Rust Remote.Access.Trojan

Antoine MARTIN, Wesley EDE, Amad MOHAMMAD, Denis REMACLE

April 10, 2022

Sommaire

Qu'est-ce qu'un Remote.Access.Trojan ?

Et pourquoi on en code un !

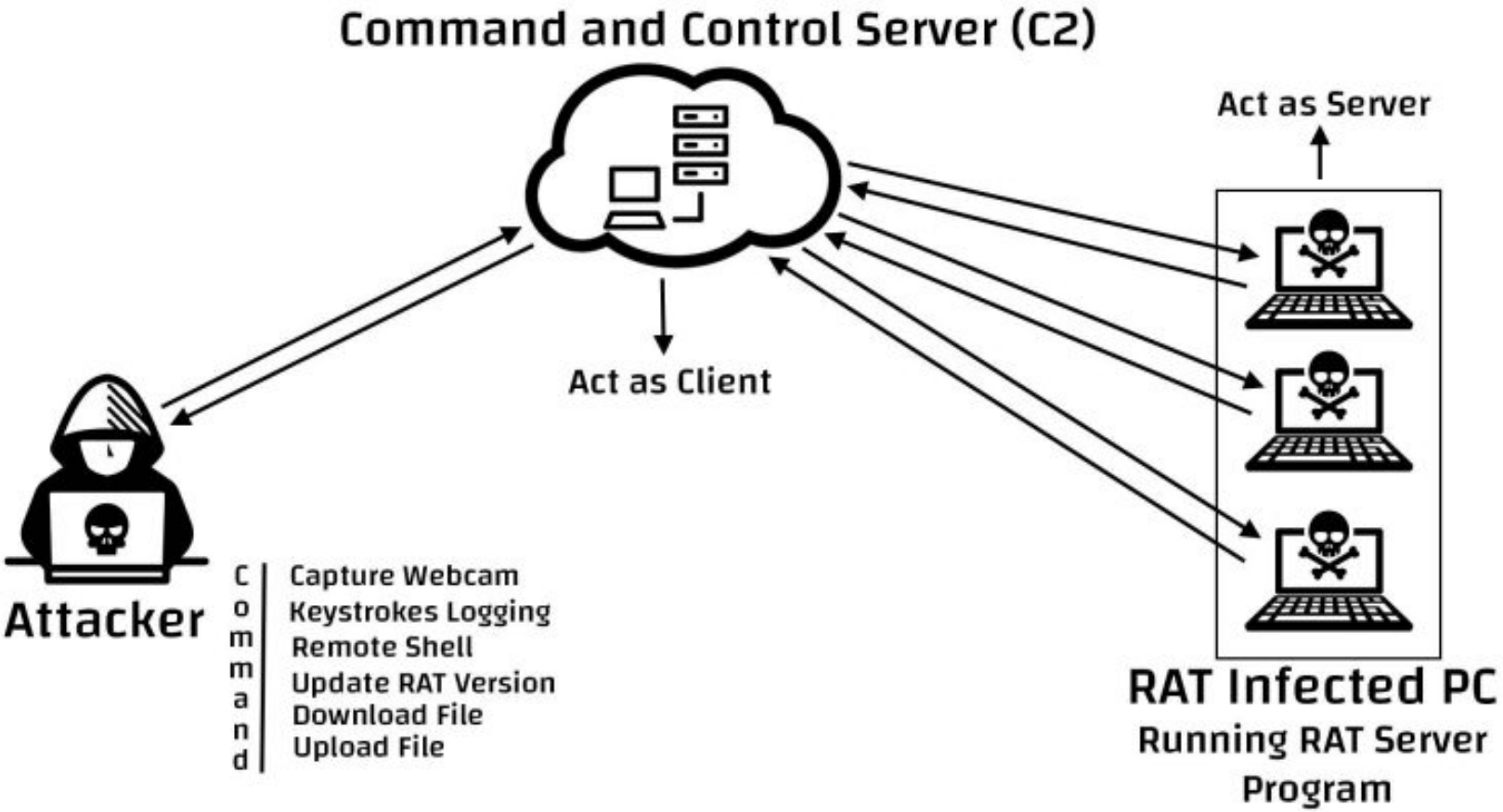
Mais pourquoi en RUST absolument ?

Comment va-t-il fonctionner en somme ?

Qu'est-ce qu'un Remote.Access.Trojan ?

- Un malware qui permet de prendre controle à distance et exécuter des commandes sur un poste infecté.
- Exemple notable : DarkComet, NanoCore

Qu'est-ce qu'un Remote.Access.Trojan ?



Et pourquoi on en code un !

- Un challenge stimulant
- Une occasion d'apprendre un langage dont l'importance ne fait que croitre

Mais pourquoi en RUST absolument ?

- Un langage permettant un code sur avec une orientation bas niveau
- Un langage qui prends de l'importance avec son utilisation : noyau linux, moteur html de firefox
- Une communaute grandissante et active

Comment fonctionne-t-il en somme ?

- Utiliser le port 53 en UDP pour se camoufler parmis les flux DNS
- Envoyer un heartbeat a intervalle aléatoire allant de 30 min à 1 heure
- Envoyer les ordres dans la réponse au heartbeat