

Project Plan

Step 1: Phishing

For this step to be functional, the victim would have to download the malicious software that will encrypt their files through a phishing method via job post and the user will enter their information.

Thank you for your application! We look forward to working with you!

About Us

At Tech Tonic, we're looking for driven people who can sustain our high standards of quality while creating practical solutions to challenging problems.

Feel free to contact us

- Address: N. Elm Street, Denton, TX 76207
- Phone: (123)456-7893
- Email: TechTonic@geek.com

Please provide your information below

Name:

Email:

Phone number:

Address:

The user will then receive an email that will cause them to open to a new portal

Tech Tonic

Dear applicant,

Thank you so much for your application. You have been selected for the role that you have applied for.

Please click on the link attached: <https://tinyurl.com/ycl38n8r>

```
(venv)root@attckergroup1: jjob_portal

root@attckergroup1:~#
root@attckergroup1:~# apt install python3 python3-pip python3-venv -y
python3 is already the newest version (3.13.1-2).
python3 set to manually installed.
python3-venv is already the newest version (3.13.1-2).
python3-venv set to manually installed.
The following packages were automatically installed and are no longer required:
  libpython3.12-dev python3.12-dev python3.12-venv
python3.12 python3.12-minimal
Use 'apt autoremove' to remove them.

Upgrading:
  python3-pip python3-pip-whl

Summary:
Upgrading: 2, Installing: 0, Removing: 0, Not Upgrading: 1546
Download size: 2,977 kB
Space needed: 157 kB / 63.2 GB available

Get:1 http://http.kali.org/kali kali-rolling/main amd64 python3-pip all 25.0.1+dfsg-1 [1,455 kB]
Get:2 http://http.kali.org/kali kali-rolling/main amd64 python3-pip-whl all 25.0.1+dfsg-1 [1,522 kB]
Fetched 2,977 kB in 1s (2,757 kB/s)
(Reading database ... 401900 files and directories currently installed.)
Preparing to unpack .../python3-pip-25.0.1+dfsg-1_all.deb ...
Unpacking python3-pip (25.0.1+dfsg-1) over (24.3.1+dfsg-1) ...
Preparing to unpack .../python3-pip-whl_25.0.1+dfsg-1_all.deb ...
Unpacking python3-pip-whl (25.0.1+dfsg-1) over (24.3.1+dfsg-1) ...
Setting up python3-pip-whl (25.0.1+dfsg-1) ...
Setting up python3-pip (25.0.1+dfsg-1) ...
Processing triggers for man-db (2.13.0-1) ...
Processing triggers for kali-menu (2024.4.0) ...

root@attckergroup1:~#
root@attckergroup1:~# mkdir /job_portal
root@attckergroup1:~# cd /job_portal
root@attckergroup1:/job_portal#
root@attckergroup1:/job_portal# python3 -m venv venv
root@attckergroup1:/job_portal#
root@attckergroup1:/job_portal# source venv/bin/activate
(venv)root@attckergroup1:/job_portal#
(venv)root@attckergroup1:/job_portal# pip install flask
Collecting flask
  Downloading flask-3.1.0-py3-none-any.whl.metadata (2.7 kB)
Collecting Werkzeug >= 3.1 (from flask)
  Downloading werkzeug-3.1.3-py3-none-any.whl.metadata (3.7 kB)
```

Kaylyn King, Tasmania Tamboli, Jean-Charles Hekamanu, Ujjwal Rana Magar

CSCE 5550

Spring 2025

```
(root@attckergroup1)-[~/ransomware-project]
# pyinstaller --onefile encryptor.py --name payload.exe
21 DEPRECATION: Running PyInstaller as root is not necessary nor sensible. Do not use PyInstaller with sudo. PyInstaller 7.0 will block this.
2351 INFO: PyInstaller: 6.11.0, contrib hooks: 2024.9
2351 INFO: Python: 3.13.2
2356 INFO: Platform: Linux-6.11.2-amd64-x86_64-with-glibc2.40
2356 INFO: Python environment: /usr
2358 INFO: wrote /root/ransomware-project/payload.exe.spec
2387 INFO: UPX is available but is disabled on non-Windows due to known compatibility problems.
2389 INFO: Module search paths (PYTHONPATH):
['/usr/lib/python313.zip',
 '/usr/lib/python3.13',
 '/usr/lib/python3.13/lib-dynload',
 '/usr/local/lib/python3.13/dist-packages',
 '/usr/lib/python3/dist-packages',
 '/usr/lib/python3.13/dist-packages',
 '/usr/lib/python3/dist-packages/setuputils/_vendor',
 '/root/ransomware-project']
pygame 2.6.0 (SDL 2.30.9, Python 3.13.2)
Hello from the pygame community. https://www.pygame.org/contribute.html
3419 INFO: checking Analysis
3419 INFO: Building Analysis because Analysis-00.toc is non existent
3419 INFO: Running Analysis Analysis-00.toc
3420 INFO: Target bytecode optimization level: 0
3420 INFO: Initializing module dependency graph...
3420 INFO: Initializing module graph hook caches...
3447 INFO: Analyzing base_library.zip ...
4297 INFO: Processing standard module hook 'hook-heapq.py' from '/usr/lib/python3/dist-packages/PyInstaller/hooks'
4376 INFO: Processing standard module hook 'hook-encodings.py' from '/usr/lib/python3/dist-packages/PyInstaller/hooks'
5903 INFO: Processing standard module hook 'hook-pickle.py' from '/usr/lib/python3/dist-packages/PyInstaller/hooks'
6973 INFO: Caching module dependency graph...
7048 INFO: Looking for Python shared library...
7080 INFO: Using Python shared library: /lib/x86_64-linux-gnu/libpython3.13.so.1.0
7080 INFO: Analyzing /root/ransomware-project/encryptor.py
7088 INFO: Processing module hooks (post-graph stage)...
7092 INFO: Performing binary vs. data reclassification (2 entries)
7129 INFO: Looking for ctypes DLLs
7132 INFO: Analyzing run-time hooks ...
7133 INFO: Including run-time hook 'pyi_rth_inspect.py' from '/usr/lib/python3/dist-packages/PyInstaller/hooks/rthooks'
7137 INFO: Looking for dynamic libraries
7424 INFO: Warnings written to /root/ransomware-project/build/payload.exe/warn-payload.exe.txt
7429 INFO: Graph cross-reference written to /root/ransomware-project/build/payload.exe/xref-payload.exe.html
7437 INFO: checking PYZ
7437 INFO: Building PYZ because PYZ-00.toc is non existent
7437 INFO: Building PYZ (ZlibArchive) /root/ransomware-project/build/payload.exe/PYZ-00.pyz
7577 INFO: Building PYZ (ZlibArchive) /root/ransomware-project/build/payload.exe/PYZ-00.pyz completed successfully.
7592 INFO: checking PKG
7592 INFO: Building PKG because PKG-00.toc is non existent
7592 INFO: Building PKG (CArchive) payload.exe.pkg
9869 INFO: Building PKG (CArchive) payload.exe.pkg completed successfully.
9870 INFO: Bootloader /usr/lib/python3/dist-packages/PyInstaller/bootloader/Linux-64bit-intel/run
9870 INFO: checking EXE
9870 INFO: Building EXE because EXE-00.toc is non existent
9870 INFO: Building EXE from EXE-00.toc
```

```
(root@attckergroup1)-[~/ransomware-project]
# cd dist

(root@attckergroup1)-[~/ransomware-project/dist]
# ll
total 7748
-rwxr-xr-x 1 root root 7933544 Mar 31 23:48 payload.exe

(root@attckergroup1)-[~/ransomware-project/dist]
#

(root@attckergroup1)-[~/ransomware-project/dist]
# cp payload.exe /var/www/html/job_portal

(root@attckergroup1)-[~/ransomware-project/dist]
#

(root@attckergroup1)-[~/ransomware-project/dist]
#

(root@attckergroup1)-[~/ransomware-project/dist]
# cd /var/www/html/job_portal

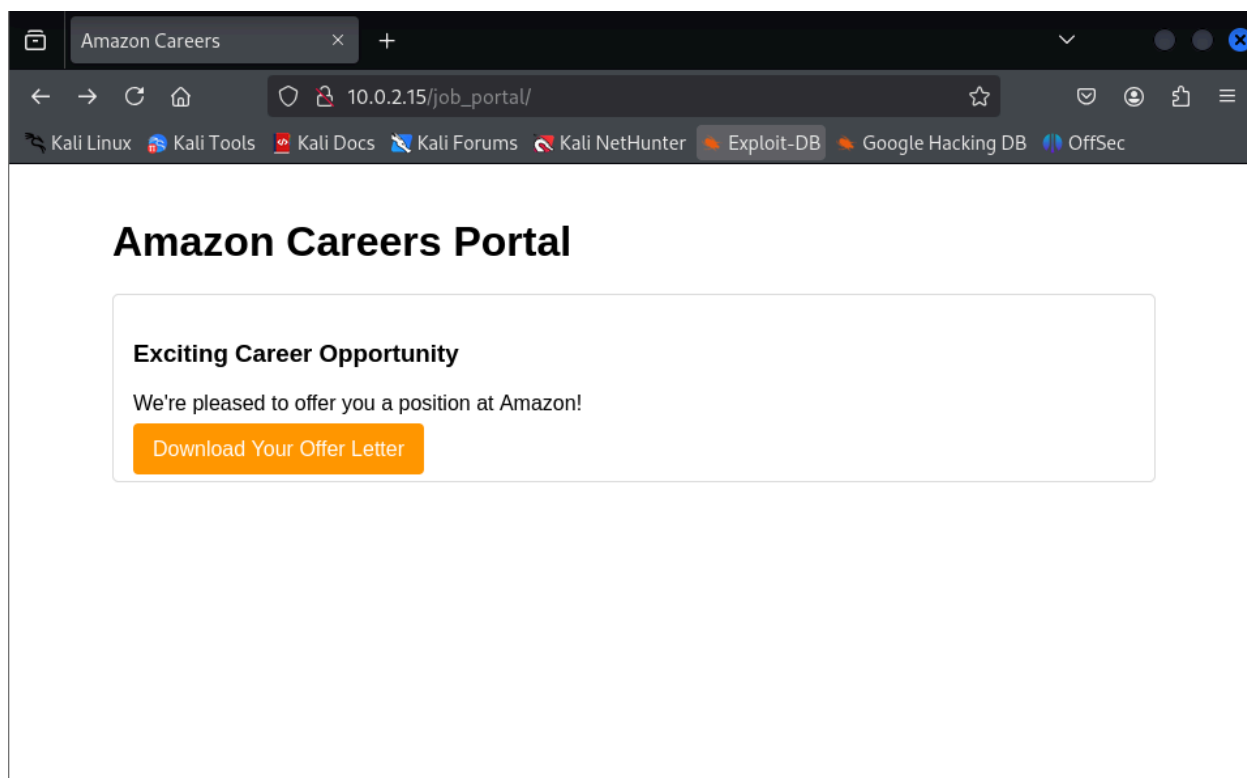
(root@attckergroup1)-[/var/www/html/job_portal]
# ll
total 7752
-rw-r--r-- 1 root root 706 Mar 31 23:37 index.html
-rwxr-xr-x 1 root root 7933544 Mar 31 23:49 payload.exe

(root@attckergroup1)-[/var/www/html/job_portal]
#
```

```
(root@attckergroup1)-[/job_portal]
# python3 app.py
* Serving Flask app 'app'
* Debug mode: off
WARNING: This is a development server. Do not use it in a production deployment. Use a production WSGI server instead.
* Running on http://10.0.2.15:80
Press CTRL+C to quit
```

Step 2: Download

After the user inputs their information in the job portal, the user will receive an email. They will be required to download an executable that will inject the malicious software.



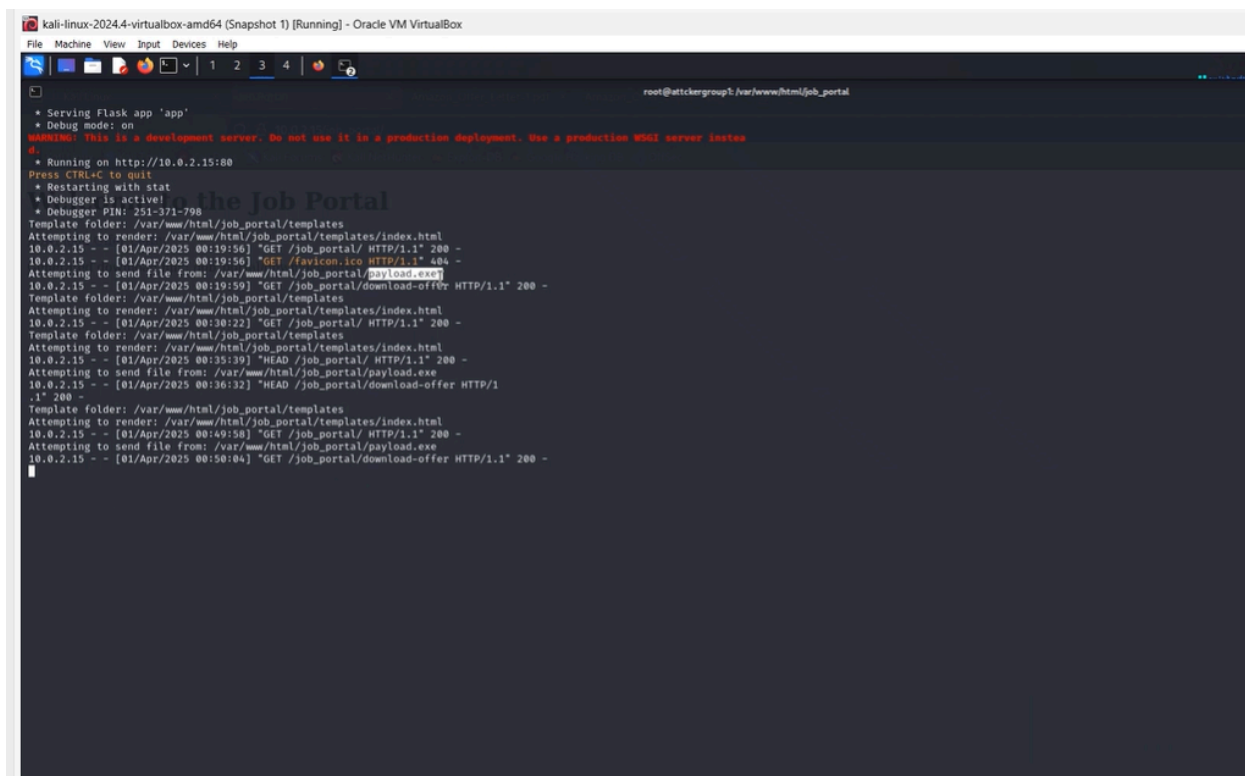
Step 3: Injection

Once the victim downloads the prompted executable file, the malware activates, and the files within the user's system are encrypted.

Step 4: Ransomware:

When the files are encrypted A ransom demand will be generated which the victim needs to meet to regain access

Kaylyn King, Tasmania Tamboli, Jean-Charles Hekamanu, Ujjwal Rana Magar
CSCE 5550
Spring 2025



The screenshot shows a Kali Linux virtual machine window titled "kali-linux-2024.4-virtualbox-amd64 (Snapshot 1) [Running] - Oracle VM VirtualBox". The terminal window displays the following output:

```
root@stickergroup: /var/www/html/job_portal

* Serving Flask app 'app'
* Debug mode: on
Warning: This is a development server. Do not use it in a production deployment. Use a production WSGI server instead.
* Running on http://10.0.2.15:80
Press CTRL+C to quit
* Restarting with stat
* Debugger is active!
* Debugger PIN: 251-371-798

the Job Portal
Template folder: /var/www/html/job_portal/templates
Attempting to render: /var/www/html/job_portal/templates/index.html
10.0.2.15 - - [01/Apr/2025 00:19:56] "GET /job_portal/ HTTP/1.1" 200 -
10.0.2.15 - - [01/Apr/2025 00:19:56] "GET /favicon.ico HTTP/1.1" 404 -
Attempting to send file from: /var/www/html/job_portal/payload.exe
10.0.2.15 - - [01/Apr/2025 00:19:59] "GET /job_portal/download-offer HTTP/1.1" 200 -
Template folder: /var/www/html/job_portal/templates
Attempting to render: /var/www/html/job_portal/templates/index.html
10.0.2.15 - - [01/Apr/2025 00:30:22] "GET /job_portal/ HTTP/1.1" 200 -
Template folder: /var/www/html/job_portal/templates
Attempting to render: /var/www/html/job_portal/templates/index.html
10.0.2.15 - - [01/Apr/2025 00:35:30] "HEAD /job_portal/ HTTP/1.1" 200 -
Attempting to send file from: /var/www/html/job_portal/payload.exe
10.0.2.15 - - [01/Apr/2025 00:36:32] "HEAD /job_portal/download-offer HTTP/1.1" 200 -
Template folder: /var/www/html/job_portal/templates
Attempting to render: /var/www/html/job_portal/templates/index.html
10.0.2.15 - - [01/Apr/2025 00:49:58] "GET /job_portal/ HTTP/1.1" 200 -
Attempting to send file from: /var/www/html/job_portal/payload.exe
10.0.2.15 - - [01/Apr/2025 00:50:04] "GET /job_portal/download-offer HTTP/1.1" 200 -
```

Step 5: Decryption

Once the demands have been met, the victim will be sent a README file and within that file, they will be given a key to decrypt the files.