Cyber Survivors – Cahier des charges

Type de jeu

- 2D
- Sprite
- Defense/Attaque contre des virus réel (ransomware…)
- Solo/Coop 30 minutes

Mise à jour potentielle

Mode de jeu : Mode classé, qui recommence chaque semaine / mois ?

Gameplay v1

Jouer avec la souris.

Raccourcis clavier.

Jeu style Survivor

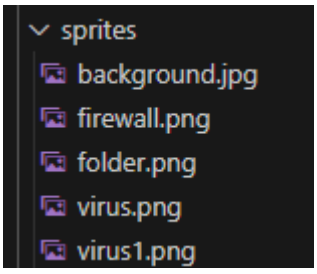
Le but ne perdre aucun dossier sur son bureau l'or d'attaque de virus

Joueur (en solo contrôler jusqu'à 4 dossier)

A 1 dossier le dossier par defaut est jaune allant jusqu'à 4 dossier (bleu, rouge, vert), si 1 dossier se trouve à côter d'un autre dossier celà renforce ces dossiers

Inventaire du joueur

S'affiche sur le côté gauche ou droite de la page (au quel on pourrait mettre des modules d'extension) par dossier, un dossier pour les extension en trop



c'est quoi les module d'extension

- arme
- défense (regene, détection de virus camouflé etc…)

- support (buff les dossiers proche de lui)

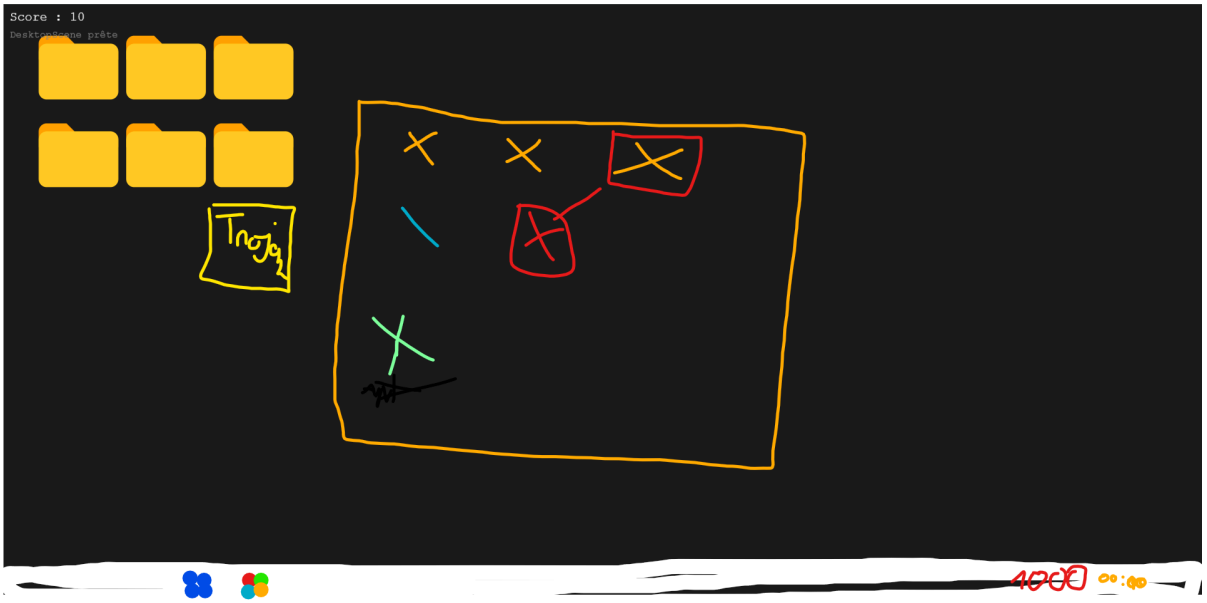
Système d'amélioration des modules on peut fusionné 2 module d'extension de rareté 1 pour une rareté 2

Il n'y a pas d'xp en place mais de la money virtuel se déblocant en tuant des virus, cette monnaie sert à ouvrir des loots box (stade 1, 2, 3 plus en plus chère mais meilleur est le module d'extension) permettant d'avoix aléatoirement un module d'extension

Un shop qui affiche 5 article qu change toute les 3 mins permet d'acheter des extensions mais plus chere que d'ouvrire une loot box

Evenement :

Spawn aléatoirement des plaque de préssion de couleur définie le dossier devra se poser dessus pour éviter de recevoir des malus



Apparition des virus qui apparaisse des rebord de la page web

Apparition des virus qui peuvent sortir d'un adware

—----------

BackdoorBazar : acheter pare-feu, antivirus, configurations de pare-feu et pour antivirus, …

Interface pour voir le contenu des dossiers.

Les virus peuvent entrer dans un dossier et attaquer un fichier spécifique.

Les defenses peuvent etre déplacée en dehors du dossier ou dans un autre dossier.

Tous les gains en jeu monnaie non payants CHF, sera remis en jeu dans le dossier de départ, Si un spyware réussi a voler au maximum 10% de la monnaie total du joueur, la monnaie est perdu si le joueur ne la pas tué a temps. ratio si 1000 credit le spyware peut prendre 10% ce qui fait 100 monnaie mais en 100 secondes.

Catégories de virus (du plus gentil au plus méchant)

- **Adware (logiciels publicitaires)** **Pop up**

appuyer sur la croix, les boss seront plus difficile a fermer.

  - **Description :** Bien que souvent moins nuisibles que les autres types de virus, les adwares affichent des publicités non désirées sur un ordinateur. Certains peuvent être considérés comme des virus s'ils perturbent fortement l'expérience de l'utilisateur.

- **Spyware (logiciels espions)** **Vol de monnaie**

  - **Description :** Ces programmes malveillants collectent discrètement des informations sur un utilisateur sans son consentement, comme des mots de passe, des habitudes de navigation, des informations personnelles, etc. Certains peuvent se comporter comme des virus dans le sens où ils s'infiltrent dans le système.

- **Virus de fichiers** **Blocage utilisation arme, bouclier…, possible blocage du marché**

  - **Description :** Ces virus infectent les fichiers exécutables (.exe, .com, .bat, etc.). Lorsqu'un fichier infecté est lancé, le virus se propage et peut infecter d'autres fichiers sur le même système ou d'autres systèmes si le fichier est transféré.

- **Virus de macro**

  - **Description :** Ils infectent des documents contenant des macros (comme les fichiers Microsoft Word ou Excel). Ces virus s'activent lorsqu'un document infecté est ouvert et la macro est exécutée.

- **Rogueware (Faux antivirus)** **affecte le marché**

  - **Description :** Ce type de virus se présente comme un logiciel antivirus légitime, mais il est conçu pour tromper les utilisateurs afin qu'ils achètent une version complète qui n'offre aucune protection réelle.

- **Virus de réseau** **dropé par les vers -> virus random spyware, adware, virus de fichier**

(pare-feu ?)

  - **Description :** Ces virus se propagent principalement via les réseaux informatiques, en exploitant des failles de sécurité dans les systèmes pour infecter plusieurs ordinateurs connectés au même réseau.

- **Vers (Worms)** **est affecté par le pare-feu**

  - **Description :** Contrairement aux virus classiques, les vers ne nécessitent pas d'hôte pour se propager. Ils exploitent les failles de sécurité des systèmes et des réseaux pour

se répliquer et se propager d'un ordinateur à l'autre, souvent sans interaction de l'utilisateur.

- **Trojans (Chevaux de Troie)**

  - **Description :** Bien qu'il s'agisse d'un type de logiciel malveillant distinct, les chevaux de Troie sont souvent inclus dans la catégorie des virus en raison de leur capacité à se dissimuler sous une apparence innocente. Ils ne se répliquent pas comme un virus, mais permettent l'accès à un système pour d'autres formes de logiciels malveillants.

- **Botnets** attaquer le pare-feu

  - **Description :** Ce sont des réseaux d'ordinateurs infectés par des virus et contrôlés à distance par un cybercriminel. Les ordinateurs infectés (appelés « bots ») peuvent être utilisés pour envoyer des spams, mener des attaques DDoS, ou effectuer des activités malveillantes sans que les utilisateurs en soient conscients.

- **Virus polymorphes** change sous n'importe quelle forme de virus

configuration spéciale pour antivirus pour se protéger

  - **Description :** Ce type de virus modifie son code à chaque infection, ce qui rend son identification plus difficile par les logiciels antivirus traditionnels. Ils changent constamment pour éviter d'être détectés.

- **Virus d'amorçage (Boot sector virus)**

  - **Description :** Ces virus infectent le secteur de démarrage d'un disque (disque dur, clé USB, etc.). Ils se lancent au démarrage de l'ordinateur avant que le système d'exploitation ne soit chargé, rendant leur élimination plus compliquée.

- **Virus métamorphes**

  - **Description :** Semblables aux virus polymorphes, mais ils changent non seulement leur code, mais aussi leur structure de manière plus complexe. Ils sont plus difficiles à détecter et à désinfecter.

- **Rootkits**

  - **Description :** Ces virus sont conçus pour masquer d'autres logiciels malveillants, souvent à un niveau très profond dans le système d'exploitation. Leur but est de permettre à un attaquant d'avoir un accès non autorisé à un système sans être détecté.

- **Ransomware (Rançongiciels)** Prends en otage un dossier

  - **Description :** Ce type de logiciel malveillant prend en otage les fichiers d'un utilisateur ou d'une organisation en les cryptant, et exige une rançon pour les décrypter. Bien qu'il soit souvent classé comme un virus, son objectif spécifique (extorsion de fonds) le distingue.

📦 Caractéristique du dossier génésis

- Nombre de point de vie 200
- Contient des fichiers leurre
- Stockage de modules pour pare-feu/antivirus
- Peut héberger un virus
- Skin du dossier selon ses points de vie
- Fichier de base QuantumCash.wallet non modifiable par le joueur, possible répartition de l'argent sur plusieurs dossiers pour minimiser la perte
- Module de réparation automatique (selon un objectif ?)
- **Renforcement du skin du dossier** : Le dossier pourrait se renforcer au fur et à mesure de la progression, gagnant une "armure" qui réduit les dégâts reçus des virus.
- **Effet de synergie avec d'autres dossiers** : Si le dossier Genesis est placé près d'un autre dossier, une synergie spéciale pourrait apparaître, comme une régénération accrue des points de vie ou une meilleure défense

Module de protection avancé

- **Extension de module** : Un module spécial peut être ajouté au dossier Genesis, comme un **"Quantum Shield"** qui absorbe une certaine quantité de dégâts avant de se désactiver.

📦 Caractéristique d'un dossier supplémentaire

Les dossiers supplémentaires ont des bonus/malus chacun différent et apportent une vulnérabilité différente.

Virulence accrue des virus dans ce dossier : Les dossiers supplémentaires pourraient héberger des versions plus puissantes des virus. Par exemple, un virus dans un dossier supplémentaire pourrait avoir un comportement plus agressif, rendant l'attaque plus difficile à contrer.

- Nombre de point de vie 200
- Contient des fichiers leurre
- Stockage de modules pour pare-feu/antivirus
- Peut héberger un virus
- Skin du dossier selon ses points de vie
- Fichier de répartition Save.wallet
- Contient un fichier Récompense.docx

- Apparition d’un dossier tous les 3 min (max 4 sur le terrain)
    - **Déblocage de récompenses exclusives** : Le fichier "Récompense.docx" pourrait être un fichier dynamique, avec des récompenses qui évoluent en fonction des actions du joueur (par exemple, tuer un type particulier de virus, ou réussir une mission sans perdre de dossiers).
    - **Récompenses pour les missions secondaires** : Des missions ou objectifs secondaires pourraient être créés pour chaque dossier supplémentaire, permettant de gagner des récompenses sous forme de nouveaux modules ou des bonus de défense.

🛡️ Protection dans les dossiers

- **Antivirus :** Selon les modules installés, placé dans un dossier, seul lui peut éliminer le virus au bout d’un certain temps.
- **Le joueur ne peut pas supprimer un virus dans un dossier** autrement qu’avec un antivirus.

🛡️ Pare-feu

1. Placé à l'extérieur (Zone Globale)

    - **3 à 5 emplacements pour modules** (à régler pour l'équilibre du jeu)
    - **PV de base :** 50 PV

        - Le pare-feu dans cette configuration représente une protection générale, donc il n’est pas aussi robuste qu’un pare-feu spécifique placé dans un dossier, mais il a l'avantage de couvrir une zone large.

    - **Caractéristiques :**

        - **Défense contre les attaques multiples :** Ce pare-feu peut subir des attaques de manière continue (par exemple, des virus ou des tentatives d’intrusion sur plusieurs fichiers en

même temps) et a une résistance moyenne.

- **Régénération :** Il pourrait avoir une régénération lente (par exemple, récupérer 1 PV toutes les 5 secondes) une fois qu'il a été endommagé ou épuisé. Cette régénération lente est un mécanisme qui permet de ne pas rendre le joueur trop dépendant de ce type de protection.

- **Limitations :**

  - **Si le pare-feu atteint 0 PV,** il est désactivé pendant un certain temps (ex : 10-15 secondes) avant de pouvoir se régénérer. Cela laisse le joueur vulnérable, forçant la gestion stratégique de la protection.

Placé dans un Dossier (Protection Renforcée)

- **PV de base : 100 PV**

  - Ce pare-feu offre une protection renforcée, adaptée à un dossier important ou critique. Il représente une zone plus sécurisée, mais cela vient avec des avantages et des risques spécifiques.

- **Caractéristiques :**

  - **Protection forte :** Ce pare-feu est capable de bloquer plusieurs attaques et d'absorber plus de dégâts que le pare-feu général. Cela fait de lui une solution idéale pour les dossiers importants.

  - **Régénération active :** Une fois placé dans un dossier, le pare-feu peut se régénérer activement, et cette régénération est plus rapide que pour le pare-feu externe.

    - Par exemple, le pare-feu dans le dossier pourrait récupérer 2 PV par seconde, mais il ne peut pas régénérer au-delà de ses 100 PV initiaux.

        - **Bonus de régénération :** Si le pare-feu est intact pendant un certain temps (par exemple, après 10 secondes sans être attaqué), sa régénération pourrait devenir plus rapide (par exemple, 3 PV par seconde pendant 5 secondes) pour encourager une gestion proactive.

- **Limitations :**

    - **Si ce pare-feu est éliminé,** il faudra déplacer ou remplacer le pare-feu dans le dossier, et il faudra attendre qu'un nouveau pare-feu soit mis en place ou que le précédent se régénère de manière plus lente pendant cette période.

🔍 Antivirus

- **2 à 4 emplacements pour modules** (à régler pour l'équilibre du jeu)

Placer dans un Dossier :

- Les modules antivirus doivent être placés dans un dossier spécifique pour activer leurs effets. Une fois placés, ces modules peuvent scanner le contenu du dossier à la recherche de virus. Chaque module a une durée d'activation ou temps de réactivation différent, et certains d'entre eux nécessitent un certain temps pour éliminer les menaces.
- **Antivirus :** Placé en dehors d'un dossier, attaque de zone

Élimination des Virus

Lorsqu'un virus est présent dans un dossier, il faut du temps pour que l'antivirus (et ses modules) le **détecte** et le **supprime**. Selon le module utilisé, le temps et les méthodes d'élimination peuvent varier :

- **Antivirus Basic** : Le virus est nettoyé après **5 sec**.
- Lors de l'apparition d'un **virus polymorphe**, l'antivirus doit **sortir du dossier** pour activer des capacités de détection avancées.

⚔️ **Attaque** (Armes)

Modules d’attaque possibles à mettre dans un dossier:

- **Souris balistique :** Logiciel place des croix sur le terrain qui supprime les bugs
- **Thermal paste** : ralenti l'ennemi dans la zone et leur fait des dégâts
- **Outlook Canon :** Tire des e-mails mines
-
- **Arc plasma :** suis l'ennemi puis reviens au dossier (similaire au boomerang de bloon td6)
- **Lag Spike :** Fonctionne comme le laurier mais il téléporte le virus
- **Electro arc** : Pose des tourelles qui sont reliés entre eux à la chaîne

- **DirectX Beam :** inflige des dégâts continus, tire en ligne droite
- **Blue screen Grenade**

- **Module scanner :** repère les virus invisibles
- **BitLocker Shield :** Bouclier crypté, absorbe les dégâts pendant un temps limité.

💡 Synergies

Synergie	Modules Combinés	Effet / Comportement
Parfait contre les virus polymorphes	Deep Packet Scanner (pare-feu) + Signature Updater (antivirus)	Améliore la détection et l'élimination des virus polymorphes, rendant les deux modules complémentaires dans la lutte contre des virus difficiles à identifier.
Bouclier optimisé contre les vers et virus de réseau	Network Choke (pare-feu) + Overclocked Nodes (pare-feu)	Réduit la vitesse de propagation des vers et optimise le temps de recharge du pare-feu, créant une défense plus rapide et plus efficace contre les attaques de virus en réseau.
Détection maximale, même des virus invisibles dans les dossiers	Cloak Detector (antivirus) + Heuristic Hunter (antivirus)	Permet de détecter des virus camouflés ou en veille, offrant une détection avancée et une couverture complète contre les menaces invisibles.
Combo défensif ultime contre les ransomware et attaques critiques	Anti-Ransom Protocol (antivirus) + Core Guardian (antivirus)	Blocage des ransomwares avant qu'ils ne compromettent les dossiers et protection renforcée des fichiers critiques, offrant une défense puissante contre les attaques de ransomware.

💰 Économie et loot

Monnaie virtuelle QuantumCash gagnée en tuant des virus

Monnaie utilisée pour **:**

- **Loot box** (niveau 1 à 3, de plus en plus chères et puissantes)
- **Shop** (5 articles changent toutes les 3 minutes, + cher que loot box)

La monnaie est déposée au sol, peut être volée par un spyware qui la ramasse.

🔄 Mécaniques qui obligent à déplacer les dossiers

1. ⚡ Zones de surcharge virale (zones rouges temporaires)

- **Des zones sur le bureau deviennent instables (clignotantes en rouge), générant un champ de corruption toutes les X secondes.**
- **Si un dossier reste dans cette zone trop longtemps :**
  - **Il perd des PV passivement.**
  - **Les virus y deviennent invisibles / plus puissants.**
- **But : obliger le joueur à bouger régulièrement ses dossiers pour éviter une infection inévitable.**

2. 💲 Récupérer la monnaie : Le dossier qui contient le fichier **QuantumCash.wallet** doit être déplacé pour récupérer la monnaie.

3. 🟦 Plaques de pression bonus/malus (déjà mentionnées) — approfondissement

- Ces plaques apparaissent aléatoirement, et le joueur **doit déplacer un dossier dessus dans les 10 secondes** :
    - 💎 Bonus : +QuantumCash, +module gratuit, buff temporaire de défense. ?? a voir
    - 💀 Si ignorée : spawn de virus autour du dossier le plus riche.

4. 🧲 Attracteurs de données (hameçons numériques)

- De faux fichiers apparaissent : "FreeBoost.exe", "RewardsPack.zip", etc.
- Si un **dossier va dessus**, le joueur peut obtenir :
    - un **module d'extension rare**
    - une **récupération de monnaie perdue**
    - ou… un **virus déguisé (trojan)**
- Encourage le joueur à **prendre des risques et bouger ses dossiers**, au prix d'une potentielle infection.

🔧**BackdoorBazaar.exe** (loot genshin)

Permet d'obtenir :

- Pare-feu
- Antivirus
- Configurations personnalisées
- Fichiers leurre
- Améliorations de défense ou d'économie
- Interface
- Amélioration pour l'interface

- Visualiser le contenu des dossiers
- Déplacer les défenses entre dossiers
- Pouvoir déplacer les dossiers

Modules pour Antivirus

Nom du module	Rareté de base	Effet / Comportement	Placement dossier
Antivirus Basic	1	Nettoie automatiquement un virus présent dans le dossier après 5 sec.	Intérieur
Behavioral Scanner	1	Réduit le temps de scan à 3 sec pour les virus connus (spyware, adware, fichiers).	Intérieur
Signature Updater	2	Augmente la vitesse de détection des nouveaux types de virus (ex. : polymorphe).	Extérieur
Heuristic Hunter	3	Peut détecter des virus même non activés (macro, Trojan en veille).	Extérieur
Anti-Ransom Protocol	3	Permet de bloquer un ransomware avant qu'il ne prenne un dossier en otage (une fois par partie).	Extérieur
Pulse Antivirus	2	Dégâts en AOE (zone), 1 fois toutes les 10 secondes. Utile en dehors des dossiers.	Extérieur
Code Purifier	4	Élimine instantanément tous les virus de rareté 1 ou 2 dans le dossier en 2 secondes.	Intérieur
Cloak Detector	2	Dévoile les virus camouflés (invisibles), utile contre Rootkits et	Intérieur

		virus réseau.	
Core Guardian	4	Si placé dans le dossier principal, protège tous les fichiers pendant 15 sec après attaque. Recharge lente.	Intérieur

🔥 Modules pour Pare-feu

Nom du module	Rareté de base	Effet / Comportement	Placement
Firewall Basic	1	Pare-feu standard : bloque les vers et ralentit les virus réseau.	Extérieur
Deep Packet Scanner	1	Identifie les virus polymorphes et métamorphes qui traversent le pare-feu.	Extérieur
Adaptive Barrier	2	Le pare-feu adapte son blocage selon les types de virus récents (dernier type détecté).	Extérieur
Overclocked Nodes	2	Réduit le temps de rechargement du pare-feu (plus rapide à bloquer des vagues successives).	Extérieur
Electro Trap	3	Le pare-feu inflige des dégâts mineurs aux virus qui tentent de le traverser.	Extérieur
ICE Spike	3	Ralentit massivement les virus touchés + chance de les "geler" (0,5 sec).	Extérieur
Quantum Firewall	4	A une chance (20%) de "téléporter" un virus vers un rebord aléatoire (reboot de sa trajectoire).	Extérieur
Botnet Breaker	3	Réduit l'efficacité des attaques coordonnées de botnets (affaiblit leur attaque de zone).	Extérieur
Network Choke	2	Réduit la vitesse de propagation des vers dans un rayon de 3 unités autour.	Extérieur

🦠Viruses

Catégorie de Virus	Description	Comportement du Virus	Comment le Contrer	Récompense 💰	Dégâts au dossier
Adware (Logiciels publicitaires)	Affiche des publicités non désirées sous forme de pop-ups.	Gène l'expérience de l'utilisateur, affiche des publicités, certains les boss sont difficiles à fermer.	Fermer sur le X, les boss faut trouver. Utiliser un **module antivirus** de détection de logiciels publicitaires et un **pare-feu** pour bloquer les connexions indésirables. Utiliser **Behavioral Scanner** (Antivirus) et	1-3 QuantumCash Les boss 5-8	

			Firewall Basic (Pare-feu).		
Spyware (Logiciels espions)	Collecte des informations personnelles sans le consentement de l'utilisateur (mots de passe, habitudes de navigation, etc.).	Vol de monnaie	Utiliser **Cloak Detector** (Antivirus) et **Heuristic Hunter** (Antivirus).	10 QuantumCash de base. S'il a volé de l'argent sur le sol ou dans un dossier, alors si pare-feu installé avec module anti-spyware (récupération total de l'argent qu'il a pris)	
Virus de fichiers	Infecte les fichiers exécutables (.exe, .com, .bat, etc.).	Blocage utilisation arme, bouclier…, possible blocage du marché	Utiliser **Pulse Antivirus** (Antivirus).	💡 Module d'attaque de base ou crédits 20-30.	
Virus de macro	Infecte les documents contenant des macros (ex. : fichiers Word ou Excel).	S'active lorsque le document infecté est ouvert et exécute la macro malveillante. Récompense.docx	Utiliser **Behavioral Scanner** (Antivirus) et **Heuristic Hunter**	📦 Module utilitaire aléatoire (support/défense).	
Rogueware (Faux antivirus)	Se fait passer pour un antivirus légitime, mais est conçu pour tromper l'utilisateur et lui faire acheter une version payante inutile.	Trompe l'utilisateur pour qu'il achète une version payante sans protection réelle.	Utiliser **Code Purifier** (Antivirus) et **Deep Packet Scanner** (Pare-feu).	40-50 + chance de rare drop (module rare).	

Virus de réseau	Se propage via les réseaux informatiques, en exploitant des failles de sécurité.	Se propage à travers un réseau, infecte plusieurs systèmes connectés, souvent difficile à détecter en raison de son caractère invisible.	Utiliser **Botnet Breaker** (Pare-feu) et **Network Choke** (Pare-feu).		
Vers (Worms)	Se réplique et se propage sans interaction de l'utilisateur.	Se propage automatiquement sans interaction de l'utilisateur, exploite les failles de sécurité pour infecter d'autres systèmes.	Utiliser **Firewall Basic** (Pare-feu).		
Trojans (Chevaux de Troie)	Se dissimule sous une apparence innocente et permet l'accès à un système pour d'autres formes de malwares.	Ne se réplique pas mais ouvre un accès non autorisé à d'autres malwares.	Utiliser **Heuristic Hunter** (Antivirus) et **Cloak Detector** (Antivirus).		
Botnets	Réseau d'ordinateurs infectés contrôlés à distance par un cybercriminel.	Utilise des ordinateurs infectés pour lancer des attaques DDoS, envoyer des spams ou effectuer d'autres actions malveillantes.	Utiliser **Botnet Breaker** (Pare-feu).		

Virus polymorphes	Modifie son code à chaque infection pour éviter la détection par les antivirus.	Change constamment de forme pour éviter d'être détecté par les antivirus traditionnels.	Utiliser **Signature Updater** (Antivirus) et **Deep Packet Scanner** (Pare-feu).		
Virus d'amorçage (Boot sector virus)	Infecte le secteur de démarrage d'un disque dur, clé USB, etc.	S'active au démarrage du système, avant même le chargement de l'OS, rendant son élimination difficile.	Utiliser **Code Purifier** (Antivirus).		
Virus métamorphes	Change non seulement son code mais aussi sa structure pour éviter d'être détecté.	Modifie continuellement son code et sa structure pour se rendre indétectable par les antivirus classiques.	Utiliser **Signature Updater** (Antivirus) et **Heuristic Hunter** (Antivirus).		
Rootkits	Masque d'autres malwares à un niveau profond du système d'exploitation.	Permet à l'attaquant d'avoir un accès non autorisé tout en restant indétecté.	Utiliser **Cloak Detector** (Antivirus).		
Ransomware (Rançongiciels)	Prend en otage les fichiers d'un utilisateur en les cryptant, exigeant une rançon pour les décrypter.	Crypte les fichiers et demande une rançon pour les décrypter, rendant les données inaccessibles sans paiement.	Utiliser **Anti-Ransom Protocol** (Antivirus) et **Core Guardian** (Antivirus).		

Système de Progression Long Terme : Cyber Survivors

⏱ Durée d'

une partie30 minutes, avec une difficulté progressive, de plus en plus intense, avec :

- des **paliers de menace** tous les 5 minutes (nouveaux types de virus, nouvelles mécaniques)
- des **récompenses croissantes** pour la survie longue
- des **classements (mode classé hebdomadaire)** optionnels

Gameplay v2

🧬 Factions

Les factions représentent des **origines de cybersécurité**. Chacune donne un **bonus passif**, des **apparences uniques** et **des modules exclusifs** :

Faction	Style	Bonus passif	Exemple de module exclusif
Quantum Watch	High-tech défensif	+10% PV sur tous les pare-feux	Quantum Firewall Overdrive
DeepTrace	Détection furtive	+20% vitesse de détection des virus cachés	Signature Auto-Indexer
NetSec Syndicate	Aggressif offensif	+15% dégâts infligés par les modules d'attaque	Lag Spike Mk II
GreyCloud	Économie & contrôle	+25% de QuantumCash récupéré	CrytoSiphon (vole la monnaie des virus)

🧑‍💼 Rôles de joueur

Chaque joueur choisit un **rôle à chaque partie**, qui oriente ses modules, sa stratégie et ses compétences :

Rôle	Description	Bonus principaux
Defender	Renforce les dossiers	+PV +vitesse de réparation
Operator	Spécialiste modules	+emplacements de modules
Hunter	Axé combat virus	+dégâts armes, +détection
Tech-Merchant	Économie et loot	Réduction prix shop, drop bonus

---

🛠️ Métiers (permanents, progression entre les parties)

Les métiers offrent des **capacités passives** et **crafts** via QuantumCash ou ressources lootées :

Métier	Fonction principale	Exemple
Cryptologue	Améliore antivirus	Crée un scanner modifié détectant virus dormants
Firewall Engineer	Renforce pare-feux	Module ICE Spike renforcé
Code Broker	Gère les loots	Convertit QuantumCash en loot rare
Archiviste	Optimise stockage	Réduit temps de recharge modules

---

🌲 Arbre de compétences (personnage)

Système à 3 branches, progressif entre les parties. Chaque **niveau** donne 1 point à répartir.

- **Sécurité active** : +PV, +régen pare-feu, +slots de modules
- **Contre-mesures** : +dégâts armes, -CD antivirus, dégâts AoE
- **Réseau & loot** : +QuantumCash, shop réduit, bonus sur plaques