# PYTHON: LES MALWARES

DR. CHRISTIAN ADJA

# SOMMAIRE

- Intro:
  - Les libraires OS et SyS
  - Exercices
- Les malwares

# LES LIBRAIRIES STANDARDS

- Les librairies sont très importantes en python car elle permettent d'ajouter de nouvelles fonctionnalités.
- Comment utiliser une libraire?
  - Avec la keyword "import" pour les librairies standard
    - « import sys »
    - « import os »
  - Avec la keyword « from » pour importer a partir d'un paquet
    - from x import y

# LES LIBRAIRIES PERSONNELLES

- Python permet a tous développeurs de créer sa propre libraire
  - Une libraire est fichier (.py) qui contient des classes et/ou des fonctions
  - Ce fichier est appelé a travers un « import »
    - Ex: module.py
    - Import module
  - Le fichier peut se trouver:
    - À l'intérieur du même répertoire que celui du fichier appelant
    - Ou ailleurs
      - Il faut dans ce cas l'inclure dans la variable d'environnement PYTHONPATH

# LES VARIABLES D'ENVIRONNEMENT

Les variables d'environnement **sont des chaînes qui contiennent des informations sur l'environnement pour le système, et l'utilisateur ayant une session en cours.**

- Vous pouvez accéder aux variables d'environnement à travers la librairie OS
  - import OS
  - os.environ
    - C'est un dictionnaire dans lequel vous trouvez la liste et le contenu des variable d'environnement système
    - Ex os.environ['PATH']
      - Pour accéder à la variable PATH
    - Il est aussi possible de modifier les variables
      - os.environ['nomVariable']=Valeur

# LES OPTIONS

Python permet de récupérer dans le code les options données pour l'exécution d'un programme

- Ex
  - ./script.py sqy mcs 24.1
- Nous récupérons les options ainsi
  - import sys
  - nomprogramme= sys.argv[0]
  - site = sys.argv[1]
  - promo = sys.argv[1]
  - Print("Nom du programme : ",nomprogramme, "site : ", site, "Promo : ",promo)

# LA DATE

Python mets à disposition des primitives qui permettent d'obtenir la date actuelle sous plusieurs formats

- Obtenir la date actuelle dans le format d'une estampille temporelle
  - time()
- La date actuelle
  - from datetime import date, time, datetime
  - datetime.now()
  - today = date.today()
  - today.day
- Geler l'exécution d'une partie ou de tout le code pendant un certain moment
  - sleep(n)

# GESTION DES FICHIERS

- Création de fichier
  - file_object = open("filename","mode")
  - file = open('test.txt','a')
- Modifier, ajouter du contenu
  - file.write(data)
- Pour lire un fichier
  - Data = file.read(dataQuantity)
- Fermeture d'un fichier
  - file.close()

| Modes | Définition |
|---|---|
| r | Lecture |
| r+ | Lecture et écriture |
| rb+ | Lecture et écriture binaire |
| w | Ecriture. Le fichier est créer s'il n'existe pas et écrasé s'il existe déjà |
| w+ | Ecriture et lecture |
| a | Modification. Le fichier est crée s'il n'existe pas et mis en mode écriture. Les données ne sont pas écrasées si le fichier existe, mais plutôt actualisé. |
| a+ | Lecture et écriture. Le fichier est crée s'il n'existe pas et mis en mode écriture. Les données ne sont pas écrasées si le fichier existe, mais plutôt actualisé. |
| x | A partir de python 3! Le mode x ouvre le fichier pour une création exclusive, à défaut si le fichier portant ce nom existe déjà. Lorsque la création exclusive est spécifiée, cela signifie que ce mode ne créera pas de fichier si le fichier portant le nom spécifié existe déjà. En mode x, le fichier est uniquement accessible en écriture, mais en mode x+, le fichier est ouvert à la fois lisible et inscriptible. |

# GESTION DES FICHIERS

- Ex:
  - file= open("test.txt","w+")
  - file.write("Bonjour 2021 ")
  - file.close()

# LA LIBRAIRIE OS

- Lister un répertoire
  - import os
  - os.listdir(path)
- Afficher le répertoire courant
  - import os
  - os.getcwd()
- Exemple
  - import os
  - dirs=os.listdir(os.getwd())
  - for dd in dirs:

        print(dd)

# LA LIBRAIRIE OS

- Changer de répertoire
  - import os
  - os.chdir('/tmp')
- Renommer un fichier
  - import os
  - os.rename(src,dst)
- Détruire un fichier
  - import os
  - os.remdir(« nomRepertoie »)

# LA LIBRAIRIE OS

- Vérifier l'existence d'un fichier
  - import os.path as path
  - path.exists(file fullpath)
- Vérifier si c'est un répertoire
  - import os.path as path
  - path.isdir(« nomFichier »)
- Vérifier si c'est un fichier
  - import os as path
  - path.isfile(« nomFichier »)

# LA LIBRAIRIE OS: GESTION D'UN TERMINALE (LINUX)

Python mets à disposition des primitives pour créer et/ou fermer des terminaux.

- os.system()

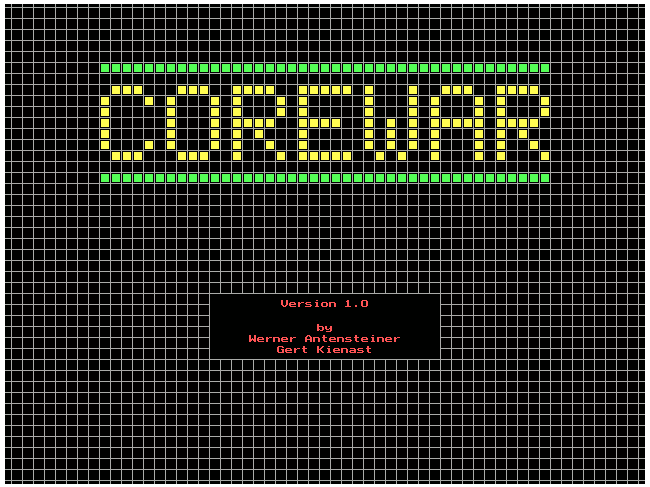
```
import os
os.system('gnome-terminal – sh -c "ls ;bash"')
os.system('xterm – sh -c "cwd ;bash"')
os.system('gnome-terminal – sh -c ";bash"'.format(commandName))
```

# LES MALWARES

**Def:** un malware (logiciel malveillant) est une catégorie de programmes plus ou moins autonomes visant à modifier le fonctionnement normal d'un ordinateur de façon plus ou moins grave. C’est-à-dire virus informatique, vers, cheval de Troie, ransomware, spyware, adware, scareware, etc.

# LES MALWARES: FONDAMENTEAUX

- Années 60 : Jeu core Ware
  - Le principe consiste à implanter dans la mémoire d'un ordinateur deux programmes qui vont alors, sans aucune intervention humaine, lutter l'un contre l'autre en cherchant à se localiser et à se détruire mutuellement. Chaque programme peut en outre se défendre en s'autoréparant en cas de dommage causé par l'adversaire, et en se dupliquant dans la mémoire. La partie est terminée lorsque l'un des joueurs a perdu tous ses programmes ou si ceux-ci ont été modifiés au point d'être rendus inactifs.
- 1972 : deux dérivés de Core War , Darwin et Worm.
- …



# LES MALWARES: ACTEURS ET OBJECTIFS

- Agir contre les exigences de l'utilisateur de l'ordinateur
- Peuvent être utilisés
  - par des cybercriminels (pirates, ecc )
  - Des gouvernements
- Pour:
  - voler des renseignements personnels, financiers ou commerciaux
  - À des fins de sabotage
  - Des motivations politiques et idéologique

# LES MALWARES: MÉTHODES D'INFECTION

- Bugs logiciels
  - Par exploitation des failles de sécurité des systèmes ou logiciels applicatifs
- Ingénierie sociale et erreurs d'utilisation
  - Par intégration de fichiers exécutables associés à des programmes légitimes
- Vulnérabilités du système d'exploitation
  - Par l'exploitation des vulnérabilités des systèmes d'exploitation

# LES MALWARES: STRATÉGIE DE DISTRIBUTION

- Réseaux sociaux
  - Utilisation de faux comptes pour transmettre des chaînes d'e-mails et des liens malveillants, partager des contenus inappropriés ou usurper des identités d'utilisateurs à des fins malveillantes
- Sites web contrefaits
  - Par utilisation d'un site Web pour télécharger et installer des scripts malveillants chez les visiteurs
- Jeux en ligne
  - Par intégration de jeux en ligne, en particulier ceux destinés aux jeunes enfants. Ainsi les utilisateurs l'utilisateur à cliquer et à accepter une condition quelconque pour continuer
- Publicités en ligne
  - Par infection des utilisateurs par la simple d'un site web, même légitime.

# LES MALWARES: LES TYPES

Les malwares sont définis par leur intention malveillante, il existe donc plusieurs types de malware

- Spywares (logiciel espion)
  - Logicielle conçu pour surveiller les actions de la victime
- Ransomwares
  - Ces logicielles affectent d'une manière ou d'une autre un Système Informatique et exigent un paiement pour le ramener à son état normal
- Rootkit
  - Ce malware permet au pirate d'installer une série d'outils pour accéder à distance à l'ordinateur hacké.

# LES MALWARES: LES TYPES

Les malwares sont définis par leur intention malveillante, il existe donc plusieurs types de malware

- Virus
  - C'est un programme contagieux qui infecte un logiciel et se propage de fichier en fichier sur un système
- Le ver
  - Le vers est un logicielle qui se propage comme un virus lorsqu'ils infectent un ordinateur
- Le cheval de Troie
  - C'est un malware déguisé en programme fiable conçu pour tromper les utilisateurs de sorte qu'ils l'installent sans le vouloir sur leur propre système

# LES MALWARES: LES TYPES

Les malwares sont définis en fonction d'ou ils logent:

- Malwares de programmes
  - ajoutent leur code à celui d'un programme présent sur le disque dur(ou autre support) ou en le remplaçant une partie
- Malwares du système
  - En raison de la manière dont le système d'exploitation démarre et prend le contrôle des disques, les premiers secteurs du disque dur (secteur de la table de partition et secteur d'amorçage) peuvent contenir un bout de code exécutable.
  - Il faudrait le fichier source du système d'exploitation soit infecté

# LES MALWARES: LES TYPES

Les malwares sont définis en fonction d'ou ils logent:

- Malwares de Macro
  - Les applications sophistiquées contiennent un langage de programmation qui permet d'automatiser des opérations complexes grâce à l'écriture de macro-instructions (connues sous le nom de macros) exécutées par l'application.
- Malwares de mails
  - L'apparition de ce type de programme a été rendue possible par le fait qu'on peut attacher à des mails des fichiers divers

# LES MALWARES: LES TYPES

Les malwares sont définis en fonction d'ou ils logent:

- Les Hoaxes
  - Un hoax (canular en français) est un message que vous recevez d'une personne inconnue ou d'un correspondant qui vous l'a fait suivre.

# LES MALWARES: LES DOMMAGES

Les dommages dépendent du type de virus qui vous a infecté:

- Destruction de données
  - Données chiffrées, effacés ou inaccessibles
- Vols d'informations personnels
  - Espionnage, vol de crédentiaux, etc
- Usurpation d'identité

# LES MALWARES: RANSOMWARES

- Ransom - ware ( rançon ) ?
  - C’est un logiciel d’extorsion qui peut verrouiller votre ordinateur et demander un rançon en échange du déverrouillage de celui-ci
  - Ce dernier bloque l'accès au système ou chiffre ses données
- Vos données ont de la valeur !

# LES MALWARES: RANSOMWARES

- Cibles
  - Systèmes d'exploitation
    - Linux
      - Linux.Encoder.1, hellokitty ransomware, ecc
    - Windows:
      - Cryptolocker, cryptowall 4, teslacrypt, hive, ecc
  - Entités
    - Hôpitaux
    - Services de polices
    - Entreprises
    - Utilisateurs

# LES MALWARES: RANSOMWARES

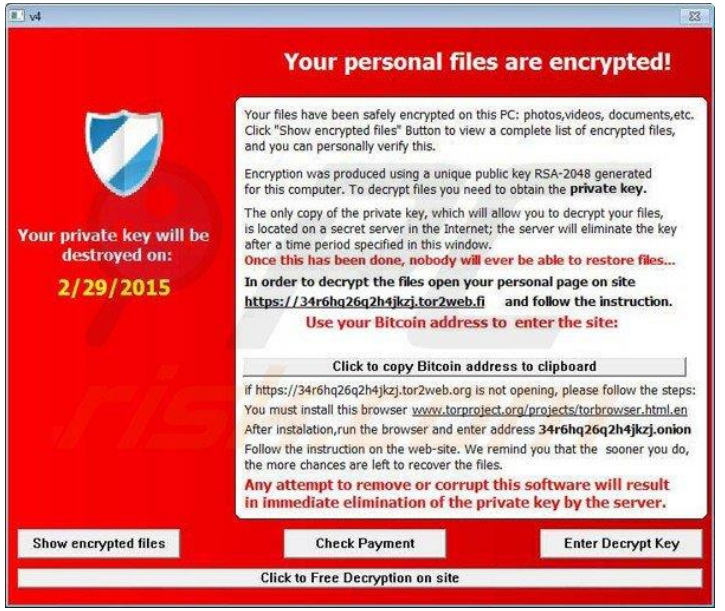
- Méthode d'infection
  - Infection de la cible
  - Analyse du système d'exploitation de la victime
  - Ciblage des fichiers à attaquer
  - Chiffrement des fichiers
  - Demande de rançon

# LES MALWARES: RANSOMWARES

- Il existe deux principales formes
  - **Le ransomware Locker**
    - Bloque l'accès aux fonctionnalités de base des victimes (refuser l'accès des administrateurs)
    - Moins dangereux car ne touche pas aux fichiers critiques du système
  - **Le ransomware Crypto**
    - Chiffre les données critiques des utilisateurs (documents images videos)

# LES MALWARES: RANSOMWARES

- TeslaCrypt
  - Détecté en février 2015
  - Il infecte le plus souvent les fichiers de l'univers des jeux: parties sauvegardées, profils d'utilisateurs, etc.
  - Ne chiffre pas les fichiers dont la taille excède 268 Mo
  - Les fichiers sont cryptés avec l'algorithme AES et la clé de déchiffrement est cryptée avec l'algorithme RSA-2048
  - Une rançon de 500 dollars est demandé
    - Cette rançon double en cas de retard de paiement

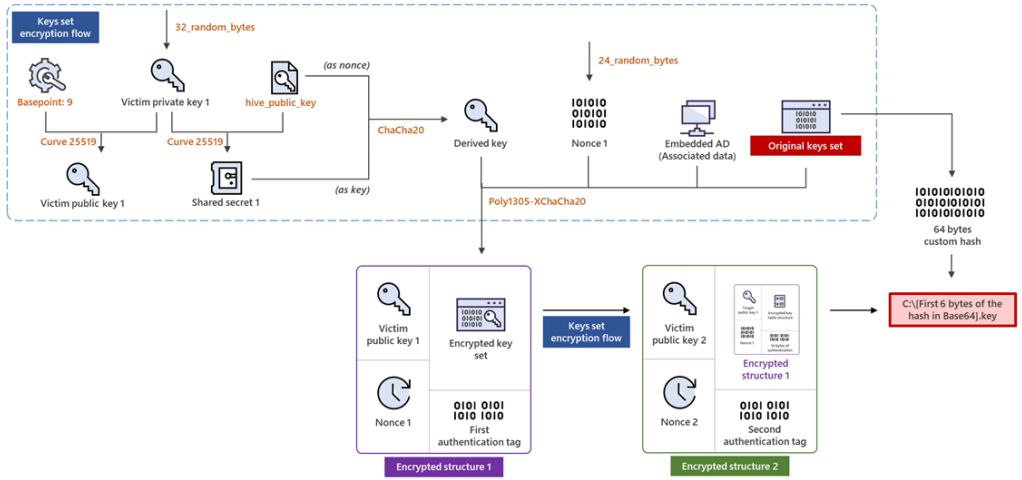


# LES MALWARES: RANSOMWARES

- Cryptowall 4.0
  - C'est cryptoware qui installe plusieurs copies de lui-même
  - Les données ne sont pas cryptés immédiatement après l'installation du malware
    - Il se connecte plutôt à un serveur externe pour récupérer les clés de chiffrements
  - Il utilise de AES pour chiffrer les fichiers
    - Vos fichiers ainsi que les noms des fichiers seront chiffrés
    - La clé de chiffrement sera elle-même chiffré par un clé asymétrique
  - Un message sout forme .html, .png, .txt est laissé dans chaque répertoire

# LES MALWARES: RANSOMWARES

- Hive
  - Le ransomware recherche les processus associés aux sauvegardes, à l'antivirus/antispyware et à la copie de fichiers et y met fin
  - L'extension *.hive* est ajout é aux fichiers cryptés
  - Un script *hive.bat* dans le répertoire courant, ce fichier va permettre de faire un nettoyage après le chiffrement. Le fichier est ensuite supprimé.
  - Un deuxième fichier shadow.bat est créer pour s'auto-supprimer ainsi que le malware lui-même
  - Une note « *HOW_TO_DECRYPT.txt* » est déposée dans chaque répertoire concerné



# LES MALWARES: RANSOMWARES

- Faire preuve de vigilance (mieux vaut prévenir que guérir)
  - Aux logiciels installés
  - Aux sites visités
  - Aux mails et etc.
- Utiliser de bon antivirus
  - Faire les actualisations
- Faire régulièrement des back-ups

# LES MALWARES: LES VERS

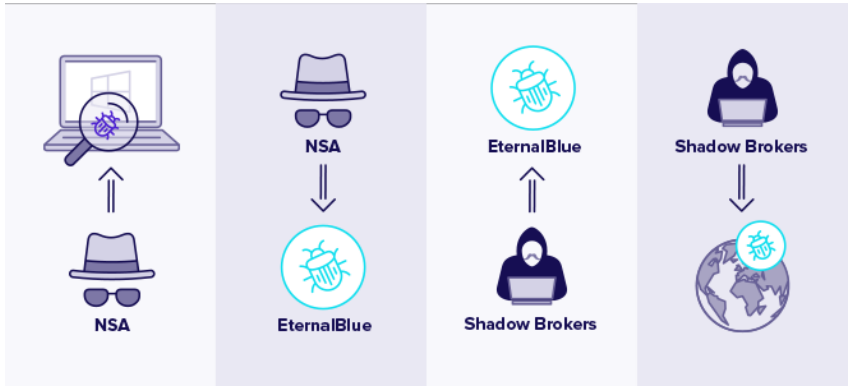
- Les vers sont très proches des virus, sauf qu'ils son autonomes
  - Pas de fichiers hôtes nécessaire, ni d'action de la victime
- Peuvent se répliquer et se propager sans impliquer l'action humaine
  - Ses capacités de réplication sont exponentielles
- L'infection s'effectue néanmoins par un fichier

# LES MALWARES: LES VERS

- Stuxnet (2010)
  - premier malware à avoir un effet sur des infrastructures physiques
  - Découvert par des experts en cybersécurité du Bélarus fin 2010
  - conçu et déployé pour attaquer les installations nucléaires iraniennes
    - ciblait les centrifugeuses nucléaires dans l'objectif de perturber le programme nucléaire
  - Une fois infiltré les installations, ce dernier s'est mis à la recherche des ordinateurs connectés aux contrôleurs programmables qui géraient les centrifugeuses et autres installations industrielles utilisées dans la production de combustible nucléaire militaire. Ensuite au code du contrôleur programmable pour faire en sorte que les centrifugeuses tournent trop vite et trop longtemps, tout en envoyant de fausses données pour donner l'apparence d'un fonctionnement normal.
  - Les ordinateurs n'étaient pas connectés a internet, comme le virus a –t'il pu les infectées?

# LES MALWARES: MENACES MIXTES

- WannaCry (avril 2017)
  - C'est une combinaison de vers et ransomware
  - Celui-ci infectait les ordinateurs via EternalBlue(CVE-2017-0144), l'exploit développé par la NSA
    - Windows non actualisé
  - L'infection de la cible était suivi par une demande de rançon et échange de restitution
  - Il était capable de se répliquer a travers le réseau
    - 10000 PC / par heure
    - 300000 ordinateurs dans 150 pays




Ref: https://www.lexpress.fr/actualite/monde/vague-internationale-de-cyberattaques_1907798.html

# LES MALWARES: LES VIRUS

- C’est un malware qui nécessite d’un hôte (fichier exécutable ou document) pour se propager
- Il exploite les ressources de son hôte pour se répliquer et se propager
- Le virus reste inactif jusqu’à ce que son utilisateur lance son exécution ou réalise une action spécifique

# LES MALWARES: CLASSIFICATION DES VIRUS

- Virus visant le secteur de démarrage
- Virus des scripts Web
- Détourneur de navigateur (browser hijacker)
- Virus résident
  - Un virus qui peut accéder à la mémoire de l'ordinateur et rester inactif jusqu'à ce qu'une charge utile soit délivrée est considéré comme un virus résident.
- Virus à action directe
  - inoffensif contenant un code malveillant, délivrent immédiatement une charge utile quand exécuté

# LES MALWARES: CLASSIFICATION DES VIRUS

- Virus polymorphe
  - Difficile à détecter et a supprimer par un antivirus
- Virus infecteur de fichiers
- Virus multipartite
  - Ces programmes malveillants se propagent sur un réseau ou d'autres systèmes en se copiant ou en injectant du code dans des ressources informatiques critiques
- Virus Macros

# LES MALWARES: VIRUS

- Dérangement
- Perte de performances informatiques
- Perte de données ou d'argent, vol d'identité
- Perte financière, atteinte à l'image de marque
- Attaques d'États-nations (à grande échelle)
- Le virus reste inactif jusqu'à ce que son utilisateur lance son exécution ou réalise une action spécifique

# LES MALWARES: LES ROOTKITS

- Ce sont des malwares conçu pour permettre à un intrus d'obtenir un accès non autorisé à un ordinateur ou à un réseau
- Facile a dissimuler et donc difficile à détecter
- La machine infecté devient une sorte de zombie et peut être totalement contrôlé a distance par l'attaquant

# LES MALWARES: LES ROOTKITS

- Une fois infecté, le rootkit est susceptible de modifier tous les éléments que l'administrateur est autorisé à modifier pour
  - Masquer des malwares
  - Obtenir un accès à distance
  - Modifier ou désactiver les programmes de sécurité
  - Voler des données
  - Créer une porte dérobée permanente (backdoors)
  - Vous espionner
  - Contraindre votre vie privée

# LES MALWARES: LES SPYWARE

- C’est un malware espion qui reste dissimulé pendant qu'il enregistre secrètement des informations et suit vos activités en ligne sur vos ordinateurs ou appareils mobile
  - Masquer des malwares
  - Obtenir un accès à distance
  - Modifier ou désactiver les programmes de sécurité
  - Voler des données
  - Créer une porte dérobée permanente (backdoors)
  - Vous espionner
  - Contraindre votre vie privée

# LIENS BIBLIOGRAPHIQUES


- https://www.pandasecurity.com/fr/security-info/infection-techniques/
- https://www.kaspersky.fr/resource-center/threats/ransomware
- https://www.oracle.com/fr/cloud/malware-logiciel-malveillant.html
- https://miashs-www.u-ga.fr/prevert/SpecialiteIHS/Documents/Securite-Malwares.pdf
- https://linux.developpez.com/actu/328427/Le-ransomware-Hive-chiffre-desormais-les-systemes-Linux-et-FreeBSD-mais-cette-variante-du-ransomware-est-encore-boguee-et-ne-fonctionne-pas-toujours/
- https://www.avast.com/fr-fr/c-eternalblue
- https://www.journaldunet.fr/web-tech/dictionnaire-du-webmastering/1445234-ver-informatique-definition-concrete-et-illustree/
- https://www.avast.com/fr-fr/c-rootkit
- https://www.proofpoint.com/fr/threat-reference/computer-virus
- https://www.avast.com/fr-fr/c-spyware