Hive Pro®

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

⚔ ATTACK REPORT

LockBit's Resurgence After Operation Cronos

Date of Publication	Admiralty Code	TA Number
February 26, 2024	A1	TA2024076

Summary

Attack Began: February 25, 2024
Targeted Countries: Worldwide
Targeted Industries: Government, Financial services, Food and Agriculture, Education, Energy, Healthcare, Technology, Manufacturing, Aviation, Defense, and Transportation
Malware: LockBit Ransomware
Affected Platforms: Windows, Linux, MacOS and VMware Exsi
Attack: LockBit ransomware, previously known as "ABCD," remains a significant threat despite the recent takedown of its operations by global law enforcement. It reemerged within 4 days and its Affiliates were found exploiting vulnerabilities in ScreenConnect to install LockBit ransomware and deploy other malware. This underscores Lockbit's resilience, as it vows to return stronger than before. Organizations must promptly patch vulnerabilities and implement robust cybersecurity measures to effectively defend against such attacks.

Attack Regions

LockBit
Gang
Powered by Bing
© Australian Bureau of Statistics, GeoNames, Microsoft, Navinfo, Open Places, OpenStreetMap, TomTom, Zenrin

Attack Details

#1

LockBit ransomware, previously known as "ABCD," has continued to pose a significant threat to worldwide organizations, including critical infrastructure and government agencies. Despite a recent global law enforcement takedown named Operation Cronos, the group resurfaced on the dark web within 4 days of these actions, using new infrastructure and exploiting vulnerabilities in ScreenConnect deploying the encryptor.

#2

A significant crackdown on LockBit ransomware occurred unfolded with Operation Cronos, involving law enforcement taking over darknet domains associated with LockBit, disrupting their operations. The law agencies further dismantled LockBit by arresting individuals, freezing crypto accounts, and providing a decryption tool for victims. LockBitSupp, the group's operators, engaged with law enforcement, despite these efforts LockBit resurfaced on the dark web shortly after, showcasing its resilince.

#3

LockBit first emerged in September 2019, initially known as the ".abcd virus" due to the file extension it used for encryption. By January 2020, it had transitioned to a RaaS (Ransomware-as-a-Service) model, offering its encryption tool to other attackers for a share of the ransom. In September 2020, LockBit established its presence on hacking forums, creating a platform to showcase its operations and intimidate victims who refused to pay. A network of 194 hackers or 'affiliates' is there in the gang.

#4

The group has continuously released new versions of its ransomware, including LockBit 2.0/LockRed (2021), LockBit 3.0/LockBlack (June 2022), and the current iteration LockBit Green (Jan 2023), also secretly developing a new version called LockBit-NG-Dev prior to its infrastructure being dismantled. Each version aimed to improve encryption strength and evade detection. Unlike widespread spam campaigns, LockBit focuses on targeted attacks, often against small and medium-sized businesses, demanding an average ransom of approximately $85,000.

#5

They are recognized for exploiting over 10 vulnerabilities, the most recent being CVE-2024-1709, an authentication bypass in ConnectWise ScreenConnect. They have implemented custom encryption algorithm, employs multi-threaded encryptors and have boasted of having one of the fastest encryptor.

#6

Following the seizure of their servers, LockBit moved their data leak portal to a new .onion address. The group has also listed a few new victims as of the latest update. The administrator behind LockBit admitted that critical PHP flaws likely led to the confiscation of some websites, citing personal negligence and irresponsibility for failing to update PHP promptly.

#7

In a follow-up message, LockBit claimed that the U.S. Federal Bureau of Investigation (FBI) targeted their infrastructure following a ransomware attack on Fulton County in January, which potentially compromised sensitive documents relevant to upcoming U.S. elections. They called for more frequent attacks on the ".gov sector" and revealed that the authorities obtained over 1,000 decryption keys from a server, although there were almost 20,000 decryptors on the server.

#8

The group also attempted to discredit law enforcement agencies, questioning their actions and affiliations. They pledged to enhance security measures, including manual processes for trial decryption and maximum protection for every build, to prevent future breaches.

#9

Despite the setback, LockBit remains defiant, showcasing a willingness to learn from past mistakes and adapt their tactics accordingly. The gang's determination to upgrade their infrastructure and enhance security measures reflects their commitment to maintaining operational efficiency. As they navigate through the fallout of recent events, LockBit's resilience serves as a stark reminder of the ongoing battle against cybercrime and the ever-evolving nature of digital threats.

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.

Enhance Endpoint Security: Employ reputable antivirus and anti-malware solutions to detect and block known malware signatures. Regularly update and patch operating systems and software to address vulnerabilities that threat actors may exploit.

Network Segmentation: Implement network segmentation to restrict the lateral movement of attackers within the network. Segment critical systems and sensitive data from less secure areas of the network to minimize the impact of a successful breach.

Patch Management: Maintain a rigorous patch management process to ensure that all software, including operating systems, web browsers, and security applications, is up-to-date with the latest security patches. Promptly apply patches released by software vendors to mitigate known vulnerabilities.

Potential MITRE ATT&CK TTPs

TA0001 Initial Access	**TA0002** Execution	**TA0003** Persistence	**TA0004** Privilege Escalation
TA0007 Discovery	**TA0008** Lateral Movement	**TA0009** Collection	**TA0011** Command and Control
TA0010 Exfiltration	**TA0040** Impact	**T1219** Remote Access Software	**T1562.001** Disable or Modify Tools
T1562 Impair Defenses	**T1482** Domain Trust Discovery	**T1072** Software Deployment Tools	**T1003** OS Credential Dumping
T1095 Non-Application Layer Protocol	**T1003.001** LSASS Memory	**T1555.003** Credentials from Web Browsers	**T1555** Credentials from Password Stores
T1572 Protocol Tunneling	**T1082** System Information Discovery	**T1588.006** Vulnerabilities	**T1046** Network Service Discovery
T1021.001 Remote Desktop Protocol	**T1021** Remote Services	**T1588.005** Exploits	**T1071.001** Web Protocols

T1048 Exfiltration Over Alternative Protocol	T1189 Drive-by Compromise	T1190 Exploit Public-Facing Application	T1133 External Remote Services
T1566 Phishing	T1078 Valid Accounts	T1059.003 Windows Command Shell	T1059 Command and Scripting Interpreter
T1072 Software Deployment Tools	T1569.002 Service Execution	T1569 System Services	T1547 Boot or Logon Autostart Execution
T1548 Abuse Elevation Control Mechanism	T1484 Domain Policy Modification	T1484.001 Group Policy Modification	T1480.001 Environmental Keying
T1480 Execution Guardrails	T1070.004 File Deletion	T1027 Obfuscated Files or Information	T1027.002 Software Packing
T1486 Data Encrypted for Impact	T1588 Obtain Capabilities		

Indicators of Compromise (IOCs)

TYPE	VALUE
SHA256	a340d3ddacb9a9890f94c995510611099a682cf482323b6fd9922c2311c93782, d4f150a8b26e9edccae4987433fb5b8a105970db143ba196f13652730c635668, 2e83048c7ed1193f09ae8d293b42c105662828f2ab56a2fa1f81379ee250fc46, 6fcee00c908b40aac5a7e50007f485fc35ebfbdc2ae6a6d5e0a1f37636caca75, e32dc551a721b43da44a068f38928d3e363435ce0e4d2e0479c0dfdb27563c82, 73406e0e7882addf0f810d3bc0e386fd5fd2dd441c895095f4125bb236ae7345, f0db0d23b83b54d8a565f8e9bd66b4ae7be8b2f8efffc471b6e5ef95298376e8,

TYPE	VALUE
SHA256	b65b65c3ccf923af7be7db31b3919120e47849cc3e870afdac1bc555fc25b200, b14a55a5dbc52dc58ee5447ced1caaac304e77aca7b5805a25456e2c2338309f, e51155ce803bd9b96b91c822e41969c89e0c9e162aebc7643c23ed9489eb75b4, 4cd8104440fb28afb5cadcfbdc529f57f62db479b679117c0c461fdae5796997, 954d1ef6afce8843a96769f710d52f407777a6c294ecb3539da592f3f72a560c, b8c53972ca8e7c683183a34b5a4e17f04d9bca80d8d2e156e99fb8973d41f6b9, b2c3beda4b000a3d9af0a457d6d942ec81696f3ed485f7cf723b18008a5f3d10, 9b5f1ec1ca04344582d1eca400b4a21dfff89bc650aba4715edd7efb089d8141, 8b6946cca11e9507df8234e0c68567f19a893c3f08b1d384b88808846d67d7eb, 0447c931bb8efc6dc531f69a891f2a0f28a85a18b25e04366fdb59bf827b2eb1, c431cd8702361f700751745a64802a177c8db6bf58d5a428948cdc7bd0def7e7, 110372c328433649abf49f1079ea0c6610770cf9b22e7f9dfd55144dffa21aa4, 2da975fee507060baa1042fb45e8467579abf3f348f1fd37b86bb742db63438a, a50d9954c0a50e5804065a8165b18571048160200249766bfa2f75d03c8cb6d0, 707bb3b958fbf4728d8a39b043e8df083e0fce1178dac60c0d984604ec23c881, a736269f5f3a9f2e11dd776e352e1801bc28bb699e47876784b8ef761e0062db, 32cf89ca7cccc410ca4ad9bc58e22fe8920131687ef2a0d9f61d215c9d50d661, fc073ee5e385a148e0f4d0fd9c1af696d16bd6c8d3507a98d409c2eda858ce23, f01909eee3dec5474a5a845deea3f8fb5502ac006f65060a7e945f91c966e266, 655f0d2974bf6da082463a2e1c5cf9ae87dcc873058e5e33cb47ca9490e158c2, 77a41f2ea91e559f5f1b0a24e0eedf28c4c74a1983641cff434be417f7ac20f7, 492ac25608dda01b3f776b46a7631bb8cd91a0ce0168931ec5bb9a846e702e39, 91c614d4868abe9c71d77aa77e881851dec34524afff8cad20bdb2087e58433d, 853ed24a495d866d64a922922e5d5329ed165fe102cef00007095ee92ba3746d, 2fcad226b17131da4274e1b9f8f31359bdd325c9568665f08fd1f6c5d06a23ce,

TYPE	VALUE
SHA256	74c8269a9ec642c0fd432fc9e0d7506a079b6d32c2c3e5313d96205726629233, 6dd44d852226fd9e7fc914c6edbaf185bfcaacdc7a4dcdb7268440e6fc811618, 71895d170c7578dc8d5dba7e3136e514d8c42f502e5dc88aff532f11dac01f32, ea0094eec469916f81aa039d87700c88c89f7e10b9c90243127de1c7ad2cfbc0, 63b9637406042b4a9ab162e581c935e7f2c20b64ca504c4ae4e947aa43565b52,

Recent Breaches

silganhodlings.com
sterncor.com
mcs360.com
igs-inc.com
groupe-idea.com
apeagers.com.au
dunaway.com
stsaviationgroup.com
fultoncountyga.gov
nationaldentex.com
crbgroup.com
gatesshields.com
aeromechinc.com
equilend.com

References

https://samples.vx-underground.org/tmp/Lockbit_Statement_2024-02-24.txt

https://www.nationalcrimeagency.gov.uk/news/nca-leads-international-investigation-targeting-worlds-most-harmful-ransomware-group

https://twitter.com/vxunderground/status/1761031957104750864

https://www.hivepro.com/threat-advisory/critical-vulnerabilities-in-screenconnect-under-active-exploitation/

https://twitter.com/NCA_UK/status/1761050859423543741

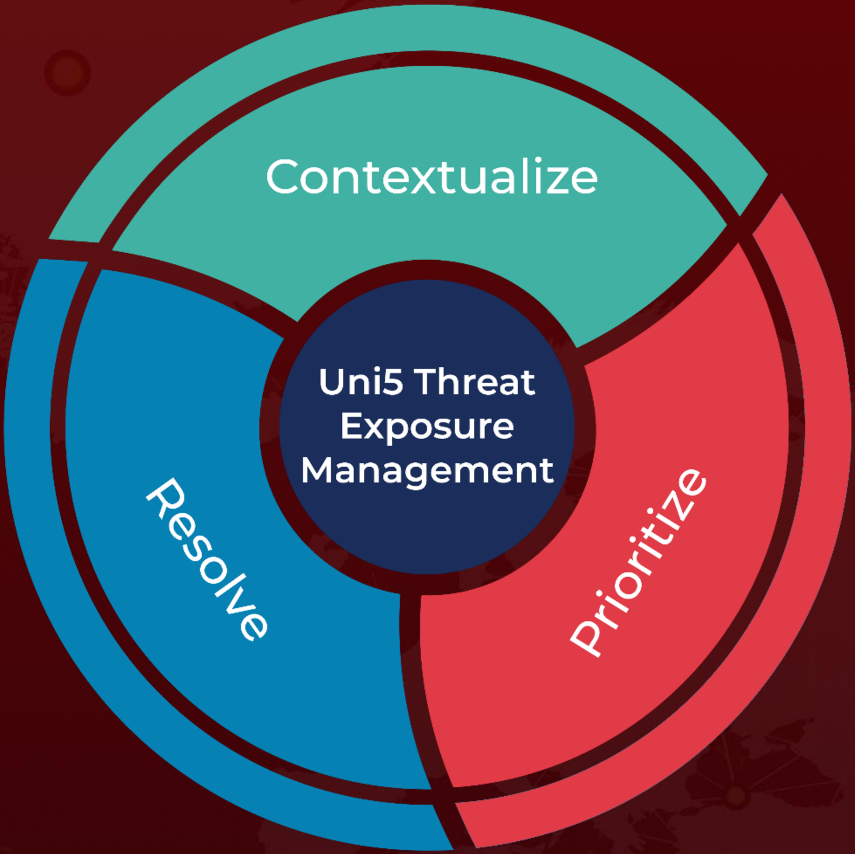
https://www.nomoreransom.org/uploads/Decryption_Checker_for_LockBit_Guide.pdf

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

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

February 26, 2024 • 11:30 PM

More at www.hivepro.com