LockBit
Ransomware Group and performed attacks

Fábio Sá
FEUP - M.EIC
Porto - Portugal
up202007658@fe.up.pt

Inês Gaspar
FEUP - M.EIC
Porto - Portugal
up202007210@fe.up.pt

José A. Gaspar
FEUP - M.EIC
Porto - Portugal
up202008561@fe.up.pt

Lucas Sousa
FEUP - M.EIC
Porto - Portugal
up202004682@fe.up.pt

***Abstract*—This report aims to theoretically explore some of the attacks carried out by the infamous ransomware group LockBit, as well as the most recent attack against them. It also explores the practical side of one of the attacks carried out by the group. Throughout the document, the group is introduced, followed by a timeline of the main attacks they have perpetrated and the attack they have recently been the target of, on the theoretical side. Furthermore, we do a practical exploration of one of the attacks carried out by the group, as well as how we managed to replicate it.**

I. Introduction

LockBit is a cybercriminal group [1] that sells ransomware as a service (RaaS). The group sells these malicious programs to other criminal groups to ease their attacks. Besides, they also perform numerous cybercrimes.

In 2022, LockBit was the most common ransomware worldwide. Early in 2023, it was expected to be in charge of 44% of ransomware occurrences worldwide.

Their team is composed of unethical hackers from all over the world and no government agencies have attributed the group to any nation-state.

This report contains, initially, a general description of LockBit, and the impact they have and enumerates some of the performed attacks. Later on, a practical example of one of those attacks will be demonstrated.

II. LockBit

Based on several articles and forums that can be found online, this section intends to give insights about the LockBit group.

A. Tactics and techniques

The process of an attack has 3 main stages [2]. The first one consists of gaining some confidential information about their target. This involves the exploitation of several vulnerabilities. Some of the attacks performed by LockBit are going to be described later on this report and one of them is going to be replicated. The second stage consists in encrypting all the stolen data. The goal is not to delete but to make the data inaccessible to their target. Then they threaten to leak this information and in exchange for it, they demand payment of a ransom.

B. Impact

Around 1,700 ransomware attacks in the US between January 2020 and May 2023 were employed by Lockbit, making them US$91 million in ransom during that time.[1]

Some big and well-known companies were victims of LockBit's actions, such as Continental, Accenture, Boeing, and so on.

Their relentless pursuit of profit underscores the urgent need for robust cybersecurity measures to mitigate the threat posed by such malicious actors.

C. Attacks timeline

March 2021: F5 BIG-IP and BIG-IQ faced CVE-2021-22986, allowing unauthenticated remote code execution. Attackers could compromise systems via the iControl REST interface [3]. Mitigation included updates and access restrictions. Indicators of compromise: unusual processes and exposed interfaces.

October 2022: Pendragon PLC [4], a UK automotive retailer, faced a ransom demand of US$60 million. Despite the severity of the attack, Pendragon PLC stood resilient and refused to meet the demands.

December 2022, the LockBit hacker group orchestrated an attack targeting the Port of Lisbon Administration (APL) [5], the third-largest port in Portugal. The ransom demand amounted to US$1.5 million, with a deadline set for January 18, 2023. While the attack did not disrupt port operations, the ransomware group claimed responsibility and threatened to leak sensitive data stolen during the breach. LockBit alleges to have accessed financial reports, contracts, cargo information, and personal data of customers and port personnel. This incident underscores the growing threat of ransomware to critical infrastructure and the urgent need for heightened cybersecurity measures in such sectors.

January 2023: Royal Mail's international export services [6] suffered disruptions due to a ransomware attack, showcasing the widespread impact of cyber threats on essential services.

May 2023: Voyageurs du Monde [7] faced a data breach, with approximately 10,000 identity documents stolen, highlighting the ongoing risks of cyberattacks to businesses and data security.

III. TASKFORCE

Considering the importance and dominance of this ransomware group in the world of cybercrime, a task force of law enforcement has emerged. This task force is made up of agencies from 10 countries, which has been named Operation Cronos, in order to control the attacks carried out by this group.

This case against LockBit was opened at Eurojust in April 2022 at the request of the French authorities.

The countries and authorities involved in Operation Cronos are as follows: France, Germany, The Netherlands, Sweden, Australia, Canada, Japan, the United Kingdom, the United States, and Switzerland [9].

A. Attack to LockBit

This operation, Operation Cronos, lasted several months and resulted in the compromise of LockBit's main platform, as well as other critical infrastructures that enabled their attacks [10].

According to LockBit, this task force attack may have consisted of exploiting a software vulnerability (CVE-2023-3824). This is a critical PHP vulnerability that could lead to stack buffer overflow and potentially memory corruption or remote code execution. According to LockBit, the main servers have not been properly updated, so the vulnerability in question has not been fixed, even though a new version already exists. However, their backup servers were already up to date, so this seems to be the most likely cause.

Thus, 34 servers around the world were brought down. In addition, at the request of the French authorities, two LockBit members were arrested in Poland and Ukraine. There were also three international arrest warrants and five indictments issued by the French and US judicial authorities. The authorities have frozen more than 200 cryptocurrency accounts linked to the criminal organization. The UK's National Crime Agency has taken control of the technical infrastructure that allows all elements of the LockBit service to function, as well as their dark web leak site, where they previously stored data stolen from victims in ransomware attacks [8].

IV. CVE-2021-22986

In this section, we will analyze the CVE-2021-22986 vulnerability leveraged by Lockbit against Accenture in March 2021.

A. Affected Software: BIG-IP, BIG-IQ (F5)

F5 BIG-IP is a smart and flexible product suite that includes modules for traffic management, security, access, and optimization, providing a broad set of application services for ensuring reliable, secure, and fast delivery of applications. BIG-IQ Centralized Management, on the other hand, is a platform that provides a unified point of control for managing and automating BIG-IP devices and modules, enabling administrators to centrally manage security, policies, licensing, and more, thereby simplifying operations and increasing efficiency.[12]

BIG-IP Affected Versions:

- 16.0.x before 16.0.1.1,
- 15.1.x before 15.1.2.1,
- 14.1.x before 14.1.4,
- 13.1.x before 13.1.3.6,
- 12.1.x before 12.1.5.3

BIG-IQ Affected Versions:

- 7.1.0.x before 7.1.0.3,
- 7.0.0.x before 7.0.0.2 [13]

B. Vulnerability

This vulnerability allows for unauthenticated attackers with network access to the iControl REST interface, through the BIG-IP management interface and self-IP addresses, to execute arbitrary system commands, create or delete files, and disable services. This vulnerability can only be exploited through the control plane and cannot be exploited through the data plane. Exploitation can lead to complete system compromise. The BIG-IP system in Appliance mode is also vulnerable.[13]

An attack can exploit a pre-authentication server-side request forgery vulnerability in the iControl Rest API */mgmt/shared/authn/login* endpoint to generate an X-F5-Auth-Token that allows for remote code execution without authentication.[14]

Assumptions: Attacker has network access

C. Severity

Base Score: 9.8 Critical

Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

- **Attack Vector (AV):** Network
- **Attack Complexity (AC):** Low
- **Priviledges Required (PR):** None
- **User Interaction (UI):** None
- **Scope (S):** Unchanged
- **Confidentiality (C):** High
- **Integrity (I):** High
- **Availability (A):** High

Impact Score: 5.9

metasploitability Score: 3.9

Weakness Enumeration: CWE-918: Server-Side Request Forgery (SSRF) [11]

D. Mitigation

Fixes: Apply Software Updates

1) Block iControl REST access through the self IP address: All access to the iControl REST Interface of a BIG-IP system can be blocked through the use of self-IP addresses. Just set 'Port Lockdown' to 'Allow None' for each self-IP. [13]

E. Technical Assessment

The exploitation of this vulnerability, CVE-2021-22986, necessitates a two-step process. Initially, the SSRF vulnerability is leveraged to bypass authentication and obtain an authenticated session token. This session can then be utilized to interact with REST API endpoints that would typically require authentication.

The *tm/util/bash* endpoint is particularly beneficial for an attacker as it permits an authenticated user to execute commands on the underlying server with root privileges. [15]

To evaluate the success of our attack, we can use some indicators of compromise that are available in BIG-IP software.

F. Indicators of Compromise

1) F5 iHealth indicator flags of compromise in uploaded QKView diagnostic files: F5's iHealth diagnostic tool includes heuristics designed to identify potential indicators of compromise in the QKView diagnostic files that users upload. Thus allowing for early detection and mitigation of any potential threats related to this vulnerability.

F5 has iHealth heuristics designed to detect the following:

- Unknown processes running (Heuristic H511618)
- When the Configuration utility iControl REST interface has been exposed to the Internet through the management interface (H444724)
- When a self IP address has Port Lockdown set to Allow All (H458565) [13]

2) Manual Checking of Compromise: Look for X-F5-Auth-Token doesn't have value in */var/log/restjavad.*.log*.

Note: Under limited ordinary circumstances, log entries containing the text X-F5-Auth-Token that don't have a value may appear in */var/log/restjavad.*.log*.

When you see the **X-F5-Auth-Token doesn't have value** message, you can compare any logs found in */var/log/restjavad.*.log* with those found in */var/log/audit* and */var/log/restjavad-audit.*.log* that share approximately the same timestamp.

Use this comparison to determine the intent and potential impact of these logs.

If the logs display any entries, this may indicate that a REST request with an empty **X-F5-Auth-Token** value from IP address **nnn.nnn.nnn.nnn** invokes command **run util bash -c id**. You must closely examine the source IP addresses in any */var/log/restjavad-audit.*.log* and */var/log/audit** entries and compare them to IP addresses you know make legitimate REST calls against the device.

Other indicators of compromise may include unexpected modifications to any files, configurations, or running processes. [13][15]

V. Exploit Replication

In this section, we describe the steps taken to reproduce and exploit the CVE-2021-22986 vulnerability in a practical demo.

A. Set up

To set up the BIG-IP software, we first needed a license. We created an F5 account and used the 30-day free trial that they provide. We downloaded the VMWare [16] image of the software's version 15.1.1. We then started a virtual machine using the VMWare hypervisor, followed by the license activation using the TMOS shell (tmsh).

Then, we set up the root/admin user authentication, with a strong password. This user and password are used both for authenticating access to the system's shell, through the Virtual Machine or SSH, and for logging in to the Web dashboard GUI.

Lastly, it was necessary to set up the system's IP address and the bridge to the host machine. We used the bridge architecture provided by VMWare and the VMnet0 bridge with subnet 172.16.1.0. The BIG-IP system itself has the 172.16.1.245 IP address.

B. Exploit

To exploit this vulnerability, the script by Al1ex@Heptagram [17] was used.

It works by sending requests to the target management server to the endpoints mentioned in the previous section. These requests are sent with empty strings as the cookies and X-F5-Auth-Tokens and the user as admin, as can be seen in the code block below. Note that no password is provided. The management server, if the vulnerability is present, returns a new valid X-F5-Auth-Token in the response. We can then use this token to bypass authentication in the Web-GUI or to execute code remotely on the server through requests to the *tm/util/bash* endpoint as the admin user.

(Headers and Data for the login endpoint)

```
headers = {
   "User-Agent": "hello-world",
   "Content-Type":"application/x-www-form-urlencoded"
}
data = {
   "bigipAuthCookie":"",
   "username":"admin",
   "loginReference":{"link":"/shared/gossip"},
   "userReference":{
      "link":
      "https://localhost/mgmt/shared/authz/users/admin"
   }
}
```

(Headers and Data for the bash endpoint)

```
header_2 = {
   'User-Agent': 'hello-world',
   'Content-Type': 'application/json',
   'X-F5-Auth-Token': '',
   'Authorization': 'Basic YWRtaW46QVNhc1M='
}
data_2 = {
   "command": "run",
   "utilCmdArgs": "-c whoami"
}
```

A real attack would seek to disrupt operations or obtain sensitive information on the network or from the machines on it. In our case, since the objective is only to simulate an attack, we added a flag.txt file to the iFile module [18] of the system. This system handles file uploading and access in the network.

Upon running the script, we obtained an X-F5-Auth-Token, which we then used to make several requests to

the *tm/util/bash* endpoint, sending the desired command in the requests body. We started with the *whoami* command and verified that we were logged in as the admin user. This user has root privileges. We then accessed the flag.txt's contents with the following command: *cat /config/filestore/-files_d/Common_d/ifile_d/:Common:flag.txt_65986_1*.

C. Indicators of Compromise

Now that our attack is complete, we took the role of a cybersecurity analyst to assess whether our management server had been compromised.

In a previous section, we mentioned two ways to check compromise, a manual option and the F5 iHealth module. Our version of the software did not have the F5 iHealth module included, so we opted for the manual option.

We started by checking the */var/log/audit* log. This shows the commands executed on the server. There we found suspicious commands executed by the admin user such as *whoami, pwd* and *cat* of the flag.txt file. We then checked the */var/logs/restjavad-audit.0.log* log, where the calls to the server's endpoints are logged. Here we found several instances where a *null* user called the login endpoint and got a *"status":200* response. Immediately following that, the admin user sent requests to the bash endpoint. Both of these requests were sent from the same IP address. Suspicious entries of both logs can be found below. This shows that a non-authenticated user managed to get access to the admin user, confirming the management server's compromise.

(/var/log/audit suspicious entries)

```
AUDIT - PID=11363 user=admin folder=/Common
    module=(tmos)# status=[Command OK]
    cmd_data=run util bash -c whoami
AUDIT - PID=11363 user=admin folder=/Common
    module=(tmos)# status=[Command OK]
    cmd_data=run util bash -c pwd
AUDIT - PID=11363 user=admin folder=/Common
    module=(tmos)# status=[Command OK]
    cmd_data=run util bash -c "cat
    /config/config/filestore/files_d/Common_d
    /ifile_d/:Common_d:flag.txt_65986_1"
```

(/var/logs/restjavad-audit.0.log suspicious entries)

```
{
   "user":"local/null",
   "method":"POST",
   "uri":"http://localhost:8100/mgmt
       /shared/authn/login",
   "status":200,
   "from":"172.16.1.1"
},{
   "user":"admin",
   "method":"POST",
   "uri":"http://localhost:8100/mgmt
       /tm/util/bash",
   "status":200,
   "from":"172.16.1.1"
}
```

REFERENCES

[1] Wikipedia, 2024, *LockBit*, Retrieved March 04, 2024 from https://en.wikipedia.org/wiki/Lockbit

[2] Kaspersky, 2024, *Ransomware LockBit — O que você precisa saber*, Retrieved March 04, 2024 from https://www.kaspersky.com.br/resource-center/threats/lockbit-ransomware

[3] F5, 2024, *Demystifying IControl REST API*, Retrieved March 04, 2024 from https://clouddocs.f5.com/api/icontrol-rest/

[4] Pendragon PLC, *Pendragon PLC Business*, 2022, Retrieved March 02, 2024 from https://www.pendragonplc.com/about-us/our-business/

[5] APL, *Port of Lisbon Administratio*, 2022, Retrieved March 10, 2024 from https://www.portodelisboa.pt

[6] Royal Mail, *Royal Mail's international export services business*, 2024, Retrieved March 05, 2024 from https://www.royalmail.com/business

[7] Voyageurs du Mond, *Voyageurs du Monde*, 2024, Retrieved March 04, 2024 from https://www.voyageursdumonde.fr/voyage-sur-mesure

[8] InfoSecurity Magazine, 2024, *LockBit Ransomware Takedown: What You Need to Know about Operation Cronos*, Retrieved March 06, 2024 from https://www.infosecurity-magazine.com/news/operation-cronos-lockbit-takedown/

[9] Europol, 2024, *law-enforcement-disrupt-worlds-biggest-ransomware-operation*, Retrieved March 06, 2024 from https://www.europol.europa.eu/media-press/newsroom/news/law-enforcement-disrupt-worlds-biggest-ransomware-operation

[10] World Economic Forum, 2024, *LockBit: How an international operation seized control of the 'world's most harmful cybercrime group'*, Retrieved March 10, 2024 from https://www.weforum.org/agenda/2024/02/lockbit-ransomware-operation-cronos-cybercrime/

[11] NIST, 2021, *CVE-2021-22986 Detail*, Retrieved March 09, 2024 from https://nvd.nist.gov/vuln/detail/CVE-2021-22986

[12] F5, 2021, *F5: BIG-IP Application Delivery Services*, Retrieved March 09, 2024 from https://www.f5.com/products/big-ip-services

[13] F5, 2021, *K03009991: iControl REST unauthenticated remote command execution vulnerability CVE-2021-22986*, Retrieved March 09, 2024 from https://my.f5.com/manage/s/article/K03009991

[14] wvu, Rich Warren, 2021, *F5 iControl Server-Side Request Forgery / Remote Command Execution*, Retrieved March 09, 2024 from https://packetstormsecurity.com/files/162059/F5-iControl-Server-Side-Request-Forgery-Remote-Command-Execution.html

[15] RIFT: Research and Intelligence Fusion Team, 2021, *RIFT: Detection capabilities for recent F5 BIG-IP/BIG-IQ iControl REST API vulnerabilities CVE-2021-22986*, Retrieved March 09, 2024 from https://research.nccgroup.com/2021/03/18/rift-detection-capabilities-for-recent-f5-big-ip-big-iq-icontrol-rest-api-vulnerabilities-cv

[16] Inc. VMware Workstation Pro, 2007, *VMware* Retrieved May 15, 2024 from https://www.vmware.com/products/workstation-pro.html

[17] Al1ex@Heptagram, 2021, *CVE-2021-22986 Github repository* Retrieved May 15, 2024 from https://github.com/Al1ex/CVE-2021-22986

[18] iFile, 2024, *iFile F5* Retrieved May 10, 2024 from https://clouddocs.f5.com/api/irules/ifile.html