Hive Pro

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

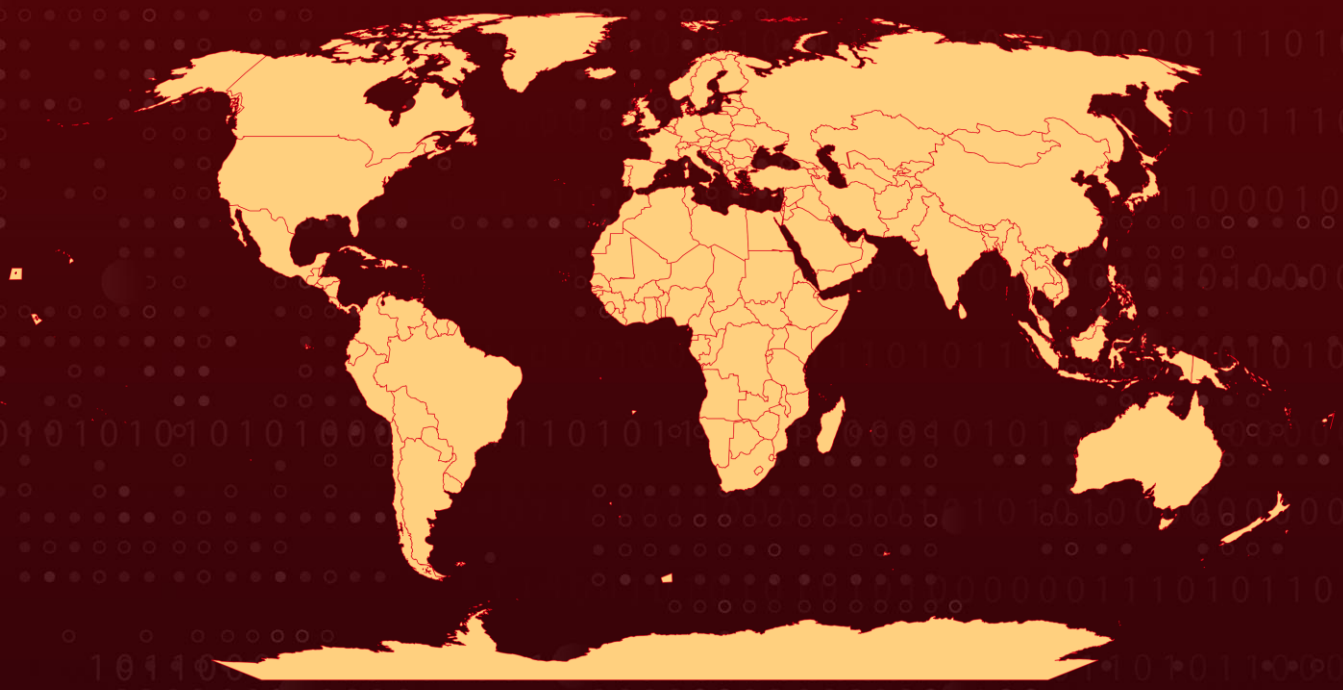
LockBit 3.0 Builder Unleashed Custom Ransomware on the Rise

Date of Publication	Admiralty Code	TA Number
April 17, 2024	A1	TA2024151

Summary

Attack Began: March 10, 2024
Targeted Countries: Worldwide
Malware: LockBit 3.0 ransomware (aka LockBit Black)
Affected Platform: Windows
Attack: A leaked LockBit 3.0 builder tool is enabling attackers to create highly dangerous customized ransomware variants. These customized variants pose a heightened threat as they can exploit stolen administrator credentials to propagate across a network and erase logs, significantly hindering incident response efforts.

Attack Regions



Attack Details

#1 Threat actors exploit the LockBit 3.0 ransomware for its advanced encryption capabilities, allowing them to effectively encrypt victims' files and demand a ransom for decryption keys. The availability of a leaked LockBit 3.0 builder tool, which was leaked in 2022, empowers attackers to craft highly dangerous customized ransomware variants. These tailored strains can exploit stolen administrator credentials to swiftly propagate through a network and erase logs, complicating response efforts to an attack.

#2 The leaked builder simplifies the creation of personalized ransomware, allowing attackers to tailor the malware to specific targets. These custom variants can be particularly damaging because they can be configured to impersonate administrator accounts, granting them extensive access and privileges within a network.

#3 The ransomware can also be programmed to spread automatically across the network using PsExec, a legitimate tool, and erase logs on infected systems to hinder forensic investigations. Despite Operation Cronos dismantling LockBit's infrastructure in February 2024, the group quickly resurfaced. While law enforcement obtained decryption keys, their effectiveness varied. Incidents involving the leaked builder tool have been reported worldwide.

#4 This incident underscores the widespread impact of attacks utilizing the leaked LockBit builder, with occurrences documented in numerous countries. It also emphasizes the intricate nature of modern ransomware attacks and the critical importance of adopting proactive defense measures.

Recommendations

Keep Software Up-to-Date: Ensure that all software, including operating systems, applications, and security tools, is regularly updated with the latest patches and security updates. This helps to address known vulnerabilities that attackers may exploit.

Conduct Regular Data Backups and Test Restoration: Ensure backups are adequately protected, employ 3-2-1-1 back up principle and Deploy specialized tools to ensure backup protection. In the event of a ransomware attack, having up-to-date backups will allow organizations to restore their systems and data without paying the ransom. Regularly test the restoration process to verify the integrity and availability of backups.

Implement Multi-Factor Authentication (MFA): Enforce the use of multi-factor authentication for accessing sensitive systems and accounts. This additional layer of security can significantly reduce the risk of unauthorized access, even if credentials are compromised.

Network Segmentation: Segment your network to limit the spread of ransomware in the event of a breach. Isolate critical systems and sensitive data to minimize the impact of an attack and prevent lateral movement within the network.

Potential MITRE ATT&CK TTPs

TA0001 Initial Access	TA0005 Defense Evasion	TA0003 Persistence	TA0004 Privilege Escalation
TA0007 Discovery	TA0006 Credential Access	TA0008 Lateral Movement	TA0040 Impact
T1588 Obtain Capabilities	T1588.002 Tool	T1027 Obfuscated Files or Information	T1190 Exploit Public-Facing Application
T1486 Data Encrypted for Impact	T1078.002 Domain Accounts	T1078 Valid Accounts	T1036 Masquerading
T1555 Credentials from Password Stores	T1021 Remote Services	T1059 Command and Scripting Interpreter	T1046 Network Service Discovery
T1070.001 Clear Windows Event Logs	T1562 Impair Defenses		

Indicators of Compromise (IOCs)

TYPE	VALUE
SHA256	07926e060b7083bbe639b36e9c79cce23404ba9dcaa58c190ee40d7d415ff96f, 707bb3b958fbf4728d8a39b043e8df083e0fce1178dac60c0d984604ec23c881, 5e006f895382525e762a33e5dd5e8416bef56ae859f5e96f820cfba5c4c11226, c9dd51d4295c33e1df0d275669a1de9e1de374a51eb88d7f7b1a1e65f49f7794, 72a18c1e65869e5fce28667ce2b9069f9c180f4af3437193a12566fa1aa9d1a1, f7d05c0e9430ba0621020caad12fa1e8e62acb3bda349cd03240c1938ce7a887, 4dfa2dcbcfe39550255fcf5daaa4ee3b74e7ea3a32666c91c100fb6b8508544b, b2c3beda4b000a3d9af0a457d6d942ec81696f3ed485f7cf723b18008a5f3d10, e81d18241b9af3d08b7a8e98148d690489eaf8891ec7b00e932d9efccbc41860, 2d2a9923c2676d5950473cb9ecb0d4c0db55035ca7540ef5717d8cae2733ac5e, be05716fd6f750c771974985de80d71892e1842c8a760038888ff5008cb6f3e0, 988f9936c4990bc9769bade8353ce321983afb83026295a6b70537e5f1151040, 54e75fae8ee8ffbbee075c7694a7fbb1ed838030d36e9e9c4e454010229e230d, b7147a76c6695b750a84de55d4569f71f694b33aeefeef5daa09318ebabd9a24

References

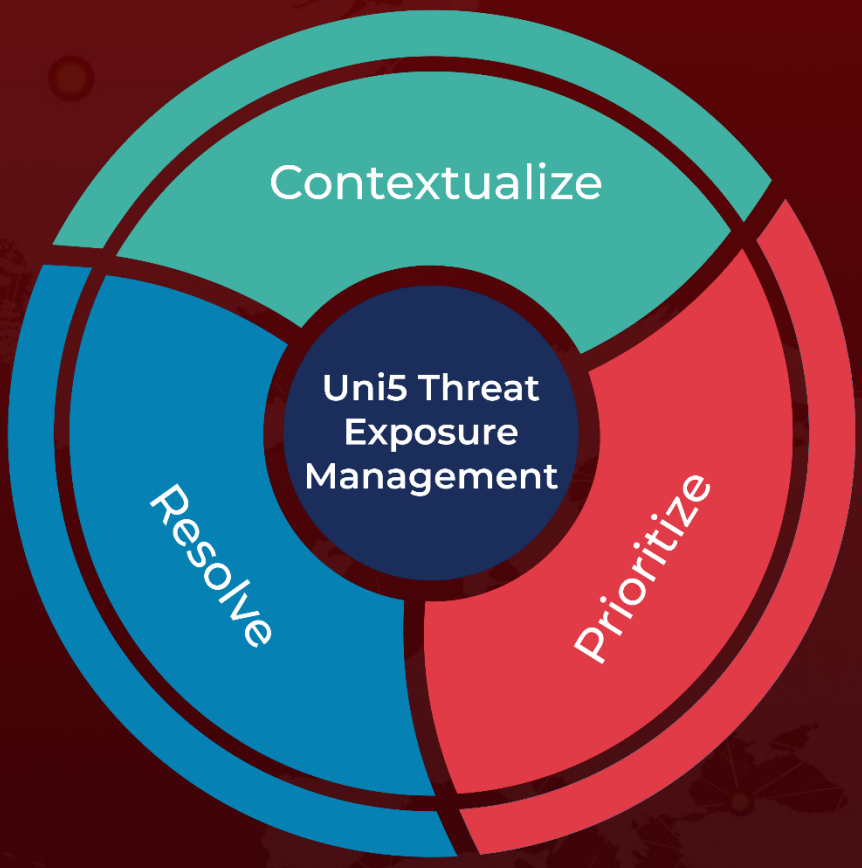
https://securelist.com/lockbit-3-0-based-custom-targeted-ransomware/112375/

https://www.hivepro.com/threat-advisory/lockbits-resurgence-after-operation-cronos/

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

April 17, 2024 • 5:30 AM

More at www.hivepro.com