Activity Report

LockBit 3.0 Ransomware Attacks Within The Israeli Cyberspace

Written by

Sophy Starik
Head of Cyber-Crime Team

Tamir Mashihov
CTI Researcher

April 2024

TLP:CLEAR

INCD
Israel National
Cyber Directorate

Table Of Contents

Part I:

Introduction

Background

LockBit ransomware has long held a dominant position at the forefront of the most active and prevalent threats in the cyber landscape. Since its debut in the ransomware arena in 2019 with its first version, LockBit has orchestrated numerous attacks targeting entities across diverse sectors, regardless of their size or global location. The threat group behind LockBit operates as a Ransomware-as-a-Service (RaaS), allowing affiliates to deploy the ransomware and share profits with the operators behind the ransomware service.

LockBit Versions

The LockBit group made its debut as a ransomware under the alias "ABCD" (named after its file extension), and a few months later, the ransomware emerged as highly similar variant under the notorious name "LockBit". A year later, the group released an upgraded version of the ransomware called "LockBit 2.0" (or "LockBit Red"), which included another built-in malware known as "StealBit". This component was responsible for data exfiltration and sensitive information theft (info-stealer). The latest version, "LockBit 3.0" (also known as "LockBit Black"), emerged in 2022 with new features, including security evasion techniques and even a Bug Bounty program.

LockBit Source Code

In September 2022, the source code of the LockBit 3.0 was leaked by an unknown individual under the alias "ali_qushji" on the X platform (formerly Twitter). The leak included several files that could be utilized to develop the original ransomware (using a builder) by providing a public and private key. On one hand, the leak enabled an in-depth analysis of the ransomware, while on the other hand, it triggered a wave of new ransomware variants, some of which are based entirely or partially on the source code of LockBit 3.0.

Leveraging LockBit

Since the leak of the source code, several variants leveraging it have surfaced. Concurrently, additional threat actors have used the same version to conduct ransomware attacks. Over the past few months, numerous attacks of the LockBit ransomware were observed in Israel, many of which have been reported to INCD’s 119 call center. The LockBit 3.0 variant has been the dominant variant in the majority of these incidents in Israel. Some attackers appear to be affiliated with LockBit, while others exploited the source code to deploy the ransomware for their personal gains (whether financial or otherwise).

The mentioned ransomware attacks led the INCD to identify activity clusters associated with attackers leveraging this particular ransomware. The following report describes a detailed overview of the observed activity within the Israeli cyberspace.

Part II:

Activity Clusters

INCD
Israel National
Cyber Directorate

Activity Cluster #1 – “TronBit”

A connection is being established to the targeted endpoint through TeamViewer, presumably by using leaked credentials or those acquired through the deployment of info-stealer malware. The following TeamViewer logs were observed in the aftermath of the attacks:

```
HWC-HWP-7866150 06-12-2023 14:39:45 06-12-2023 14:41:35 [USER] RemoteControl [GUID]
```

The endpoint that established the connection for several minutes was "HWC-HWP-7866150". This behavior closely resembles findings from a report by Huntress[1], describing similar activity involving connections via TeamViewer to execute the ransomware.

Windows Defender is disabled, occasionally as part of a sequence of actions disabling security services. Additionally, a query of VolumeShadowCopy is been executed to encrypt backups and to prevent the recovery of encrypted files. The following command is executed: SELECT * FROM Win32_ShadowCopy.

Upon executing the .exe file of the LockBit 3.0, the desktop background changes to a black screen with a brief message notifying the ransomware attack has occurred and guides the user to the ransom note deployed in each folder named ID.README.txt. Additionally, some files icons are replaced with the LockBit 3.0 icon. The ransom note displayed as follows:

```
                 >>>> Your data are stolen and encrypted

      if you do not pay the ransom The Your data permanently deleted

>>>>What guarantees that we will not deceive you?

      We are not a politically motivated group and we do not need anything
other than your money.
      If you pay, we will provide you the programs for decryption and your
data will not be disclosed .
      Life is too short to be sad. Be not sad, money, it is only paper.
    You can contact us and use your personal decryption ID to decrypt a
file for free
>>>>Your personal DECRYPTION ID: [ID]
      If we do not give you decrypters after payment, then nobody will pay
us in the future.
      Therefore, our reputation is very important to us.

>>>>Pay ransom amount 1000$
>>>>Payment cryptocurrency address USDT-TRC20
>>>>[USDT-TRC20 ADDRESS]
>>>>payment is completed, send the payment photo to Email:    [EMAIL
ADRESS]
>>>>payment is completed Send via email we will provide you the programs
      You can contact me by email.
      Email:[EMAIL ADRESS]
```

[1] https://www.huntress.com/blog/ransomware-deployment-attempts-via-teamviewer

```
      Sometimes you will need to wait for our answer because we attack 
many companies.
    we will provide you the programs

    Warning! Do not DELETE or MODIFY any files, it can lead to recovery 
problems!
```

It should be noted that this is the sole activity cluster associated with LockBit 3.0 ransomware that was observed using USDT-TRC20 as a means of payment, to be differentiated from the prevalent use of Bitcoin in the broader spectrum of LockBit 3.0 ransomware activities.

The following email addresses patterns were identified in ransom notes:

- spiroshalkis[@]mail.com
- ericducke[@]mail.com
- contactbit8cca[@]proton.me
- tpichughinn[@]mail.com
- donahuerolland[@]proton.me

The victimology in this operation is extensive, spanning across sectors on a global scale, resembling the modus operandi seen in many opportunistic attacks carried out by the LockBit ransomware. However, the focus of these attacks tends to be primarily on SMBs (small and medium-sized businesses).

Activity Cluster #2 – “CriptomanGizmo”

The execution of ransom attacks using LockBit 3.0 was by an entity known as "CriptomanGizmo" (derived from the attacker’s indicators). These attacks specifically target relatively "small" entities, such as individual computers and small businesses, with minimal lateral movement within the network. This entity has previously utilized various ransomware strains, including STOP/DJVU.

We assess that the initial access vector is, but not limited to, insecure Remote Desktop Protocol (RDP) connections. This implies that leaked credentials, weak passwords, and poorly configured RDP servers exposed to the internet allow remote connections by those malicious actors. Additional potential attack vectors may involve exploiting software vulnerabilities enabling Remote Code Execution (RCE), and possibly malicious emails and attachments.

An example of a ransom note in a CriptomanGizmo ransomware attack:

```
                        YOUR FILES ARE ENCRYPTED!!!
For data recovery contact us you will need to pay us:
returnback[@]cyberfear.com
returnbac[@]onionmail.org
@returnbacc
https://t[.]me/returnbacc
1. In the first letter, indicate your personal ID!
2. In response, we will send you instructions.

>>>> Your personal DECRYPTION ID: [ID]
```

The following indicators were found in the ransom notes[2]:

returnback[@]cyberfear.com	Email address
returnbac[@]onionmail.org	Email address
warthunder089[@]mailfence.com	Email address
warthunder089[@]tutanota.de	Email address
help_havaneza[@]cryptolab.net	Email address
help_havaneza[@]bastardi.net	Email address
mrbrook[@]msgsafe.io	Email address
fireco[@]onionmail.com	Email address
firecorecoverfiles[@]msgsafe.io	Email address
@firecorecoverfiles	Telegram indicator
carabas1337[@]proton.me	Email address
fiileky2023[@]onionmail.com	Email address

[2] https://id-ransomware.blogspot.com/2022/10/criptomangizmo-ransomware.html

Activity Cluster #3 – “Tina Turner”

Other than using the LockBit 3.0 builder to create personal ransomware variants, some affiliates were also observed conducting attacks using the ransomware. Such attacks can be discerned primarily through the attack infrastructure identified in an event and/or through the ransom note which is guiding to a Dedicated Leak Site (DLS) on the TOR network.

This is the only activity cluster in which LockBit 3.0 was used and the attacker initiates mass printing of the ransom note, activating every available network-connected printing device, including invoice and office printers. An example of such a ransom note, generated during a ransomware attack by a LockBit 3.0 affiliate under this operational cluster, is provided below:

```
                         LockBit Black Ransomware

                      Your data are stolen and encrypted
                    The data will be published on TOR website
  hxxp://LockBitapt2yfbt7lchxejug47kmqvqqxvvjpqkmevv4l3azl3gy6pyd[.]onion
        and hxxp://LockBitapt[.]uz if you do not pay the ransom

   You can contact us and decrypt one file for free on these TOR sites
  hxxp://LockBitsupa7e3b4pkn4mgkgojrl5iqgx24clbzc4xm7i6jeetsia3qd[.]onion
  hxxp://LockBitsupn2h6be2cnqpvncyhj4rgmnwn44633hnzzmtxdvjoqlp7yd[.]onion
                         hxxp://LockBitsupp[.]uz

                           Decryption ID: [ID]
```

During this activity, distinctive tactics have been observed that deviate slightly from typical ransom attacks and specifically from LockBit 3.0 ransomware attacks. Messages are sent via email, in addition to the ransom note that is deployed on encrypted endpoints. The reference is to email addresses identified in several different attacks, with some of them featuring unique addresses. Moreover, in some attacks, messages were also sent via WhatsApp, aiming to conduct negotiations (a highly unusual tactic). In these attacks, a leak occurred, which was published on the Telegram platform. The leak was shared in Telegram channels under the alias "\us/". Below are the email addresses identified in several attacks (from which the name of the operational cluster is derived):

- tinanews[@]ro.ru
- tinanews[@]privatemail.com

The victimology is opportunistic, spanning across various sectors with a focus on Small and Medium-sized Businesses (SMBs). Attacks have been detected in the healthcare, agriculture, and food sectors. Based on the chosen targets and observed behavior in these ransom incidents, it can be inferred, as mentioned, that the attackers do not have a specific sector preference. Instead, they seem to target sectors that, in their estimation, will yield profits from the ransom demand. Despite this, there are instances of attacks against law firms and accounting offices, suggesting a potential specific target selection.

In this ransomware campaign, the threat actor has demonstrated a utilization of legitimate tools as part of the attack strategy. Notably, the GMER program, an open-source tool designed for rootkit detection and removal, has been deployed to obfuscate the attacker's behavior during the intrusion. This modus operandi is consistent with historical LockBit operations. Furthermore, some attacks revealed the execution of Mimikatz, a tool deployed for credential harvesting, enabling seamless logins through the exploitation of vulnerabilities in the Windows authentication system.

In this campaign, attackers used TeamViewer to gain control over the victim endpoint, similar to the previously mentioned activity cluster. Moreover, the attacker utilizes other Remote Monitor and Management (RMM) tools such as AnyDesk, TightVNC, and more. In a specific incident, the attack vector was Foritnet VPN. These tactics align with LockBit's established methods of exploiting RMM systems and VPN or RDP services as initial access vectors for executing ransom attacks.

Part III:

Summary & Recommendations

Summary

In the overall activity of LockBit 3.0, whether utilized by the group's affiliates or external actors leveraging the leaked source code, it appears that the primary initial access vectors are:

a) Unsecured RDP connections

b) Leveraging leaked credentials for RMM services

c) Compromised VPN product

The use of LockBit 3.0 typically involves minimal changes to the core functionality of the ransomware itself. However, variations in ransomware deployment tactics include the printing the ransom notes in some cases, utilizing new indicators such as unique emails, redirecting to Telegram channels instead of referencing the DLS website, and specifying independent cryptographic currency addresses unrelated to the infrastructure of the LockBit group.

Besides the information provided in this report, there are numerous instances of external actors leveraging the leaked source code with slight variations in tactics. Due to the extensive range of attack types of LockBit 3.0 ransomware, not all cases are detailed here. Nonetheless, the core usage of the ransomware remains unchanged, utilizing a builder to create a customized ransomware file adapted for each attacker.

** This report includes a list of IOCs associated to different LockBit 3.0 ransomware attacks. The IOCs include a large number of indicators, mostly hashes, due to the myriad of variants of the ransomware and its utilization by numerous actors.*

Mitigation Recommendations

a) Enforce robust password policies to prevent brute-force attacks. Using complex, lengthy passwords that incorporate a combination of lowercase and uppercase alphanumeric characters, alongside special symbols.

b) Implementing Multi-Factor Authentication (MFA). Leveraging additional authentication measures such as SMS or authentication applications like Google/Microsoft Authenticator.

c) Prioritize software updates to mitigate vulnerabilities in Remote Desktop Protocol (RDP) configurations, thereby minimizing the risk of exploitation.

d) Mitigate exposure of external connections to the internet by adopting secure methods like Virtual Private Network (VPN) connections, as opposed to exposing Remote Monitoring and Management (RMM) or RDP connections directly through less secure channels.

e) Implement monitoring of anomalous usage of external connections. Deploying advanced detection capabilities to identify potential exploitation of remote login services.

f) Using white/black lists. Creating user whitelists for RMM applications or implementing rules to restrict specific connections through a well-defined blacklist.

** For additional recommendations in this context and overall guidance against LockBit attacks, please refer to recent publications by CISA.*

Part IV:

Appendices

Appendix A | Tools, techniques, & procedures used by LockBit and/or its users:

Tool	Description	MITRE ATT&CK
RDP	Initial Access	T1563.002
Drive-by Compromise	Initial Access	T1189
Phishing campaigns	Initial Access	T1566
Legitimate Accounts Exploitations- use of leaked credentials, typically acquired in dark marketplaces from Initial Access Brokers (IAB) suppliers	Initial Access	T1078
exploiting vulnerabilities in exposed services	Initial Access	T1190
Targeting servers running vulnerable VPN services using brute-force attacks.	Initial Access	T1133 T1110
The ransomware may move laterally using PsExec or with GPOs with the SMB protocol	Privilege Escalation	T1484 T1021
The ransomware can send encrypted information about the host to the C2 server	Command and Control	T1071.001
Attackers using LockBit 3.0 may utilize StealBit, a customized tool for data exfiltration. This tool is also deployed in the older version, LockBit 2.0, as well as rclone or public file-sharing services such as MEGA, to exfiltrate sensitive information before encryption.	Exfiltration	T1567
Public file-sharing services used to exfiltrate data: • Premiumize.com • Anonfiles.com • Sendspace.com • Fex.net • Transfer.sh • Send.exploit.in • FreeFileSync	Exfiltration	T1567
Chocolatey	Windows Package Manager	T1072
FileZilla	FTP Solution	T1071.002
Impacket	Python 3 class collection for network packet access	T1040 T1569 T1047 T1003
ProcDump	CLI application for CPU monitoring, among others	T1003.001
PuTTY Link (Plink)	Terminal emulation and network file transfer	T1021.004

Mimikatz	Tool used to obtain password and login credentials in Windows	T1098 T1555 T1003
Ngrok	Reverse proxy tool	T1572 T1567 T1102 T1090
SoftPerfect Network Scanner	Free network discovery tool	T1046
Splashtop	Public RMM tool	T1021.001
WinSCP	SSH file transfer tool	T1048.003
AnyDesk	Public RMM tool	T1219
Atera Remote Monitoring & Management (RMM)	Public RMM tool	T1219
TeamViewer	Public RMM tool	T1219
EHorus תוכנת – RMM	Public RMM tool	T1219
ConnectWise (ScreenConnect)	Public RMM tool	T1219
Fgdump	Password dump tool	T1003.002
Terminator	Public tool to block security services and log cleanup	T1562
RustDesk	Public RMM tool	T1219
NetScan	Free network discovery tool	T1049
TruesightKiller	Public tool to block security services; the tool exploits the driver truesight.sys	T1562
Action1 RMM	Public RMM tool	T1219
Total Software	Public RMM tool	T1219
Nirsoft web browser password viewer	Password recovery tool	T1555.003
GMER	Public tool to remove rootkits and to disable EDRs	T1562.001
PCHunter	Process and EDR disabling tool	T1562.001
7-ZIP	Archive compression tool	T1562
AdFind	AD query tool used for privilege escalation and lateral movement	S0552
Advanced Internet Protocol (IP) Scanner	Network scanning and endpoint detection tool	T1046
Advanced Port Scanner	Used for UDP and TCP open port detection	T1046
AdvancedRun	Allows for privilege escalation	TA0004
Backstab	Used for EDR disabling	T1562.001
Bat Armor	Encodes PowerShell payload into BAT files	T1562.001
Bloodhound	Open source tool that identifies attack paths and relationships in AD	T1482
Defender Control	Allows for Microsoft Defender disabling	T1562.001

ThunderShell	Allows for remote access by HTTP requests	T1071.001
TDSSKiller	Used to disable EDRs	T1562.001
Seatbelt	Perform “safety checks” on the Windows host and collects system data	T1082
Process Hacker	Used to disable EDRs	T1562.001
PowerTool	Used to disable EDRs	T1562.001
PasswordFox	Password recovery from Firefox	T1555.003
ExtPassword	Password recovery from Windows machines	T1003
LaZagne	Password recovery from different operating systems	S0349
Ligolo	Allows for reverse TCP/TLS tunneling connection	T1095
LostMyPassword	Password recovery from Windows machines	T1003

Appendix B | Externally facing services vulnerabilities exploitation:

- Microsoft exchange server
- PaperCut
- Weaver E-Cology OA Systym
- Log4j
- Citrix NetScaler ADC, Gateway

Appendix C | CVEs actively used by LockBit and the users of its ransomware:

- CVE-2023-4966
- CVE-2023-27532
- CVE-2021-42278
- CVE-2020-1472
- CVE-2023-0669
- CVE-2023-27350
- CVE-2021-22986
- CVE-2019-0708
- CVE-2018-13379