Hive Pro

Threat Level

Red

CISA: AA23-165A

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

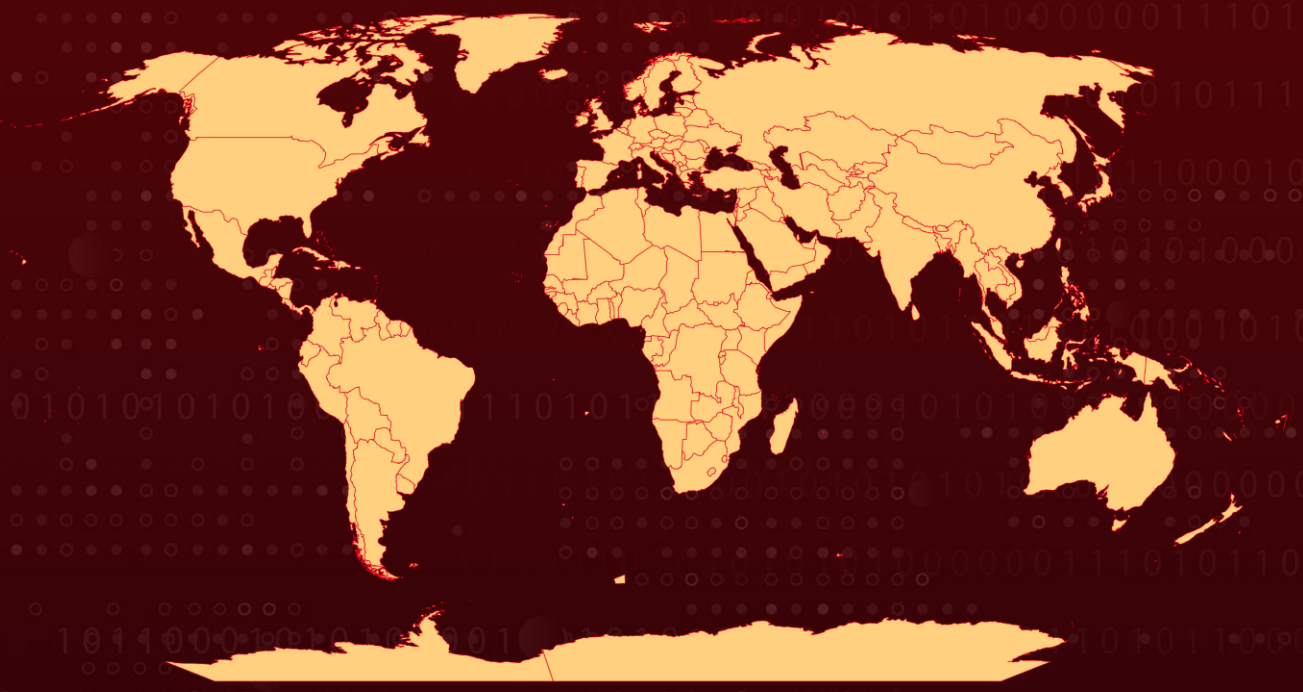
LockBit Ransomware Evolving Tactics and Pervasive Impact in 2023

Date of Publication	Last updated date	Admiralty Code	TA Number
June 15, 2023	March 6, 2024	A1	TA2023264

Summary

First Appearance: January 2020
Malware: LockBit Rasnomware
Targeted Countries: Worldwide
Targeted Industries: Critical infrastructure sectors, including financial services, food and agriculture, education, energy, government and emergency services, healthcare, Technology manufacturing, and transportation
Affected Platforms: Windows, Linux, MacOS and VMware Exsi
Attack: LockBit ransomware, a highly impactful Ransomware-as-a-Service (RaaS) variant targeting critical sectors globally, has led victims in the US alone to pay around $91 million in ransom payments since 2020. Recently taken down by global law enforcement, it reemerged within 4 days, with its affiliates exploiting vulnerabilities in ScreenConnect to install LockBit ransomware and deploy other malware, highlighting LockBit's resilience as it vows to return stronger than before.

Attack Regions



CVEs

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2023-0669	Fortra GoAnywhere MFT Remote Code Execution Vulnerability	Fortra GoAnywhere MFT	✓	✓	✓
CVE-2023-27350	PaperCut MF/NG Improper Access Control Vulnerability	PaperCut MF/NG	✗	✓	✓
CVE-2021-44228	Apache Log4j2 Remote Code Execution Vulnerability	Apache Log4j2	✓	✓	✓
CVE-2021-22986	F5 BIG-IP and BIG-IQ Centralized Management iControl REST Remote Code Execution Vulnerability	F5 BIG-IP and BIG-IQ Centralized Management	✗	✓	✓
CVE-2020-1472	Microsoft Netlogon Privilege Escalation Vulnerability	Microsoft Netlogon	✗	✓	✓
CVE-2019-0708	Microsoft Remote Desktop Services Remote Code Execution Vulnerability	Microsoft Remote Desktop Services	✗	✓	✓
CVE-2018-13379	Fortinet FortiOS SSL VPN Path Traversal Vulnerability	Fortinet FortiOS	✗	✓	✓
CVE-2023-4966	Citrix NetScaler ADC and NetScaler Gateway Buffer Overflow Vulnerability (Citrix Bleed)	Citrix NetScaler ADC and NetScaler Gateway	✓	✓	✓
CVE-2020-0796	Microsoft SMBv3 Remote Code Execution Vulnerability	Microsoft SMBv3	✗	✓	✓
CVE-2021-36942	Microsoft Windows Local Security Authority (LSA) Spoofing Vulnerability	Microsoft Windows	✗	✓	✓
CVE-2022-3653	Google Chrome Heap buffer overflow Vulnerability	Google Chrome	✗	✗	✓
CVE-2024-1708	ConnectWise ScreenConnect Path-Traversal Vulnerability	ConnectWise ScreenConnect	✗	✗	✓
CVE-2024-1709	ConnectWise ScreenConnect Authentication Bypass Vulnerability	ConnectWise ScreenConnect	✗	✓	✓

Attack Details

#1 LockBit ransomware has been one of the most widespread and active variants in the world, with affiliates targeting organizations across various critical infrastructure sectors. LockBit operates as a Ransomware-as-a-Service (RaaS) model, where affiliates are recruited to conduct attacks using LockBit tools and infrastructure. The tactics, techniques, and procedures (TTPs) employed by LockBit affiliates vary significantly, posing a challenge for organizations trying to defend against ransomware.

#2 The ransomware has undergone several iterations, including LockBit 2.0, LockBit 3.0, and LockBit Green, each with its own enhancements and features. The Cybersecurity and Infrastructure Security Agency (CISA), along with other international partners, has released a cybersecurity advisory detailing observed LockBit activity and providing recommended mitigations.

#3 LockBit has gained popularity among affiliates by assuring payment and allowing them to receive ransom payments before sending a cut to the core group. They have also engaged in publicity-generating activities and developed a user-friendly interface for their ransomware, making it accessible to less technically skilled individuals. LockBit has undergone several evolutions, introducing new versions with expanded capabilities and incorporating source code from other ransomware variants.

#4 LockBit has been responsible for a significant percentage of ransomware incidents in various countries, such as Australia, Canada, New Zealand, and the United States. The ransom payments made to LockBit by victims in the US alone have amounted to approximately $91 million since 2020. LockBit activity has been observed as early as 2020 in different countries, with the most recent instances occurring as recently as May 2023. LockBit affiliates have been observed using legitimate freeware and open-source tools for malicious purposes during their intrusions.

#5 They have also exploited both older and newer vulnerabilities, such as CVE-2023-0669, CVE-2023-27350, CVE-2021-44228, CVE-2021-22986, CVE-2020-1472, CVE-2019-0708, CVE-2018-13379, CVE-2023-4966, CVE-2020-0796, CVE-2021-36942, CVE-2022-3653, CVE-2024-1709 . After successfully targeting an organization, LockBit affiliates may attempt secondary ransomware extortion by targeting the organization's customers or other associated networks.

#6 LockBit ransomware was recently taken down by global law enforcement. However, it reemerged within 4 days, with its affiliates 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.

Recommendations

Implement Robust Endpoint Protection: Deploy advanced endpoint protection solutions that include behavior-based detection, machine learning algorithms, and threat intelligence. These solutions can detect and block malicious activities associated with LockBit ransomware, such as file encryption and unauthorized processes. Regularly update endpoint security software to ensure protection against the latest threats.

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 and prevent unauthorized access to their networks.

Conduct Regular Data Backups and Test Restoration: Implement a robust data backup strategy that includes regular backups of critical data and systems. Ensure backups are stored offline or in a secure, isolated environment to prevent them from being compromised in the event of an attack. Regularly test the restoration process to verify the integrity and availability of backups. 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.

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	TA0042 Resource Development	T1562.001 Disable or Modify Tools
T1562 Impair Defenses	T1482 Domain Trust Discovery	T1072 Software Deployment Tools	T1003 OS Credential Dumping
T1071 Application Layer Protocol	T1071.002 File Transfer Protocols	T1567.002 Exfiltration to Cloud Storage	T1567 Exfiltration Over Web Service

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	T1219 Remote Access Software	T1046 Network Service Discovery
T1021.001 Remote Desktop Protocol	T1021 Remote Services	T1588.006 Vulnerabilities	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
T1588.005 Exploits	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
T1588 Obtain Capabilities			

Indicators of Compromise (IOCs)

TYPE	VALUE
SHA256	0845a8c3be602a72e23a155b23ad554495bd558fa79e1bb849aa75f79d069194, 498e3b7a867d41b5a3af3910d2aa6231612c787ce8a4bc14ab03f800caab130f, af4c28fb1c65ebe93181b67d279733e864cafab5919a7aa7eced93fc8113df16, 984d96730ae19d4532325c6fcbd34580fb02fbe454781b589d2eea6090ea2b6d, 2cee882bd0dc4267bacf099ac4571c319ac547be12b955f7ccb2f0144ae40876, 40406fd8c1d7e3c44dff7dfe669dd0a681e22aea3a4a31ba7df7e3a9c5e4be75, 8022060ef633e157518037122a6003813cc0a3066d456a1164275a211efc8f5c, a736269f5f3a9f2e11dd776e352e1801bc28bb699e47876784b8ef761e0062db, 5a13ac97ce91d5b095c7154fe756615fa0730c17ddf432ae4af6c42d2c29946d, 9aa5bcee06109d52fade97ad21317ff951abc656ba4c800441bacfec00328fd8, 379c4620d6f482e153d7033bba21da5d8027387c0e60e3497b63d778dcafd888, b964a5253c25465633ef8c2e7f77703d27227bfc0b13a7ca49d187dadc4d38ae, ba0eefdfbd1421d37d47f3feaae8e768a4679d6b544bb97f5237319e8ab0b122, f9dbdb825067616070c64565b6b27dc872c4a7219856eb5f8eb3eb1eb1463423, 2e218735fa53e036659ea721bfd7b97e2af67b7eda648e9e2579356eb20899d9, 1f0e4cbc1a4b52b6d7e4188e4a835a904cf783c75db9a066df4201452bd9647d, de7f501e4a17898e85229b962e2f43b9a20d995c8a9fe0cad4536adc8fbd9f48, 8989a9aec8d2c4d61fa399a97807f8e62814b1a55fecbd38d11d4d35fdf4a7d1, 01bf78841b63bcdd8280157c486b45ad74811c0251140a054de81a925ce7f716, ab4d20b73c7358f1e3a60145d5debc791a17416e2a88eb39f80ec1f53985fad5, 9366a5b8021d0283156986bbf020c99ae5e2a3dcbbaa03db934e94bfa7088b86, 4bdda7dd3bbe1f9cb0a7d42f6947ba0f6442e52758bd2638541f9409b573d5c9,

TYPE	VALUE
SHA256	6b4502d8ba3cff1a3139f72cdad863d53551b65b8c38d7b838d64212822e4630, 4d0f95028bb6a04e64550872ddeef6b0c6fa4a5bd368736da47401420df2bee7, cfc45c36b4c731f2308e19a087c3dc3fb7b12eef93e171e8e86e2134ead325ee, 4134d5d8f7b038e23e7887db56bb3ad295341a1aaf0bebe6be21d901d06dd662, 153fc9e90b955e2cfaf91b86888a29fdd8685144a3802f5e90b95b64116cdd33, 00accc2c186201607d3e36c1b013872ac51d4f805f23e625dc70154fb58fd4f4, 48a0366841e2f59b533510f532b220458d3fd489efc4b71d00d2b9429b292fb9, 149d691411f10f8ec7af43f0237ccfab5b65a9ae73718acf1e0cc0dbdea36ebd, cb83eb6f5fd42f59b1c1a34826df48e5a5882c45e4a7f34c80c0830c26cb30dd, 4d4bc9d78db93c25548a679de06e267363a31a400e2e37caf9d1fce91b65fe8d, b9872ad6ec82d3f2f9a8c6af7e5838f91712e52ece265cd04f4452378bd5bcfd, a8939a43feb8cc258507ffd0be564d56a2874c220729e00da8ad204c3b4012c5, fef1f9664fde9b23754c691b15a05fdc35a51a0ceb8a18fb9a5a0166e6377c69, 734955fdb84b29fa1aa87aa0af2ebf155125917a6b61ffe4b4dc7030dd212309, e47b928d0fc16348b828abeb3c2106a6d752512f60ef4583d6532cc0dbebebbf, 239c9969fd07e1701a129cfd033a11a93ee9e88e4df4f79b7c5c0dd5bba86390, a439c5093801d3b12e2f79b64c0b65bdf148eb6eca8c1e3d179af5ab4995034d, 54ac7ac6db6fcec5234454430513d1d2787ee8a48aa60fbf95c1af27534fdb4a, A9abab8ab44ccec6321da83d9960a1f30ba783e02b6e0ba3f2e9d19cee76b39b, 286726ecca68f8c2752116258aba0cd35c051a6342043ee1add84b890654276f, 3a659609850664cbc0683c8c7b92be816254eb9306e7fb12ad79d5a9af0fb623, 2da975fee507060baa1042fb45e8467579abf3f348f1fd37b86bb742db63438a
MD5	af9ff037caca1f316e7d05db86dbd882, b7f1120bcff47ab77e74e387805feabe, 4d25a9242eac26b2240336fb94d62b1e, 84866fca8a5ceb187bca8e257e4f875a, f91095ae0e0632b0f630e0c4eb12ba10, b0916724ff4118bf213e31cd198c0afd,

TYPE	VALUE
MD5	6fc418ce9b5306b4fd97f815cc9830e5, 66b9ccb41b135f302b3143a5d53f4842
IPv4	139[.]60[.]160[.]200, 93[.]190[.]139[.]223, 45[.]227[.]255[.]190, 193[.]162[.]143[.]218, 168[.]100[.]11[.]72, 93[.]190[.]143[.]101, 88[.]80[.]147[.]102, 193[.]38[.]235[.]234, 174[.]138[.]62[.]35, 185[.]215[.]113[.]39, 185[.]182[.]193[.]120, 185[.]81[.]68[.]180
SHA1	844e9b219aaecb26de4994a259f822500fb75ae1, a185904a46b0cb87d38057fc591a31e6063cdd95, c7b2d4a22f788b1b942f993fff33f233dca960ce, 038bc02c0997770a1e764d0203303ef8fcad11fb, 6c4040f2a76e61c649e1ff4ac564a5951c15d1fa, 12ac32d012e818c78d6db790f6e11838ca75db88, 95838a8beb04cfe6f1ded5ecbd00bf6cf97cd564, 3d532697163e7c33c7c906e8efbb08282d3efd75
Tor Address	hxxp://lockbitapt6vx57t3eeqjofwgcglmutr3a35nygvokja5uuccip4ykyd[.]onion, hxxp://lockbitsap2oaqhcun3syvbqt6n5nzt7fqosc6jdlmsfleu3ka4k2did[.]onion, hxxp://lockbitsup4yezcd5enk5unncx3zcy7kw6wllyqmiyhvanjj352jayid[.]onion,

Recent Breaches

https://sunwave.com.cn
https://central.k12.or.us
https://valoremreply.com
https://earnesthealth.com
https://stockdevelopment.com
https://jovani.com
https://aerospace.com
https://unitednotions.com
https://roehr-stolberg.de
https://esser-ps.de

https://schuett-grundei.de
https://starkpower.de
https://smuldes.com
https://gapsolutions.com.au
https://sundbirsta.com
https://easternshipbuilding.com
https://vertdure.com
https://npgandour.com
https://prattindustries.com
https://silganholdings.com
https://ernesthealth.com
https://silganhodlings.com
https://dunaway.com
https://apeagers.com.au
https://fbi.gov
https://crbgroup.com
https://equilend.com
https://nationaldentex.com
https://etisalat.ae
https://spaldingssd.com
https://theclosingagent.com
https://tormetal.cl
https://centralepaysanne.lu
https://pradiergranulats.fr
https://coreengg.com
https://sitrack.com
https://carlfischer.com
https://champion.com.co
https://hatsinteriors.com
https://mmiculinary.com
https://studiogalbusera.com
https://rajawali.com
https://auruminstitute.org
https://doprastav.sk
https://motilaloswal.com
https://wsnelson.com
https://adioscancer.com
https://cabc.com.ar
https://paltertonprimary.co.uk
https://jacksonvillebeach.org
https://robs.org
https://sealco-leb.com
https://isspol.gov
https://silverairways.com
https://lyon.co.uk
https://kabat.pl
https://envie.org

https://camarotto.it
https://germaintoiture.fr
https://grotonschools.org
https://dienerprecisionpumps.com
https://fidcornelis.be
https://vhprimary.com
https://textiles.org.tw
https://plexustelerad.com
https://parkhomeassist.co.uk
https://lacolline-skincare.com
https://aisg-online.com
https://grupomoraval.com
https://verdimed.es
https://maximumresearch.com
https://seymourct.org
https://moneyadvicetrust.org
https://cdtmedicus.pl
https://bsaarchitects.com
https://northseayachtsupport.nl
https://macqueeneq.com
https://soken-ce.co.jp
https://alfiras.com
https://indoramaventures.com
https://perkinsmfg.com
https://water.cc
https://originalfootwear.com
https://aeromechinc.com
https://bucher-strauss.ch
https://galbusera.it
https://vimarequipment.com
https://tecasrl.it
https://axsbolivia.com
https://fultoncountyga.gov
https://magierp.com

Patch Links

https://my.goanywhere.com/webclient/DownloadProductFiles.xhtml

https://www.papercut.com/kb/Main/PO-1216-and-PO-1219

https://msrc-blog.microsoft.com/2021/12/11/microsofts-response-to-cve-2021-44228-apache-log4j2/

https://support.f5.com/csp/article/K03009991

https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1472

https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0708

http://www.fortiguard.com/psirt/FG-IR-20-233

https://support.citrix.com/article/CTX579459/netscaler-adc-and-netscaler-gateway-security-bulletin-for-cve20234966-and-cve20234967

https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0796

https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-36942

https://chromereleases.googleblog.com/2022/10/stable-channel-update-for-desktop_25.html

https://www.connectwise.com/company/trust/security-bulletins/connectwise-screenconnect-23.9.8

References

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

https://www.cisa.gov/news-events/alerts/2023/06/14/cisa-and-partners-release-joint-advisory-understanding-ransomware-threat-actors-lockbit

https://www.fsisac.com/hubfs/Knowledge/LockBit-AccessEncryptionExfiltrationMitigation.pdf

https://news.sophos.com/en-us/2024/02/23/connectwise-screenconnect-attacks-deliver-malware/

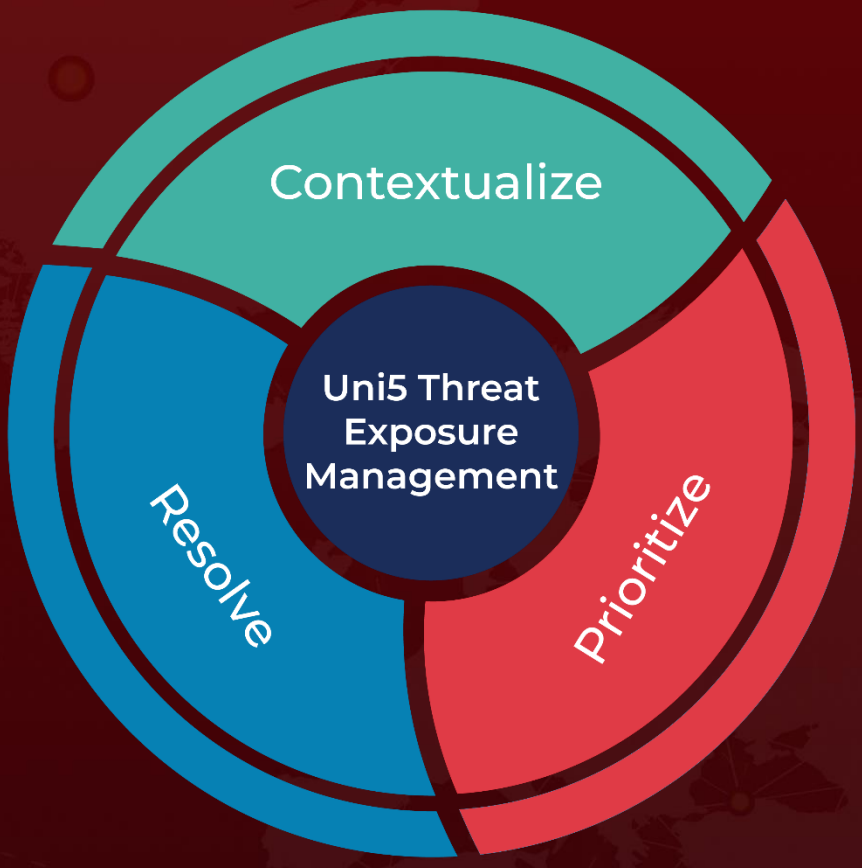
https://www.hivepro.com/threat-advisory/lockbits-resurgence-after-operation-cronos/

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

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

June 15, 2023 • 6:30 AM

More at www.hivepro.com