

Rust Remote.Access.Trojan

Antoine MARTIN, Wesley EDE
Amad MOHAMMAD, Denis REMACLE

April 26, 2022

Sommaire

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

Pourquoi un R.A.T ?

Mais pourquoi en RUST absolument ?

Comment fonctionne-t-il en somme ?

Etat des avancements

Etat des avancements (GAANT)

Etat des avancements (GAANT suite)

PoC de notre solution

PoC de notre solution (Démonstration)

Batterie de fonctionnalités restant à implémenter

Batterie de fonctionnalités restant à implémenter (Suite)

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

- ▶ Un R.A.T est un logiciel qui n'est pas forcément malveillant et qui permet la prise de contrôle à distance d'un PC
- ▶ Dans notre cas c'est un malware qui permet de prendre contrôle à distance et exécuter des commandes sur un poste ou un ensemble de postes infecté(s).
- ▶ Exemples notables : DarkComet, NanoCore, NJRat...

Pourquoi un R.A.T ?

- ▶ Un challenge stimulant et enrichissant
- ▶ Choix cohérent avec les compétences diverses du groupe
- ▶ Une occasion d'apprendre un langage dont l'importance ne fait que croître

Mais pourquoi en RUST absolument ?

- ▶ Un langage permettant un code "sur" orienté bas niveau
- ▶ Un langage qui prends sans cesse de l'importance de part son utilisation : noyau linux, moteur HTML de firefox, etc.
- ▶ Une communaute grandissante et active

Comment fonctionne-t-il en somme ?

- ▶ Kptain-Ratz est capable pour l'instant :
- ▶ D'utiliser le port 53 en UDP pour se camoufler parmi les flux DNS
- ▶ D'envoyer un heartbeat a intervalle aléatoire allant de 30 min à 1 heure, le serveur est capable de l'interpréter et d'envoyer les instructions dans la réponse au heartbeat
- ▶ Il est codé en RUST

Etat des avancements

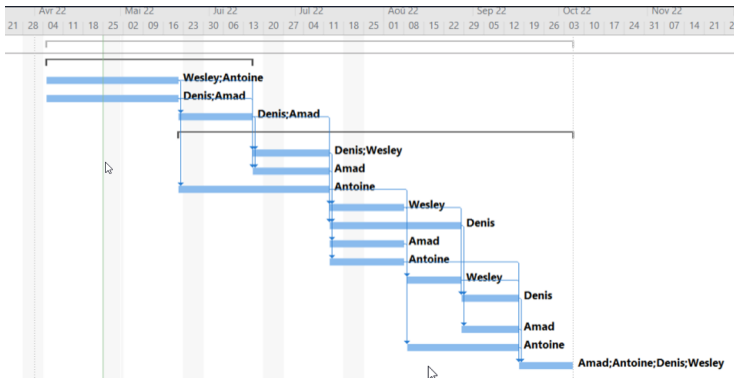
- ▶ Mise en revue du GAANT associé au Projet
- ▶ Différentes difficultés rencontrées

Etat des avancements (GAANT)

Nom de la tâche ▾	Durée ▾
Projet_annuel	56 jours
▸ Création de la base	21 jours
Configuration du client	14 jours
Configuration du serveur	14 jours
Interface utilisateur	7 jours
▸ Création des differents Plug-In	42 jours
Chiffrement des connexion	7 jours
Keylogger	7 jours
Gestion de fichier	14 jours
Gestionnaire de tache	7 jours
Envoi de message	14 jours
exécution de programme	7 jours
screenshot	7 jours
écoute du micro	7 jours
récupération des mots de passe navigateur	7 jours
Shell distant	7 jours
mode persistant	14 jours
Correction de bug	7 jours



Etat des avancements (GAANT suite)



PoC de notre solution

- ▶ Voici les étapes qui constituent l'initiation d'une connexion entre le client et le serveur :
- ▶ Chiffrement de la connexion
- ▶ Envoi des instructions
- ▶ Réception et interprétation du Heartbeat envoyé par le client



Batterie de fonctionnalités restant à implémenter

- ▶ Une interface graphique, des fonctionnalités diverses :
- ▶ Keylogger, Remote Desktop, SCP etc.
- ▶ L'interface cible devra être semblable à celle-ci :

Batterie de fonctionnalités restant à implémenter (Suite)



Blackshades NET - Connections: 14

	ID	WAN	LAN	DOS	IM	USB	Username	Comp.Name
Local (11)								
new (3)								
Local		112.205.54.230	112.205.54.230				Administrator	ANONYMOUS
Local		91.187.103.50	10.90.96.246				Administrator	CYBERSPAC
new		109.185.251.122	192.168.1.5				Ààèèééôôââôâ	CTRLSOFT-7...
new		178.65.113.131	178.65.113.131				PatrickStar	SAMLAB
Local		94.250.20.187	192.168.1.2				tsunjo	TRUNJO-PC
Local		79.117.186.83	192.168.1.100				kostas	VLAKAS
Local		91.140.62.112	192.168.1.38				XRHSTOS	XRHSTOS-PC
Local		203.117.58.130	203.117.58.130				Ramly	RAMLY-PC
Local		82.178.117.254	192.168.1.102				ÀÀÔÔÈÈ àæñ	ÀÀÔÔÈÈ àæñ
Local		201.14.126.66	10.2.2.88				Administrator	ADMIN
Local		212.25.60.10	192.168.221.10				IFcho	IVAKA
new		121.54.78.162	192.168.0.102				Admin	ADMIN-PC
Local		87.97.141.150	192.168.2.101				pc	PC-D36A524...
Local		189.68.10.0	189.68.10.8				PC	PC-829C5637...

Connections | Create Server | Create Station | Statistics | Settings | Database | Tasks | Transfers | Onion | Alarms