypt and/or

		decompress data if the correct password is entered.
<u>Credential Access</u>		
Technique Title	ID	Use
OS Credential Dumping: LSASS Memory	T1003.001	LockBit 3.0 uses Microsoft Sysinternals ProDump to dump the contents of LSASS.exe.
<u>Discovery</u>		
Technique Title	ID	Use
Network Service Discovery	T1046	LockBit 3.0 uses SoftPerfect Network Scanner to scan target networks.
System Information Discovery	T1082	LockBit 3.0 will enumerate system information to include hostname, host configuration, domain information, local drive configuration, remote shares, and mounted external storage devices.
System Location Discovery: System Language Discovery	T1614.001	LockBit 3.0 will not infect machines with language settings that match a defined exclusion list.
<u>Lateral Movement</u>		
Technique Title	ID	Use
Remote Services: Remote Desktop Protocol	T1021.001	LockBit 3.0 uses Splashtop remote- desktop software to facilitate lateral movement.

<u>Command and Control</u>		
Technique Title	ID	Use
Application Layer Protocol: File Transfer Protocols	T1071.002	LockBit 3.0 uses FileZilla for C2.
Protocol Tunnel	T1572	LockBit 3.0 uses Plink to automate SSH actions on Windows.
<u>Exfiltration</u>		
Technique Title	ID	Use
Exfiltration	TA0010	LockBit 3.0 uses Stealbit, a custom exfiltration tool first used with LockBit 2.0, to steal data from a target network.
Exfiltration Over Web Service	T1567	LockBit 3.0 uses publicly available file sharing services to exfiltrate a target's data.
Exfiltration Over Web Service: Exfiltration to Cloud Storage	T1567.002	LockBit 3.0 actors use (1) rclone, an open source command line cloud storage manager to exfiltrate and (2) MEGA, a publicly available file sharing service for data exfiltration.

<u>Impact</u>		
Technique Title	ID	Use
Data Destruction	T1485	LockBit 3.0 deletes log files and empties the recycle bin.
Data Encrypted for Impact	T1486	LockBit 3.0 encrypts data on target systems to interrupt availability to system and network resources.
Service Stop	T1489	LockBit 3.0 terminates processes and services.
Inhibit System Recovery	T1490	LockBit 3.0 deletes volume shadow copies residing on disk.
Defacement: Internal Defacement	T1491.001	LockBit 3.0 changes the host system's wallpaper and icons to the LockBit 3.0 wallpaper and icons, respectively.

Their attack lifecycle follows the Cyber Kill Chain model, progressing from reconnaissance and weaponization to delivery, exploitation, installation, command and control (C2), and ultimately, actions on objectives (AoO) such as data encryption and ransom demands.

5. IOCs or IOAs:

IoCs from US Governmental Agencies' #StopRansomware initiation [report](#) on LockBit 3.0;

File Sharing Sites:

- [https://www.premiumize\[.\]com](https://www.premiumize[.]com)
- [https://anonfiles\[.\]com](https://anonfiles[.]com)
- [https://www.sendspace\[.\]com](https://www.sendspace[.]com)
- [https://fex\[.\]net](https://fex[.]net)
- [https://transfer\[.\]sh](https://transfer[.]sh)
- [https://send.exploit\[.\]in](https://send.exploit[.]in)

Freeware and Open-Source Tools:

Chocolatey, FileZilla, Impacket, MEGA Ltd MegaSync, Microsoft Sysinternals ProcDump and PsExec, Mimikatz, Ngrok, PuTTY Link (Plink), Rclone, SoftPerfect Network Scanner, Splashtop, and WinSCP.

Mutex:

- Global

UAC Bypass via Elevated COM Interface:

- C:WindowsSystem32dllhost.exe

Volume Shadow Copy Deletion:

- Select * from Win32_ShadowCopy

Registry Artifacts:

- HKCR.
- HKCRDefaultIcon
- HKCUControl PanelDesktopWallPaper
- SOFTWAREPoliciesMicrosoftWindowsOOBE
- SOFTWAREMicrosoftWindows NTCurrentVersionWinlogon

IP Address and Hash values:

Type	Value
IP	212[.]102[.]39[.]138
IP	194[.]32[.]122[.]35
IP	178[.]175[.]129[.]35
IP	178[.]162[.]209[.]138
IP	178[.]162[.]209[.]137
IP	172[.]93[.]181[.]238
IP	156[.]146[.]41[.]94
IP	216[.]24[.]213[.]7
IP	37[.]46[.]115[.]29
IP	37[.]46[.]115[.]26
IP	37[.]46[.]115[.]24
IP	37[.]46[.]115[.]17
IP	37[.]46[.]115[.]16
IP	212[.]102[.]35[.]149
IP	178[.]175[.]129[.]37
IP	91[.]90[.]122[.]24
SHA256	5fff24d4e24b54ac51a129982be591aa59664c888dd9fc9f26da7b226c55d835
SHA256	bb574434925e26514b0daf56b45163e4c32b5fc52a1484854b315f40fd8ff8d2
SHA256	9a3bf7ba676bf2f66b794f6cf27f8617f298caa4ccf2ac1ecdcbef260306194
SHA1	e141562aab9268faa4aba10f58052a16b471988a
SHA1	3d62d29b8752da696caa9331f307e067bc371231
SHA1	3d62d29b8752da696caa9331f307e067bc371231
MD5	03f82d8305ddda058a362c780fe0bc68
MD5	fd8246314ccc8f8796ae2d7cbb02b1
MD5	f41fb69ac4fccbfc7912b225c0cac59d
MD5	ee397c171fc936211c56d200acc4f7f2
MD5	dfa65c7aa3ff8e292e68ddfd2caf2cea
MD5	d1d579306a4ddf79a2e7827f1625581c
MD5	b806e9cb1b0f2b8a467e4d1932f9c4f4
MD5	8ff5296c345c0901711d84f6708cf85f
MD5	8af476e24db8d3cd76b2d8d3d889bb5c
MD5	6c247131d04bd615cfac45bf9fbd36cf
MD5	58ea3da8c75afc13ae1ff668855a63

Yara Rules:

```
import "pe"

rule LockBit_3_dll
{
    meta:
        author = "VMware TAU" //bdana
        date = "2022-Oct-12"
        description = "Identifies LockBit 3.0 DLL encryptor by exported function names."
        rule_version = "1"
        yara_version = "4.2.3"
        exemplar_hash = "c2529655c36f1274b6aaa72911c0f4db7f46ef3a71f4b676c4500e180595cac6"

    condition:
        pe.exports("del") and
        pe.exports("gdel") and
        pe.exports("gdll") and
        pe.exports("gmod") and
        pe.exports("pmod") and
        pe.exports("sdll") and
        pe.exports("wdll")
}

rule LockBit_3_exe
{
    meta:
        author = "VMware TAU" //bdana
        date = "2022-Oct-12"
        description = "Identifies LockBit 3.0 exe encryptor section names, and artifact section names."
        rule_version = "1"
```

```
yara_version = "4.2.3"
```

```
exemplar_hash = "5202e3fb98daa835cb807cc8ed44c356f5212649e6e1019c5481358f32b9a8a7"
```

strings:

```
$text = ".text" ascii wide
```

```
$itext = ".itext" ascii wide
```

```
$data = ".data" ascii wide
```

```
$rdata = ".rdata" ascii wide
```

```
$idata = ".idata" ascii wide
```

```
$xyz = ".xyz" ascii wide
```

```
$reloc = ".reloc" ascii wide
```

```
$bss = ".bss" ascii wide
```

condition:

```
#text > 2 and
```

```
#itext > 1 and
```

```
#data > 1 and
```

```
#rdata > 2 and
```

```
#idata > 3 and
```

```
$reloc and
```

```
$bss and $xyz and not
```

```
for any i in (0..pe.number_of_sections-1) : (
```

```
    pe.sections[i].name == ".xyz" or
```

```
    pe.sections[i].name == ".bss"
```

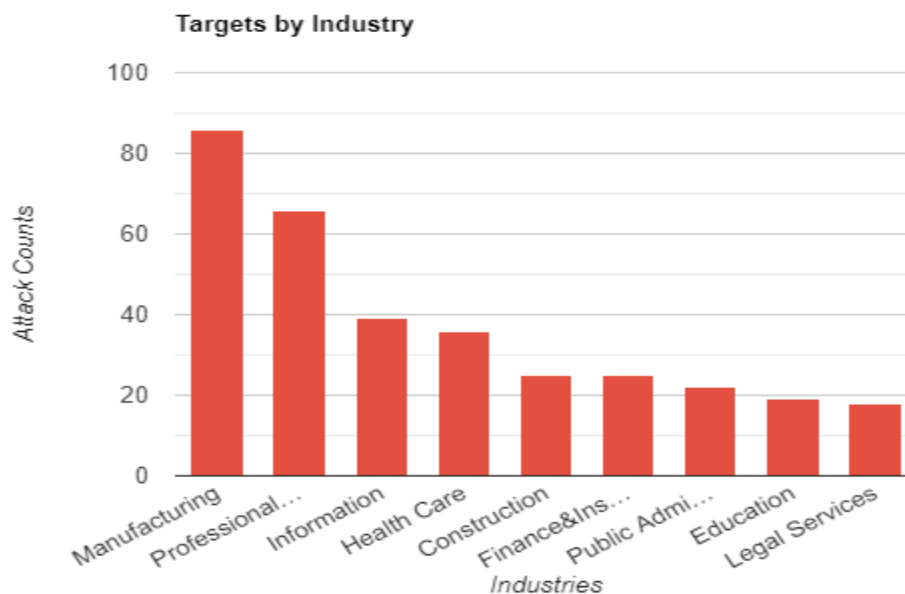
```
)
```

```
}
```

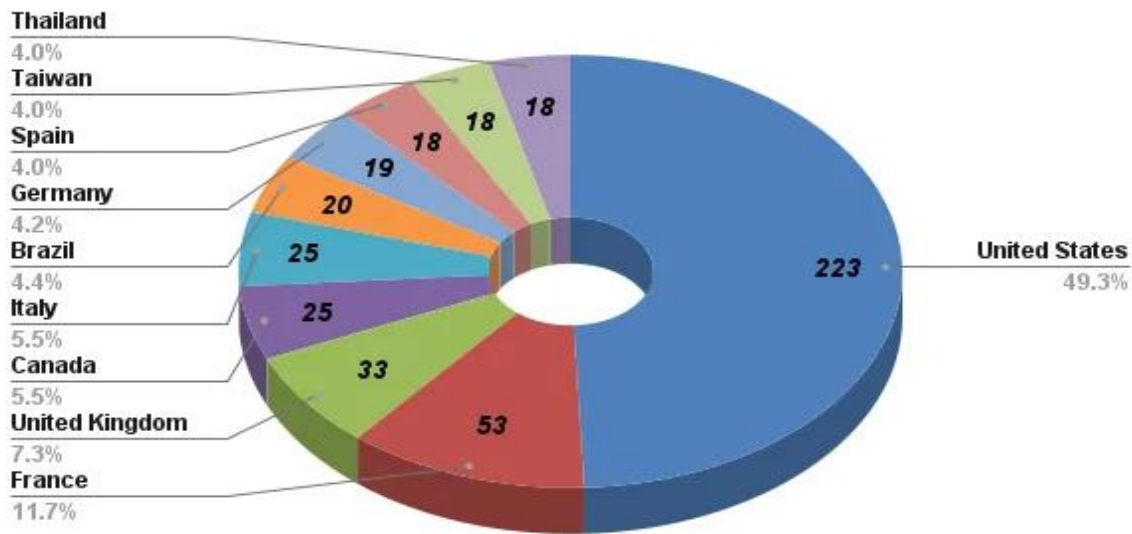
6. Impact and Mitigation:

Impact:

LockBit 3.0 group's ransomware attacks have resulted in significant financial losses, operational disruptions, and reputational damage for victim organizations, highlighting the need for robust cybersecurity measures and incident response capabilities. Following are the Top targeted industries and countries.



Top targeted industries by LockBit 3.0 [[Source](#)]



Ransomware victims of LockBit 3.0 by country of origin. [Source]

Mitigation:

Mitigation strategies include regular software patching, employee training on cybersecurity best practices, implementation of network segmentation and access controls, deployment of endpoint detection and response (EDR) solutions, and regular backups of critical data to mitigate the impact of ransomware attacks.

1. Data Protection and Recovery:

- Implement robust backup and recovery strategies to safeguard sensitive data and maintain multiple copies in secure, segmented locations.
- Adhere to NIST standards for password management, emphasizing longer passwords, hashed storage, and multifactor authentication to mitigate credential-based attacks.

2. Network and Endpoint Security:

- Segment networks to limit the spread of ransomware and deploy network monitoring tools to detect abnormal activity indicative of ransomware traversal.
- Maintain up-to-date operating systems, software, and firmware, and enable real-time detection with antivirus software on all hosts.

3. Access Controls and Privilege Management:

- Review and audit user accounts regularly, disabling unused ports and implementing time-based access controls, including Just-in-Time (JIT) access for privileged accounts.
- Disable command-line and scripting activities to prevent privilege escalation and lateral movement by threat actors.

4. Backup Validation and Security Controls:

- Validate security controls against MITRE ATT&CK techniques relevant to ransomware threats, testing and tuning security technologies to enhance detection and prevention capabilities.
- Maintain offline, encrypted backups covering the entire organization's data infrastructure to ensure data integrity and availability in the event of a ransomware attack.

By proactively implementing these recommendations and continually assessing and validating security controls, organizations can enhance their resilience against ransomware threats, including those posed by sophisticated adversaries like LockBit 3.0.

Detailed Mitigation Steps are available on <https://www.cisa.gov/>

Leverage available [decryption tools](#), such as the LockBit decryptor provided by No More Ransom, to recover encrypted files without paying the ransom. This can significantly reduce the impact of a ransomware attack and restore normal operations without incurring financial losses or data compromise.

DISCLAIMER The information in this report is being provided “as is” for informational purposes only. The authoring organizations do not endorse any commercial product or service, including any subject of analysis. Any reference to specific commercial products, processes, or services by service mark, trademark, manufacturer, or otherwise, does not constitute or imply endorsement, recommendation, or favoring by the authoring organizations.

7. References:

- [1] <https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-165a>
- [2] <https://www.cybereason.com/hubfs/dam/collateral/reports/Threat-Analysis-Assemble-LockBit-3.pdf>
- [3] <https://socradar.io/dark-web-profile-lockbit-3-0-ransomware/>
- [4] <https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-075a>
- [5] <https://www.txone.com/blog/malware-analysis-lockbit-3-0/>
- [6] <https://www.securin.io/articles/all-about-lockbit-ransomware/>
- [7] <https://blogs.vmware.com/security/2022/10/lockbit-3-0-also-known-as-lockbit-black.html>
- [8] <https://www.manageengine.com/log-management/cyber-security/lockbit-ransomware.html>
- [9] <https://www.sentinelone.com/anthology/lockbit-3-0-lockbit-black/>
- [10] <https://academy.blackperldfir.com/learn>
- [11] [https://www.nomoreransom.org/uploads/Decryption Checker for LockBit Guide.pdf](https://www.nomoreransom.org/uploads/Decryption%20Checker%20for%20LockBit%20Guide.pdf)