00. Overview (LockBit)

History:

LockBit ransomware first emerged in September 2019, and was originally known as “ABCD” ransomware because the group used the file extension “.abcd virus” when performing encryptions. In January 2020, the ransomware group began operations as a ransomware-as-a-service (RaaS) and adopted the name LockBit.

The ransomware group announced the creation of its own website in September 2020 on Exploit. The website serves as a space for the ransomware group to announce recent attacks against victims and publish data of victims who did not pay the ransom. The group primarily posts in Russian and English, but according to its website, the group claims to be located in the Netherlands and to not be politically motivated.

LockBit has attacked a variety of organizations across sectors, including the education, finance, healthcare, internet software and services, and professional services sectors. A 2022 Trend Micro report stated that 80.5 percent of LockBit victims are small and medium-size businesses and only 19.5 percent of its victims are larger enterprises.

LockBit 2.0 appeared in 2021 and came into the spotlight with their attack on Accenture the same year, where an insider probably helped the group entering the network. LockBit published some of the data stolen in this attack.

In January 2022, the electronics company Thales was one of the victims of Lockbit 2.0.

In July 2022, the administrative and management services of La Poste Mobile were attacked.

In September 2022, the group's hackers claimed cyberattacks against 28 organizations, 12 of which involved French organizations. Among them, the Corbeil Essonnes hospital was targeted with a ransom demand of US$10 million.

In October 2022, the Lockbit group claimed responsibility for an attack on Pendragon PLC, a group of automotive retailers in the UK, demanding a ransom of US$60 million to decrypt the files and not leak them; the company stated that they refused the demand.

On October 31, 2022, the Lockbit hacker group claimed to have attacked Thales Group for the second time and did not demand a ransom, but said that the data would be released. The hacker group offered assistance to Thales customers affected by the theft, in order to lodge a complaint against Thales, a group "that has greatly disregarded confidentiality rules". On November 10, 2022, the LockBit 3.0 group published on the darknet a 9.5 GB archive with stolen information on Thales contracts in Italy and Malaysia.

In November 2022, OEHC - Office d'Équipement Hydraulique de Corse - was the victim of a cyberattack that encrypted the company's computer data. A ransom demand was made by the hacker group, to which OEHC did not respond.

In December 2022, the Lockbit hacker group claimed responsibility for the attack on the California Finance Administration. The governor's office acknowledged being the victim of an attack, without specifying its scale. Lockbit claims to have stolen 246,000 files with a total size of 75.3 GB.

In December 2022, the hacker group claimed to have attacked the port of Lisbon. The ransom was set at US$1.5 million, to be paid by January 18, 2023.

On December 18, 2022, a group of hackers attacked Toronto's Hospital for Sick Children. After realizing their blunder, the hacker group stopped the attack, apologized and offered a free solution to recover the encrypted files.

LockBit 3.0
In late June 2022, the group launched "LockBit 3.0", the latest variant of their ransomware, after two months of beta testing. Notably, the group introduced a bug bounty program, the first of its kind in the realm of ransomware operations. They invited security researchers to test their software to improve their security, offering substantial monetary rewards ranging from US$1,000 to $1 million.

In August 2022, German equipment manufacturer Continental suffered a Lockbit ransomware attack. In November 2022, with no response to its ransom demand, the hacker group published part of the stolen data and offered access to all of it for 50 million euros. Among the stolen data are the private lives of the Group's employees, as well as exchanges with German car manufacturers. Beyond the theft of data, the danger lies in opening the way to industrial espionage. Indeed, among the exchanges with Volkswagen are IT aspects, from automated driving to entertainment, in which Volkswagen wanted Continental to invest.

In November 2022, the United States Department of Justice announced the arrest of Mikhail Vasiliev, a dual Russian and Canadian national, in connection with the LockBit ransomware campaign. According to the charges, Vasiliev allegedly conspired with others involved in LockBit, a ransomware variant that had been used in over 1,000 attacks globally as of November 2022. According to reports, the operators of LockBit had made at least $100 million in ransom demands, of which tens of millions had been paid by victims. The arrest followed a 2.5 year investigation into the LockBit ransomware group by the Department of Justice.

In January 2023, the hacker group claimed to have attacked the French luxury goods company Nuxe and ELSAN, a French group of private clinics. The hacker group filched 821 GB of data from the company's headquarters. The same month, Royal Mail's international export services were severely disrupted by a Lockbit ransomware attack.

In February 2023, the group claimed responsibility for an attack on Indigo Books and Music, a chain of Canadian bookstores.

In March 2023, the group claimed responsibility for attacking BRL Group, a water specialist in France.

On May 16, 2023, the hacker group claimed responsibility for attacking the Hong Kong branch of the Chinese newspaper China Daily. This is the first time the hacker group has attacked a Chinese company. Lockbit does not attack Russian entities and avoids attacking Russian allies.

In May 2023, the hacker group claimed responsibility for the attack on fr:Voyageurs du Monde. The hacker group stole some 10,000 identity documents from the company's customer files.

In June 2023, the United States Department of Justice announced criminal charges against Ruslan Magomedovich Astamirov, a Russian national, for his alleged participation in the LockBit ransomware campaign as an affiliate. The charges allege that Astamirov directly executed at least five ransomware attacks against victims and received a portion of ransom payments in bitcoin.

At the end of June 2023, the TSMC group fell victim to a ransomware attack via one of its suppliers. LockBit demanded a $70 million ransom.

In July 2023, Lockbit attacked the Port of Nagoya in Japan, which handles 10% of the country's trade. The attack forced a shutdown of container operations. In October 2023, Lockbit claimed to have stolen sensitive data from Boeing. Boeing acknowledged they were aware of a cyber incident affecting some of their parts and distribution business a few days later, though it did not affect flight safety; they did not name the suspected attackers.

In November 2023, Lockbit attacked the U.S. subsidiary of the Chinese state-owned Industrial and Commercial Bank of China. Bloomberg reported that the US unit of ICBC at the time was considered the world's largest lender by assets.

In November 2023, Lockbit released internal data that the group had stolen a month earlier from Boeing onto the Internet.

In November 2023, the Lockbit gang attacked the Chicago Trading Company and Alphadyne Asset Management. Bloomberg reported that the CTC had been hacked in October, and that over the prior year Lockbit had "become the world’s most prolific ransomware group." Since 2020, it had reportedly carried out 1,700 attacks and extorted $91 million, according to the US Cybersecurity and Infrastructure Security Agency. The Register reported in late November 2023 that LockBit was facing growing internal frustrations, and that its leaders were overhauling some of its negotiation methods with victims in response to the low pay rate achieved.

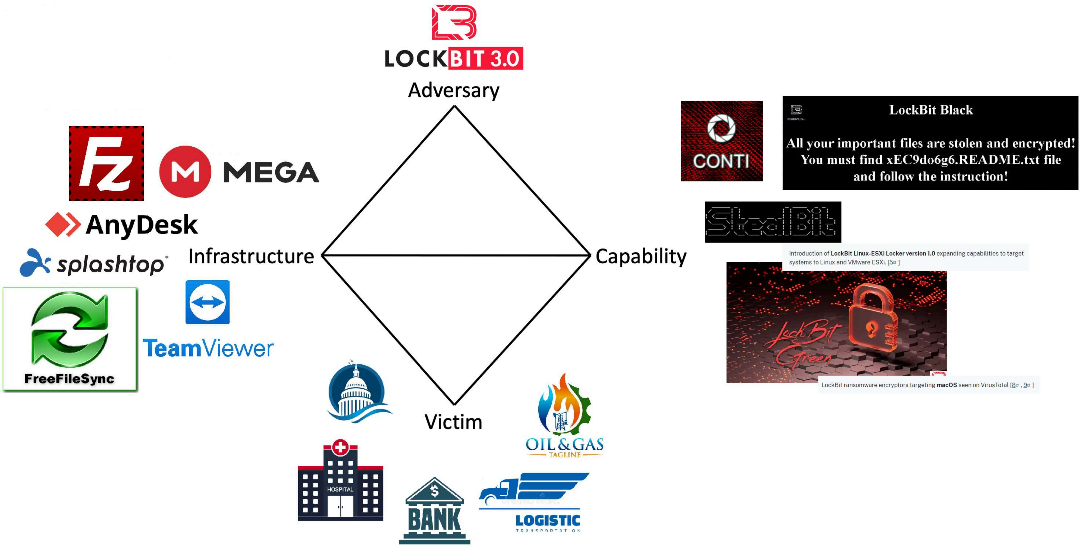
In January 2024, the Lockbit gang attacked Fulton County computers. The county released a statement on the attack the following month, saying they had not paid the ransom, that it was not associated with the election process, they were not aware of any extraction of sensitive information about citizens or employees.

TTPs:

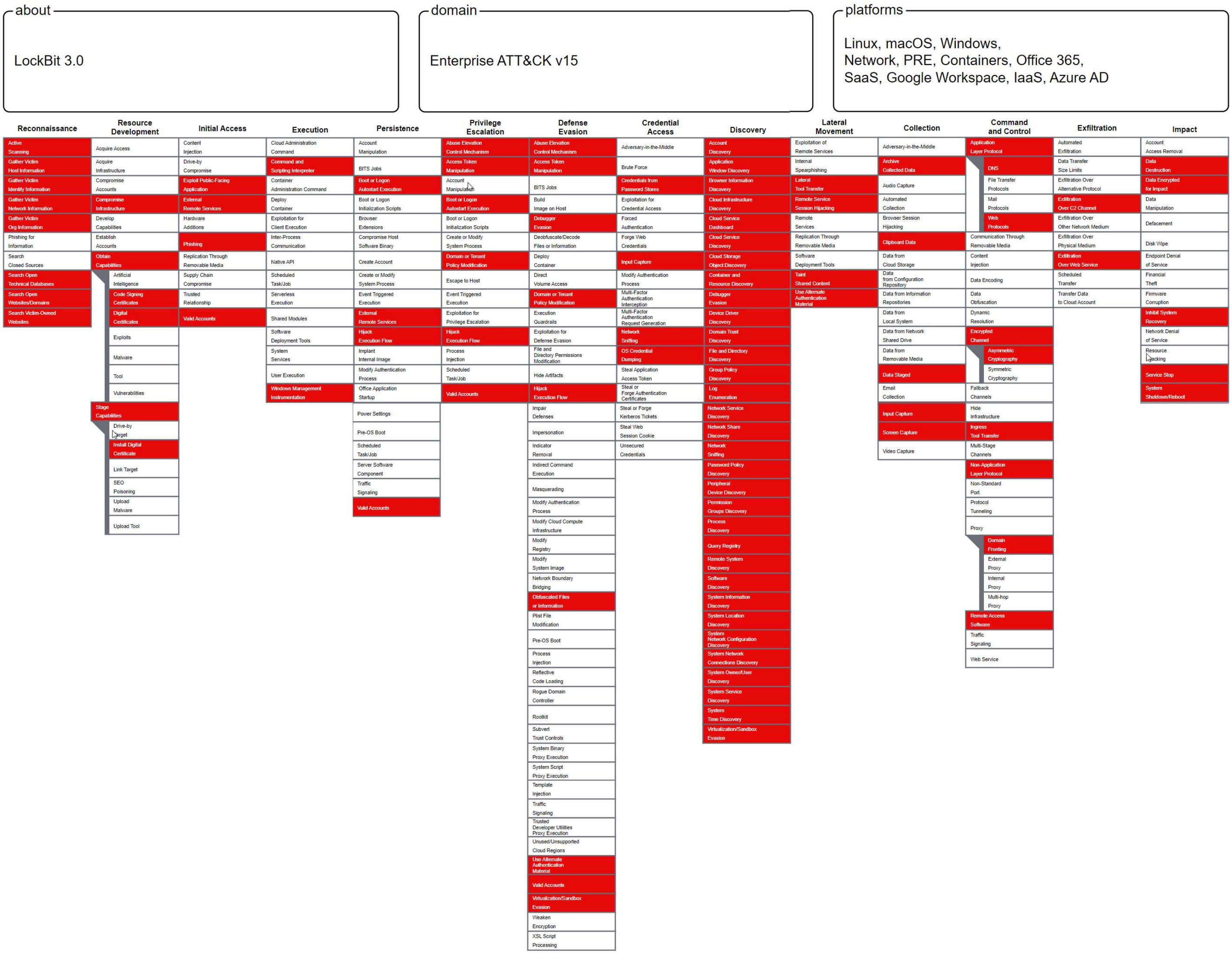
- StealBit: The threat gang introduced StealBit, a malware tool used for encryption in the LockBit 2.0 version. It is believed to be the fastest and most efficient encryption tool.
- Spreads Fast: StealBit spreads to other devices in the network automatically, using tools like Windows Powershell and Server Message Block (SMB), which makes it difficult to confine immediately.
- Attacks Windows and Linux: Initially, they had targeted only Windows systems, but LockBit 2.0 was improvised to attack Linux systems as well.
- Evasion Tactics: Their evasion tactics are well strategized, making it hard to get flagged by the system defenses.
- Bug Bounty: LockBit conducts bug bounty programs to improve their defenses and establish that they are professional hackers. Anyone who finds a flaw in their malware kit is rewarded generously.
- Marketing: They actively market towards affiliates to join them and carry out attacks. These marketing activities have garnered quite the attention and work well for the group in getting highly-skilled threat actors.
- ZCash: LockBit 3.0 introduced ZCash payment options for collecting ransom from victims, as well as for paying their affiliates, with less disruption from law enforcement.
- Double Extortion: LockBit is known for its double extortion technique wherein they steal data and also encrypt the system data making it harder for victims to recover it.
- Triple Extortion: In August 2022, LockBit announced that it would use triple extortion on its victims via data leaks, encryption, and DDoS attacks.
- File Deletion: A notable tactic of the third version of LockBit includes a file deletion technique, where instead of using cmd.exe to execute a batch file to perform the deletion.
- Exfiltrator-22: A new attack framework was created by affiliates of the former LockBit 3.0 operation that includes features found commonly in other post-exploitation toolkits, but has added features that enhance ransomware deployment and data theft. The EX-22, as it is referred to, is designed to spread ransomware quickly in corporate networks while evading detection.
- AV and EDR: The LockBit ransomware group started a campaign in early January 2023, that used combinations of techniques effective against AV and EDR solutions.
- Exfiltrate Data: In a recent campaign, the LockBit gang introduced a new method to allow it to exfiltrate data from high-profile organizations by bypassing the Mark of The Web (MOTW) protection mechanism.
- Avoids Certain Languages: LockBit 3.0 also checks the victim’s UI language before carrying out an attack. They avoid infecting systems with the following languages:
  - Arabic (Syria)
  - Armenian (Armenia)
  - Azerbaijani (Cyrillic Azerbaijan)
  - Azerbaijani (Latin Azerbaijan)
  - Belarusian (Belarus)
  - Georgian (Georgia)
  - Kazakh (Kazakhstan)
  - Kyrgyz (Kyrgyzstan)
  - Romanian (Moldova)
  - Russian (Moldova)
  - Russian (Russia)
  - Tajik (Cyrillic Tajikistan)
  - Turkmen (Turkmenistan)
  - Tatar (Russia)
  - Ukrainian (Ukraine)
  - Uzbek (Cyrillic Uzbekistan)

- Uzbek (Latin Uzbekistan)

Diamond model:


LOCKBIT 3.0
Adversary
Infrastructure
Capability
Victim
MEGA
AnyDesk
splashtop
TeamViewer
FreeFileSync
CONTI
LockBit Black
All your important files are stolen and encrypted!
You must find xEC9do6g6.README.txt file
and follow the instruction!
StealBit
Introduction of LockBit Linux-ESXi Locker version 1.0 expanding capabilities to target systems to Linux and VMware ESXi.
LockBit ransomware encryptors targeting macOS seen on VirusTotal
HOSPITAL
OIL & GAS
BANK
LOGISTIC

MITRE ATT&CK Mapping:



about

LockBit 3.0

domain

Enterprise ATT&CK v15

platforms

Linux, macOS, Windows,
Network, PRE, Containers, Office 365,
SaaS, Google Workspace, IaaS, Azure AD

Reconnaissance

- **Active Scanning**
- **Gather Victim Host Information**
- **Gather Victim Identity Information**
- **Gather Victim Network Information**
- **Gather Victim Org Information**
- Phishing for Information
- Search Closed Sources
- **Search Open Technical Databases**
- **Search Open Websites/Domains**
- **Search Victim-Owned Websites**

Resource Development

- Acquire Access
- Acquire Infrastructure
- Compromise Accounts
- **Compromise Infrastructure**
- Develop Capabilities
- Establish Accounts
- **Obtain Capabilities**
  - Artificial Intelligence
  - **Code Signing Certificates**
  - **Digital Certificates**
  - Exploits
  - Malware
  - Tool
  - Vulnerabilities
- **Stage Capabilities**
  - Drive-by Target
  - **Install Digital Certificate**
  - Link Target
  - SEO Poisoning
  - Upload Malware
  - Upload Tool

Initial Access

- Content Injection
- Drive-by Compromise
- **Exploit Public-Facing Application**
- **External Remote Services**
- Hardware Additions
- **Phishing**
- Replication Through Removable Media
- Supply Chain Compromise
- Trusted Relationship
- **Valid Accounts**

Execution

- Cloud Administration Command
- **Command and Scripting Interpreter**
- Container Administration Command
- Deploy Container
- Exploitation for Client Execution
- Inter-Process Communication
- Native API
- Scheduled Task/Job
- Serverless Execution
- Shared Modules
- Software Deployment Tools
- System Services
- User Execution
- **Windows Management Instrumentation**

Persistence

- Account Manipulation
- BITS Jobs
- **Boot or Logon Autostart Execution**
- Boot or Logon Initialization Scripts
- Browser Extensions
- Compromise Host Software Binary
- Create Account
- Create or Modify System Process
- Event Triggered Execution
- **External Remote Services**
- **Hijack Execution Flow**
- Implant Internal Image
- Modify Authentication Process
- Office Application Startup
- Power Settings
- Pre-OS Boot
- Scheduled Task/Job
- Server Software Component
- Traffic Signaling
- **Valid Accounts**

Privilege Escalation

- **Abuse Elevation Control Mechanism**
- **Access Token Manipulation**
- Account Manipulation
- **Boot or Logon Autostart Execution**
- Boot or Logon Initialization Scripts
- Create or Modify System Process
- **Domain or Tenant Policy Modification**
- Escape to Host
- Event Triggered Execution
- Exploitation for Privilege Escalation
- **Hijack Execution Flow**
- Process Injection
- Scheduled Task/Job
- **Valid Accounts**

Defense Evasion

- **Abuse Elevation Control Mechanism**
- **Access Token Manipulation**
- BITS Jobs
- Build Image on Host
- **Debugger Evasion**
- Deobfuscate/Decode Files or Information
- Deploy Container
- Direct Volume Access
- **Domain or Tenant Policy Modification**
- Execution Guardrails
- Exploitation for Defense Evasion
- File and Directory Permissions Modification
- Hide Artifacts
- **Hijack Execution Flow**
- Impair Defenses
- Impersonation
- Indicator Removal
- Indirect Command Execution
- Masquerading
- Modify Authentication Process
- Modify Cloud Compute Infrastructure
- Modify Registry
- Modify System Image
- Network Boundary Bridging
- **Obfuscated Files or Information**
- Plist File Modification
- Pre-OS Boot
- Process Injection
- Reflective Code Loading
- Rogue Domain Controller
- Rootkit
- Subvert Trust Controls
- System Binary Proxy Execution
- System Script Proxy Execution
- Template Injection
- Traffic Signaling
- Trusted Developer Utilities Proxy Execution
- Unused/Unsupported Cloud Regions
- **Use Alternate Authentication Material**
- **Valid Accounts**
- **Virtualization/Sandbox Evasion**
- Weaken Encryption
- XSL Script Processing

Credential Access

- Adversary-in-the-Middle
- Brute Force
- **Credentials from Password Stores**
- Exploitation for Credential Access
- Forced Authentication
- Forge Web Credentials
- **Input Capture**
- Modify Authentication Process
- Multi-Factor Authentication Interception
- Multi-Factor Authentication Request Generation
- **Network Sniffing**
- **OS Credential Dumping**
- Steal Application Access Token
- Steal or Forge Authentication Certificates
- Steal or Forge Kerberos Tickets
- Steal Web Session Cookie
- Unsecured Credentials

Discovery

- **Account Discovery**
- **Application Window Discovery**
- **Browser Information Discovery**
- **Cloud Infrastructure Discovery**
- **Cloud Service Dashboard**
- **Cloud Service Discovery**
- **Cloud Storage Object Discovery**
- **Container and Resource Discovery**
- **Debugger Evasion**
- **Device Driver Discovery**
- **Domain Trust Discovery**
- **File and Directory Discovery**
- **Group Policy Discovery**
- **Log Enumeration**
- **Network Service Discovery**
- **Network Share Discovery**
- **Network Sniffing**
- **Password Policy Discovery**
- **Peripheral Device Discovery**
- **Permission Groups Discovery**
- **Process Discovery**
- **Query Registry**
- **Remote System Discovery**
- **Software Discovery**
- **System Information Discovery**
- **System Location Discovery**
- **System Network Configuration Discovery**
- **System Network Connections Discovery**
- **System Owner/User Discovery**
- **System Service Discovery**
- **System Time Discovery**
- **Virtualization/Sandbox Evasion**

Lateral Movement

- Exploitation of Remote Services
- Internal Spearphishing
- **Lateral Tool Transfer**
- **Remote Service Session Hijacking**
- Remote Services
- Replication Through Removable Media
- Software Deployment Tools
- **Taint Shared Content**
- **Use Alternate Authentication Material**

Collection

- Adversary-in-the-Middle
- **Archive Collected Data**
- Audio Capture
- Automated Collection
- Browser Session Hijacking
- **Clipboard Data**
- Data from Cloud Storage
- Data from Configuration Repository
- Data from Information Repositories
- Data from Local System
- Data from Network Shared Drive
- Data from Removable Media
- **Data Staged**
- Email Collection
- **Input Capture**
- **Screen Capture**
- Video Capture

Command and Control

- **Application Layer Protocol**
  - **DNS**
  - File Transfer Protocols
  - Mail Protocols
  - **Web Protocols**
- Communication Through Removable Media
- Content Injection
- Data Encoding
- Data Obfuscation
- Dynamic Resolution
- **Encrypted Channel**
  - **Asymmetric Cryptography**
  - Symmetric Cryptography
- Fallback Channels
- Hide Infrastructure
- **Ingress Tool Transfer**
- Multi-Stage Channels
- **Non-Application Layer Protocol**
- Non-Standard Port
- Protocol Tunneling
- Proxy
  - **Domain Fronting**
  - External Proxy
  - Internal Proxy
  - Multi-hop Proxy
- **Remote Access Software**
- Traffic Signaling
- Web Service

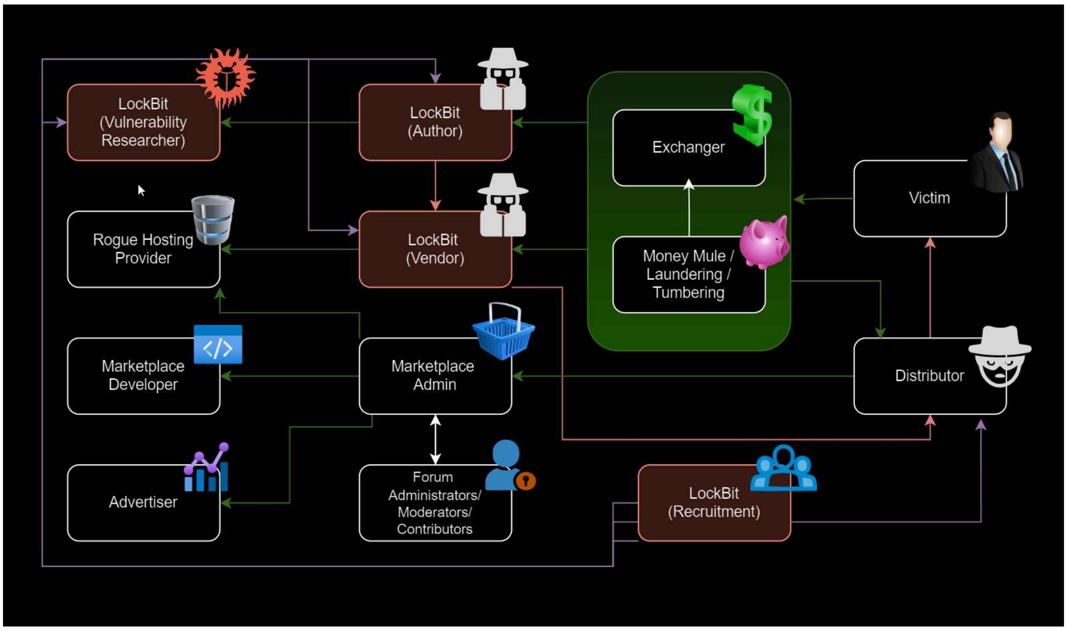
Exfiltration

- Automated Exfiltration
- Data Transfer Size Limits
- Exfiltration Over Alternative Protocol
- **Exfiltration Over C2 Channel**
- Exfiltration Over Other Network Medium
- Exfiltration Over Physical Medium
- **Exfiltration Over Web Service**
- Scheduled Transfer
- Transfer Data to Cloud Account

Impact

- Account Access Removal
- **Data Destruction**
- **Data Encrypted for Impact**
- Data Manipulation
- Defacement
- Disk Wipe
- Endpoint Denial of Service
- Financial Theft
- Firmware Corruption
- **Inhibit System Recovery**
- Network Denial of Service
- Resource Hijacking
- **Service Stop**
- **System Shutdown/Reboot**

RaaS Architecture Lockbit:



Deception Ideas:

1. **Honeypots**: These are decoy systems or networks designed to attract attackers, allowing security teams to monitor their activities and gather intelligence.
2. **Decoy Files**: Placing fake files or data within a system that appear valuable to attackers but are actually designed to divert their attention and waste their time.
3. **Honeynets**: Similar to honeypots, honeynets are entire networks of interconnected honeypots, providing a more extensive environment for deception and monitoring.
4. **Deceptive Links**: Embedding misleading links within websites, emails, or documents to lure attackers into clicking on them, leading to trap pages or monitoring systems.
5. **Deceptive User Interfaces**: Designing user interfaces that mimic legitimate systems but are actually controlled by security teams, allowing them to observe attacker behavior and gather intelligence.
6. **Tarpits**: Slowing down network connections intentionally to frustrate attackers and prolong their engagement, giving security teams more time to respond and gather information.
7. **Deceptive Routing**: Redirecting malicious traffic to decoy servers or network segments, which mimic legitimate services but are designed to analyze and mitigate threats.
8. **Honey Credentials**: Creating fake user accounts, passwords, or access tokens that appear legitimate but lead attackers to restricted areas or monitored systems.
9. **Canary Tokens**: Deploying digital tokens or markers within a network or system that trigger alerts when accessed, indicating unauthorized or suspicious activity.
10. **DNS Deception**: Manipulating DNS records to redirect attackers to decoy servers or IP addresses, where their activities can be monitored or blocked.
11. **Repacking**: Repackaging makes real assets look as irrelevant as possible. Assets that can’t be masked as well can be repackaged to hide their true value, making them easy to gloss over.

KQL Queries:

Service stopping (KQL):

```
SecurityEvent
| where EventID in (7035, 7036, 7040, 7045)
| where TimeGenerated > ago(1d)
| project TimeGenerated, EventID, AccountName, TargetUserName, TargetDomainName, ServiceName, Image
```

Find attempts to stop processes using net stop (KQL):

```
DeviceProcessEvents
| where Timestamp > ago(1d)
| where FileName =~ "net.exe" and ProcessCommandLine has "stop"
| summarize netStopCount = dcount(ProcessCommandLine), NetStopList = make_set(ProcessCommandLine) by DeviceId, bin(Timestamp, 2m)
| where netStopCount > 10
```

Find attempts to stop processes using taskkill.exe (KQL):

```
DeviceProcessEvents
| where Timestamp > ago(1d)
| where FileName =~ "taskkill.exe"
| summarize taskKillCount = dcount(ProcessCommandLine), TaskKillList = make_set(ProcessCommandLine) by DeviceId, bin(Timestamp, 2m)
| where taskKillCount > 10
```

Turning off services using sc.exe (KQL):

```
DeviceProcessEvents
| where Timestamp > ago(1d)
| where ProcessCommandLine has "sc" and ProcessCommandLine has "config" and ProcessCommandLine has "disabled"
| summarize ScDisableCount = dcount(ProcessCommandLine), ScDisableList = make_set(ProcessCommandLine) by DeviceId, bin(Timestamp,
5m)
| where ScDisableCount > 10
```

Deleting shadow copies and backups (KQL):

```
SecurityEvent
| where EventID in (1102, 4690, 4691, 4692, 4693)
| where TimeGenerated > ago(1d)
| project TimeGenerated, EventID, AccountName, TargetUserName, TargetDomainName, LogonType, LogonProcessName, IpAddress
```

```
DeviceProcessEvents
| where FileName =~ "wmic.exe"
| where ProcessCommandLine has "shadowcopy" and ProcessCommandLine has "delete"
| project DeviceId, Timestamp, InitiatingProcessFileName, FileName,
ProcessCommandLine, InitiatingProcessIntegrityLevel, InitiatingProcessParentFileName
```

Deletion of data on multiple drives using cipher.exe (KQL):

```
// Look for cipher.exe deleting data from multiple drives
DeviceProcessEvents
| where Timestamp > ago(1d)
| where FileName =~ "cipher.exe"
// cipher.exe /w flag used for deleting data
| where ProcessCommandLine has "/w"
| summarize CipherCount = dcount(ProcessCommandLine),
CipherList = make_set(ProcessCommandLine) by DeviceId, bin(Timestamp, 1m)
// cipher.exe accessing multiple drives in a short timeframe
| where CipherCount > 1
```

Turning off system restore (KQL):

```
DeviceProcessEvents
//Pivoting for rundll32
| where InitiatingProcessFileName =~ 'rundll32.exe'
//Looking for empty command line
and InitiatingProcessCommandLine !contains " " and InitiatingProcessCommandLine != ""
//Looking for schtasks.exe as the created process
and FileName in~ ('schtasks.exe')
//Disabling system restore
and ProcessCommandLine has 'Change' and ProcessCommandLine has 'SystemRestore'
and ProcessCommandLine has 'disable'
```

Look for use of wevtutil to clear multiple logs (KQL):

```
DeviceProcessEvents
| where Timestamp > ago(1d)
| where ProcessCommandLine has "WEVTUTIL" and ProcessCommandLine has "CL"
| summarize LogClearCount = dcount(ProcessCommandLine), ClearedLogList = make_set(ProcessCommandLine) by DeviceId,
bin(Timestamp, 5m)
| where LogClearCount > 10
```

DLL Hijacking (KQL):

-
  ```
  DeviceImageLoadEvents | extend FileName = tolower(FileName), FolderPath = tolower(FolderPath), InitiatingProcessFileName = tolower(InitiatingProcessFileName)
  | where (FileName == "acrodistdll.dll" and not(FolderPath contains "c:\\program files\\adobe\\acrobat " and FolderPath contains "\\acrobat") and (InitiatingProcessFileName endswith "acrodist.exe"))
  or (FileName == "vender.dll" and not(FolderPath contains "c:\\program files\\asus\\gpu tweakii" or FolderPath contains "c:\\program files\\asus\\vga com\\") and (InitiatingProcessFileName endswith "asusgpufanservice.exe"))
  or (FileName == "wsc.dll" and not(FolderPath contains "c:\\program files\\avast software\\avast") and (InitiatingProcessFileName endswith "wsc_proxy.exe"))
  or (FileName == "windowsperformancerecorderui.dll" and not(FolderPath contains "c:\\program files\\windows kits\\10\\windows performance toolkit") and (InitiatingProcessFileName endswith "wprui.exe"))
  | invoke FileProfile("SHA1", 1000)
  ```

mpclient.dll non-standard location (KQL):

```
DeviceFileEvents
| join DeviceFileCertificateInfo on DeviceName //This is for checking if it is a signed version of the dll joined on Device Name for distinct usage

| where Timestamp > ago(7d) // look back over the past week

| where InitiatingProcessFolderPath contains "\\programdata\\microsoft\\windows defender\\platform" // makes sure that the intiating process is in the proper directory

| where InitiatingProcessFileName == "MpCmdRun.exe" and IsSigned // checks to make sure that mpclient is being run

| where FolderPath !contains "\\programdata\\microsoft\\windows defender\\platform" // do not check the normal location for the dll being run

| where FileName contains "mpclient"// checks for the misused dlls.

| distinct DeviceName, Timestamp, FileName, FolderPath, InitiatingProcessFileName, InitiatingProcessFolderPath
```

IOCs:

~~~
## LockBit ransomware IoCs

Ransom gates
- lockbitkodidilol.onion
- lockbitks2tvnmwk.onion

Ransom note
- Restore-My-Files.txt

Ransom extension
- .lockbit

E-mail
- ondrugs@firemail.cc

Persistence
- HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\XO1XADpO01

Mutex
- Global\{BEF590BE-11A6-442A-A85B-656C1081E04C}

Executed commands
- bcdedit /set {default} recoveryenabled No
- bcdedit /set {default} bootstatuspolicy ignoreallfailures
- vssadmin delete shadows /all /quiet
- wbadmin DELETE SYSTEMSTATEBACKUP -deleteOldest
- wbadmin DELETE SYSTEMSTATEBACKUP
- wbadmin delete catalog -quiet
- wevtutil cl system
- wevtutil cl security
- wevtutil cl application
- wmic SHADOWCOPY /nointeractive
- wmic shadowcopy delete
- ping 1.1.1.1 -n 22 > Nul & \"%s\"
- ping 127.0.0.7 -n 3 > Nul & fsutil file setZeroData offset=0 length=524288 "%s" & Del /f /q "%s"

Registry keys
- SOFTWARE\LockBit
- SOFTWARE\LockBit\full
- SOFTWARE\LockBit\Public

Folders skip-list
```
$windows.~bt
intel
msocache
$recycle.bin
$windows.~ws
tor browser
boot
system volume information
perflogs
google
application data
windows
windows.old
appdata
Windows nt
Msbuild
Microsoft
All users
Mozilla
```

Files skip-list
```
ntldr
ntuser.dat.log
bootsect.bak
autorun.inf
```

Service stop-list
```
wrapper
DefWatch
ccEvtMgr
ccSetMgr
SavRoam
Sqlservr
sqlagent
sqladhlp
Culserver
RTVscan
sqlbrowser
~~~

```
SQLADHLP
QBIDPService
Intuit.QuickBooks.FCS
QBCFMonitorService
sqlwriter
msmdsrv
tomcat6
zhudongfangyu
vmware-usbarbitator64
vmware-converter
dbsrv12
dbeng8
MSSQL$MICROSOFT##WID
MSSQL$VEEAMSQL2012
SQLAgent$VEEAMSQL2012
SQLBrowser
SQLWriter
FishbowlMySQL
MSSQL$MICROSOFT##WID
MySQL57
MSSQL$KAV_CS_ADMIN_KIT
MSSQLServerADHelper100
SQLAgent$KAV_CS_ADMIN_KIT
msftesql-Exchange
MSSQL$MICROSOFT##SSEE
MSSQL$SBSMONITORING
MSSQL$SHAREPOINT
MSSQLFDLauncher$SBSMONITORING
MSSQLFDLauncher$SHAREPOINT
SQLAgent$SBSMONITORING
SQLAgent$SHAREPOINT
QBFCService
QBVSS
YooBackup
YooIT
svc$
MSSQL
MSSQL$
memtas
mepocs
sophos
veeam
backup
bedbg
PDVFSService
BackupExecVSSProvider
BackupExecAgentAccelerator
BackupExecAgentBrowser
BackupExecDiveciMediaService
BackupExecJobEngine
BackupExecManagementService
BackupExecRPCService
MVArmor
MVarmor64
stc_raw_agent
VSNAPVSS
VeeamTransportSvc
VeeamDeploymentService
VeeamNFSSvc
AcronisAgent
ARSM
AcrSch2Svc
CASAD2DWebSvc
CAARCUpdateSvc
WSBExchange
MSExchange
MSExchange$
LanmanWorkstation
WebClient
```

Process kill-list

```
wxServer
wxServerView
sqlmangr
RAgui
supervise
Culture
Defwatch
winword
QBW32
QBDBMgr
qbupdate
```

```
axlbridge
httpd
fdlauncher
MsDtSrvr
java
360se
360doctor
wdswfsafe
fdhost
GDscan
ZhuDongFangYu
QBDBMgrN
mysqld
AutodeskDesktopApp
acwebbrowser
Creative Cloud
Adobe Desktop Service
CoreSync
Adobe CEF Helper
node
AdobeIPCBroker
sync-taskbar
sync-worker
InputPersonalization
AdobeCollabSync
BrCtrlCntr
BrCcUxSys
SimplyConnectionManager
Simply.SystemTrayIcon
fbguard
fbserver
ONENOTEM
wsa_service
koaly-exp-engine-service
TeamViewer_Service
TeamViewer
tv_w32
tv_x64
TitanV
Ssms
notepad
RdrCEF
oracle
ocssd
dbsnmp
synctime
agntsvc
isqlplussvc
xfssvccon
mydesktopservice
ocautoupds
encsvc
firefox
tbirdconfig
mydesktopqos
ocomm
dbeng50
sqbcoreservice
excel
infopath
msaccess
mspub
onenote
outlook
powerpnt
steam
thebat
thunderbird
visio
wordpad
bedbh
vxmon
benetns
bengien
pvlsvr
beserver
raw_agent_svc
vsnapvss
CagService
DellSystemDetect
EnterpriseClient
VeeamDeploymentSvc
```

Extension list

```
.msstyles
.sqlitedb
.sqlite3
.diagcab
.diagcfg
.diagpkg
.sqlite
.db-shm
.db-wal
.dacpac
.theme
.icns
.lock
.tmd
.ckp
.dbc
.sql
.mwb
.rar
.dbv
.frm
.mdf
.dbt
.qry
.ndf
.sdb
.myd
.mrg
.db3
.dbs
.dbf
.sdf
.zip
.rdp
.bin
.hlp
.shs
.drv
.wpx
.bat
.rom
.msc
.spl
.ps1
.msu
.ics
.key
.exe
.dll
.lnk
.ico
.hlp
.sys
.drv
.cur
.idx
.ini
.reg
.mp3
.386
.cmd
.ani
.adv
.msi
.msp
.com
.nls
.ocx
.mpa
.cpl
.mod
.hta
.prf
.rtp
```

Ransom note:

```
All your important files are encrypted!
Any attempts to restore your files with the thrid-party software will be fatal for your files!
RESTORE YOU DATA POSIBLE ONLY BUYING private key from us.
There is only one way to get your files back:
```

~~~
| 1. Download Tor browser - https://www.torproject.org/ and install it.
| 2. Open link in TOR browser - http://lockbitks2tvnmwk.onion/?
This link only works in Tor Browser!
| 3. Follow the instructions on this page

 ###  Attention! ###
 # Do not rename encrypted files.
 # Do not try to decrypt using third party software, it may cause permanent data loss.
 # Decryption of your files with the help of third parties may cause increased price(they add their fee to our)
 # Tor Browser may be blocked in your country or corporate network. Use https://bridges.torproject.org
 # Tor Browser user manual https://tb-manual.torproject.org/about

!!! We also download huge amount of your private data, including finance information, clients personal info, network diagrams, passwords and so on. Don't forget about GDPR.
```

SHA256
- 0a937d4fe8aa6cb947b95841c490d73e452a3cafcd92645afc353006786aba76
- 0e66029132a885143b87b1e49e32663a52737bbff4ab96186e9e5e829aa2915f
- 0f178bc093b6b9d25924a85d9a7dde64592215599733e83e3bbc6df219564335
- 0f5d71496ab540c3395cfc024778a7ac5c6b5418f165cc753ea2b2befbd42d51
- 13849c0c923bfed5ab37224d59e2d12e3e72f97dc7f539136ae09484cbe8e5e0
- 15a7d528587ffc860f038bb5be5e90b79060fbba5948766d9f8aa46381ccde8a
- 1b109db549dd0bf64cadafec575b5895690760c7180a4edbf0c5296766162f18
- 1e3bf358c76f4030ffc4437d5fcd80c54bd91b361abb43a4fa6340e62d986770
- 256e2bf5f3c819e0add95147b606dc314bbcbac32a801a59584f43a4575e25dc
- 26b6a9fecfc9d4b4b2c2ff02885b257721687e6b820f72cf2e66c1cae2675739
- 2b8117925b4b5b39192aaaea130426bda39ebb5f363102641003f2c2cb33b785
- 3f29a368c48b0a851db473a70498e168d59c75b7106002ac533711ca5cfabf89
- 410c884d883ebe2172507b5eadd10bc8a2ae2564ba0d33b1e84e5f3c22bd3677
- 4acc0b5ed29adf00916dea7652bcab8012d83d924438a410bee32afbcdb995cc
- 5b9bae348788cd2a1ce0ba798f9ae9264c662097011adbd44ecfab63a8c4ae28
- 6292c2294ad1e84cd0925c31ee6deb7afd300f935004a9e8a7a43bf80034abae
- 69d9dd7fdd88f33e2343fb391ba063a65fe5ffbe649da1c5083ec4a67c525997
- 83ab7a2bcac146db472f3b930c01af5b6d3d978ead7b14a9d0ac16e1a76e9f9d
- 9bc98d15f243257c1b5bca59464abe68c680cd5482ba9f5082201dde41a016cf
- a03326ac8efa930e10091a374d40ddab9f7c2f12246d6ef7983bad93256f1f3a
- a0085da4a920e92d8f59fefa6f25551655ca911382b5e34df76a9333ac8b7214
- a08fbf01d02097094b725101309b2bf7fefc2e27724654b840b87e091aa5c9b9
- a1360645cf3113715cc023d2e4cf9f6f3a6278abcf4499f0ba7cd76c82839eb0
- c8205792fbc0a5efc6b8f0f2257514990bfaa987768c4839d413dd10721e8871
- ce8559871b410e23057393eb2d9fb76ec902da2ff1f8006ad312c81852a41f6f
- e3f236e4aeb73f8f8f0caebe46f53abbb2f71fa4b266a34ab50e01933709e877
- ec88f821d22e5553afb94b4834f91ecdedeb27d9ebfd882a7d8f33b5f12ac38d
- ffbb6c4d8d704a530bdd557890f367ad904c09c03f53fda5615a7208a0ea3e4d

Decryptors
- 09e956d140d6879cf7eacbb65dcbfbe1dea1961a31c5d0f834343ef2c886ccc1
- 9bc98d15f243257c1b5bca59464abe68c680cd5482ba9f5082201dde41a016cf

VT perks:
- vhash:"015036656d5223z12z3e05031f1z37z406001a5zb7z"
- imphash:"be232aa2621354bf5dd7b405cc99198c"

YARA rules
```
rule lockbit_clsids
{
   meta:
      author = "Albert Zsigovits, SophosLabs"

   strings:
      $id1 = "{3E5FC7F9-9A51-4367-9063-A120244FBEC7}" ascii wide
      $id2 = "{D2E7041B-2927-42fb-8E9F-7CE93B6DC937}" ascii wide
      $id3 = "{02B49784-1CA2-436C-BC08-72FA3956507D}" ascii wide
      $id4 = "{BEF590BE-11A6-442A-A85B-656C1081E04C}" ascii wide

   condition:
      3 of them
}
```

rule lockbit_mutex
{
   meta:
      author = "Albert Zsigovits, SophosLabs"

   strings:
      $mutex = "XO1XADpO01" ascii wide

   condition:
      all of them
}

rule lockbit_uac
{
   meta:
      author = "Albert Zsigovits, SophosLabs"
~~~

```
    strings:
        $uac0 = "Elevation:Administrator!new:" ascii wide
        $uac1 = "DisplayCalibrator" ascii wide
        $uac2 = "Software\Microsoft\Windows NT\CurrentVersion\ICM\Calibration" ascii wide

    condition:
        all of them
}

rule lockbit_cmd
{
    meta:
        author = "Albert Zsigovits, SophosLabs"

    strings:
        $cmd0 = "vssadmin Delete Shadows /All /Quiet" ascii wide
        $cmd1 = "bcdedit /set {default} recoveryenabled No" ascii wide
        $cmd2 = "bcdedit /set {default} bootstatuspolicy ignoreallfailures" ascii wide
        $cmd3 = "wbadmin DELETE SYSTEMSTATEBACKUP" ascii wide
        $cmd4 = "wbadmin DELETE SYSTEMSTATEBACKUP -deleteOldest" ascii wide
        $cmd5 = "wmic SHADOWCOPY /nointeractive" ascii wide
        $cmd6 = "wevtutil cl security" ascii wide
        $cmd7 = "wevtutil cl system" ascii wide
        $cmd8 = "wevtutil cl application" ascii wide

    condition:
        6 of them
}

rule both
{
    meta:
        author = "Albert Zsigovits, SophosLabs"

    strings:
        $masq = { ff 15 [1-4] 85 ?? 0f [1-5] 68 04 01 00 00 8d [1-5] 50 ff 15 [1-4] 8b [1-5] 8d [1-5] 0f ?? ?? 8d ?? ?? 66 ?? ?? 8d ?? ?? 66 ?? ?? 75 ?? 0f ?? ?? [1-4] be 3f [1-3] 66 ?? ?? c7 45 ?? [1-4] 66 ?? ?? ?? }
        $priv = { ff 15 [1-4] 85 ?? 74 ?? 8d ?? ?? 50 8d ?? ?? 50 6a 00 ff 15 [1-4] 85 ?? 74 ?? 39 ?? ?? 75 ?? 8d ?? ?? 50 6a 04 8d ?? ?? 50 6a 13 ff 75 ?? ff 15 [1-4] 85 ?? 7? ?? ?? ?? [1-4] 3d [1-4] 74 ?? 3d [1-4] 74 ?? 85 ?? 7f ?? 8b ?? eb ?? 0f ?? ?? 81 [1-5] eb ?? 8d ?? ?? 50 8d ?? ?? 50 ff 75 ?? ff 15 }

    condition:
        $masq or $priv
}
```