FS-ISAC

LockBit: Access, Encryption, Exfiltration, & Mitigation

November 2023

LockBit: Access, Encryption, Exfiltration, & Mitigation

November 2023

Overview

Since 2019, LockBit[i] has become one of the most prolific ransomware groups in the world[ii], running a Ransomware-as-a-Service (RaaS) operation which allows their "affiliates," or customers, to deploy ransomware attacks using their product. LockBit and its affiliates are known to employ double extortion tactics, exfiltrating data before performing encryption to encourage ransom payment.[iii]

The use of affiliates and the leak of the LockBit 3.0 builder in September 2022, mean that there are various threat actors using a variety of tactics to deploy LockBit ransomware. As a result, mitigation is a complex mix of vulnerability and patch management and cyber hygiene fundamentals. (See US Cybersecurity and Infrastructure Security Agency's (CISA's) valuable insights into Lockbit's tactics, techniques, and procedures.)

Initial Access

Affiliates deploying LockBit 3.0 ransomware often gain initial access to victim networks via:

- Remote desktop protocol (RDP) exploitation [T133]
- Drive-by compromise [T1189]
- Phishing campaigns [T1566]
- Abuse of valid accounts [T1078]
- Exploitation of public-facing applications [T1190]

During installation, if privileges are not sufficient, LockBit 3.0 attempts to escalate to the required privileges [TA0004].

Lockbit 3.0 includes tools to target Windows systems. However, other Lockbit variants have proven capable of affecting Linux, MacOS, and VMware Exsi.

Financial institutions can mitigate against these attempts in the following ways:

Mitre ATT&CK Techniques	Mitre ATT&CK Mitigations	
Remote desktop protocol (RDP) exploitation [T133]	M1042 M1035 M1032 M1030	Disable or Remove Feature or Program Limit Access to Resource Over Network Multi-Factor Authentication Network Segmentation
Drive-by compromise [T1189]	M1048 M1050 M1021 M1051	Application Isolation and Sandboxing Exploit Protection Restrict Web-Based Content Update Software
Phishing campaigns [T1566]	M1049 M1031 M1021 M1054 M1017	Antivirus/Antimalware Network Intrusion Prevention Restrict Web-Based Content Software Configuration User Training
Abuse of valid accounts [T1078]	M1013 M1027 M1026 M1018 M1017	Application Developer Guidance Password Policies Privileged Account Management User Account Management User Training
Exploitation of public-facing applications [T1190]	M1048 M1050 M1030 M1026 M1051 M1016	Application Isolation and Sandboxing Exploit Protection Network Segmentation Privileged Account Management Update Software Vulnerability Scanning

Encryption

LockBit 3.0 attempts to spread across a victim network by using a preconfigured list of credentials hardcoded at compilation time or a compromised local account with elevated privileges [T1078]. When compiled, LockBit 3.0 may also enable options for spreading via Group Policy Objects and PsExec using the Server Message Block

(SMB) protocol. LockBit 3.0 attempts to encrypt [T1486] data saved to any local or remote device but skips files associated with core system functions.

After files are encrypted, LockBit 3.0 drops a ransom note with the new filename <Ransomware ID>.README.txt and changes the host's wallpaper and icons to LockBit 3.0 branding [T1491.001]. If needed, LockBit 3.0 will send encrypted host and bot information to a command and control (C2) server [T1027].

Once completed, LockBit 3.0 may delete itself from the disk [T1070.004] as well as any Group Policy updates that were made, depending on which options were set at compilation time.

Exfiltration

LockBit 3.0 affiliates often use *Stealbit*, a custom exfiltration tool used previously with LockBit 2.0 [TA0010]; *rclone*, an open-source command line cloud storage manager [T1567.002]; and publicly available file sharing services, such as *MEGA* [T1567.002], to exfiltrate sensitive company data files prior to encryption. LockBit 3.0 affiliates often use other publicly available file sharing services to exfiltrate data as well [T1567].

Mitigations: Patching CVEs

LockBit has previously exploited the below Common Vulnerabilities and Exposures (CVEs). We recommend patching these vulnerabilities immediately.

CVE-2023-4966 and CVE-2023-4967: Citrix NetScaler ADC and NetScaler Gateway, also known as Citrix Bleed *(see below for more details)*

CVE-2023-0669: Fortra GoAnyhwere Managed File Transfer (MFT) Remote Code Execution Vulnerability

CVE-2023-27350: PaperCut MF/NG Improper Access Control Vulnerability

CVE-2018-13379: Fortinet FortiOS Secure Sockets Layer (SSL) Virtual Private Network (VPN) Path Traversal Vulnerability

CVE-2020-0796: Windows SMBv3 Client/Server Remote Code Execution Vulnerability, or also known as SMBGhost, or CoronaBlue.

CVE-2021-22986: A remote command execution vulnerability in the BIG-IP and BIG-IQ iControl REST API.

CVE-2021-36942: PetitPotam is an NTLM relay attack that could be used against a Windows server, forcing it to share credentials and then relaying these to generate an authentication certificate.

CVE-2022-3653: Heap buffer overflow in Vulkan

Others: CVE-2021-20028, CVE-2021-34473, CVE-2021-34523, CVE-2021-3120

LockBit also has a variant designed to target Linux-based systems and systems like VMware ESXi, which impact VMware hypervisors, virtual machines, and vCenter management systems. [iv]

Citrix Bleed Vulnerability Exploited by Lockbit

Citrix released a security bulletin for two CVEs affecting Citrix NetScaler ADC and NetScaler Gateway (CVE-2023-4966 and CVE-2023-4967).

Citrix NetScaler is a network device providing load balancing, firewall, and VPN services. NetScaler Gateway usually refers to the VPN and authentication components, whereas ADC refers to the load balancing and traffic management features.

The vulnerability now dubbed "Citrix Bleed" allows advisories to extract valid session tokens from internet facing vulnerable NetScaler devices' memory. The compromised session tokens can then be used to impersonate active sessions, which bypass authentication, (even multi-factor) and gain complete access to the appliance. This vulnerability can still occur even if the vulnerability is patched and rebooted, as copied tokens will remain valid unless further steps are taken.

Multiple security researchers have observed threat actors successfully attempting to exploit these vulnerabilities, and whilst Citrix issued a patch for the flaw on 10 October 2023, both CISA and Citrix has stressed the urgency urging administrators to now patch, terminate/invalidate all active sessions tokens, check whether attackers left behind web shells or backdoors, and secure their systems.

Due to exploitation activity, many incident responders have shared artifacts and noted post-intrusion activities that attackers have engaged in, which include but not limited to network reconnaissance, theft of account credentials, lateral movement via RDP, deployment of remote monitoring and management tools, and high profile ransomware infections from LockBit.

The supported versions of NetScaler ADC and NetScaler Gateway are affected by the vulnerability:

- NetScaler ADC and NetScaler Gateway 14.1 before 14.1-8.50
- NetScaler ADC and NetScaler Gateway 13.1 before 13.1-49.15
- NetScaler ADC and NetScaler Gateway 13.0 before 13.0-92.19
- NetScaler ADC 13.1-FIPS before 13.1-37.164
- NetScaler ADC 12.1-FIPS before 12.1-55.300
- NetScaler ADC 12.1-NDcPP before 12.1-55.300

Cyber Hygiene Fundamentals to Protect Against Ransomware

These cyber hygiene practices are not unique to protecting against Lockbit or any other type of ransomware. However, the reason why they are called cyber hygiene fundamentals is because they are effective.

- **Implement a recovery plan** to maintain and retain multiple copies of sensitive or proprietary data and servers [CPG 7.3] in a physically separate, segmented, and secure location (e.g., hard drive, storage device, the cloud).
- **Require all accounts** with password logins (e.g., service account, admin accounts, and domain admin accounts) to comply with National Institute for Standards and Technology (NIST) standards for developing and managing password policies [CPG 3.4].
- **Require phishing-resistant multi-factor authentication** [CPG 1.3] for all services to the extent possible, particularly for webmail, virtual private networks, and accounts that access critical systems.
- **Keep all operating systems, software, and firmware up to date.** Timely patching is one of the most efficient and cost-effective steps an organization can take to minimize its exposure to cybersecurity threats.
- **Segment networks** [CPG 8.1] Network segmentation can help prevent the spread of ransomware by controlling traffic flows between—and access to—various subnetworks and by restricting adversary lateral movement.
- **Identify, detect, and investigate abnormal activity and potential traversal of the indicated ransomware with a networking monitoring tool.** [CPG 5.1]. Endpoint detection and response (EDR) tools are particularly useful for detecting lateral

connections as they have insight into common and uncommon network connections for each host.

- **Install, regularly update, and enable real time detection for antivirus software** on all hosts.
- **Review domain controllers, servers, workstations, and active directories** for new and/or unrecognized accounts.
- **Audit user accounts** with administrative privileges and configure access controls according to the principle of least privilege [CPG 1.5].
- **Disable unused ports.**
- **Consider adding an email banner to emails** [CPG 8.3] received from outside your organization.
- **Disable hyperlinks** in received emails.
- **Implement time-based access for accounts set at the admin level and higher.** This is a process where a network-wide policy is set in place to automatically disable admin accounts at the Active Directory level when the account is not in direct need. Individual users may submit their requests through an automated process that grants them access to a specified system for a set timeframe when they need to support the completion of a certain task.
- **Disable command-line and scripting activities and permissions.** If threat actors are not able to run these tools, they will have difficulty escalating privileges and/or moving laterally.
- **Maintain offline backups of data,** and regularly maintain backup and restoration [CPG 7.3]. By instituting this practice, the organization ensures they will not be severely interrupted, and/or only have irretrievable data.
- **Ensure all backup data is encrypted, immutable** (i.e., cannot be altered or deleted), and covers the entire organization's data infrastructure [CPG 3.3].

[i] https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-165a
[ii] https://www.wired.com/story/lockbit-ransomware-attacks/
[iii] https://www.hhs.gov/sites/default/files/lockbit-3-analyst-note.pdf
[iv] https://www.fortinet.com/blog/threat-research/lockbit-most-prevalent-ransomware

