CYBERPUNK RED

NETRUNNING
Règles Maison

Créé par Sephter

Source de l'image de couverture: https://pixabay.com/illustrations/security-internet-crime-cyber-4700815/

Table des matières

Introduction

Cette aide de jeu a été grandement inspirée par le travail de *Slymz et Hegumile* (*http://cyberpunk-jdr.fr/fichiers/aides/creations_personnages/netrunner.pdf*). L'objectif est multiple :

- Retirer l'aspect *Liste de sorts* que donne le système décrit dans les règles de base de CP RED.
- Rendre le netrunner plus amusant à jouer entre deux plongées dans un réseau NET
- Offrir un gameplay assez proche de CP 2077
- Libérer le MJ de la nécessité de préparer moulte réseaux NET pour ses psychopathes de joueurs.
- Offrir aux psychopathes susnommés la possibilité de faire joujou avec tout ce que la vie moderne offre comme objets connectés.

J'espère que cela vous plairaet n'oubliez pas :

« vivre vite, vivre fort et vivre sur le fil du rasoir. Ne stresse pas, choom. Ce n'est pas comme si t'allais en sortir vivant, si ? »

Si vous avez des questions ou des suggestions, je vous invite à me les poser sur discord (Sephter#2115).

Merci à Gormarius, sans qui la présente mise en page n'aurait jamais vu le jour.

Cyberdeck

Le Cyberdeck moderne est un éclat, une carte dans le crâne de l'utilisateur branché dans l'un de ses ports. Un Cyberdeck a autant d'emplacement que ceux dans les règles de base. Un cyberdeck peut comporter des upgrades matériels (tels que Hardened Circuitry ou Range Upgrade) comme ceux dans les règles de base. En raison de la miniaturisation du cyberdeck, ces upgrades doivent être intégrés à l'achat du cyberdeck. Il n'est donc pas possible de les changer ultérieurement ; il faut racheter un cyberdeck avec tous les upgrades désirés. Les emplacements non utilisés pour des upgrades matériels peuvent être utilisés comme points de connexion. Ces points de connexion sont utilisés pour la fonctionnalité Load balancing et pour maintenir une connexion sur plusieurs équipements (voire rester connecté dans *Hacker un équipement*.)

Upgrades

Filtre de bio-feedback : Cette upgrade filtre les signaux envoyés par une barrière offensive anti-personnel et diminue les dégâts infligés par cette dernière de 3 points. Plusieurs filtres ne se cumulent pas (même prix qu'une upgrade standard : 100 ed, très coûteux).

Circuit renforcé : Un cyberdeck doté de circuits renforcés ne peut être désactivé ou détruit par une IEM

Disque dur de sauvegarde : une copie du système d'exploitation du cyberdeck est conservée sur un espace mémoire, hors d'atteinte de l'extérieur. Cela permet, en cas de crash total du cyberdeck, de le réinstaller en une minute (20 tours) au lieu d'une heure. Cette réinstallation ne nécessite pas d'accéder à un ordinateur. **Occupe 2 espaces d'upgrade**.

Extension de portée : augmente la portée de base du cyberdeck de 3m. Plusieurs extensions de portée ne se cumulent pas.

Implants

Cette aide de jeu implique quelques modifications dans le fonctionnement des implants cybernétiques :

Lien neural : inclut deux ports de connexion, permettant l'insertion d'éclats de données ou d'un câble de connexion. Le lien neural est connecté directement sur le cortex visuel, permettant ainsi de visualiser les données. Lorsque cela se produit, les images transmises par le nerf optique sont temporairement remplacées par celles de l'éclat ou de la liaison, laissant le personnage aveugle le temps de la connexion. Ces slots d'éclats ne peuvent PAS être utilisés pour installer du chipware.

Ports d'interface neurale : ajoute un câble de liaison et une prise de connexion externe derrière l'oreille permettant tous deux un contrôle actif. Il permet également l'utilisation d'éclats actifs, tels qu'un éclat cyberdeck ou de pilotage à distance.

Cyberoptique virtualité : permet un affichage des données en surimpression avec le frigo à viande (a.k.a. le *monde réel*) permettant ainsi de pirater sans rester aveugle.

Collection de malwares

En 2045, l'informatique à la papa, c'est terminé. À la suite des avancées technologiques faites durant la guerre et les changements drastiques dus au datakrash, les systèmes experts contenus dans le moindre système un tant soit peu évolué sont aujourd'hui capables de s'adapter aux menaces connues. Tout netrunner qui se respecte utilise donc ses propres logiciels. Cet ensemble de codes, virus, logiciels d'intrusions est connu sous le surnom de collection de malware.

Un netrunner peut posséder plusieurs collections, mais une seule peut être chargée sur un cyberdeck à un moment donné. Changer de collection demande une heure et l'accès à un ordinateur, ainsi qu'à la collection.

Charger la collection dans un réseau rendra cette collection spécifique complètement inutile contre ledit réseau, ainsi que contre tout système connecté à ce réseau. Pour ces raisons, un netrunner ne partagera probablement jamais ses secrets. Pas volontairement.

Composer une collection de malwares

Il s'agit d'un travail de longue haleine. Cela demande 8 heures par niveau avec un maximum de niveaux égal au score d'INTERFACE du netrunner. Pour chaque niveau, le netrunner choisit une ligne et une colonne dans le tableau des fonctionnalités. Chacune des fonctionnalités incluses dans cette ligne et cette colonne gagne un niveau. La fonctionnalité située à l'intersection de la ligne et de la colonne ne gagne qu'un seul niveau.

Tableau de fonctionnalités

Les 9 fonctionnalités décrites sont réparties en 3 lignes et 3 colonnes.

Lignes de fonctionnalité

- **Data mining** qui inclut les fonctionnalités

  Wireless, géolocalisation et profiling
- **Intrusion** qui inclut les fonctionnalités

  quickdata, saute-mouton et load balancing
- **Sécurité** qui inclut les fonctionnalités

  Red Alert, Bastion et Blackwall

Colonnes de fonctionnalité

- **Quick Hacks** concerne essentiellement le piratage d'équipement set inclut les fonctionnalités

  wireless, quick data et red alert
- **Deep Hacks** concerne essentiellement le piratage de réseauxet inclut les fonctionnalités

  geolocalisation, load balancing et bastion
- **Life Hacks** concerne essentiellement le piratage, l'la récolte et l'utilisation de données publiqueset inclut les fonctionnalités

Description des fonctionnalités

Wireless : (Data mining / Quick Hacks)

Le netrunner est capable d'optimiser le signal sans fil de son matériel. Sans rang dans Wireless, il doit se trouver à moins de 5 m de sa cible pour utiliser ses programmes sur elle. Chaque rang dans cette compétence étend la distance de 2m. A partir du niveau 5, il peut effectuer un hack à n'importe quelle distance tant qu'il a un visuel sur la cible, au prix d'un malus de -1 par 5m supplémentaire de sa portée max qui le sépare de celle-ci. Au niveau 8, il est capable de relever les signaux à travers les murs peu épais (le MJ décide) et peut hacker ses cibles.

Geolocalisation : (Data mining / Deep Hacks)

En prenant un tour complet, le Netrunner peut lancer un scan approfondi du réseau. Il doit alors faire un jet de TECH + Geolocalisation vs pare-feu pour dévoiler les périphériques (défenses, imprimantes,) liés à ce réseau et leur localisation physique.

Profiling : (Data mining /Life Hacks)

Le Netrunner peut effectuer, au prix d'une action de mouvement, un jet de INT + Profiling dont le SD est égal à la TECH x3 de la cible. Il connaît alors des informations basiques (nom, lieu de résidence, affiliations, implants ainsi qu'un accès à son agent). Le Netrunner, ainsi que les personnes ayant ces informations, gagnent un bonus de +3 en corruption, Psychologie, Interrogation et Persuasion contre la cible.

Quick Data : (Intrusion / Quick Hacks)

Le Netrunner est capable de trouver de petites failles de sécurité chez les victimes de ses hacks ainsi que d'optimiser leur téléchargement. Ainsi chaque 2 rang dans Quickdata permet de réduire le temps nécessaire à uploader un hack chez une victime de 1 action NET (minimum 1)

Saute-Mouton : (Intrusion / Life Hacks)

Le Netrunner peut utiliser un équipement piraté pour en attaquer un autre. Pour se faire il doit installer un rootkit dans l'équipement, qui fera alors office de proxy pour lui dans la zone. La connexion n'est pas des plus stables, ainsi chaque rang dans Saute-mouton lui permet d'allonger la distance qui peut le séparer de son proxy le plus éloigné de 5m par rang.

Load Balancing : (Intrusion / Deep Hacks)

Chaque 2 rangs dans load balancing permet d'utiliser un port de connexion supplémentaire pour se connecter à un réseau. Une barrière simple devra couper chaque connexion pour réellement déconnecter le netrunner. Ces connexions sont établies lors de l'intrusion et ne peuvent pas être réinitialisées tant que ne netrunner est connecté sur ce réseau.

Red Alert : (Sécurité / Quick Hacks)

Lorsqu'un Netrunner ennemi tente d'hacker le personnage ou ses alliés, le personnage peut faire un jet de INT+Red Alert contre l'Interface x3 de l'assaillant. S'il réussit, il arrête l'attaque en cours et le localise plus ou moins précisément. Il localise le Netrunner dans un rayon de 25m, réduit de 5m par tranche de deux points au-dessus du SD

Bastion : (Sécurité / Deep Hacks)

Pour chaque 2 rangs dans Bastion, le netrunner peut diminuer sa ME de 1 lorsqu'il échoue à son jet d'intrusion. Cela ne transformera pas un échec en réussite, mais pourra empêcher une barrière anti-logicielle de krasher le deck du netrunner.

Blackwall : (Sécurité / Life Hacks)

En extrapolant des données médicales provenant des réseaux publics, le netrunner a pu se forger un profil artificiel. Ce profil permet de tromper une black ICE et de rendre son attaque ciblée moins efficace. Les dégâts infligés par une black ICE sont diminués de 2 pour chaque rang dans Blackwall

Fonctionnement du hacking

Il existe deux types de piratage qui sont le quick hackinget le deep hacking.

Le quick hacking consiste à pirater des appareils, généralement courants, dotés d'une technologie sans fil. Cela peut inclure (sans se limiter) un système de sécurité, un implant cybernétique, un véhicule… pourvu que cet équipement soit doté d'une connexion sans fil. Bon nombre d'équipements sont pourvus de cette technologie et l'utilisent le plus souvent pour des mises à jour systèmes, de la maintenance, ou encore des gestions de licences.

Le deep hack consiste à pirater les architectures NET. Ce qui est généralement, soyons honnêtes, nettement plus dangereux. Et nettement plus rentable. Plus rentables parce que ces architectures contiennent souvent des données de valeur. Et plus dangereux parce que les gens à qui appartiennent ces données sont souvent peu enclins à les partager et n'hésiteront pas à te faire couler la cervelle par les oreilles, choomba.

Quick hacking

Pare-feu

Chaque item ou implant, même le plus médiocre, est doté d'un pare-feu. Le score de celui-ci est calculé de la manière suivante :

Soit l'item ou l'implant est possédé par un pnj insignifiant (c'est à dire un pnj trop peu important pour avoir droit à son propre nom : ganger de base, un passant dans la rue...) ou un PJ qui n'a pas envie de se prendre la tête et choisit de garder la configuration d'usine. Dans ce cas, la valeur de pare-feu est de 15 pour un matériel de qualité moyenne, 10 pour un matériel de mauvaise qualité et 20 pour un matériel de qualité excellente.

Soit l'item est possédé par un personnage important (PNJ majeur, PJ...). Dans ce cas, la valeur de pare-feu de l'équipement est égale à (sécurité électronique + TECH) de la personne en charge de l'installation du pare-feu de l'équipement multiplié par 1 pour du matériel de mauvaise qualité, 1,5 (arrondi au supérieur) pour du matériel de qualité moyenne et 2 pour du matériel de qualité excellente.

Intrusion

Pour pirater un équipement, il est nécessaire de se trouver à 5 mètres ou moins de l'équipement. Pour cela, le netrunner fait un jet INT+INTERFACE vs le niveau de pare-feu. Ce jet prend une action virtuelle.

Temps de chargement

Une fois le jet d'intrusion réussi, le netrunner a trouvé une faille et peut charger un rootkit temporaire sur l'équipement. Cela prend un nombre d'actions virtuelles égale au niveau de pare-feu de l'équipement divisé par 2 (arrondi au supérieur). Ce nombre est réduit d'un tour pour chaque 2 points de réussite.

Exemple : Face à pare-feu de 15, le netrunner fait un jet de 18. Le pare-feu impose un chargement de 8 actions virtuelles, diminuées de 1 (18-15=3, divisé par 2 et arrondi à l'inférieur=>1). Il lui faudra donc 7 actions virtuelles pour (enfin) pouvoir accéder à l'équipement.

Que faire pendant le chargement ?

Le chargement est une action automatisée, le netrunner peut donc faire d'autres choses pendant ce temps. Au hasard, se défendre contre les agents de sécurité qui lui tirent dessus, ces gens sont d'un susceptibles... ce chargement utilise un port de connexion sur le cyberdeck. Le cyber deck, quant à lui, peut être utilisé pour lancer un nouveau piratage, s' il lui reste des ports de connexion disponibles.

Rester connecté

Une fois connectéet tant qu'il reste à portée de l'équipement, le netrunner peut rester connecté à l'équipement sans se faire détecter. Chaque connexion maintenue utilise un port de connexion sur le cyberdeck.

Que peut-on faire une fois connecté

Si l'équipement est spécifiquement conçu pour un accès à distance, comme un agent, par exemple, ou un drone télécommandé, alors le netrunner peut accéder à l'interface. Dans tous les cas, les options suivantes sont disponibles :

Faire krasher l'équipement

Pour ce faire, il effectue un jet selon la nature de l'équipement (cybertech pour un implant, sécurité électronique pour une alarme sans fil...). Il peut également transférer les données sur un appareil externe pour permettre à un équipier de lui dicter comment faire (cela implique un malus de -2). Le jet se fait contre le niveau de pare-feu de l'équipement, le résultat étant déterminé par le niveau de réussite (le netrunner peut limiter son action et annoncer un résultat inférieur à son jet s'il veut juste rendre sourd un musicos pendant quelques instants, au lieu de le forcer à retourner voir son charcudoc) :

Niveau de pare-feu : Glitch. L'équipement ne tombe pas réellement en panne mais présente des défaillances pendant 1D6 tours. Pendant ce temps, toutes les actions impliquant cet équipement imposent un malus de -2. Des cyber-optiques pourraient afficher une image déformée, une tourelle automatique bouger par saccades... Réitérer cette action sur un équipement déjà glitché ne cumule pas les malus, mais permet de relancer le D6 pour la durée. Cette nouvelle durée remplace alors la précédente.

Niveau de pare-feu +3 : plantage. Les données contradictoires envoyées à l'équipement ont ruiné sa configuration, surchargé sa mémoire ou simplement figé son système d'exploitation. Quoiqu'il en soit, l'équipement est inutilisable pendant 1D6 tours. Cela déconnecte automatiquement le netrunner de l'équipement.

Niveau de pare-feu+6 : crash total. Le système d'exploitation est irrémédiablement corrompu et doit être réinstallé. Cette opération nécessite une réparation simple. Tant qu'elle ne sera pas faite, l'équipement est inutilisable.

Après chaque tentative de krasher un équipement, le netrunner devra effectuer un nouveau jet vs le pare-feu de l'équipement. En cas d'échec, le système identifiera son intrusion et l'éjectera. L'utilisation d'un rootkit est donc une bonne idée, si le timing et la compétence le permettent.

Installer un rootkit (logiciel de contrôle)

Le rootkit temporaire utilisé lors de l'intrusion initiale n'est que cela : un bidule temporaire qui n'est pas destiné à rester. Mais le netrunner peut désirer pouvoir revenir plus tard sur cet équipement. C'est à cela que sert un rootkit.

Sur un jet vs pare-feu+3, le netrunner peut installer un rootkit. Cette installation nécessite un chargement égal à pare-feu divisé par 3 (arrondi au supérieur). Celui-ci lui permettra d'accéder à l'équipement sans temps de chargement et ce, tant que le rootkit restera installé (une maintenance standard le détectera et le supprimera). Un jet d'intrusion contre le pare-feu reste malgré tout nécessaire pour entrer en contact avec le rootkit et lui ordonner d'ouvrir la connexion. Un netrunner peut se connecter au rootkit d'un autre netrunner si ce dernier lui en a fourni les accès.

Accéder à un autre équipement possédé par la même personne

Vos implants, votre agent, votre smartgun, même votre véhicule lorsque vous conduisez... tout cela fonctionne ensemble. C'est très pratique, comme votre frigo qui indique à votre agent qu'il faut racheter des bières, ou votre télé-optique gauche qui s'aligne avec le système de visée de votre fusil sniper. Mais ça implique aussi qu'un petit malin qui accède à vos éventreurs peut s'en servir de passerelle pour accéder plus au reste de votre matos.

Concrètement, une fois connecté à un équipement, le netrunner peut accéder au reste de l'équipement de sa cible au prix d'un simple jet de pare-feu, SANS temps de chargement supplémentaire.

« Alors ? T'es sûr que tu veux te faire implanter ce Mr Studd de contrebande Made In va-savoir-où, choomba ? »

Implanter un virus

Comme dans les règles de base (page 200), l'implantation d'un virus prend un nombre de tours et un jet de dés qui dépendent tous deux du MJ.

Deep Hack

Connexion

Un réseau est mieux protégé qu'un équipement simple, en raison simplement du volume disponible qui permet l'ajout d'équipements de sécurité plus efficaces. Il est donc nécessaire de se connecter physiquement, à l'aide d'un câble d'interface. Ce qui implique parfois des explications avec des gens fort peu sympathiques.

Krasher le réseau

Il est bien sûr possible de tenter de krasher le réseau, comme tout équipement, mais l'effet sera bien moindre : un jet vs pare-feu permet de faire glitcher le réseau, ce qui aura pour conséquence un malus de -2 pour les systèmes dépendant d'une communication, tels qu'alarmes, intercoms, recherche de données... ce malus s'applique également au netrunner sur ce réseau. Un plantage, ou pire, un crash total, n'est juste pas faisable sur une telle infrastructure. Pour obtenir ce genre de résultat, essaye plutôt le C4, choom.

Lister les systèmes

La beauté d'un réseau c'est que tout est connecté. Une action virtuelle permet de consulter la liste des systèmes connectés au réseau. Alarmes, tourelles, mais aussi stockage de données, arroseurs automatiques etc. A noter que ce scan donne la liste des systèmes et leur dénomination, pas leur contenu, ni leur niveau de pare-feu. Certains administrateurs aiment donner des noms cryptiques à leurs systèmes, juste pour égarer l'ingénu qui en voudrait à la tirelire.

Accéder au reste du système

La beauté d'un réseau c'est que tout est accessible. Une fois dedans, il est alors possible d'accéder en une seule action virtuelle à tous les systèmes connectés à ce réseau en utilisant le même jet de dés que celui utilisé pour se connecter. Si ce jet de dés n'est pas suffisant, il lui faudra alors faire un nouveau jet pour s'octroyer de meilleurs privilèges et accéder à ce nouveau système. Ce nouveau jet ne remplace **pas** le jet initial qui sert de référence.

Exemple : super-gégé a obtenu un score très honorable de 17 pour accéder au réseau des bureaux locaux d'une corporation mineure. 17 sera donc le score de référence. Après avoir listé les systèmes connectéset remercié le grand esprit du gwak que l'admin réseau n'aie pas donné des noms débiles à ses systèmes, il décide de se connecter à "DATA_1". Le pare-feu de DATA_1 est de 20 (il contient des données dont le manager se sert pour faire chanter certains concurrents). Il doit donc refaire un jet d'intrusion pour y accéder. S'il réussit, il pourra accéder aux dites données. Il décide après cela d'accéder au système "GARAGE". Celui-ci a un pare-feu de 18. Celui-ci est inférieur au 20 que super-gégé a obtenu en accédant à "DATA_1", mais supérieur au 17 de référence. Il doit donc refaire un jet d'intrusion. Il n'aurait pas eu à faire ce jet s'il avait tenté d'accéder à "GARBAGE" qui a un pare-feu de 10 (et gère le collecteur à ordures et le contrat avec la société de ramassage des poubelles).

Installer un rootkit

Cela fonctionne exactement comme l'installation d'un rootkit sur un équipement simple.

Barrières offensives

Bien que le niveau de pare-feu d'un réseau fonctionne comme celui d'un équipement simple, les conséquences en cas d'échec sont nettement plus inquiétantes. Un distributeur automatique de sushis ne cherchera pas à transformer ton cerveau en Kibble si tu tentes de lui extorquer un menu numéro 3 à l'œil. Une architecture NET, elle, ne va pas s'en priver.

Se faire détecter

En cas d'échec au jet d'intrusion, le pare-feu détectera automatiquement une connexion anormale et agira à la fin du tour du netrunner. Cette action dépendra du type de barrière placée sur le pare-feu que le netrunner vient de tenter de passer.

Types de barrière offensives

Barrière simple

Dès que le pare-feu détecte l'intrus, cette barrière se coupera de la connexion indésirable et éventuellement, activera l'un des systèmes du réseau (une alarme, par exemple). Cela a pour conséquence de complètement éjecter l'intrus du réseau, le forçant à reprendre son infiltration depuis le tout début. Ce genre de barrière est généralement placé aux entrées du réseau, afin

d'éviter de griller un utilisateur qui s'est connecté par erreur. C'est lourdingue, mais pas bien méchant.

Barrière anti-logiciel

Cette barrière utilisera la connexion établie par l'intrus pour remonter jusqu'au cyberdeck de ce dernier et tenter de le faire krasher. Le résultat de cette attaque dépend de la marge d'échec du netrunner. On ne va pas se le cacher, ça peut être plutôt relou.

ME 3 ou moins : la barrière parvient à déstabiliser le système d'exploitation du cyberdeck. Cela se manifeste par un malus -2 à tous les jets d'actions virtuelles effectués à l'aide de ce cyberdeck pour les prochains 1D6 round.

ME entre 4 et 6 : la barrière parvient à provoquer une instabilité suffisante pour forcer le cyberdeck à rebooter. Ce reboot prendra 1D6 round et coupera toutes les connexions du cyberdeck actuellement en cours.

ME 7+ : la barrière a pu accéder au firmware du cyberdeck. Celui-ci est complètement inutilisable jusqu'à une réinstallation complète (ce qui prendra une heure et un ordinateur). Ceci peut se manifester par une panne totale, soit par le remplacement des fonctions habituelles du deck par quelque chose d'autre : une appli publicitaire, un virus, un vieil épisode de Dora l'Exploratrice qui tourne en boucle...

Barrière anti-personnel

Évolution de la vieille technologie des black ICE, ça ne rigole plus. Cette barrière offensive va purement et simplement essayer de tuer l'intrus en retournant les fonctionnalités de réalité virtuelles contre lui. Le MJ est invité à consulter la liste des glaces dans les règles de base (page 206) pour les dégâts infligés et les éventuels effets secondaires. Stimuli induisant une crise d'épilepsie, prise de contrôle de l'interface neurale dans le but de griller le système nerveux... chaque concepteur de black ICE a ses propres méthodes. Soyez juste sûrs d'une chose : ça sera sale et ça sera fait exprès.