Hive Pro

Threat Level

Red

CISA: AA23-165A

Hiveforce Labs

# THREAT ADVISORY

ATTACK REPORT

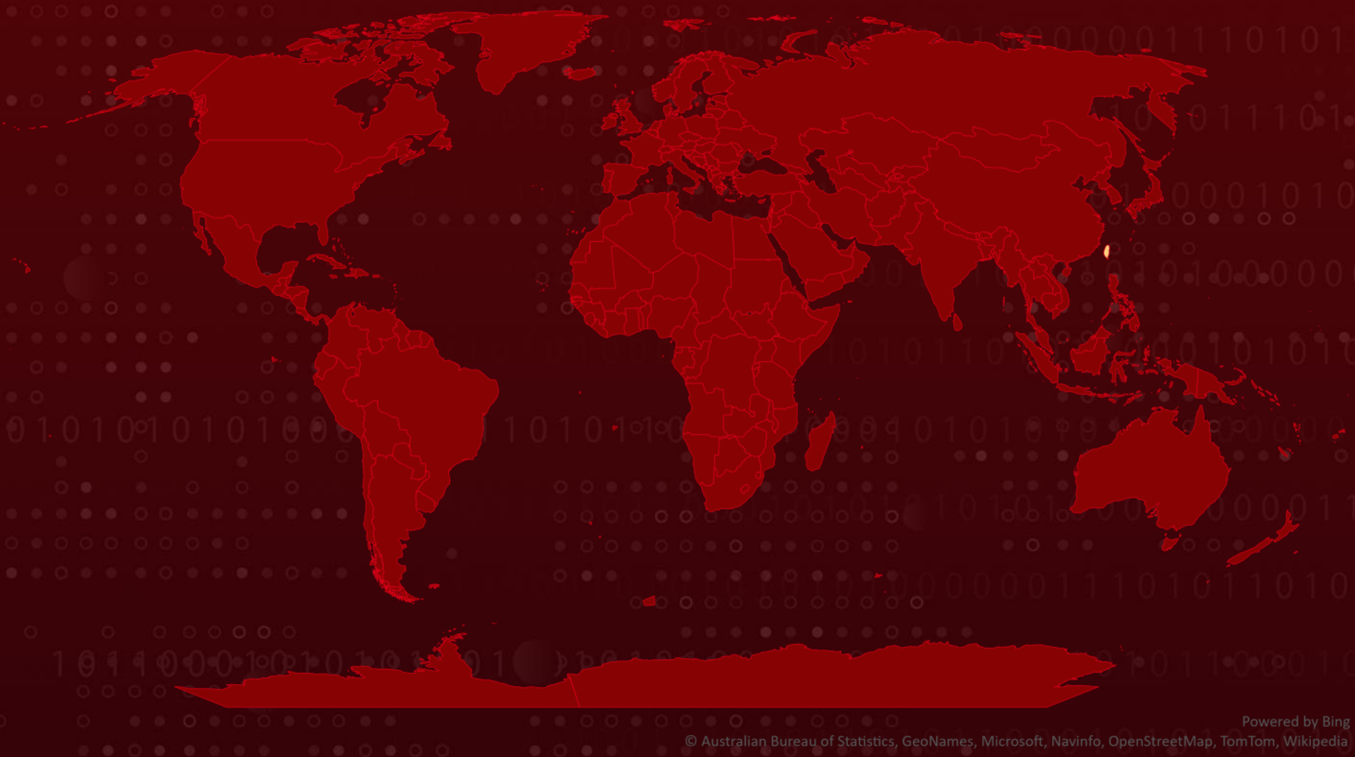
# Lockbit Ransomware strikes, demands $70-million Ransom

| Date of Publication | Admiralty Code | TA Number |
|---|---|---|
| July 03, 2023 | A1 | TA2023285 |

# Summary

**Threat Actor:** National Hazard Agency, sub-clique of Lockbit Ransomware group
**Malware:** Lockbit Ransomware
**Attack Country:** Taiwan
**Attack Industry:** Technology
**Attack Details:** Lockbit sub-group, National Hazard Agency, claims of data exfiltration from TSMC systems, allegedly deployed Ransomware and demands 70-million-dollar ransom. TSMC has clarified that their system is unaffected, and an TSMC IT supplier is impacted by the attack.

## Attack Regions



Powered by Bing
© Australian Bureau of Statistics, GeoNames, Microsoft, Navinfo, OpenStreetMap, TomTom, Wikipedia

# Attack Details

#1 The Lockbit Ransomware group, National Hazard Agency, has claimed of targeting TSMC and is demanding 70-million-dollar Ransom, Attackers are claiming to be in possession of sensitive information and threatens to release data in public domain if demand is not met.

#2 Lockbit operates as Ransomware as-a-service and is known for their fast encryption. They employ triple-extortion technique of encrypting data, threatening to leak stolen data and sell data to other adversaries/ enemies/ competing business.

#3 TSMC (Taiwan Semiconductor Manufacturing Company) is one of the world's largest semiconductor manufacturers, supplying chips to tech giants such as Apple and Qualcomm. TSMC has officially confirmed that they have not experienced any attacks or breaches, and their systems remain unaffected. However, it has been reported that one of TSMC's IT suppliers (Kinmax Technology) is impacted by cyber attack.

#4 Kinmax Technology has confirmed of a cyber attack on its engineering-test system and the leaked content mainly consisted of system installation preparation and default configurations. Kinmax also provides services to other companies like Microsoft, Citrix, Cisco, VMWare, and HPE.

# Recommendations

**Patch and Update Software:** Keep all operating systems, applications, and firmware up to date with the latest security patches and updates. LockBit affiliates often exploit known vulnerabilities to gain initial access to systems. By promptly applying patches, organizations can mitigate the risk of these vulnerabilities being exploited.

**Conduct Regular Data Backups:** Implement a robust data backup strategy that includes regular backups of critical data and systems, ad hoc and periodic backup restoration test. In the event of a LockBit ransomware attack, having up-to-date backups will allow organizations to restore their systems and data without paying the ransom.

**Protect your Backups:** Ensure backups are adequately protected, employ 3-2-1-1 back up principle and Deploy specialized tools to ensure backup integrity and availability.

Block Lockbit known Indicator of Compromise, refer Hive Pro recent alert **here**.

# Potential MITRE ATT&CK TTPs

| | | | |
|---|---|---|---|
| TA0001<br>Initial Access | TA0002<br>Execution | TA0003<br>Persistence | TA0004<br>Privilege Escalation |
| TA0007<br>Discovery | TA0008<br>Lateral Movement | TA0009<br>Collection | TA0011<br>Command and Control |
| TA0010<br>Exfiltration | TA0040<br>Impact | T1482<br>Domain Trust Discovery | T1003<br>OS Credential Dumping |
| T1095<br>Non-Application Layer Protocol | T1003.001<br>LSASS Memory | T1555<br>Credentials from Password Stores | T1082<br>System Information Discovery |
| T1048<br>Exfiltration Over Alternative Protocol | T1190<br>Exploit Public-Facing Application | T1484.001<br>Group Policy Modification | T1027<br>Obfuscated Files or Information |
| T1027.002<br>Software Packing | T1480<br>Execution Guardrails | T1070.004<br>File Deletion | T1566<br>Phishing |
| T1548<br>Abuse Elevation Control Mechanism | T1547<br>Boot or Logon Autostart Execution | T1486<br>Data Encrypted for Impact | T1059<br>Command and Scripting Interpreter |
| T1480.001<br>Environmental Keying | T1569.002<br>Service Execution | T1569<br>System Services | T1078<br>Valid Accounts |
| T1561.001<br>Disk Content Wipe | | | |

# References

https://techmonitor.ai/technology/cybersecurity/tsmc-cyberattack-ransomware-lockbit

https://www.hivepro.com/lockbit-ransomware-evolving-tactics-and-pervasive-impact-in-2023

https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-165a

https://www.hivepro.com/lockbit-ransomware-targets-macos/

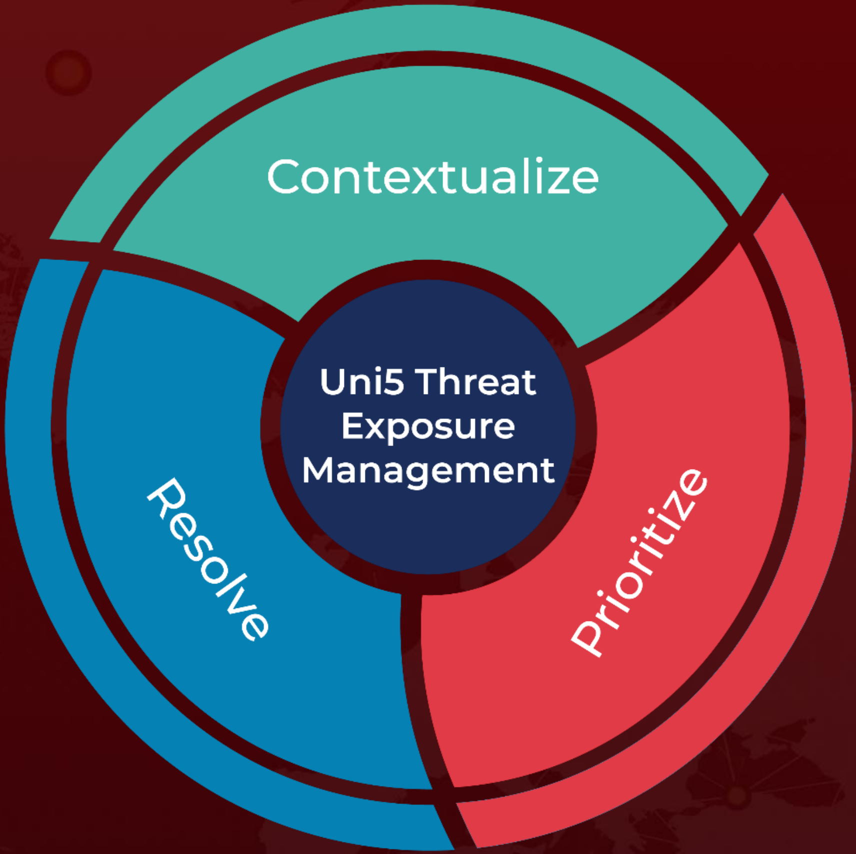
https://www.hivepro.com/lockbit-3-0-makes-a-comeback-by-exploiting-log4j/

https://www.hivepro.com/lockbit-2-0-ransomware-affiliates-targeting-renowned-organizations/

# What Next?

At **Hive Pro**, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a free demo with **HivePro Uni5**: Threat Exposure Management Platform.



REPORT GENERATED ON

**July 03, 2023 • 8:30 AM**

More at www.hivepro.com