

# Sécurité pratique

## Chapitre 2: Logiciel malveillant (*malware*)

Printemps 2022

Profs. Marcelo Pasin

**haute école**  
neuchâtel berne jura



**ingénierie**  
[www.he-arc.ch](http://www.he-arc.ch)

# Logiciel malveillant (*malware*)

- Stallings & Brown, Chapitre 6
- Types de logiciels malveillants
- Propagation (contenu infecté, exploitation de vulnérabilités, ingénierie sociale)
- Exploitation (corruption, bots, vol d'information, abus des interfaces)
- Contre-mesures

# Objectifs d'apprentissage

- Être capable de :
  - Décrire trois mécanismes généraux de propagation des programmes malveillants.
  - Comprendre le fonctionnement de base des virus, des vers et des chevaux de Troie.
  - Décrire quatre grandes catégories de logiciels malveillants par rapport au type d'information compromise (*payload*).
  - Comprendre les différentes menaces posées par les bots, les logiciels espions et les *rootkits*.
  - Décrire des techniques de détection et de combat aux logiciels malveillants.

# Logiciel malveillant (*malware*)

- Programme inséré irrégulièrement dans un système, généralement de manière sournoise
- But : compromettre, nuire
  - Confidentialité
  - Intégrité
  - Disponibilité
  - Gêner, perturber
- Fonction : une attaque
  - Aux données
  - Aux applications
  - Aux système d'exploitation de la victime
- Importante menace pour les systèmes informatiques

# Types de logiciel malveillant

- Selon le mécanismes de propagation
  - Infection de contenus exécutables par des virus
  - Exploitation des vulnérabilités logicielles (locales ou réseau/*worms*)
  - Ingénierie sociale, contourner la sécurité (chevaux de Troie, *phishing*)
- Logiciels parasites ou indépendants
- Avec ou sans réplication
- Les actions sur les données
  - Corruption
  - Vol de service (zombie)
  - Vol d'informations
  - Furtivité (se cacher)
- Les logiciels malveillants travaillent sur plusieurs dimensions

# Propagation des logiciels malveillants

**Virus** : infection

**Ver** : exploitation de vulnérabilité

**Cheval de Troie** : ingénierie sociale

# Propagation par infection, virus

- Parasites accrochés à un logiciel existant
  - Des fragments de logiciel
  - Des macros dans un fichier non-exécutable à la base
- Lorsqu'il est exécuté, il infecte d'autres logiciels
- Infection passe d'un ordinateur à l'autre
  - Clé USB, email, partage réseau
- Composants:
  - Mécanisme d'infection (vecteur d'infection)
  - Déclencheur
  - Charge utile (*payload*)
- Phases :
  - Incubation, propagation, déclenchement, exécution (*payload*)

# Classification des virus

- Par cible
  - Secteur de boot
  - Fichier
  - Macro
  - Multiple
- Par stratégie de dissimulation
  - Mutation
  - Compression
  - Chiffrement
  - Polymorphisme et métamorphisme

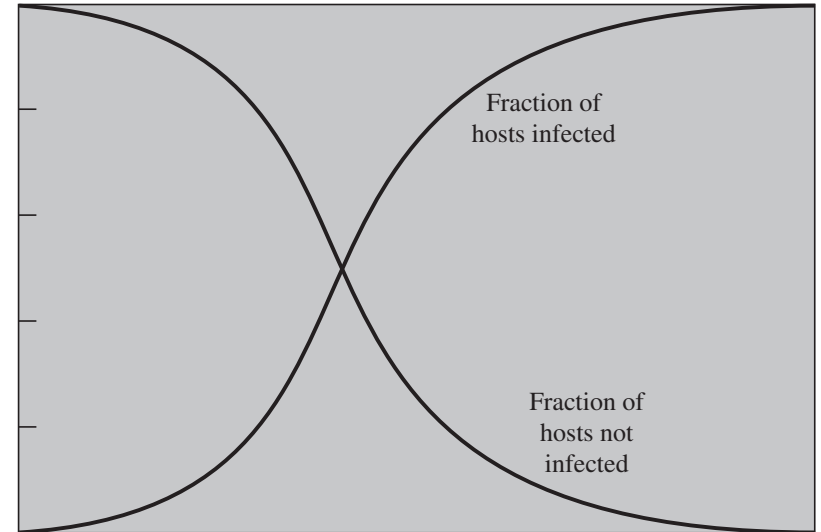


# Propagation par exploitation de vulnérabilité : *ver (worm)*

- Recherche activement des machines à infecter
  - Propagation par le réseau ou par des supports partagés
- Machines infectées servent de base de lancement
  - Attaques automatisées
- Exploitation de vulnérabilités logicielles
- Réplication :
  - Email, message instantané
  - Partage de fichiers, modification à distance, envoi de fichiers
  - Exécution à distance, login à distance
- Phases (comme les virus) :
  - Incubation, propagation, déclenchement, exécution (*payload*)

# Propagation des vers, exemples

- Stratégies
  - Aléatoire
  - Hit-list
  - Réseau local
  - Distribution topologique (info locale)
- Le ver de Morris (1988)
  - Une fois obtenu accès à une machine
    - Récupéré les identifiants des utilisateurs locaux
    - Essayé de déchiffrer les mots-de-passe (avec dictionnaire + permutations)
    - Réutilisé les mots de passe trouvés pour se connecter sur d'autres machines
  - Aussi abusé de bugs de finger et de sendmail pour se connecter
- Autres exemples :
  - ILOVEYOU, Melissa (vers via email)
  - Stuxnet, Wannacry (exploitation de services Microsoft)



# Propagation par ingénierie sociale, chevaux de Troie

- Logiciel en apparence légitime
- Contient fonctionnalité malveillante
- L'activation est faite par l'utilisateur, par erreur
- Propagation par ingénierie sociale
  - Pièces jointes des emails
  - Fausse publicité
- Spam : (ne pas confondre)
  - Communication électronique non sollicitée
  - Courrier électronique
  - Envois en grande quantité, à des fins publicitaires



# Propagation par élévation de privilèges, rootkit

- Logiciel pour prendre le pouvoir d'accès
- Exploitation d'une vulnérabilité pour élever ses privilèges (d'où le nom «root kit»)
- Propagation manuelle ou automatique
  - P.ex. dans un vers ou dans un virus
- Exemples
  - Sony BMG rootkit (2005)
    - Monitore les actions de l'utilisateur (copie induite des CDs Sony?)
    - S'installe sur la machine lorsque on joue un CD de Sony
  - PwnKit (2022)
    - Vulnérabilité de la gestion de privilèges (!) Unix
    - Le programme pkexec est vulnérable depuis 2009 (!)

# Fonctions des logiciels malveillants

**Corruption**

**Agents** (pilotage à distance)

**Vol d'informations**

**Furtivité** (cacher d'autres actions)

# Fonction : corruption du système

- Modification qui rend inutilisable
  - Des applications, le système
  - Les données de l'utilisateur
- Ransomware (logiciel à rançon)
  - Rendre le système ou les données inutilisables
  - Remettre en état en échange d'une rançon
- Des dommages au monde réel
  - Infrastructures critiques
  - Processus industriels
- Bombe logique
  - Dégât sous condition (temps, par exemple)

# WannaCry

- Rançongiciel pour Windows, détecté en 2017
- Plus de 300'000 ordinateurs dans 150 pays en moins d'une semaine
- Propagé rapidement via des courriels piégés
- Le virus s'installe sur l'ordinateur de la victime
- Utilise une vulnérabilité connue par la NSA à l'époque
- Il chiffre les données que contient le disque dur
- La rançon est 300-600 USD en bitcoins
- Les utilisateurs ne récupèrent pas leurs fichiers

# Fonction : agents (bots, zombies)

- Unités télécommandées via réseau (bots, botnet)
  - Exécutent des actions sur commande
  - Souvent l'action est programmable
- Actions communes
  - Déni de service distribué
  - Spam
  - Manipulation de sondages
  - Analyse de la communication (*sniffing*)
  - Enregistrement de touches (*keylogging*)
  - Prolifération malveillante
  - Installation malveillante



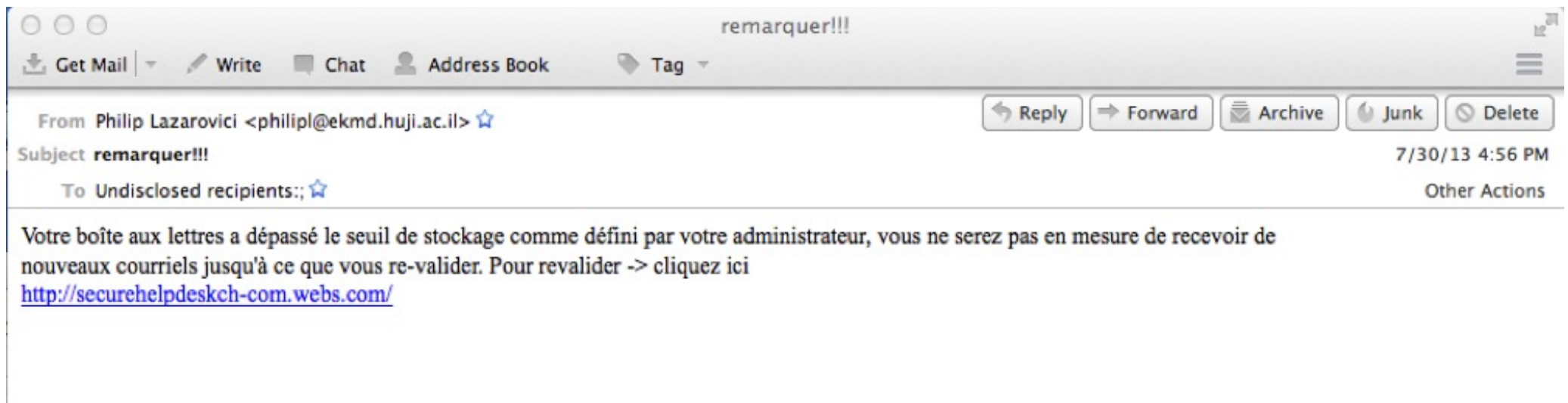
# Geinimi

- Botnet pour Android
- Détecté en décembre 2010 par Lookout Mobile Security
- Toutes les cinq minutes, envoi à une dizaine de serveurs
  - La position géographique
  - Codes personnels de carte SIM et le numéro d'identification IMEI
  - Peut télécharger ou supprimer des applications
  - Capable de recevoir des commandes distantes
- Geinimi se diffuse via certaines applications
  - Des jeux pour la plupart, d'une plateforme d'apps chinoise

# Fonction : vol d'information (*keylogger, phishing, spyware*)

- Vol d'informations
  - Profit économique (données bancaires, secrets industriels)
  - Ingénierie sociale (carnet d'adresses)
  - Espionnage et reconnaissance
- Actions communes
  - Vol d'identifiants (nom d'utilisateur, mots-de-passe, clés privées)
  - Keylogger : enregistrement des touches
  - Phishing : utilisation d'une identité volée
  - Exfiltration de données

# Exemples de email de phishing



E-Mail bestätigen aktualisieren

Get Mail

Write

Chat

Address Book

Tag

Reply

Forward

Archive

Junk

Delete

From Universität Zürich <webmaster@uzh.ch> ☆

Subject E-Mail bestätigen aktualisieren 3/30/13 7:47 PM

Reply to webdepartment2012@yahoo.co.jp ☆

To undisclosed-recipients:; ☆ Other Actions

Diese Nachricht wurde automatisch von einem Programm auf Webmail, die periodisch überprüft die Größe der Postfächer, wo neue Nachrichten empfangen werden gesendet. Das Programm wird wöchentlich, um sicherzustellen niemandes Posteingang zu groß ausgeführt werden.

Wenn Ihr Posteingang zu groß wird, werden Sie in der Lage, neue E-Mail erhalten. Kurz bevor diese Nachricht gesendet wurde, können Sie 18 Megabytes (MB) oder mehr Nachrichten im Posteingang auf Ihrem Webmail gespeichert Um uns zu helfen neu eingestellt Ihrer SPACE in unserer Datenbank vor Ihrem INBOX aufrecht erhalten werden konnte, müssen Sie auf diese E-Mail antworten und geben Sie ein:

Benutzername: {.....}

und Passwort: {.....}

Sie werden weiterhin diese Warnmeldung periodisch zu empfangen, wenn Ihr Posteingang Größe wächst auf 20 MB, dann ein Programm auf Bates Webmail wird Ihre älteste E-Mail in einem Ordner in Ihrem Home-Verzeichnis zu verschieben, um sicherzustellen, dass Sie auch weiterhin in der Lage sein zu erhalten in den kommenden Email.

Sie werden per E-Mail benachrichtigt werden, dass diese stattgefunden hat. Wenn Ihr Posteingang wächst auf 25 MB, wird es nicht möglich sein, neue E-Mail erhalten, wie es an den Absender zurückgeschickt werden.

Nachdem Sie eine Nachricht gelesen haben, ist es am besten, um die Antwort und speichern Sie eine Kopie.

danken  
Dank für Ihre Mitarbeit.  
© Universität Zürich 2013.03.29

[info] Mr. Oscar Reyes elküldte Neked ezt az oldalt: ZURIEL


Get Mail Write Chat Address Book Tag

From oscarreyes646@rocketmail.com ☆

Subject [info] Mr. Oscar Reyes elküldte Neked ezt az oldalt: ZURIEL 5/1/13 10:18 PM

Reply to info@s

To info@s Other Actions

 To protect your privacy, Thunderbird has blocked remote content in this message. [Show Remote Content](#)

[Always load remote content from oscarreyes646@rocketmail.com](#)

[ZURIEL](#)

[Mr. Oscar Reyes](#) úgy gondolja, hogy érdekelhet Téged ez az oldal, amit a [zuriel.hu](#)-n talált.

Message from Sender:

**UNITED NATIONS OFFICE OF INTERNATIONAL OVERSIGHT SERVICES Internal**  
**Audit,Monitoring,Consulting And Investigations Division**

Good Day,

This is to inform you that I came back from Africa yesterday,after series of complains from the FBI and other Security agencies from Asia,Europe, Oceania,South America and the United States of America respectively, against the Ivorian Government, Nigerian Government and the British Government for the rate of scam activities going on in these three nations.

I have met with President Goodluck Jonathan of Nigeria,and the British prime minister David Cameron and they claimed that they have been trying their best to make sure people received their outstanding payments without any complications. Right now,as directed by our secretary general Mr.Ban Ki-Moon,We are working in collaborations with the Nigerian Economic and Financial Crime Commission (EFCC) in Nigeria, The police economy in the Ivory Coast and the British secret intelligence in the U.K and have decided to waive away all your clearance fees/Charges and authorise the Government to effect the payment of your compensation of an amount of Four (4) Million United State Dollars approved by both the British government and the UN into your account without any delay.The only fee you will pay to confirm your fund in your account is waver clearance certificates to the United Nations authorized payment institution.

I would like you to urgently respond to this message so that I can advise you on how best to confirm your fund in your account within the next 72 hours.

Sincerely yours,  
Mr. Oscar Reyes

[Pályázat](#)  
by bvamos

Projekt címe: LOGalyze logelemző rendszer indexelő és adattároló alrendszerének újretervezése

Pályázati azonosító: GOP-1.3.1-09/A-2010-0148

A projekt az EU társfinanszírozásával, az Európa Terv keretében valósul meg.

A beruházás felelősségének elérhetősége:  
Gombos Szabolcs  
Tel.: +36-30-6388090

[Click here to read more on our site](#)



# Fonction : furtivité (porte dérobée [*backdoor*], *rootkit*)

- Mécanisme d'entrée dissimulé
  - Sert à exécuter des actions malveillantes
  - Normalement combiné avec un rootkit
- Installation
  - Service réseau installé de façon sournoise
  - Service réseau vulnérable, exploité
- Exemple: Sunburst (2020)
  - Porte dérobée placée par un pirate d'un service russe
  - SolarWinds (gestion réseau / Homeland Sec, OTAN)
  - Abus du processus de build

# Contre-mesures

- Principal moyen de défense : prévention
  - Prévention parfaite est pratiquement impossible
  - Idéalement : pas de partage, pas de réseau (!)
- Anti-virus : recherche des malwares connus
  - Chercher exhaustivement le code des virus
  - Enregistrer l'empreinte numérique des fichiers propres puis détecter les modifications
  - Recherche de fragments de code suspects (chiffrement du propre code p/ex)
- Observation des comportements
  - Analyse du comportement des programmes en exécution
  - Inspection (exhaustive) de la communication par le réseau

# Contre-mesures

- Bonnes pratiques
  - Installer un antivirus, le maintenir à jour
  - Installer un pare-feu, le laisser toujours en service
  - Effectuer les mises à jour de l'ordinateur (elles sont gratuites!)
- Messagerie
  - Ne pas ouvrir un fichier reçu dans un email **inattendu**
  - Chercher des virus dans la boîte d'entrée
  - Les exécutables et les documents contenant des macros sont les plus dangereux : exe, com, bat, pif, vbs, scr, doc, docx, xls,xlsx, msi, eml
  - Fichiers théoriquement inoffensifs : txt, jpg, gif, bmp, avi, mpg, asf, dat, mp3, wav, mid, ram, rm
  - Au minimum, attendre quelques jours et en parler autour de soi



# Introduction aux attaques, en pratique

- Attaques d'injection
- Attaques de dépassement de tampon



# Attaques d'injection

- Utilisateur donne du code dans les données d'entrée d'un formulaire Web
- Exemple: dans une page Web dynamique en PHP:
  - Faire un formulaire avec l'entrée d'un nom d'utilisateur et un mot de passe
  - Prendre le nom d'utilisateur (et le mot de passe) et composer une commande SELECT modifiée

# Exemple de mauvais code PHP

- Code source PHP

```
name = getRequestString("username");  
pass = getRequestString("password");  
command = "SELECT * FROM Users";  
command .= " WHERE name = '" . name . "'";  
command .= " AND pass = '" . pass . "'";  
sql_execute(command);
```

- L'utilisateur donne :

- Username:

' or ''='

- Password:

' or ''='

- Commande SQL exécutée :

```
SELECT * FROM Users  
WHERE name = ' ' or ''=' ' AND pass = ' ' or ''=' '
```

# Protection contre l'injection

- Utiliser des fonctions appropriées pour coller des valeurs d'utilisateur dans des commandes

- *Sanitizers*

```
"SELECT * FROM Users WHERE id = " + sanitize(id)
```

- Des requêtes SQL préparées

```
"SELECT * FROM Users WHERE id = @0"
```

- Ne pas monter des commandes durant l'exécution

# Attaques de dépassement de tampon (*buffer overflow*)

- L'utilisateur donne plus de données d'entrée que le programme attend, et celui-ci ne le teste pas
  - Utilisé aussi dans les E/S réseau
- Exemple dans un programme en C
  - Programme déclare un string de 10 positions, puis fait un scanf() de ce string
  - L'utilisateur tape un string de 50 positions

# Exemple de mauvais code en C

- Code source C

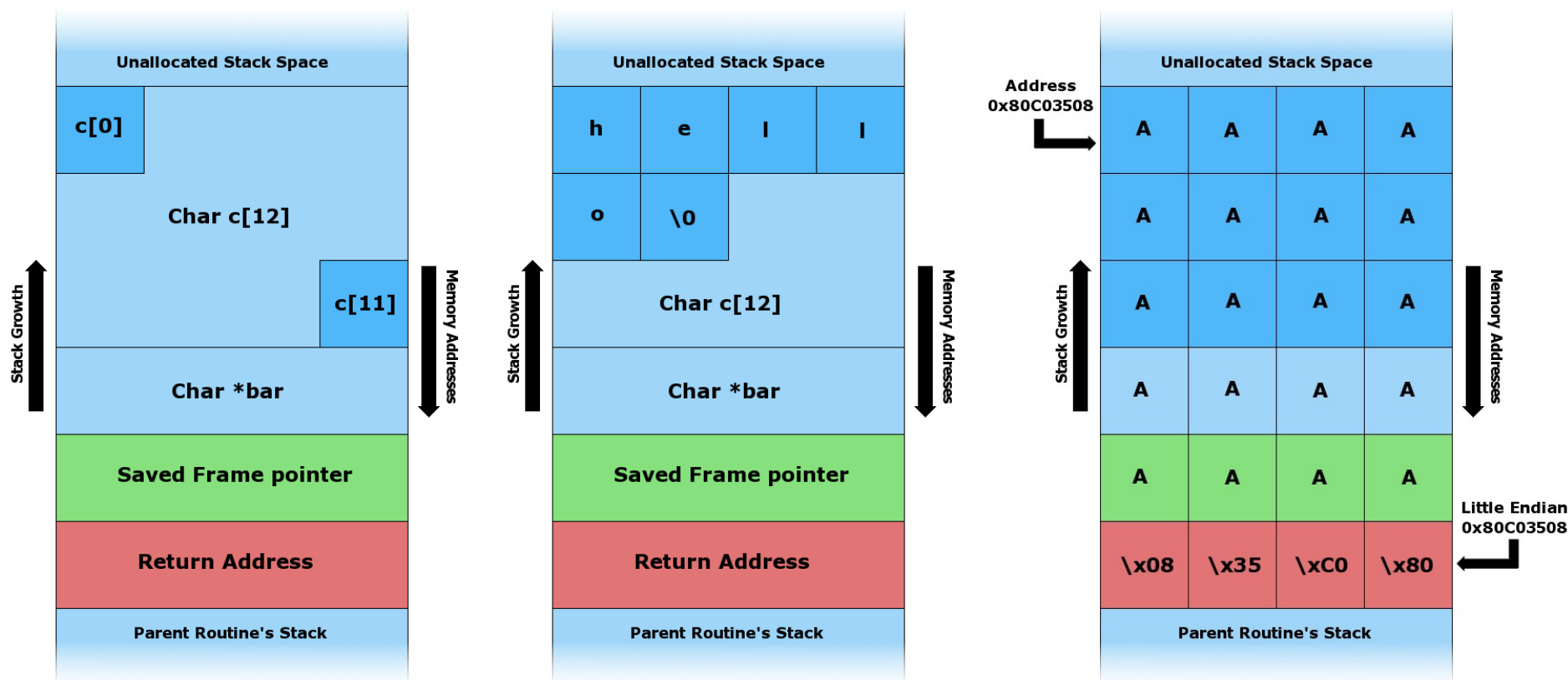
```
char command[10];  
scanf("%s", command);
```

- L'utilisateur donne comme entrée:

```
0123456789à-£787
```

- Conséquence:
  - La chaîne d'entrée va être stockée dans la mémoire du programme (en particulier, dans la pile du programme)
  - Un choix méticuleux de chaîne d'entrée peut prendre le contrôle du programme

# Exploitation de la pile dans une attaque de dépassement de tampon



Source: [Wikipedia](https://en.wikipedia.org/wiki/Buffer_overflow)

# Techniques d'exploitation du dépassement de tampon

- Comment exploiter le tampon
  - Insérer du code dans la pile
  - Changer les adresses de retour dans la pile
  - Et bien d'autres...
- Comment éviter
  - Choisir le bon langage
  - Choisir les bonnes bibliothèques de E/S
  - Utiliser des canaries
  - Empêcher l'exécution de code dans la pile
  - Charger les bibliothèques à des adresses aléatoires
  - Scanner les paquets réseau (pour chercher les dépassements)



# En résumé

- Prolifération malveillante
  - Virus : infection
  - Ver : abus de vulnérabilité
  - Cheval de Troie : tromperie
- Fonction malveillante
  - Bots, zombies : télécommande
  - Phishing : espionner
  - Backdoor, rootkit : abus de vulnérabilité
- Quelques attaques
  - Injection de code
  - Dépassement de tampon