ultraviolet

CONFIDENTIAL

THREAT REPORT:

LockBit 3.0

Services Performed By:
UltraViolet Cyber
TIDE Team
(443) 351-7630
info@uvcyber.com

Published Date:
11/08/2023

Contents

1 Executive Summary

LockBit 3.0 is the latest iteration of a longstanding, very effective, ransomware as a service (RaaS) group. This strain of malware operates by encrypting a victim's data and demanding a ransom in exchange for the decryption key, effectively holding sensitive information hostage. Its operators are known for their ruthless efficiency, utilizing double-extortion techniques, where they not only encrypt the target's data but also exfiltrate sensitive files, threatening to release them publicly if the ransom is not paid. This ransomware variant has been responsible for numerous high-profile attacks on a global scale, making it a significant concern for cybersecurity experts and organizations alike. In this era of escalating cyber threats, understanding LockBit 3.0 and its modus operandi is critical to safeguarding digital assets and data from its potentially devastating consequences.

2 Threat Activity

LockBit 3.0 was shown to be one of the most active ransomware operators in 2022. Based on the pace from this year alone, they are on target to supersede their victim list count by the end of 2023. To date - over 1700 attacks have been attributed to them with roughly $91M paid from extortion.

- January 2020: LockBit-named ransomware first seen on Russian language-based cybercrime forum
- June 2021: Appearance of LockBit 2.0 (aka LockBit Red)
- October 2021: LockBit Linux-ESXI Locker version 1.0 with focus on Linux and VMWare ESXI
- March 2022: Emergence of LockBit 3.0 (LockBit Black - Similarities to BlackMatter and ALPHV)
- September 2022: LockBit 3.0 builder leaked, increase in non-affiliate usage
- January 2023: LockBit Green found containing Conti ransomware code
- April 2023: LockBit ransomware shown to target MacOS
- November 2023: Boeing named as victim (ongoing)

(443) 351-7630 | info@uvcyber.com

3 Tactics, Techniques, and Procedures

Initial Access:

- User credential brute force attacks targeting remote desktop protocol (RDP, Port 3389) & virtual private network (VPN) access
- Purchased or stolen credentials from initial access brokers
- Credential harvesting through phishing campaigns
- MFA spamming
- Leveraging known vulnerabilities

Enumeration, Persisting Access, and Lateral Movement:

- Living off the land (LOTL) attacks (mimicking normal behavior)
    - Powershell / PsExec / WMIC (evasion, EDR disablement, and scripting)
    - NetScan (identify and enumerate internal network)
    - Rclone (data exfiltration)
    - Mimikatz (harvest credentials)
    - Cobalt Strike (C2, persistent access)
    - vssadmin (deletion of shadow copies – prevention of recovery)

Post-Exploitation:

- Once data exfiltration has completed – ransomware payload is detonated
- Victim is left with a lock screen and ransom note
- Negotiations are attempted with the victim and notice of compromise posted to hxxp[:]//lockbitapt6vx57t3eeqjofwgcglmutr3a35nygvokja5uuccip4ykyd[.]onion/
- Victim is given an expiration for negotiations resulting in public data release

4 What UltraViolet Cyber is Doing

- UltraViolet Cyber is monitoring LockBit 3.0's activity for any relevant IOCs, IOAs, or TTPs to add to our database
- Monitoring commands that are associated with malicious activity
- Monitoring network logs for traffic to known malicious sites

5 What Customers Can Do

- Up-to-date patching or proper mitigating controls to avoid compromise as quickly as possible
    - Consider validating and mitigating for CVE-2023-4966[1] (A.k.a. Citrix Bleed) and CVE-2023-20269[2] (Cisco ASA/Firepower VPN 0day)
- Enable and enforce MFA for all users for any logon event (E.g. VPN or RDP) and consider an education campaign to highlight MFA spamming
- Consider a least permissions model and restrict PsExec, PowerShell, and WMI usage

(443) 351-7630 | info@uvcyber.com

- Maintain a proper backup and recovery plan with offline storage that is encrypted
- Follow security standards for storing sensitive data as well as restriction and auditing of access

6 References

- https://socradar.io/dark-web-profile-lockbit-3-0-ransomware/
- https://blogs.vmware.com/security/2022/10/lockbit-3-0-also-known-as-lockbit-black.html
- https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-075a
- https://www.cisa.gov/sites/default/files/2023-03/aa23-075a-stop-ransomware-lockbit.pdf
- https://github.com/sophoslabs/IoCs/blob/master/Ransomware-LockBit
- https://blogs.vmware.com/security/files/2022/10/Screen-Shot-2022-10-13-at-12.09.25-PM.png
- https://blogs.vmware.com/security/files/2022/10/Screen-Shot-2022-10-13-at-12.05.02-PM.png
- https://unit42.paloaltonetworks.com/threat-brief-cve-2023-4966-netscaler-citrix-bleed/
- [1]https://www.netscaler.com/blog/news/cve-2023-4966-critical-security-update-now-available-for-netscaler-adc-and-netscaler-gateway/
- [2]https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-ravpn-auth-8LyfCkeC

(443) 351-7630 | info@uvcyber.com