



Le Reverse Engineering

Dans le monde des jeux vidéos

By Emeline Villemey



INDEX

01 Quésaco

02 LOGICIELS

03 GAMING & EXPLOITS

04 CAS CONCRETS

05 REVERSE GAMING





01



Quésaco



Quésaco



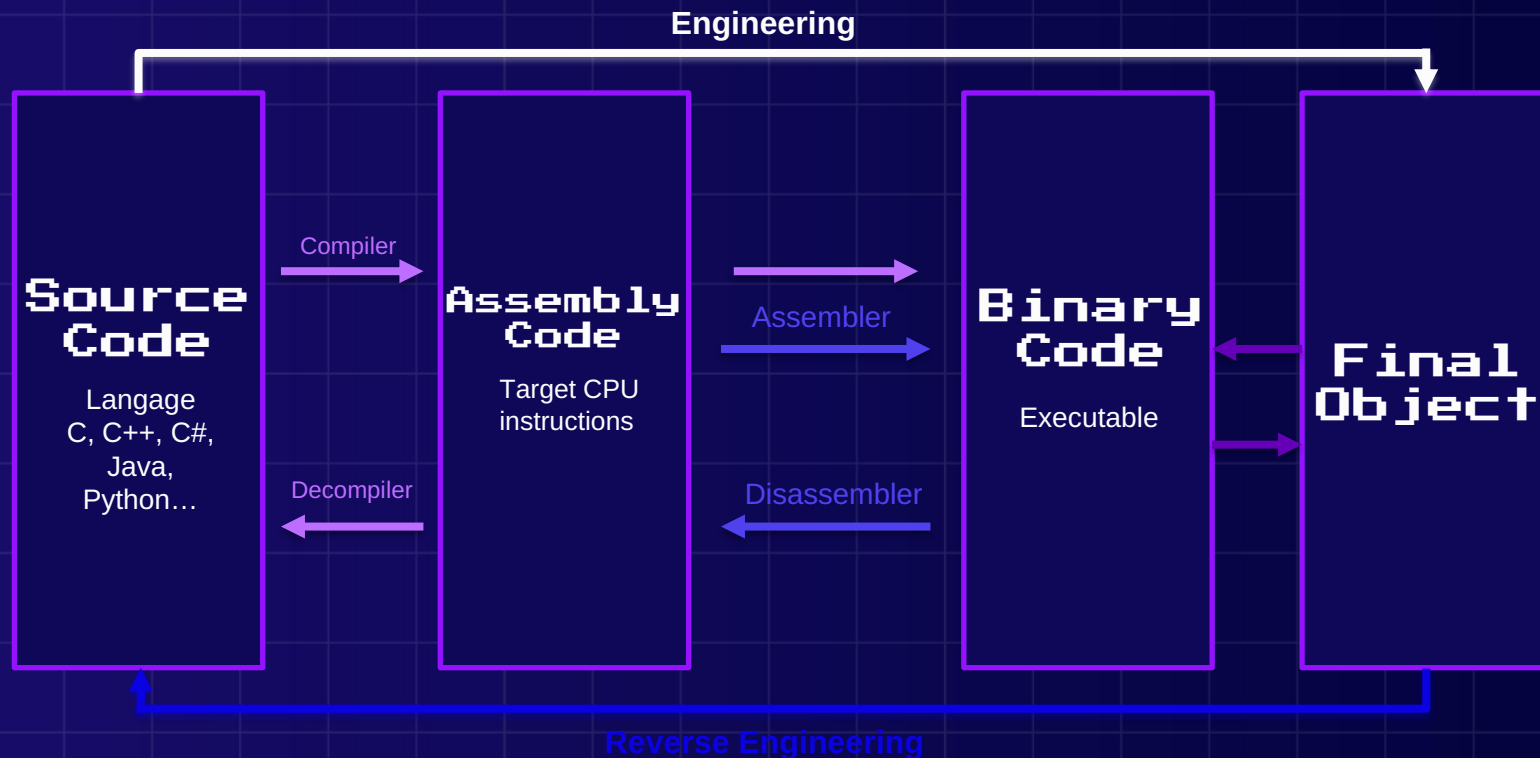
Qu'est ce que le reverse engineering ou rétro conception?
Le reverse engineering consiste à étudier un objet pour en déterminer le fonctionnement interne ou la méthode de fabrication. Ici on l'utilise dans le cadre de logiciels. C'est un procédé qui s'exécute par étapes :

- Trouver un logiciel (malveillant ou non)
- Le désassembler (désassembleur)
- Analyser et comprendre le logiciel

Pour cette veille j'ai décider de restreindre le champ de recherche au reverse engineering dans les jeux vidéos, aussi appelé le "cracking".



Schéma explicatif



CONCRETEMENT



REVERSE CYBERSECURITE

Lorsqu'un logiciel malveillant intervient sur un équipement et infecte une partie du réseau de la cible, tous le matériel est isolé et mis sous analyse afin de comprendre comment la contagion à eu lieu et comment la stopper et la nettoyer. Grâce au Reverse Engineering, on revient à la source de ce qui se passe lorsque le logiciel est exécuté et comment peut on inverser les effets pour par la suite, tout réparer.

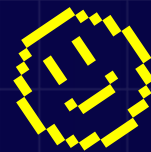
REVERSE DE JEUX VIDEOS

Durant de nombreuses années les jeux vidéos ont coexisté avec le progrès de la programmation et de la technologie, permettant de meilleurs produits et des rendus époustoufflants. Aujourd'hui, leur code, bien que sécurisé fait parfois l'objet de failles exploitables : "Exploits". Ces exploits permettent aux joueurs de progresser, tricher, détruire ou créer au sein du jeu, évidemment sans l'autorisation des auteurs de ce dernier.

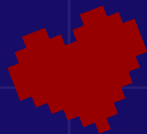




02



LOGICIELS

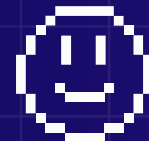




LOGICIELS

GHIDRA

Un programme de reverse engineering créer par The National Security Agency (USA), logiciel gratuit et open source. Désassembleur, permettant de générer du pseudo code.



IDAPROCV

IDA est également un programme de reverse engineering, celui ci est payant, désassembleur lui aussi.

ANDRO GUARD

Logiciel utilisé afin d'analyser la sécurité des applications Android, la revingénierie doit aussi après tout s'appliquer à tous les supports et permettre de protéger tous les utilisateurs peu importe leur plateforme.





03

GAMING & EXPLOITS





“Rien ne sera jamais
effacé”

—SNOWDEN—



GAMING & EXPLOITS



Easter Egg

“Break your day into smaller chunks and focus on one task at a time. Take short breaks in between to stay fresh”

ANTI-CHEAT

“Make time for exercise, healthy eating, and hobbies outside of work to reduce stress and promote relaxation”


PREMIER EXPLOIT

“Attend events, join professional organizations, and connect with others in your field on social media to expand your network”




CAS CONCRETS

GENSHIN IMPACT




Hoyoverse/MiHoyo est un studio Chinois ayant créé un des jeux les plus populaires actuellement : Genshin Impact. Ce jeu possède, comme beaucoup d'autres, un anti-cheat (logiciel d'anti triche). Ces derniers ont souvent besoin de privilèges sur l'ordinateur des joueurs afin de modérer les systèmes de triche, privilèges qui se traduisent souvent par des accès Kernel, c'est à dire, un accès direct à la base de toute chose dans un ordinateur. Mhyprot2.sys fait alors l'objet d'une faille de sécurité : CVE-2020-36603



Permettant à n'importe qui passant par le logiciel ou du moins, son empreinte, d'avoir des accès administrateur sur un système. De part la réputation de l'empreinte, ils passent inaperçu et accèdent au système sans se faire bloquer, puis, désactive 1 à 1 tous les antivirus et défenses de la cible jusqu'à supprimer mhyprot2.sys et par la suite installer toute leur suite de ransomware "svchost.exe". Ainsi, même sans télécharger le jeu, vous pouvez être la cible de ces pirates.

ELDER SCROLLS ONLINE



The Elder Scrolls Online est un jeu du studio Bethesda, très populaire lui aussi. Un Français du nom de Colin J. Brigato, expert en rétro-ingénierie, trouve un jour une faille du côté client, en effet le serveur enregistre les informations par confiance des échanges venant du client des joueurs. En envoyant des informations au serveur, Colin peut utiliser des compétences via cette faille.

Le studio ayant résolu le bug, ne s'attendait pas à ce que Colin analyse le nouveau code du jeu, permettant désormais de comprendre comment fonctionne le jeu côté serveur. De simple joueur il est devenu plus puissant qu'un modérateur ou un game master.

05

▶ REVERSE GAMING ◀



Liens ludiques

Elder Scrolls

[Ici, le hack Elder Scrolls Online](#)

Genshin Impact

[Article sur le bypass Kernel via l'anti-cheat de Hoyoverse](#)

D'où viennent les cheats

La plupart des cheats (codes de triche) connus viennent en réalité du reverse engineering, car, oui, la sécurité est compromise, mais l'intégrité du code aussi

Les cheats nuisent au bon fonctionnement du jeu (pensé pendant des heures, des jours, voir des mois par les développeurs) et en plus de déséquilibrer le jeu, peuvent handicaper voir pénaliser les joueurs qui eux, ne trichent pas



THANKS !

Vous avez des questions ?
Villemey.emeline.line@gmail.com

<https://sera-line.github.io/Portfolio-Villemey-Emeline/Acceuil.html>

