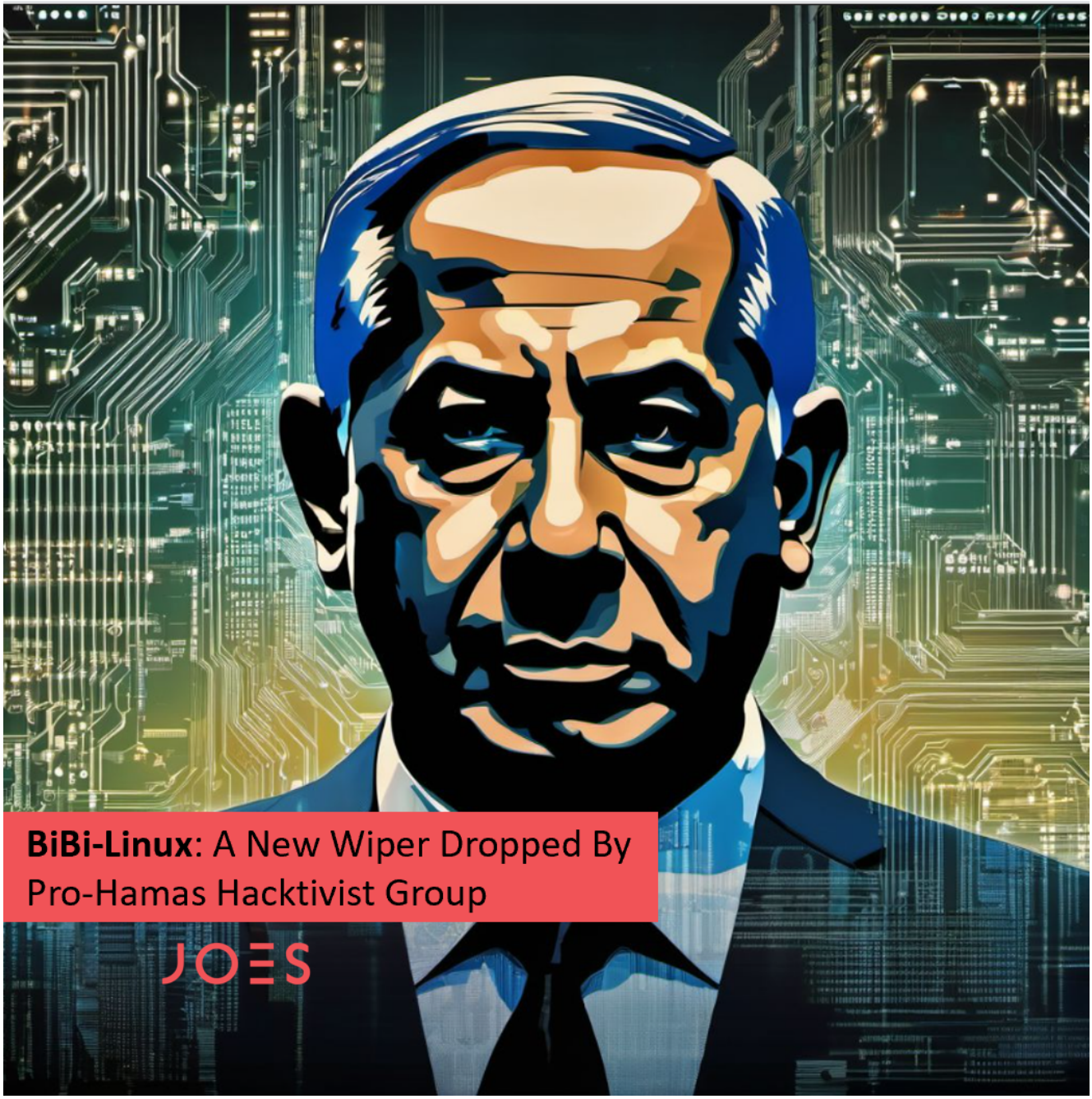
# BiBi-Linux: A New Wiper Dropped By Pro-Hamas Hacktivist Group

securityjoes.com/post/bibi-linux-a-new-wiper-dropped-by-pro-hamas-hacktivist-group

Security Joes October 30, 2023

- Security Joes
-
-
    - Oct 30
    -
    - 5 min read




Security Joes Incident Response team volunteered to assist Israeli companies during the times of war between the state of Israel and the terrorist organization Hamas. During the forensics investigation, we found what appears to be a new Linux Wiper malware we track as **BiBi-Linux Wiper.**

This malware is an x64 ELF executable, lacking obfuscation or protective measures. It allows attackers to specify target folders and can potentially destroy an entire operating system if run with root permissions. During execution, it produces extensive output, which can be mitigated

using the "nohup" command. It also leverages multiple threads and a queue to corrupt files concurrently, enhancing its speed and reach. Its actions include overwriting files, renaming them with a random string containing "BiBi," and excluding certain file types from corruption.

The article in a nutshell:

```
1. Security Joes Incident Response team voluntarily conducted a forensic investigation
within victim networks Israeli companies
2. Hamas affiliated hacktivist group broke into Israeli companies and deployed a new
cyberweapon to destroy their infrastructure
3. Notably, they decided to hardcode the name of Israeli PM in the malware name and in
every destroyed file's extension
4. The attack had no ransom note or C2 servers which increased our confidence that the
malware tracked as BiBi-Linux is indeed a Wiper aimed for data destruction
```

Security Joes is a multi-layered incident response company strategically located in nine different time-zones worldwide, providing a follow-the-sun MDR & IR coverage to respond to any incident remotely.

Contact us at response@securityjoes.com for more information about our services and technologies and get additional recommendations to protect yourself against this kind of attack vector.

---

## Warzone Cyberweapon

During these times of conflict between Israel & Hamas, our team voluntarily decided to respond to incidents affecting Israeli companies. In the course of our investigations, we encountered a highly specific malware sample that is currently targeting companies across the nation. Unlike the typical global distribution of malware, where financial gain is the common motivation, our analysis of these attacks revealed a different motive. In this case, they are not driven by monetary objectives but are deeply rooted in the political ideologies associated with the ongoing war. This leads us to believe that the specific artifacts discovered may have been created by a group of hackers affiliated with Hamas, with the intent to sow chaos amidst the backdrop of the war.

This new threat does not establish communication with remote Command & Control (C2) servers for data exfiltration, employ reversible encryption algorithms, or leave ransom notes as a means to coerce victims into making payments. Instead, it conducts file corruption by overwriting files with useless data, damaging both the data and the operating system. This category of destructive software is commonly referred to as a "Wiper" and is not a recent phenomenon.

Reports of this type of malware have been documented targeting devices in previous years, affecting both Windows and Linux systems. Historically, such threats are typically associated with complex political situations worldwide, with one notable example being the recent conflict between Ukraine and Russia.

What particularly caught our attention was the fact that the analyzed binary had never been documented before. As of the writing of this report, it has only received two detections on VirusTotal. This indicates that the malware is relatively new and not widely distributed yet, see Figure 1.

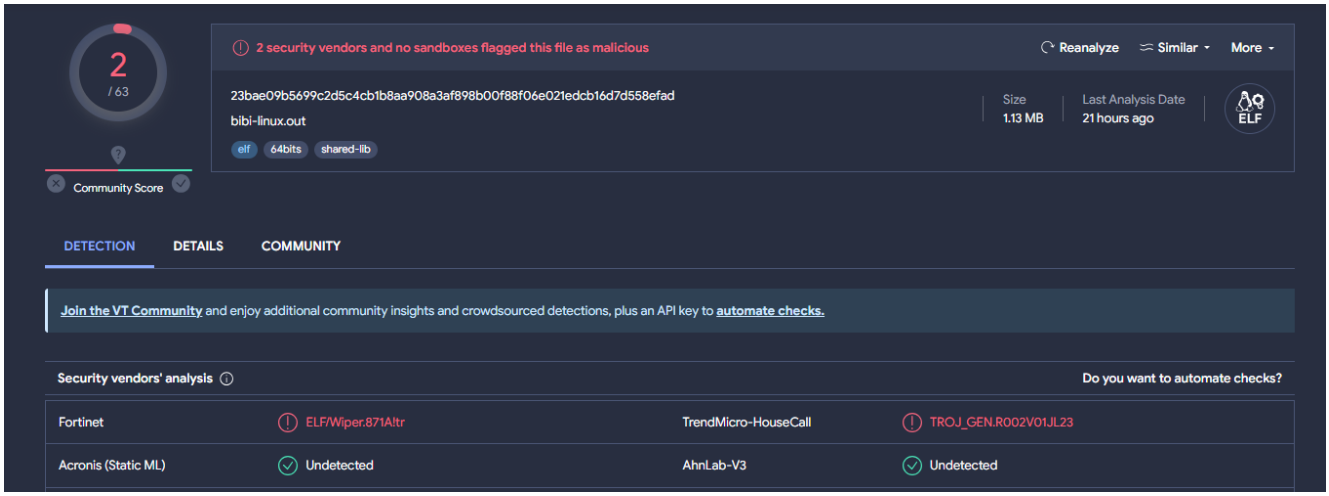


Figure 1. VirusTotal report of the malicious file discovered during an IR investigation attended by Security Joes.

The malicious file discovered on each of the compromised machines was named **bibi-linux.out**. While the string "bibi" (in the filename), may appear random, it holds significant meaning when mixed with topics such as politics in the Middle East, as it is a common nickname used for the Israeli Prime Minister, Benjamin Netanyahu.

The relevance of this particular string became even more apparent when we delved into the inner workings of the malware. Within its structure, we identified this string hardcoded, and it was also employed during the execution of the malware to generate file extensions that identifies the corrupted files.

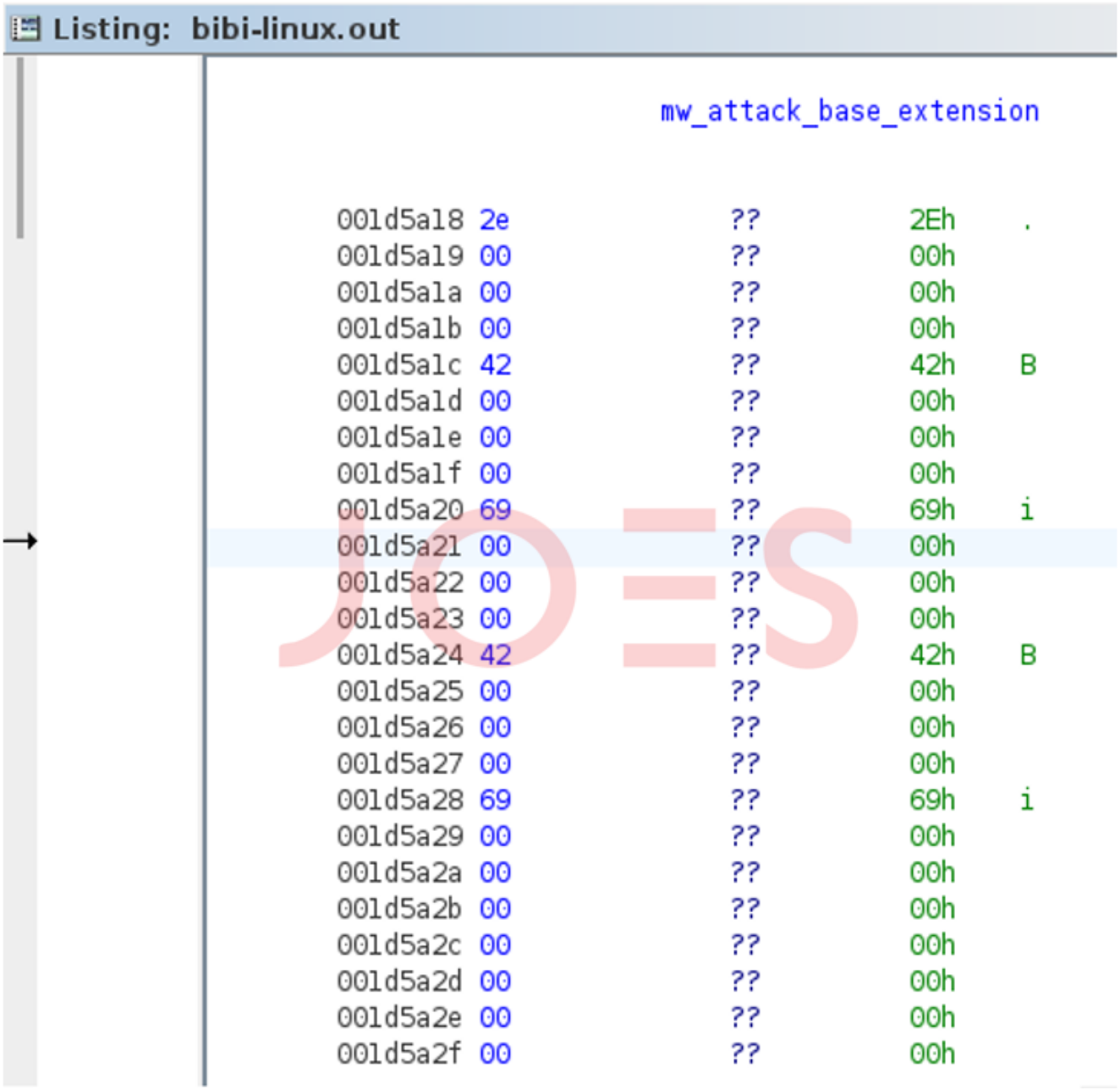



Figure 2. Hardcoded "BiBi" string within the Wiper sample used for damaged files' extension

As mentioned earlier, Wipers are typically associated with politically motivated activists who are not seeking financial gain from their attacks but aim to inflict damage on their adversaries. This case is no exception. Here, we are dealing with an artifact that has no intention of providing victims with any means of file recovery. Instead, its primary objective is to corrupt as many files as swiftly as possible. To achieve this goal, the attackers employed a multi-threaded approach to expedite their operations.

## Dissecting the new BiBi-Linux Wiper

The malware sample is an x64 ELF executable, coded in C/C++, with a file size of approximately 1.2MB. This binary was compiled using the GCC compiler. Notably, the binary lacks obfuscation, packing, or any protective measures, and it contains several strings that could provide valuable information to analysts right from the beginning of the static analysis (see Figure 3).

In terms of customization, this binary offers limited options. It only allows the threat actor to specify target folders via command-line parameters. In cases where the attacker does not provide any path, the attack will target the root directory "/", resulting in the destruction of not only files but also the entire operating system. However, to carry out this destructive action on the OS, the attacker would require root permissions.

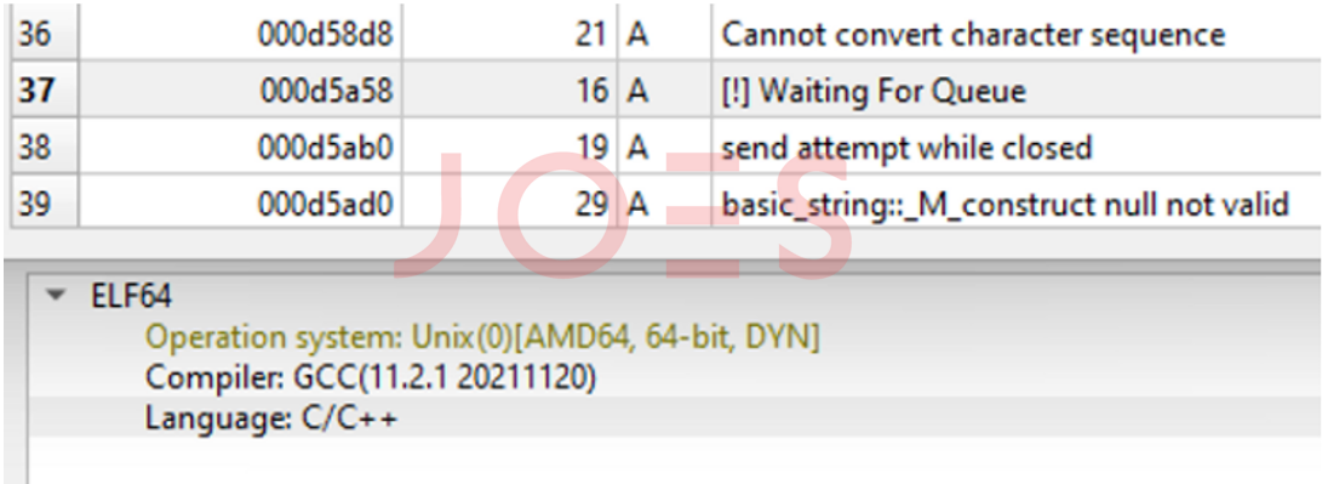



Figure 3. Strings and Compiler information found during the static analysis of the malicious artifact.

Once executed, the file exhibits a high level of verbosity, continuously printing numerous execution details to the standard output (stdout). These details include information about the targeted path, available processor cores, threads, and the progress of the wiping process. This extensive output to stdout creates a significant amount of noise during execution.

To mitigate this issue, threat actors employ the nohup command when running this tool in targeted environments. By doing so, the program can execute without continuously printing output to the terminal. Instead, the program's output is redirected to a file named **nohup.out** located in the same directory where the malicious binary was executed. Additionally, using "nohup" prevents the wiping process from halting even if the console is closed.

```
analyst@ubuntu:~$ '/home/analyst/bibi-linux.out' '/home/analyst/target/'
[+] Path: /home/analyst/target/
[+] CPU cores: 2, Threads: 6
[+] Round 0
[+] Stats: 1 | 0
[+] Round 1
[+] Stats: 2 | 0
```

Figure 4. Example of the information printed in the terminal by BiBi Wiper during its execution.
To expedite the infection process, this threat leverages multiple threads and employs a queue to synchronize their operations. This approach allows the attack to concurrently corrupt files, significantly enhancing the overall attack's reach and speed. Evidence of this can also be found within the sample's strings and the syscalls used by the application (see Figure 5). During the code analysis, we identified several Linux syscalls, including *sched_setscheduler*, *sched_getaffinity*, *sched_yield*, *set_robust_list*, *futex* and *set_tid_address*. Collectively, they offer a comprehensive set of tools for controlling the behavior of threads and processes within a Linux application.

```
001ce5ac 48 8d 54        LEA         RDX=>local_cc,[RSP + 0x5c]
         24 5c
001ce5b1 b8 90 00        MOV         EAX,0x90
         00 00
                     sched_setscheduler
001ce5b6 0f 05           SYSCALL
001ce5b8 49 89 c0        MOV         R8,RAX
001ce5bb 41 89 c4        MOV         R12D,EAX
001ce5be 49 8d 7f f0     LEA         RDI,[R15 + -0x10]
001ce5c2 f7 d8           NEG         EAX
001ce5c4 19 c0           SBB         EAX,EAX
001ce5c6 83 e0 03        AND         EAX,0x3
001ce5c9 41 87 47 f0     XCHG        dword ptr [R15 + -0x10],EAX
001ce5cd 83 f8 02        CMP         EAX,0x2
001ce5d0 75 23           JNZ         LAB_001ce5f5
001ce5d2 41 b9 ca        MOV         R9D,0xca
         00 00 00
001ce5d8 ba 01 00        MOV         EDX,0x1
         00 00
001ce5dd be 81 00        MOV         ESI,0x81
         00 00
001ce5e2 4c 89 c8        MOV         RAX,R9
                     futex
001ce5e5 0f 05           SYSCALL
001ce5e7 48 83 f8 da     CMP         RAX,-0x26
001ce5eb 75 08           JNZ         LAB_001ce5f5
001ce5ed 4c 89 c8        MOV         RAX,R9
001ce5f0 48 89 d6        MOV         RSI,RDX
```

Figure 5. Snippet of code containing syscalls "sched_setscheduler" and "futex"
Once initiated, the attack follows a relatively straightforward logic as a multi-threaded Wiper, characterized by the following actions:

- **File Bricking**: The malware's primary objective is to render files unusable, achieving this by overwriting their contents. Instead of encrypting data, it replaces all the contents of affected files with a buffer of random data of the same length as the targeted file.

- **File Renaming**: In addition to file corruption, the malware renames affected files with a random string, **appending an extension that includes the substring "BiBi"** An infected file follows the structure:

```
[RANDOM_NAME].BiBi[NUMBER]
```

**File Type Exclusions**: Notably, the malware refrains from altering files with the extensions .out or .so. This is because the threat relies on files such as **bibi-linux.out** and **nohup.out** for its operation, along with shared libraries essential to the Unix/Linux OS (.so files).


Figure 5. Example of corrupted files after a BiBi Wiper infection.

## IOCs

For the time being, we will release only the investigated Wiper sample.

| Filename | Size | SHA256 |
|---|---|---|
| bibi-linux.out | 1.2MB | 23bae09b5699c2d5c4cb1b8aa908a3af898b00f88f06e021edcb16d7d558efad |

## Yara Rule

```
rule BiBi_Linux_Wiper {
        meta:
                author ="Felipe Duarte, Security Joes"
                description ="Detects BiBi-Linux Wiper"
                sha256_reference
="23bae09b5699c2d5c4cb1b8aa908a3af898b00f88f06e021edcb16d7d558efad"

    strings:
                $str1 = "[+] Stats: "
                $str2 = { 2e 00 00 00 42 00 00 00 69 00 00 00 42 00 00 00 69 00 }
                $str3 = "[!] Waiting For Queue "
                $str4 = "[+] Round "
                $str5 = "[+] Path: "
                $str6 = "[+] CPU cores: "
                $str7 = "Threads: "

        condition:
                all of them
}
```

## TTPs

The following is the list of TTPs according to MITRE:

| Tactic | Technique | Description |
|---|---|---|
| Initial Access | Exploit Public-Facing Application | Adversaries exploited a weakness in an Internet-facing host to initially access a network. |
| Execution | Command and Scripting Interpreter: Unix Shell | Command nohup is used to launch the attack within the victim's environment. |
| Lateral Movement | Software Deployment Tools | Server administration tools were used to deploy the threat in several servers. |
| Discovery | File and Directory Discovery | Threat scans the system looking for files and folders to infect. |
| Discovery | System Information Discovery | Threat get information from the system such as the number of cores and local times. |
| Impact | Data Destruction | Files' content is replaced with useless data. |