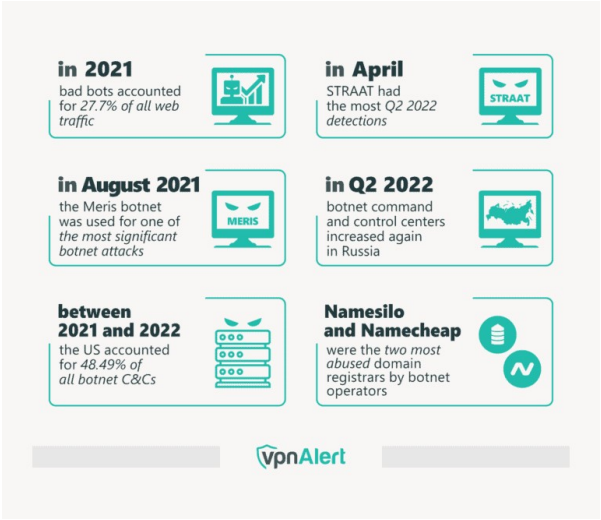
Les Botnets

Dr Salim Benayoune

Introduction

- **BotNets : une synthèse algorithmique**
- **BotNets** (contraction de ro**BOT NET**work)
  - Apparition en 2003
  - "*Bots are software programs that perform actions upon receiving commands from users or programs*".
  - Un BotNet est un **réseau malicieux** de machines infectées tombées **sous le contrôle** d'un attaquant grâce à **différents types** de codes malveillants, et ce à l'**insu** des propriétaires de ces ordinateurs, lesquels continuent de fonctionner en apparence **normalement.**
  - C'est une **menace distribuée** faisant la **synthèse des différentes algorithmiques virales connues**, en même temps qu'un **raffinement des techniques de propagation**, plus **diffuses**

Botnet Statistics



Botnet Statistics

- There were over **1.6** million botnet events in Q2 2022 (19,000 daily). it accounted for a top share of the total detected **4.379 million malware events** in the same timeframe.
- There were over **2.2** million botnet events in Q4 2022 (26,223 daily)
- **39 unique botnet variants** detected in Q2 2022
- The **Torpig.Mebroot** botnet was the most dominant in April – June 2022. this botnet accounted for **38% of all botnet activity** detections. It was followed by **Sora** (24%) and **STRRAT** (18%) in the top three.
- Botnet deployments in **DDoS** attacks averaged 4.6 terabytes to 51.65 terabytes average volumes in 2021.The average attack also lasted between 3.65 – 8.72 hours.
- Bad bots accounted for **27.7% of all web traffic** in 2021. good bots (such as those from the Google search engine) made up 14.6% of all web traffic in 2021.

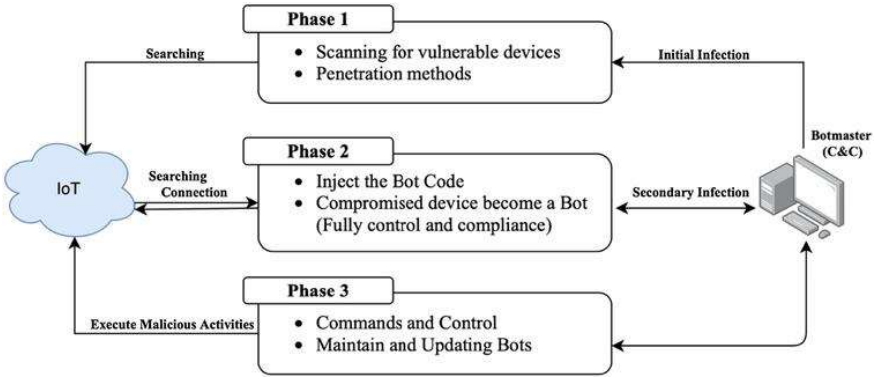
Botnet Statistics

- Evasive bad bots accounted for 65.6% of all bad bot traffic in 2021. Moderately evasive bad bots made up 39.7% of this share, while advanced bad bots claimed a 25.9% share.
- Linux botnet codes were evolving at a faster pace in 2021 (9.3%).
- The Meris botnet was used for one of the most significant botnet attacks in August 2021. 17.2 million requests per second, 20,000 bots from infected devices in 125 countries.
- Emotet botnet detections increased over 10x year-on-year.
- The Mozi botnet caused 74% of all IoT attacks in 2021.
- Moldova recorded an 81% increase in botnet C2s in Q2 2022, Netherlands (13%) and France (5%).
- Domains with .cloud extensions were the most abused by botnet operators in 2022.

Botnet Statistics

- Namesilo and Namecheap were the two most abused domain registrars by botnet operators.
- Canadian registrars hosted the most botnet C&C servers in Q2 2022.
- Chinese registrars recorded fewer botnet C&C activities on their servers in Q2 2022.
- Between 2021 and 2022, the US accounted for 48.49% of all botnet C&Cs.
- Over 4 in 10 bad bot traffic attacks (globally) in 2021 were **directed to** the United. Australia was second with 6.8%, while the UK rounded up the top three with a 6.7%.
- Germany recorded the highest bad bot share of internet traffic in 2021.Bad bots generated 39.6% of all internet traffic from Germany in 2021.
- Microsoft thwarted a 2.4Tbps botnet attack in October 2021.The attack was believed to have stemmed from 70,000 bots engineered from infected devices in the Asia-Pacific region.
- https://www.spamhaus.com/threat-map/

Architecture of Botnet

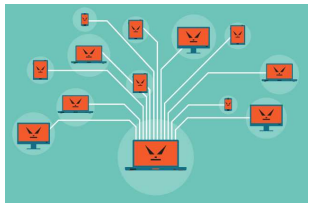


Introduction

- Le pirate va organiser, **administrer** ce réseau malicieux pour réaliser des actions malicieuses distribuées (ex DDoS).
- Les premiers botnets: Agobot, SDBot et SpyBot
- Puis, d'autres souches : Rustock, Kraken, Zeus...
  - Introduction d'autres architectures : centralisée en mode client-serveur, décentralisée avec le protocole P2P...
- d'autres modes de communication plus sécurisés :
  - protocole TOR avec Skynet ou Atrax,
  - stéganographie avec le BotNet Andomède/Gamarue,
- d'autres environnements
  - objets connectés en 2016 avec Mirai...
  - EMOTET

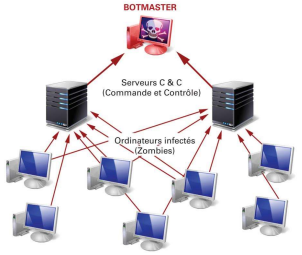
Introduction

- Les machines d'un BotNet sont distribuées dans le monde et peuvent communiquer entre elles.
  - IRC, P2P
  - Gestion décentralisée et semi-automatique
  - La taille des BotNets actuels varie de quelques centaines de machines à quelques millions de machines.
    - À ce jour, près de **deux cent millions** d'ordinateurs feraient ainsi partie d'un ou plusieurs BotNets



Introduction

- Usage des Botnets :
  - **attaques en déni de service distribué**
    - Filtrage par IP ou nom de domaine est inefficace.
    - Exemple : attaque des infrastructures informatiques de l'Estonie en mai 2007
    - 10 millions d'attaques DDoS enregistrées en 2020
    - Dans le secteur de santé, 8 400 attaques DDoS au premier trimestre 2021, soit une augmentation de 53 % par rapport à l'année précédente.



Introduction

- Usage des Botnets :
  - **Diffusion de SPAM**
    - Contourner les listes noires
  - **vol d'informations aux utilisateurs**
    - informations personnelles, identifiants bancaires...
    - Ces informations, une fois collectées, seront utilisées à des fins frauduleuses ;
      - vol de donnée de près d'1.4 million de personnes ayant passé un test PCR, mi-2020, en Ile-de-France.
  - **hébergement de sites frauduleux**
    - Stockés sur les machines du BotNet
  - **déploiement de vers** dans le cadre d'une attaque en plusieurs phases.
    - Exemple : ver Storm Worm, entre 10 et 50 millions de machines

Botnets Main Characteristics

- A botnet's lifetime consists of three main stages as follows :
  - **Stage 1—recruitment stage:**
    - This is done through infecting machines with the bot code using different mechanisms.
      - Worm propagation techniques (without user interaction)
      - Social engineering
      - phishing campaigns: malicious link or attachment
      - Physical media infection

Botnets Main Characteristics

- A botnet's lifetime consists of three main stages as follows :
  - **Stage 2—C&C (Command and Control) stage:**
    - The botmaster maintains a control over the infected machines (bots) through a C&C channel.
    - The architecture of the botnet depends on the implementation of the C&C channel.
    - Push or a Pull style

Botnets Main Characteristics

- A botnet's lifetime consists of three main stages as follows :
  - **Stage 3—botnet activity stage:**
    - Represents the set of actions and attacks that are performed by bots in response to commands
    - DDoS
    - Email spam
    - Identity theft
    - Cryptocurrency
    - Click-Fraud

Characterizing Botnets

- The Botnet Size
  - represents an important factor of the intensity and the widespread of cyberattacks.
  - **large** botnets are viewed to be a serious threat to the Internet services
  - **small** botnets are also a threat especially for attacks that do not require a large amount of traffic such as ransomware and identity theft.
  - Small botnets can be easily managed, rented, and stay undetected.
  - Botnet size is defined as the **largest connected portion of the botnet (online bots)**

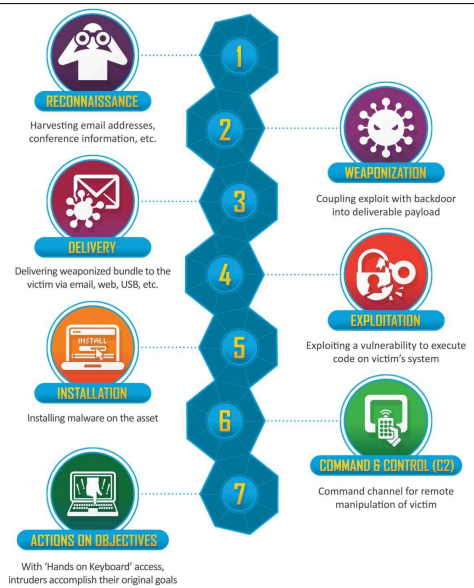
Characterizing Botnets

- The Botnet Size : techniques used to estimate the botnet size
  - **Botnet infiltration** : join the C&C channel of a botnet
  - **DNS redirection** : redirects connections that are made to the botnets' C&C server to another server (e.g., a sinkhole)
  - **DNS cache snooping :** searches the DNS servers' caches for entries of a botnet's C&C server. The number of cache hits serves as a lower bound that represents the number of the bots.
  - **Crawling P2P botnets:** Starting with one bot, a request is issued to get its peer-list. crawling must be done very quickly to get an accurate snapshot of the current P2P graph.

Characterizing Botnets

- **Geographical Distribution of Botnets**
  - Although bots can be found anywhere in the Internet, research studies show that they are concentrated in particular regions in the world
    - infection propagation mechanism that involves a region or a language.
    - Vulnerable machines tend to cluster in certain networks, which suggest that bots will cluster in these networks as well
  - The distribution of bots in the Internet represents an important issue because it can assist in developing efficient countermeasures

Techniques de communication avec le C&C



Cyber Kill Chain

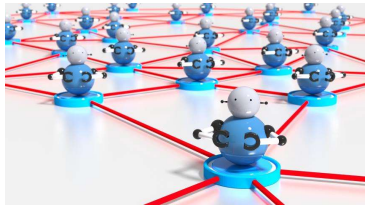
Techniques de communication avec le C&C

- **C&C** (Command and Control)
- Les canaux de communication entre le malware et son C&C et souvent **le maillon faible de la compromission**
- Objectif de l'attaquant :

  rendre ces **canaux pérennes**, **discrets** et **difficiles à couper**.

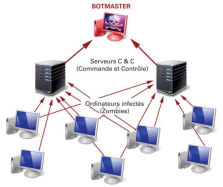
Techniques de communication avec le C&C

- La plupart des malwares interrogent les C&C via **un nom de domaine**, ce nom pointant vers une adresse IP.
- Solution:
  - rendre **indisponible l'adresse IP** ou faire pointer le nom de domaine **dans le vide.**
- Comment font les développeurs de malwares pour contourner ces contres mesures ?

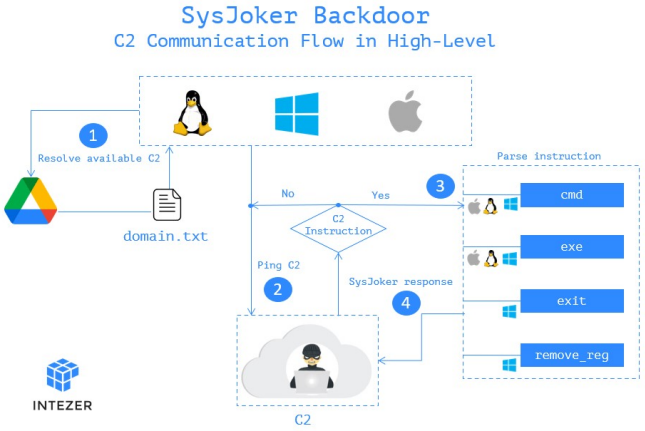


Techniques de communication avec le C&C

- Mise à jour de la liste des noms de domaine
  - Commande opérée à distance par le C&C lui-même ou via un C&C de secours.
  - Les malwares ont plusieurs adresses où ils peuvent joindre un C&C.
  - Si une de ces adresses est inaccessible, un des C&C encore actifs prévient la machine infectée en lui communiquant une ou plusieurs nouvelles adresses de C&C.
  - Cette méthode fonctionne correctement si tous les C&C ne sont pas coupés simultanément.



Techniques de communication avec le C&C
Sysjoker



https://www.intezer.com/blog/malware-analysis/new-backdoor-sysjoker/

Techniques de communication avec le C&C

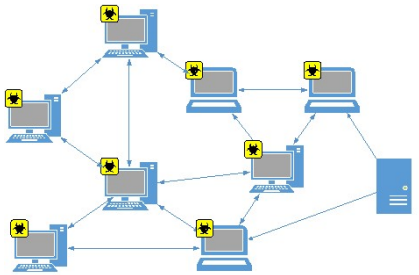
- Communication via HTTP/HTTPS/FTP/IRC
  - Les malwares utilisent des protocoles de communication connus.
    - Le malware sera discret et noyé dans la masse
    - Il existe des API pour tous les protocoles standards, ce qui facilite le développement du malware.
  - Le protocole IRC était utilisé au début des années 2000.
  - Aujourd'hui, la plupart des malwares et des botnets utilisent les protocoles HTTP ou HTTPS.
  - FTP est utilisé pour récupérer des fichier volés ou des captures
  - L'utilisation de HTTP et HTTPS est facilitée par les objets COM

Techniques de communication avec le C&C

- Communication via e-mail
  - utiliser le client mail de l'utilisateur infecté pour communiquer vers l'extérieur
  - les objets COM peuvent être utilisés afin de manipuler Microsoft Outlook et donc les e-mails de l'utilisateur, de les lire ou même d'en envoyer.

Techniques de communication avec le C&C

- Communication via un réseau P2P
  - les machines infectées ne communiquent pas directement à un C&C mais elles communiquent entre elles afin de s'échanger des informations (telles que leur configuration, etc.).
  - Exemple: malware bancaire **Gameover Zeus**.

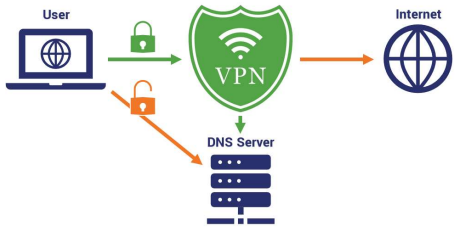


Techniques de communication avec le C&C

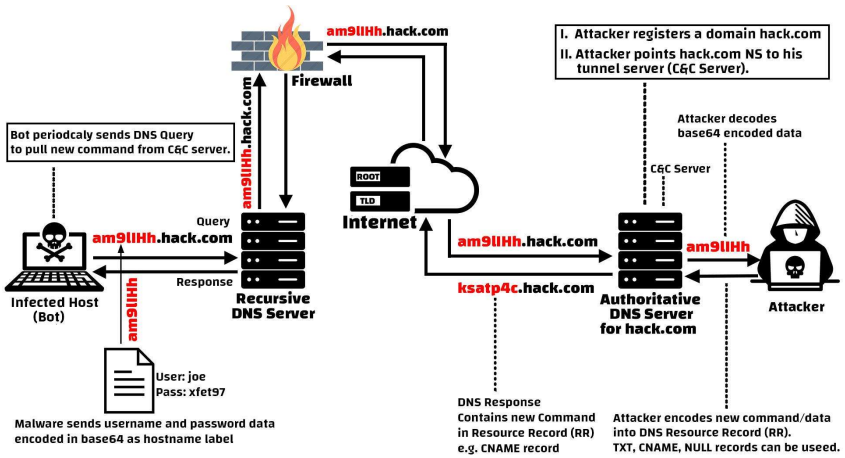
- Communication via des protocoles propriétaires
  - les auteurs de malware mettent en place un protocole propriétaire de communications vers Internet.
  - Exemple: **PoisonIvy**
  - Pas très répandue car facilement détectable.

Techniques de communication avec le C&C

- Communication via le protocole DNS
  - DNS tunneling
  - Utiliser le protocole DNS comme enveloppe de communication entre le malware et le C&C, car pas toujours controlé par les entreprise
  - Exemple: utilisé par le malware **DNSpionage** (2018)

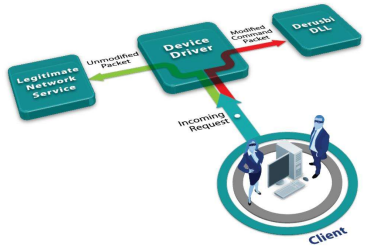


Techniques de communication avec le C&C
Communication via le protocole DNS



Techniques de communication avec le C&C

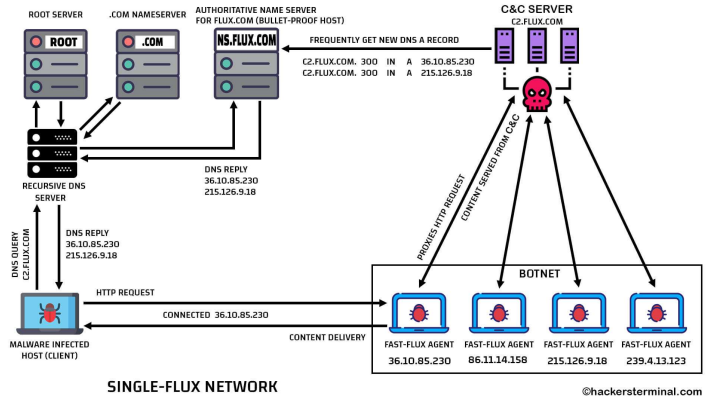
- Communication passive
  - Le malware attend passivement la sollicitation de l'attaquant.
  - le malware n'a pas besoin de connaître de serveur de commande.
  - Exemple: malware **Derusbi**
    - crée un filtre réseau sur la machine infectée et attend une séquence réseau particulière.
    - Si cette séquence est envoyée à la machine infectée, alors un flux de communication sera établi



Techniques de communication avec le C&C

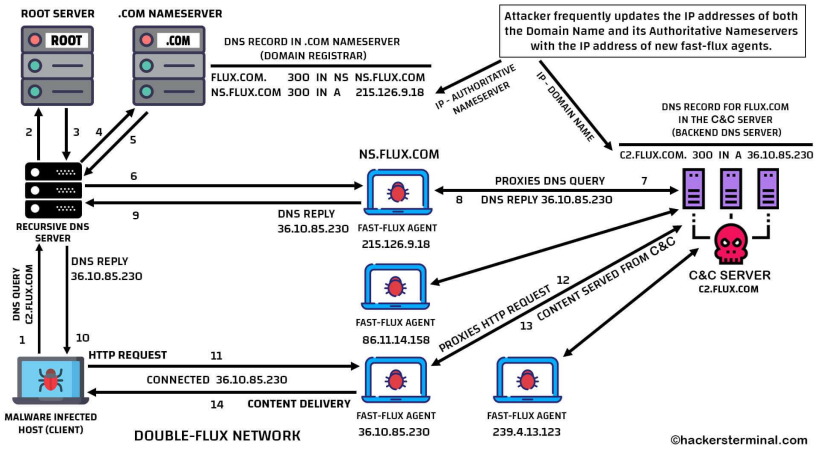
- **Fast flux DNS**
  - Le **fast flux** est une technique utilisant des caractéristiques du protocole DNS (Domain Name System) gérant les noms de domaine.
    - Associer plusieurs adresses IP au même nom de domaine
    - Enregistrer puis désenregistrer une adresse IP et la remplacer par une autre chaque quelques minutes ou secondes (short TTL)
    - Avantage : éviter le IP based Blacklisting
    - Solution: bloquer le nom de domaine

Techniques de communication avec le C&C
Single-Flux Network



https://hackersterminal.com/fast-flux-service-networks-ffsn-technique/

Techniques de communication avec le C&C
Double-Flux Network

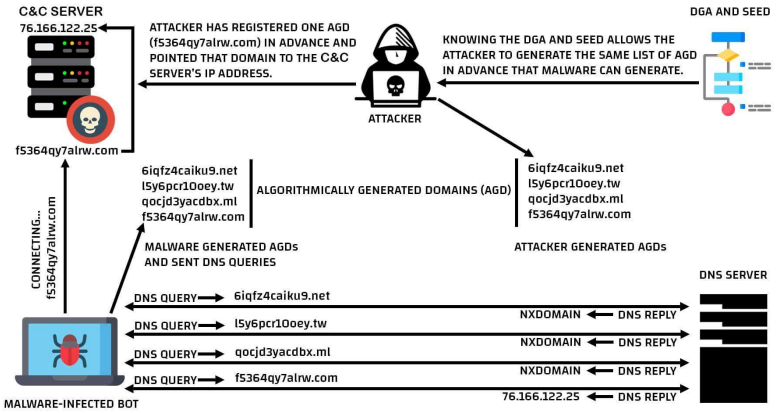


https://hackersterminal.com/fast-flux-service-networks-ffsn-technique/

Techniques de communication avec le C&C

- DGA (Domain Generation Algorithms)
  - Le DGA est une technique consistant à générer un très grand nombre d'adresses DNS pour contacter un C&C.
    - Cette technique évite le blacklisting des domaines DNS
  - Enregistrer le nom de domaine une heure avant l'attaque, le domaine reste valide 24 heure
  - Utilisé dans Zeus GameOver, Cryptolocker, PushDo, Conficker et Ramdo.
  - Par exemple, le malware Conficker.C générait près de **50 000 noms de domaine par jour.**

Techniques de communication avec le C&C
DGA (Domain Generation Algorithms)



Domain Generation Algorithm (DGA)

https://hackersterminal.com/domain-generation-algorithm-dga-in-malware/