Centro de
Investigación en
Computación

Malware families

Familias de malware

Definitions

Research

Course

Análisis y Detección de Malware

Instructor

Acosta Bermejo Raúl

Lecture notes

2024-B
4 de septiembre del 2024

Instituto
Politécnico
Nacional

Table of contents (outline)

Tabla de contenido

1. Introducción
   a. Fases
2. Taxonomias
3. Lista (No exhaustiva ni en orden)
   a. Descripción, ejemplos.

1. Adware
2. Backdoor
3. Botnet
4. Downloader
5. Dropper
6. Hacktool
7. Keylogger
7. Phishing
8. Ransomware
9. Rootkit
10. Spyware
11. Virus
12. Worm
13. Exploit Kit

Introduction

Introducción

Introduction

Introducción

Amenaza

El malware es un software malicioso especializado en realizar uno o varios ataques (vector) por lo que está compuesto por varios comportamientos.

Reto

Conocer y/o identificar los comportamientos del malware en diferentes:

Sistemas operativos (formatos ejecutables)

Protocolos de comunicación

Contextos de ejecución

Etcétera

Introduction

Introducción

La ejecución de un malware suele realizarse en etapas o fases, y las más generales son:

1. Infection phase (fase de infección).
    a. System exploit
    b. Binary loading (dropper)
2. Callback phase (fase de ejecución).
    a. Callback.
    b. Data exfiltration (extracción de datos)

Dependiendo del objetivo del malware, las fases pueden describirse con más detalle, por ejemplo:

a. Ataque a un sitio web.

Introduction

Introducción

Secuestro (rapto)

- Kidnapping (personas)
- Abduction (personas)
- Sequestration (activos, deuda)
- Hijacked (avión, vehículo, barco)

Web malware attack

Sophos information

1. Entry point
   a. You access a hijacked website. Malware downloads silently and you don't notice that you're being infected.
2. Distribution
   a. The initial malware redirects to an exploit server using fast-flux Distribution techniques based on what you're working with (Windows/Mac, IE/Safari, Java, etc.).
3. Exploit
   a. Commercially available and supported exploit packs will attempt to leverage vulnerabilities in the OS, browser, Java, PDF reader, media player and other plugins.
4. Infection
   a. The malware downloads a malicious payload that will steal data or extort money from you.

Introduction

Introducción

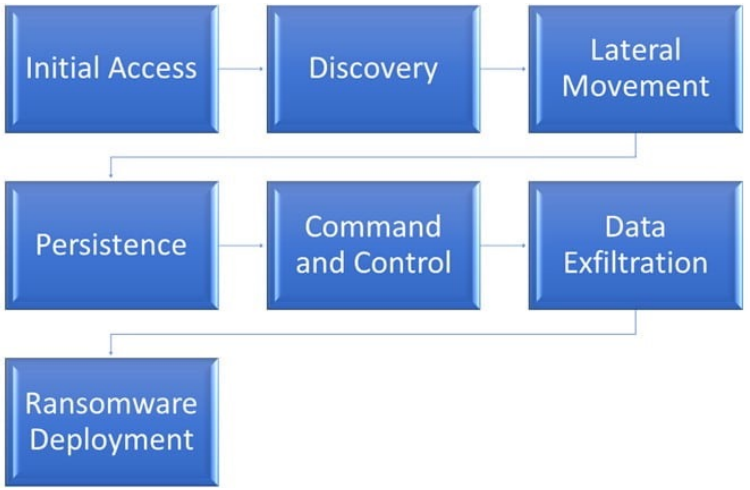
Web malware attack

Sophos information

5. Execution
    a. Malware calls home with sensitive data like credentials, banking or credit card information, or tricks you into paying directly.

Introduction

Introducción



Phases of a post-intrusion ransomware attack

Source: Secureworks

https://www.secureworks.com/research/phases-of-a-post-intrusion-ransomware-attack

1. Initial Access

   Three primary initial access vectors (IAVs) that give threat actors a foothold in victims' environments: i) Scan-and-exploit attacks against a vulnerable internet-facing system, ii) An existing malware infection initially delivered via phishing or other means, iii) Stolen or guessed credentials to log in via a remote access solution.

2. Discovery

   Threat actors attempt to discover additional information by harvesting credentials, escalating privileges, scanning and enumerating the network, and gathering data.

   i. Information Gatering

      Threat actor can begin collecting host and network data.

   ii. Network reconnaissance

      Internal network scanning and enumeration give threat actors visibility into the compromised environment in preparation for lateral movement.

Introduction

Introducción

Phases of a post-intrusion ransomware attack

3. Lateral movement

   Threat actors can use native operating system tools to perform lateral movement. They may launch files over shares and access systems via Remote Desktop Protocol (RDP) using stolen credentials.

4. Persistence

   Threat actors use various tools and techniques to establish persistence in compromised environments

5. Command & Control (C&C)
6. Data exfiltratation
7. Ransomware deployment

Cada malware o ataque es diferente!
Como protegerse? Que dicen los expertos?
Modelos de ataque / MITRE ATCK

Taxonomies

Taxonomias / Clasificaciones

Definiciones

Taxonomy

Tipos

Una taxonomía es una forma de representación del conocimiento así que hay varios tipos de taxonomías según lo que se quiera representar.

- Lecturas
  - https://www.gdatasoftware.com/blog/malware-family-naming-hell
  - Malware 101 – Viruses, Aman Hardikar (PDF).

Taxonomy

Familia

CARO (*Computer Antivirus Research Organization*)

- It is also an organization that was established in 1990 to research and study malware.
- But it is a malware naming scheme:

  [<type>://][<platform>/]<family>[.<group>][.<length>].<variant>[<modifiers>][!<comment>]

  virus://{VBS,W97M,Win32}/Foo.A@mm
- URLs
  - https://bontchev.nlcv.bas.bg/papers/naming.html

Taxonomy

Familia

MAEC / CME

- Evolución
  - Inició como: Common Malware Enumeration (CME)
  - Actualmente: MAEC (pronounced “mike”)

    Malware Attribute Enumeration and Characterization
- Que es?
  - Un lenguaje estructurado desarrollado por la comunidad para codificar y compartir información de alta fidelidad sobre malware en función de atributos como comportamientos, artefactos y relaciones entre muestras de malware.
  - Versión actual MAEC 5.
- URLs
  - https://cme.mitre.org/
  - https://maecproject.github.io/

Taxonomy

Familia

MISP

- Evolución
  - Inicio: NATO
  - Actualmente: MISP: Malware Information Sharing Project.
- URLs
  - https://www.misp-project.org/taxonomies.html o taxonomies.pdf
- Resumen
  - abusive-content: ["spam","harmful-speech", "violence"]
  - malicious-code: ["virus", "worm", "ransomware", "trojan-malware", "spyware-rat", "dialer", "rootkit"]
  - information-gathering: ["scanner", "sniffing", "social-engineering"]
  - intrusion-attempts: ["exploit-known-vuln", "login-attempts", "new-attack-signature"]
  - intrusion: ["privileged-account-compromise", "unprivileged-account-compromise", "botnet-member", "domain-compromise", "application-compromise"]
  - availability: ["dos", "ddos", "sabotage", "outage"]
  - information-content-security": ["Unauthorised-information-access", "Unauthorised-information-modification"]
  - fraud: ["copyright", "masquerade", "phishing"]
  - vulnerable: ["vulnerable-service"]
  - conformity: ["regulator", "standard", "security-policy", "other-conformity"]

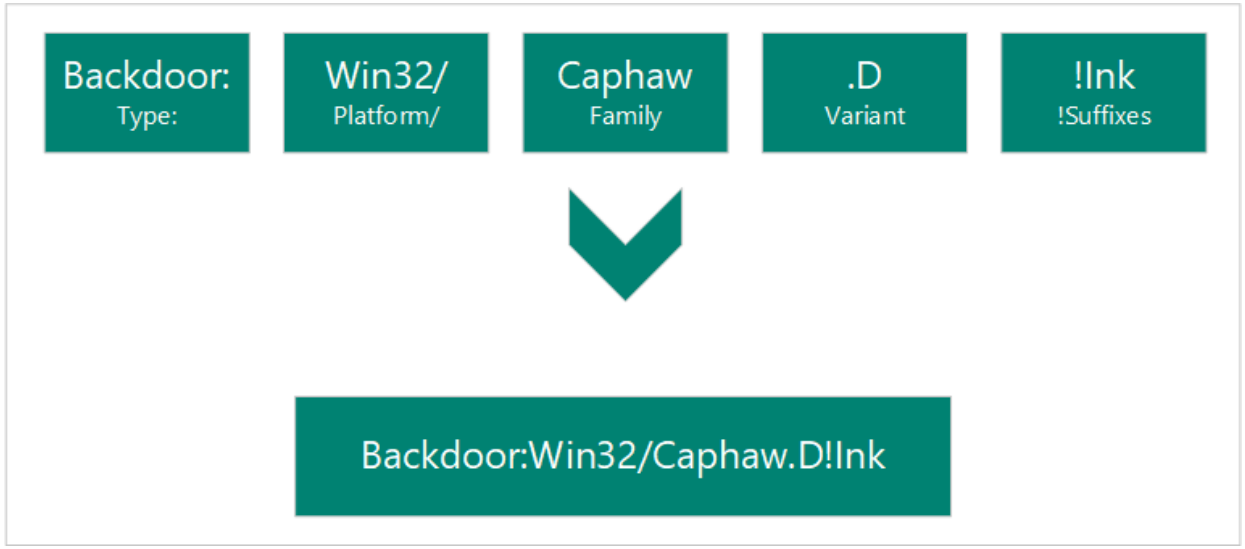
Taxonomy

Familia

Microsoft

Usa CARO

- URLs
  - https://learn.microsoft.com/en-us/microsoft-365/security/intelligence/malware-naming?view=o365-worldwide.



Types

1. Adware
2. Backdoor
3. Behavior
4. BrowserModifier
5. Constructor
6. DDoS
7. Exploit
8. HackTool
9. Joke
10. Misleading
11. MonitoringTool
12. Program
13. Personal Web Server (PWS)
14. Ransom
15. RemoteAccess
16. Rogue
17. SettingsModifier
18. SoftwareBundler
19. Spammer
20. Spoofer
21. Spyware
22. Tool
23. Trojan
24. TrojanClicker
25. TrojanDownloader
26. TrojanNotifier
27. TrojanProxy
28. TrojanSpy
29. VirTool
30. Virus
31. Worm

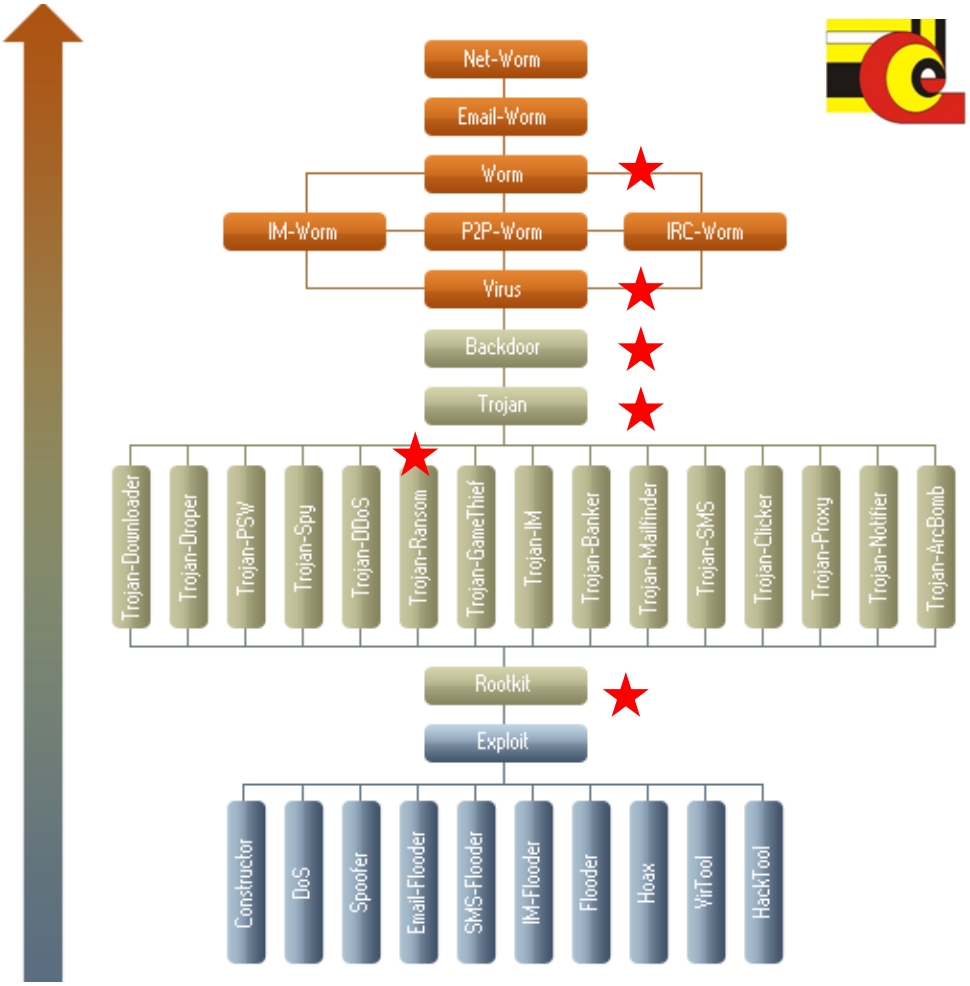
Taxonomy

Familia

Kaspersky

Usa a Classification Tree

- If a program can be categorized as a number of different behaviours, it should be classified as the most threatening of those behaviours.
- Behaviour higher up the tree takes precedence over the other behaviour.
- Highest-ranking behaviour only applies to Trojans, Viruses and Worms. It does not apply to Malicious Tools.



- URLs
  - https://encyclopedia.kaspersky.com/knowledge/rules-for-classifying/
  - https://encyclopedia.kaspersky.com/knowledge/classification/

Taxonomy

Taxonomias

En biología

La clasificación clásica es muy extensa y los 3 niveles más bajos son:

- Familia / Type
  - Hominidae / Canidae
- Género / Family
  - Homo / Canis
- Especie / Variant
  - Homo sapiens / Canis Familiaris

Arriba de Familia están: superfamilia, orden (sub, infra y parv-orden).

Taxonomy

Taxonomias

A continuación

Veremos el detalle de los Tipos principales:

- Explicación general
  - Comportamientos (no TTPs)
  - NO técnica.
- En muchos artículos científicos se presentan taxonomias por Tipo y seguido hay más de una que no usan el mismo concepto de clasificación.

Malware Types/Families

Tipos de malware

Definiciones

Malware

Familias

Lista

- Con base en todo lo anterior se pueden sugerir las siguientes familias principales:

1. Adware
2. Backdoor
3. Botnet
4. Downloader
5. Dropper
6. Hacktool
7. Keylogger
8. Phishing
9. Ransomware
10. Rootkit
11. Spyware
12. Virus
13. Worm

Malware

Familia: Virus & Worms

Definition

Viruses must be triggered by the activation of their host.
Worms do not require activation—or any human intervention—
to execute or **spread** their code.

- Virus
  - It cannot self-replicate, and it needs to be sent by a user or software to travel between two different computers.
  - It has the ability to insert its functional code into existing programs and files on your system.
  - They can be classified according to the method that they use to infect a computer: File viruses, Boot sector viruses, Macro viruses, Script viruses.
- Worm
  - A worm can replicate and spread itself (full copies) from one computer to another.
  - It often exploit network configuration, errors or security loopholes in the OS or applications.
  - Many use multiple methods to spread across networks, including the following: Email, Instant Message (IM) like SMS, Messanger, ICQ, IRC, Facebook.

Malware

Familia: Adware

Definición

Software downloaded to your computer without your permission, which inserts advertising, usually in the form of pop-up or pop-under windows.

- Pertenece a una clasificación más amplia:
  - PUA, Potentially Unwanted Application
  - PUP, Potentially Unwanted Program
  - Both are unnessary software that:
    - Found as freeware: instalado cuando otro software se instala, es decir, con el “consentimiento” del usuario.
    - El más comun es el Adware.

Malware

Familia: Backdoor

Definition

It is a method, often secret, of bypassing normal authentication in a product, computer system, cryptosystem or algorithm etc.

- Backdoors are often used for securing unauthorized remote access to a computer, or obtaining access to plaintext in cryptographic systems.
- Default passwords can function as backdoors if they are not changed by the user. Some debugging features can also act as backdoors if they are not removed in the release version.

Malware

Familia: Backdoor

- Ebury SSH
  - https://www.cert-bund.de/ebury-faq
- Reportes de los backdoors
  - https://owasp.org/www-pdf-archive/OWASP_10_Most_Common_Backdoors.pdf.

Beast, a Windows-based backdoor Trojan horse.

Malware

Familia: Backdoor

Definition

Remote Access Trojans (RATs)

They are malware designed to allow an attacker

to remotely control an infected computer.

- It can be considered a synonym to “backdoor”.
- But it usually signifies a full bundle including:
  - A client application meant for installation on the target system, and
  - A server component that allows administration and control of the individual 'bots' or compromised systems.

Malware

Familia: Downloader

Definition

A small piece of code, usually a single instruction,
used in the payload of an exploit
to silently fetch a malicious EXE file from the attacker's server.

- The content that is downloaded varies. It may comprise of, but need not be limited to, the following items:
  - Configuration/command information
  - Miscellaneous files
- Other threats or security risks, such as components related to pay per install operations.
- Misleading Applications (Engañar)
- Secondary components of, or upgrades to, the existing attack
- .

Malware

Familia: Downloader

Familias

- Some of the more frequently observed loaders are:
  - Bazar
  - Buer
  - Dridex
  - Get2
  - IcedIDQakbot
- These loaders are typically delivered via phishing campaigns.

Malware

Familia: Dropper

Definition

It is a small helper program that facilitates the delivery and installation of malware.

- Spammers and other bad actors use droppers to circumvent the signatures that anti-virus programs use to block or quarantine malicious code.
- Droppers, which essentially acts like Trojan horse counterparts, can be persistent or non-persistent.
  - Non-persistent droppers install malware and then automatically remove themselves.
  - Persistent droppers copy themselves to a hidden file and stay there until they complete the task they were created for.
- Droppers are bundled with free utility programs (such as ad blockers) to avoid detection by antivirus. When the free program executes, the dropper will first download and install malware before it unpacks and installs the legitimate utility.

Malware

Familia: Keylogger

Definition

A program that logs user input from the keyboard, usually without the user's knowledge or permission.

- Técnica general
  - Eavesdrop: Escuchar a escondidas, furtivamente.

Malware

Familia: Hacktool

- Definitions
  - Hacking tools are applications that crack or break computer and network security measures. Hacking tools have different capabilities that have been designed to penetrate systems.
  - HackTool programs add new users to the list of permitted system visitors, clean system logs of traces of criminal activity, and collect and analyze network packets. They are used to organize attacks on local or remote computers.
- Examples
  - VirTool programs can be used to modify other malicious programs so that they cannot be detected by antivirus software.
  - A Constructor is a malware creation toolkit that allows users with little technical knowledge to easily assemble a complex, malicious program from prepared 'building blocks' of code.
  - The most famous Constructors are VCL, SennaSpy, BWG, PS-MPC, TPPE and IVP.

Malware

Familia: Exploit Kit

Shellcode
which is a small malware payload

Definición

An exploit kit is a toolkit (a collection of exploits)
designed to facilitate the exploitation of client-side vulnerabilities
most commonly found in browsers and their plugins
in order to deliver malware on end users' machines.

- These kits scan devices for different kinds of software vulnerabilities and, if any are detected, deploy additional malware to further infect a device.
  - The most common method used by attackers to distribute exploits and exploit kits is through webpages, but exploits can also arrive in emails.
  - Some websites unknowingly and unwillingly host malicious code and exploits in their ads.
  - Exploits often include **shellcode** used to download additional malware from attacker-controlled networks.

Malware

Mapa mental

Virtool

Constructor

Hacktool

Conceptos similares

Exploit Kit (EK)

Exploits

Malware

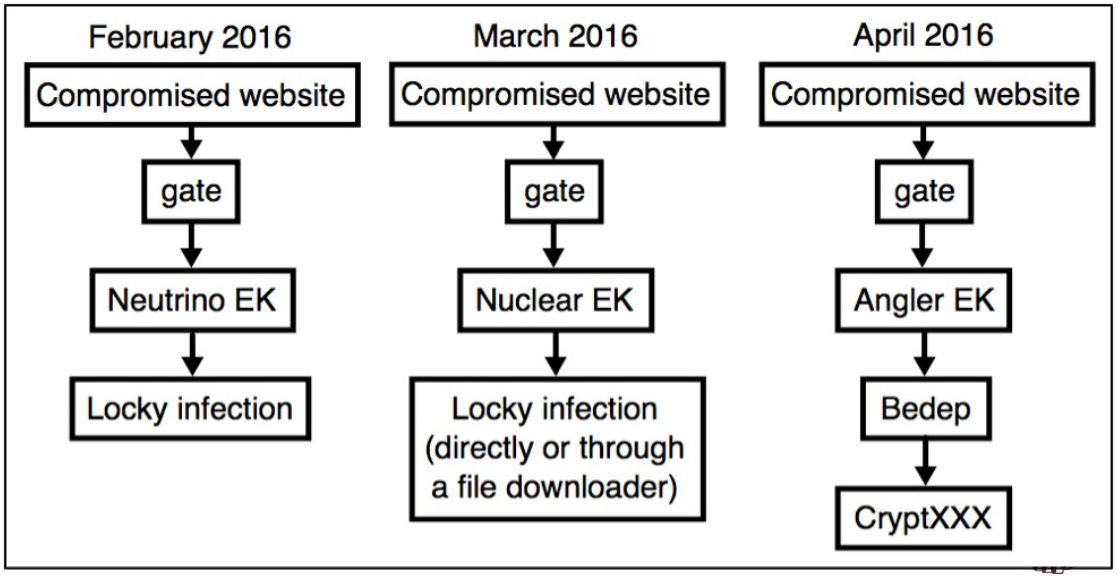
Familia: Exploit Kit

Definición

Campaign - A series of attacks using an EK and infrastructure to direct victims to that EK.

Ejemplos

- pseudo-Darkleech
  - https://unit42.paloaltonetworks.com/unit42-campaign-evolution-darkleech-to-pseudo-darkleech-and-beyond/
- Afraidgate
  - https://unit42.paloaltonetworks.com/afraidgate-major-exploit-kit-campaign-swaps-locky-ransomware-for-cryptxxx/



Malware

Familia: Trojan

Cada empresa define sus tipos de troyanos, por ejemplo, Crowdstrike define 10.

Trojan

1. TrojanBanker
2. TrojanBomb
3. TrojanClicker
4. TrojanDoS o DDoS
5. TrojanDownloader
6. TrojanDropper
7. TrojanIM
8. TrojanNotifier
9. TrojanProxy
10. TrojaPSW
11. Trojan SMS

12. TrojanRansom
13. TrojanSpy

Definición

It disguises itself as legitimate code or software.

Nadie dice que es algo malo verdad?

- Once inside the network, attackers are able to carry out any action that a legitimate user could perform, such as:
  - Exporting files.
  - Modifying data.
  - Deleting files.
  - Altering the contents of the device.
- Trojans may be packaged in downloads for games, tools, apps or even software patches.
- Many Trojan attacks also leverage social engineering tactics, as well as spoofing and phishing, to prompt the desired action in the user.

Malware

Familia: Phishing

Definition

Email or Web sites that invite you to divulge login, password or personal/confidential information by pretending to be a proper source, such as a bank, your ISP or other service you use regularly.

The word is a neologism created as a homophoneof *fishing* due to the similarity of using a **bait** (cebo, carnada) in an attempt to catch a victim.

Phishing o suplantación de identidad es un término que denomina un modelo de abuso informático y que se comete mediante el uso de un tipo de **ingeniería social**, caracterizado por intentar adquirir información confidencial de forma fraudulenta.

Malware

Familia: Logic Bomb

Definition

It is a piece of code intentionally inserted into
a software system that will set off a malicious function
when specified conditions are met.

- It lies dormant (for long periods of time) until a specific condition occurs. When this condition is met (disgruntled employee), the logic bomb is triggered — devastating a system by corrupting data, deleting files, or clearing hard drives.
- They are small bits of code contained in other programs. Although they might be malicious, they're not technically malware (AVAST).
- Trial versions of programs that offer some level of access for a specified period of time are called **trialware**. Similar to logic bombs, trialware uses a logical condition that is why part of the defining characteristics of logic bombs is their destructive nature.

Malware

Familia: Botnet

Definition

Botnets are networks of hijacked computer devices used to carry out various scams and cyberattacks.

- The term “botnet” is formed from the word’s “robot” and “network.”
- Assembly of a botnet is usually the infiltration stage of a multi-layer scheme. The bots serve as a tool to automate mass attacks, such as data theft, server crashing, and malware distribution.
- Issuing commands is a vital part of controlling a botnet. However, anonymity is just as important to the attacker. As such, botnets are operated via remote programming.
  - Command-and-control (C&C) is the server source of all botnet instruction and leadership. This is the bot herder's main server, and each of the zombie computers gets commands from it.
  - Each botnet can be led by commands either directly or indirectly in the following models: i) Centralized client-server models, ii) Decentralized peer-to-peer (P2P) models

Malware

Familia: Rootkit

Virus: Hidden & Inactive
Rootkit: Hidden & Active

Definition

It is a collection of software designed to enable access to a computer or an area of its software that is not allowed and often masks its existence or the existence of other software.

- The term rootkit is a compound of "root" (the privileged account on Unix-like OS) and the word "kit" (software components that implement the tool).
- If an intruder could replace the standard administrative tools on a system with a rootkit, the intruder could obtain root access over the system whilst simultaneously concealing these activities from the legitimate system administrator.
- It is designed to give hackers access to and control over a target device. Some rootkits can also infect your computer's hardware and firmware. Rootkits are adept at concealing their presence, but while they remain hidden, they are active.

Malware

Familia: Ransomware

Definition

It prevents or limits users from accessing their system,
either by locking the system's screen or by locking the users' files
until a ransom is paid.

- Ransom prices vary depending on the ransomware variant and the price or exchange rates of digital currencies.
  - Thanks to the perceived anonymity offered by cryptocurrencies, ransomware operators commonly specify ransom payments in bitcoin.
  - Recent ransomware variants have also listed alternative payment options such as iTunes and Amazon gift cards.
- It should be noted, however, that paying the ransom does not guarantee that users will get the decryption key or unlock tool required to regain access to the infected system or hostaged files.

Malware

Familia: Spyware

Definición

Just like a spy, a hacker uses spyware to track your internet activities and steal your information without you being aware of it.

- What kind of information is likely to be stolen by Spyware?

  Two common targets:

  - Credit card numbers
  - Passwords.

Conclusiones

Conclusiones

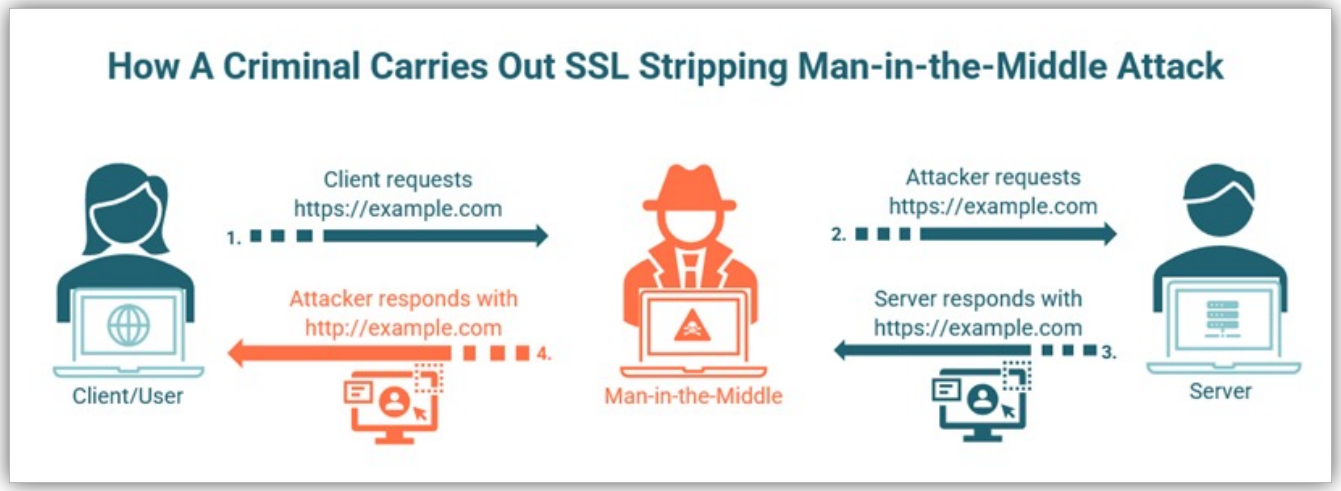
Conclusiones

Resumen

- El malware usa diferentes técnicas de ataque local y remoto.
- Una de las más usadas es:

  MITM (*Man in the Middle*)
- Muchas variantes del ataque (8)

  https://cheapsslsecurity.com/blog/types-of-man-in-the-middle-attacks/



Conclusiones

Resumen

Comparativo de comportamientos

Tipo \ Carcaterísticas	Replicación	Red	MiTM	Ing Social	Esconder	C&C
Virus / Worm	Human / Solo	Inicio Local			Si	
Adware				Generador		
Backdoor		inicio Remoto				Si
Downloader						
Dropper						
Keylogger			Local			
Hacktool						
Troyan				Si		
Phisiing				Si		
Logic Bomb					Si	Condiciones Locales
Botnet	Si	inicio Local				Si
Rootkit					Asimismo y Actividad	
Ransomware						
Spyware		L o R	Si		Si	Si

The end

Contacto

Raúl Acosta Bermejo

http:www.cic.ipn.mx
http://www.ciseg.cic.ipn.mx/

racostab@ipn.mx
racosta@cic.ipn.mx

57-29-60-00
Ext. 56652