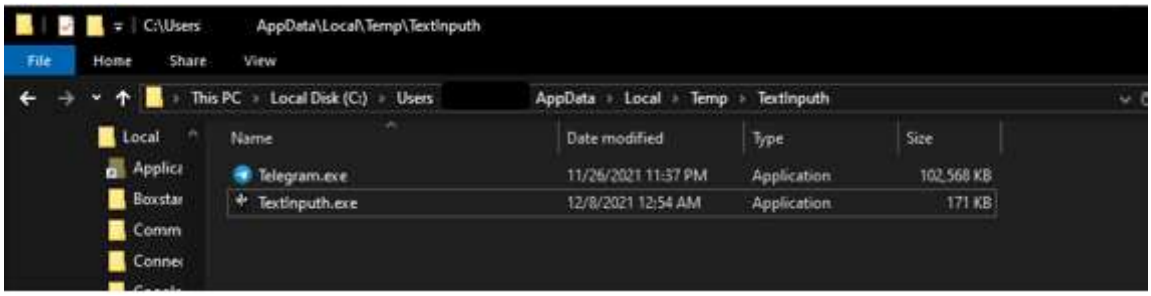
Malware Purple Fox distribué via des installateurs Telegram malveillants

by **Julien**
3 janvier 2022, 21h45

Un programme d'installation malveillant de Telegram for Desktop distribue le malware Purple Fox pour installer d'autres charges utiles malveillantes sur les appareils infectés.

Le programme d'installation est un script AutoIt compilé nommé « Telegram Desktop.exe » qui supprime deux fichiers, un programme d'installation de Telegram réel et un téléchargeur malveillant.

Bien que le programme d'installation légitime de Telegram déposé à côté du téléchargeur ne soit pas exécuté, le programme AutoIT exécute le téléchargeur (TextInputh.exe).



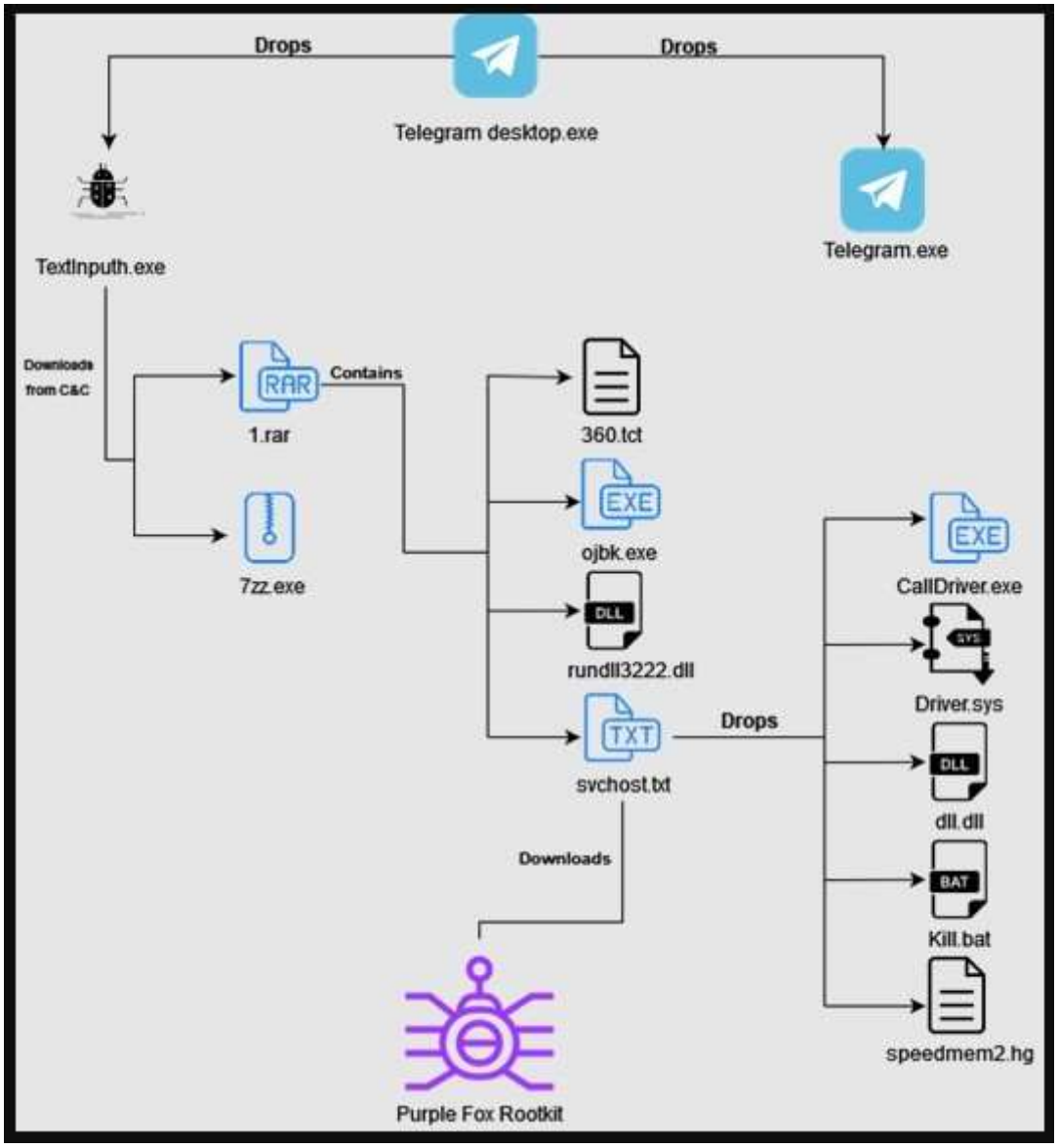
Fichiers supprimés sur la machine infectée
Source : Minerva Labs

Lorsque TextInputh.exe est exécuté, il crée un nouveau dossier (« 1640618495 ») sous « C:UsersPublicVideos » et se connecte au C2 pour télécharger un utilitaire 7z et une archive RAR (1.rar).

L'archive contient la charge utile et les fichiers de configuration, tandis que le programme 7z décompresse tout dans le dossier ProgramData.

Comme détaillé dans une analyse de Laboratoires Minerva, TextInputh.exe effectue les actions suivantes sur la machine compromise :

- Copie 360.tct avec le nom « 360.dll », rundll3222.exe et svchost.txt dans le dossier ProgramData
- Exécute ojbk.exe avec la ligne de commande « ojbk.exe -a »
- Supprime 1.rar et 7zz.exe et quitte le processus



Flux d'infection du renard pourpre
Source : Minerva Labs

Ensuite, une clé de registre est créée pour la persistance, une DLL (rundll3222.dll) désactive l'UAC, la charge utile (scvhost.txt) est exécutée et les cinq fichiers supplémentaires suivants sont déposés sur le système infecté :

1. Calldriver.exe
2. Driver.sys
3. dll.dll
4. tuer.bat
5. speedmem2.hg

Le but de ces fichiers supplémentaires est de bloquer collectivement le lancement de processus 360 AV et d'empêcher la détection de Purple Fox sur la machine compromise.

La prochaine étape pour le malware consiste à rassembler des informations système de base, à vérifier si des outils de sécurité sont en cours d'exécution dessus, et enfin à envoyer tout cela à une adresse C2 codée en dur.

Une fois ce processus de reconnaissance terminé, Purple Fox est téléchargé à partir du C2 sous la forme d'un fichier .msi qui contient un shellcode crypté pour les systèmes 32 et 64 bits.

Lors de l'exécution de Purple Fox, la machine infectée sera redémarrée pour que les nouveaux paramètres de registre prennent effet, le plus important, le contrôle de compte d'utilisateur (UAC) désactivé.

Pour ce faire, le fichier dll.dll définit les trois clés de registre suivantes sur 0 :

1. HKLMSOFTWAREMicrosoftWindowsCurrentVersionPoliciesSystem ConsentPromptBehaviorAdmin
2. HKLMSOFTWAREMicrosoftWindowsCurrentVersionPoliciesSystemEnableLUA
3. HKLMSOFTWAREMicrosoftWindowsCurrentVersionPoliciesSystemPromptOnSecureDesktop

```
sub     esp, 8
push    esi
lea     eax, [esp+0Ch+phkResult]
push    eax             ; phkResult
push    offset SubKey   ; "SOFTWARE\\Microsoft\\Windows\\CurrentVe"...
push    80000002h       ; hKey
mov     [esp+18h+phkResult], 0
call    ds:RegOpenKeyA
mov     edx, [esp+0Ch+phkResult]
mov     esi, ds:RegSetValueExA
push    4               ; cbData
lea     ecx, [esp+10h+Data]
push    ecx             ; lpData
push    4               ; dwType
push    0               ; Reserved
push    offset ValueName ; "ConsentPromptBehaviorAdmin"
push    edx             ; hKey
mov     dword ptr [esp+24h+Data], 0
call    esi ; RegSetValueExA
mov     ecx, [esp+0Ch+phkResult]
push    4               ; cbData
lea     eax, [esp+10h+Data]
push    eax             ; lpData
push    4               ; dwType
push    0               ; Reserved
push    offset aEnablelua ; "EnableLUA"
push    ecx             ; hKey
call    esi ; RegSetValueExA
mov     eax, [esp+0Ch+phkResult]
push    4               ; cbData
lea     edx, [esp+10h+Data]
push    edx             ; lpData
push    4               ; dwType
push    0               ; Reserved
push    offset aPromptonsecure ; "PromptOnSecureDesktop"
push    eax             ; hKey
call    esi ; RegSetValueExA
mov     ecx, [esp+0Ch+phkResult]
push    ecx             ; hKey
call    ds:RegCloseKey
xor     eax, eax
pop     esi
```

Dll désactivant l'UAC sur le système cible
Source : Minerva Labs

La désactivation du contournement de l'UAC est vitale car elle donne à tout programme qui s'exécute sur le système infecté, y compris les virus et les logiciels malveillants, des privilèges d'administrateur.

En général, l'UAC empêche l'installation non autorisée d'applications ou la modification des paramètres système, il doit donc rester actif sur Windows à tout moment.

Le désactiver permet à Purple Fox d'exécuter des fonctions malveillantes telles que la recherche et l'exfiltration de fichiers, la suppression de processus, la suppression de données, le téléchargement et l'exécution de code, et même le vermifugeage vers d'autres systèmes Windows.

À l'heure actuelle, on ne sait pas comment le malware est distribué, mais des campagnes de malware similaires se faisant passer pour un logiciel légitime ont été diffusées via des vidéos YouTube, des spams sur les forums et des sites de logiciels louches.