INSTITUTO FEDERAL
Bahia

MALWARES

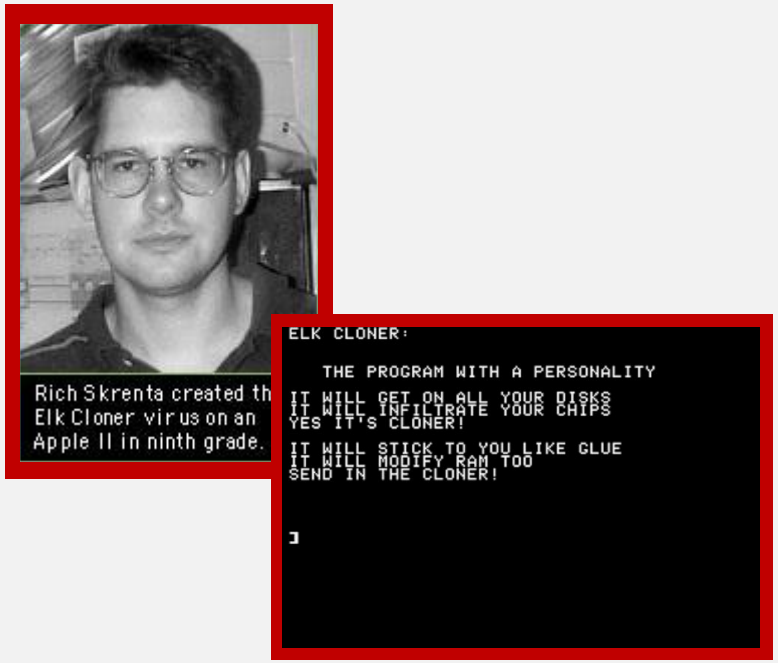
“Se você colocar uma chave debaixo do tapete permitirá que um ladrão encontre-a. [...]Se eles sabem que há uma chave escondida em algum lugar, eles farão de tudo para encontrá-la.”

COOK, Tim – CEO da Apple Inc.

O QUE É UM MALWARE?.

Malware é todo e qualquer software malicioso, que tem objetivo de atacar um sistema operacional ou um conjunto de deles, tentando danificar, coletar dados, chantagear ou até assustar o mesmo.

O primeiro Malware de distribuição ampla da história foi o Elk Cloner criado por Rich Skrenta, em 1982. Porém antes em 1966 o cientista húngaro John von Neumann já havia criado um protótipo de Malware.



SEUS PRINCIPAIS TIPOS SÃO:

WORMS E BOTNETS

CRIMEWARE

BACKDOORS

VÍRUS

SPYWARES

RANSOMWARE

ROOTKIT

TROJAN HORSE

WORMS E BOTNETS

- Worm é um programa capaz de se propagar automaticamente através de redes, enviando cópias de si mesmo de computador para computador.

- Diferente do vírus, o Worm não embute cópias de si mesmo em outros programas ou arquivos e não necessita ser explicitamente executado para se propagar.

- Worms são notadamente responsáveis por consumir muitos recursos assim diminuindo o desempenho da máquina.

- Já o Botnet ou só Bot, é um Malware capaz se propagar automaticamente de modo similar ao Worm, explorando vulnerabilidades existentes ou falhas na configuração de softwares instalados em um computador.

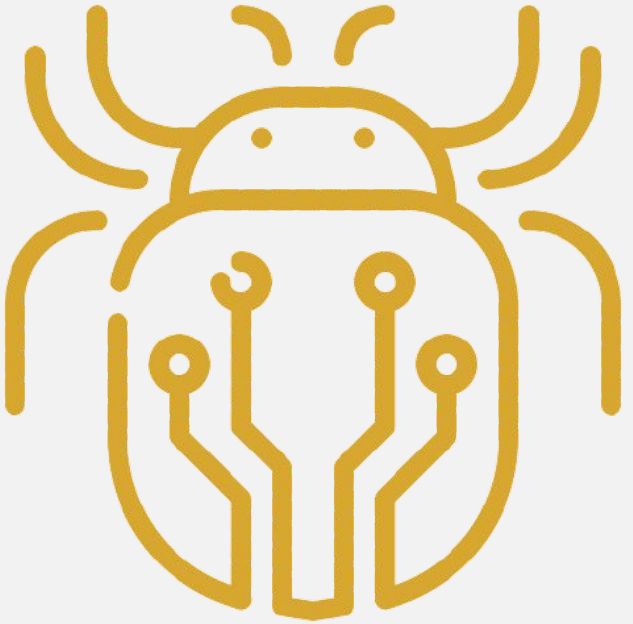
- Porém, diferente do Worm ele dispõe de mecanismos de comunicação com o invasor, permitindo que o Bot seja controlado remotamente, geralmente através de um servidor de IRC.

VÍRUS

- Um vírus é um Malware que pode ser um programa ou parte de programa que se propaga infectando, isto é, inserindo cópias de si mesmo e se tornando parte de outros programas e arquivos de um computador.

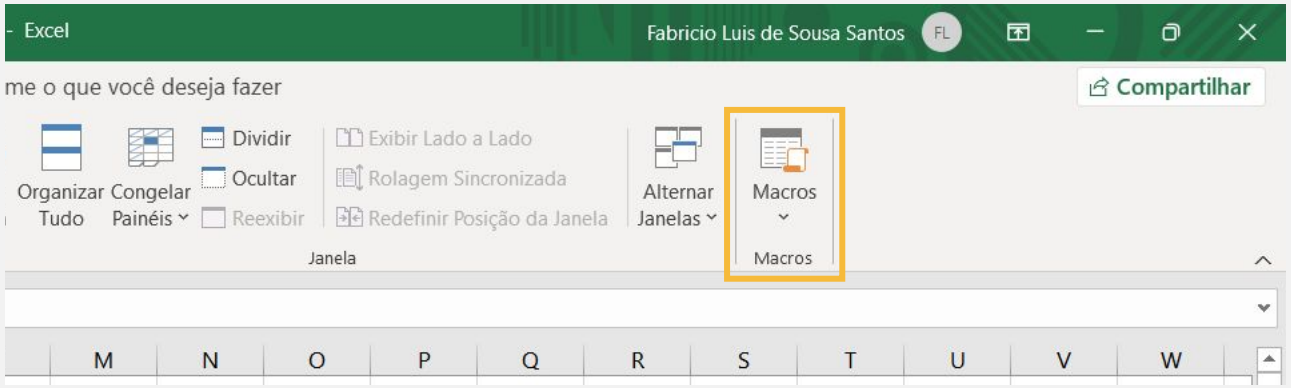
- O vírus depende da execução do programa ou arquivo hospedeiro para que possa se tornar ativo e dar continuidade ao processo de infecção.

- Podem se propagar por E-mail, mídias removíveis, etc...



O QUE É MACRO?.

Macro é uma função de alguns programas, principalmente do pacote Office que tem como objetivo automatizar alguma função dentro do mesmo usando a linguagem do Microsoft Visual Basic ou gravando o passo a passo com o gravador de Macros.



Execute uma macro quando abrir a planilha:

Sub Auto_Open()
MsgBox "Mensagem"
End Sub

MALWARE DE MACRO

Malware de macro é um código malicioso que é programado na linguagem Visual Basic dentro de um software com suporte da função “Marcos". Esse Malware vem geralmente através de anexos de e-mails, dentro de arquivos Office. Exemplo: Melissa e Concept.

SPYWARE

- Spyware é um tipo de malware que tem como objetivo a espionagem e o recolhimento de informações de um dado usuário.

- Existem diversas subcategorias de Spywares, tais como:

  - Keylogger
  - Screenlogger
  - Riskware
  - Adware

POP-UPS

Isso não é um Adware.

Jovem de Valença viraliza na web com seus truques para queimar gordura localizada!

A estudante de veterinária mostra de forma simples como é possível reduzir drasticamente a gordura da barriga.

Centro em Emagrecimento Zero Peso | Patrocinado

RANSOMWARE

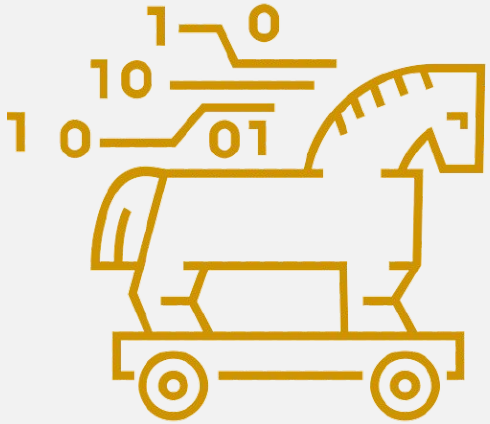
- Invade a máquina
- Bloqueia o acesso dos usuários, sistema completo de empresas;
- Resgate – Criptomoedas
- Infecção – e-mails, sites downloads.
- Atualização de navegadores, Antivírus e sistema operacional;
- 2021 – COLONIAL PIPELINE - USA, JBS – US$11mi – USA, CANADÁ E AUSTRÁLIA;

TROJAN HORSE

- Ou simplesmente Cavalo de Tróia, é um dos mais perigosos tipos de Malware. Sua estrutura é vim disfarçado de um programa simples porém ao ser executado sua carga útil vem a tona.

- Sua principal característica é fazendo a analogia ao real Cavalo de Tróia da história, que é poder carregar um ou mais tipos diferentes de Malwares dentro do mesmo.

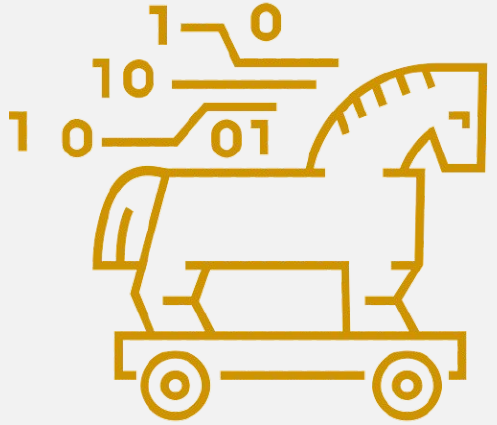
- Em grande parte das vezes, técnicas como Phishing levam qualquer usuário a executar esse malware acreditando ser um programa inofensivo.



TROJAN HORSE

- Algumas de suas subcategorias são:

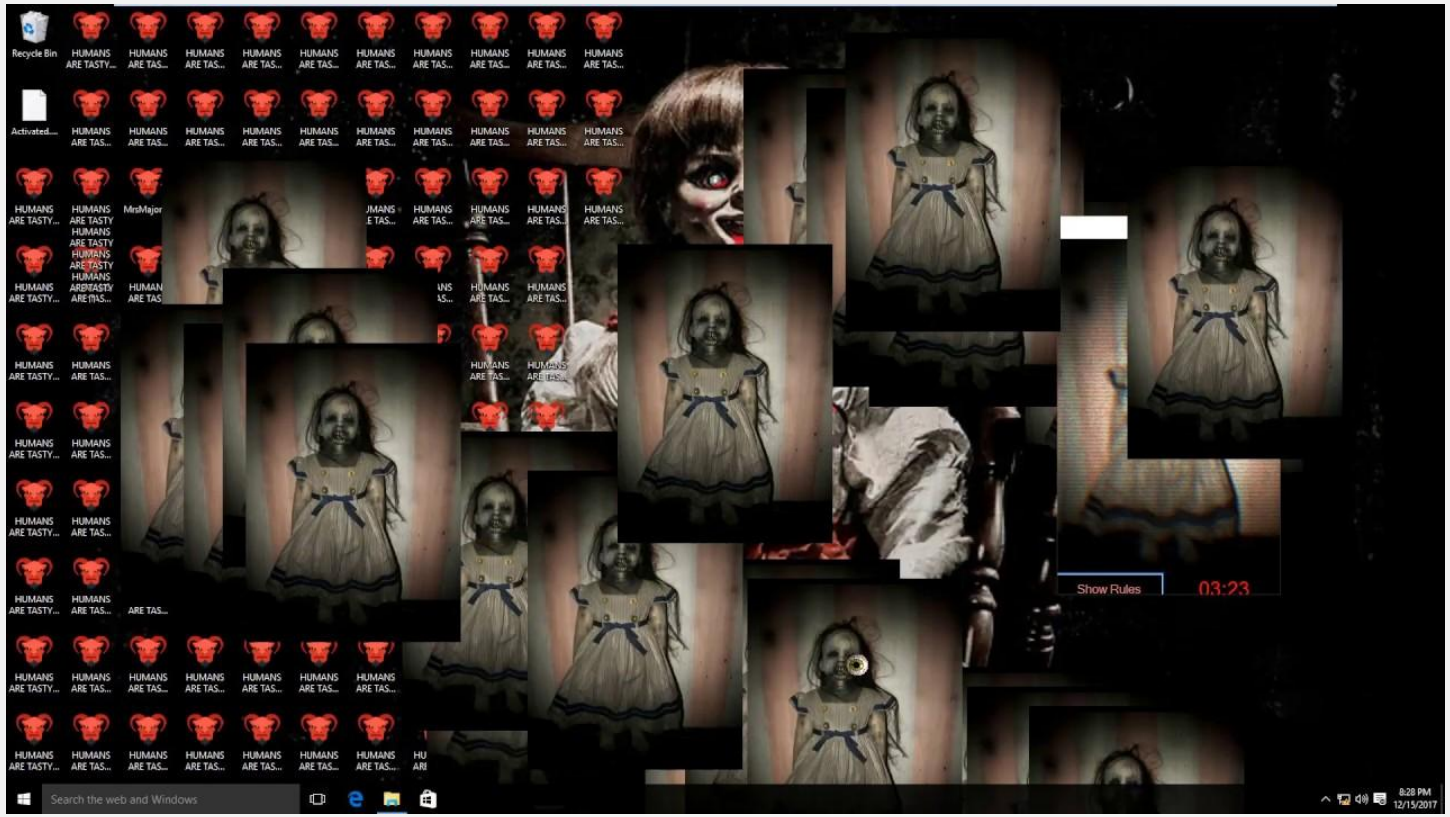
  - Trojans de backdoor
  - Trojan Rootkit
  - Trojans dropper/downloader
  - Trojans bancários
  - Trojan GameThief
  - Trojan IM (mensagens instantâneas)
  - Trojan Ransom
  - Trojan Espião



EXEMPLOS DE MALWARES

MRS MAJOR

TROJAN

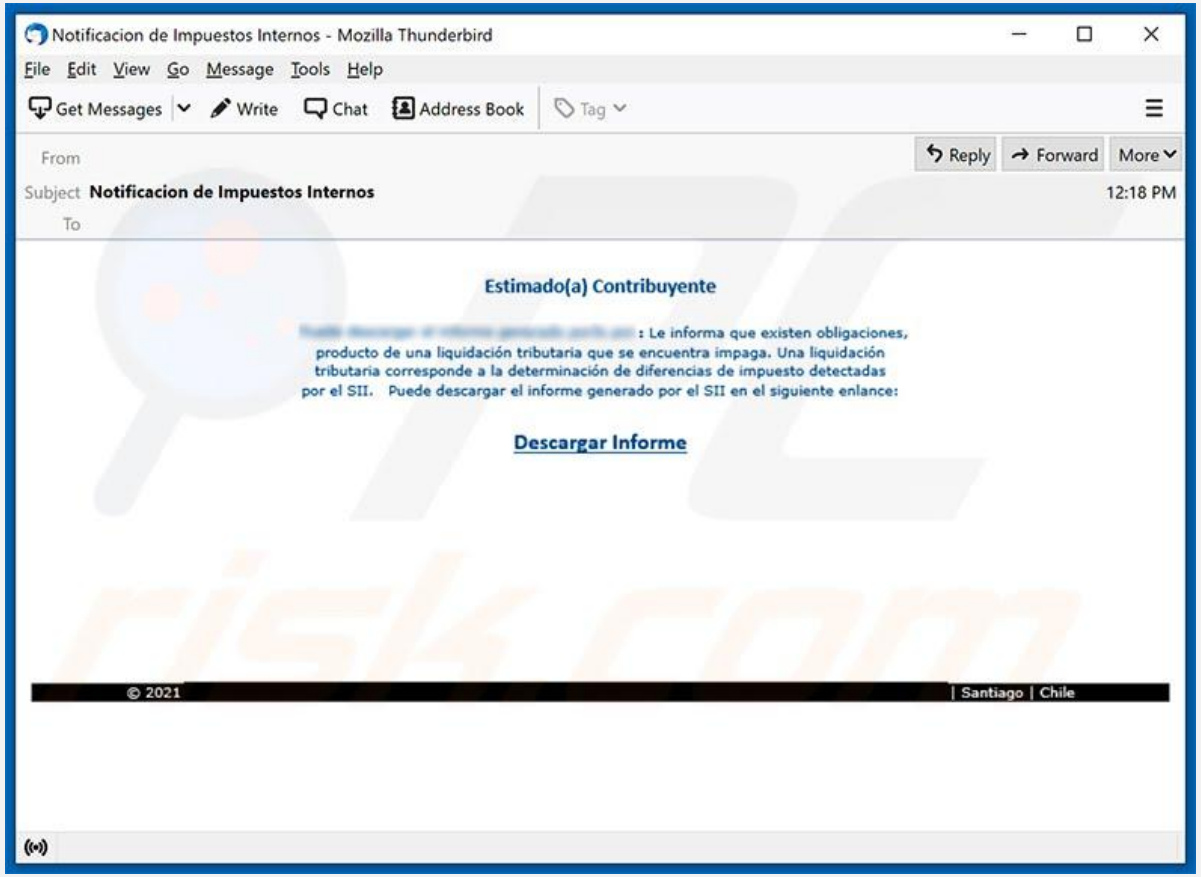


Disponível em:
https://github.com/Gork3m/MrsMajor-3.0

EXEMPLOS DE MALWARES

BIZARRO

BANKER TROJAN



EXEMPLOS DE MALWARES

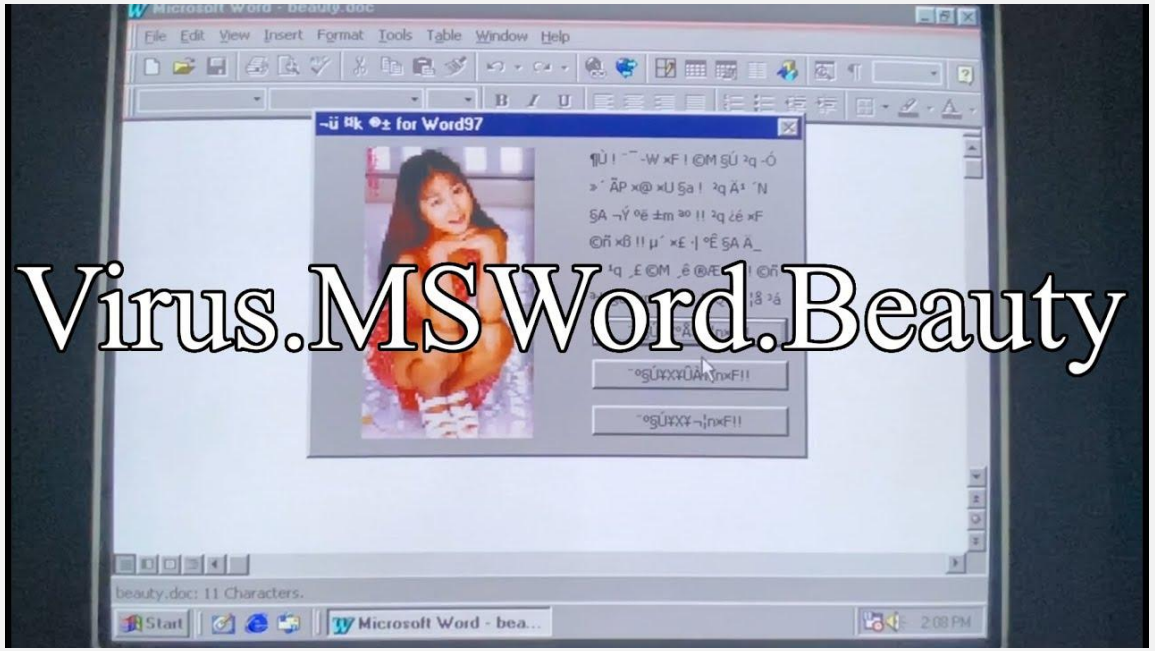
WANNA CRY

RANSOMWARE

EXEMPLOS DE MALWARES

MSWORD. BEAUTY

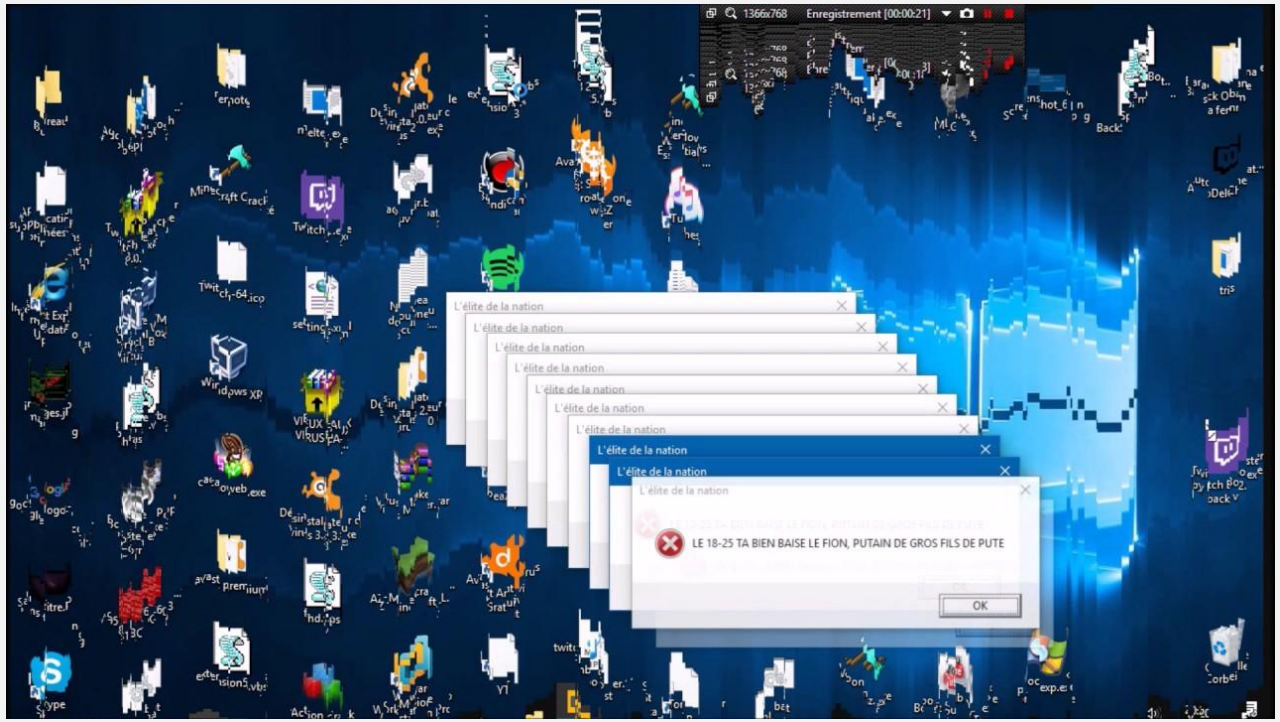
VÍRUS DE MACRO



EXEMPLOS DE MALWARES

TWITCH BOOSTER.EXE

VÍRUS



EXEMPLOS DE MALWARES

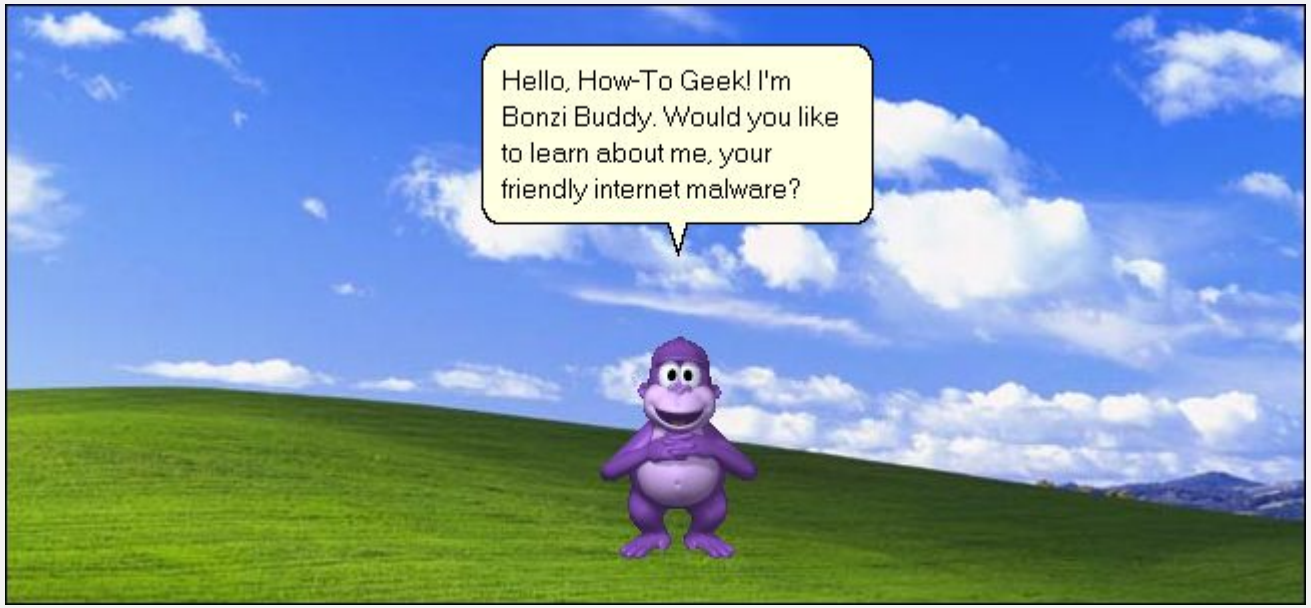
CHILLED WINDOWS

JOKE MALWARE

EXEMPLOS DE MALWARES

BONZIKILL

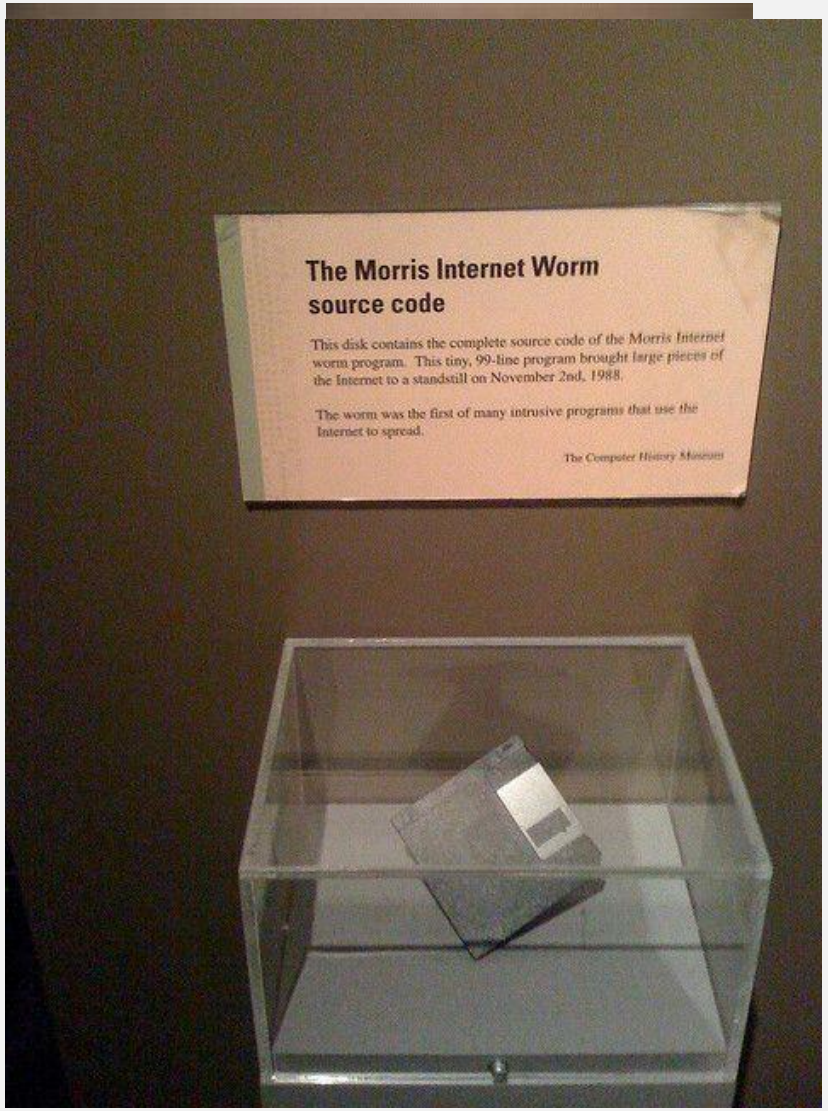
SPYWARE



EXEMPLOS DE MALWARES

MORRIS WORM

WORM



PROPAGAÇÃO E ATAQUE

- **O tipo de propagação mais comum de Malwares é o Phishing, que consiste em utilizar técnicas de engenharia social para ludibriar usuários de redes sociais de modo a espalhar algum tipo de Malware.**

  - **E-mails de Spam(Macro por exemplo)**
  - **Download de arquivos falsos**
  - **Mineração de criptomoedas em backdoor**
  - **Roubo de dados bancários em páginas falsas**

PROPAGAÇÃO E ATAQUE

- **Tipos de ataques:**
  - **Brute Force**
  - **SQL Injection**
  - **Bombas Lógicas**
  - **Envenenamento de DNS**
  - **Cross-site scripting (XSS)**

O QUE É PAYLOAD?

Payload ou carga útil é parte maliciosa escondida em todo Malware e o seu poder de fogo.

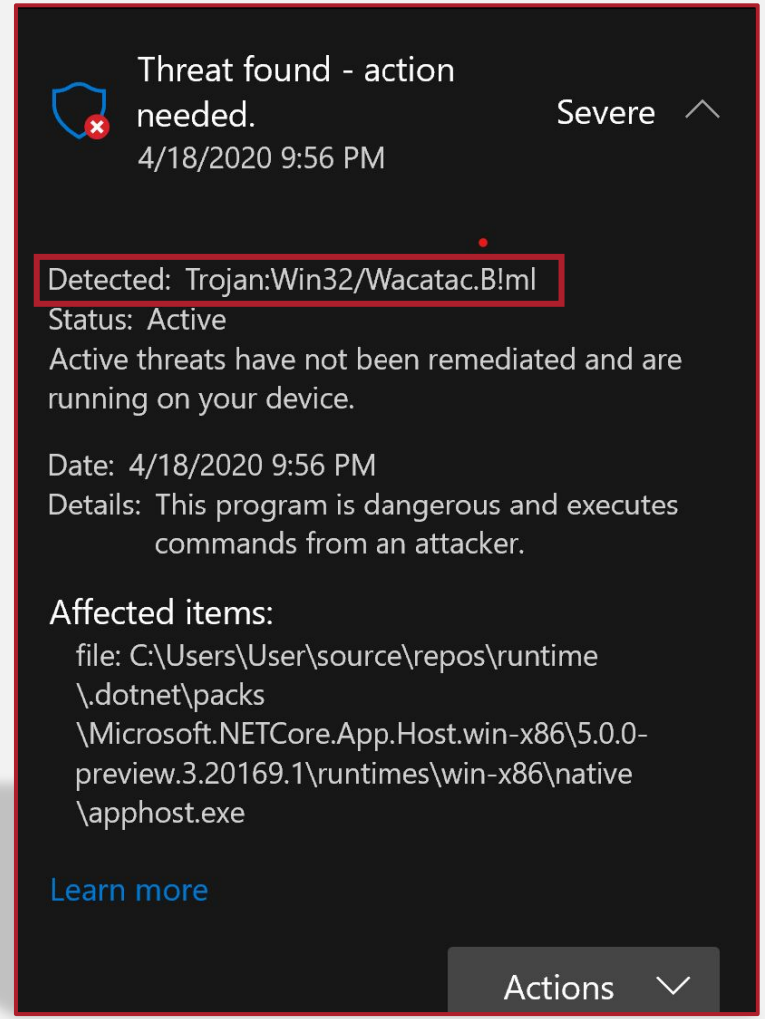
- **Alguns exemplos de cargas são: destruição de dados, mensagens ofensivas, quebra de segurança, roubo de informações.**

O QUE É UM ANTI-MALWARE?.

Diferente do Malware o Anti-Malware é um programa usado para prevenir, localizar e destruir arquivos e programas maliciosos.

- **Um Anti-Malware deve ser capaz de:**

  - **Proteger o sistema.**
  - **Detectar assinaturas de softwares maliciosos.**
  - **Analisá-los em quarentena.**
  - **Os remover se for necessário.**



O QUE É UM ANTI-MALWARE?.

- **Alguns tipos de Anti-Malware:**

  - **Antivírus**
  - **Anti Spam**
  - **Anti Spyware**
  - **Anti Trojan**

DEMONSTRAÇÃO DE RANSOMWARE

Disponível em:
https://github.com/FabricioLuisdeSousaSantos/Ransomware_in_Python---Fabr-cio_Lu-s-

REFERÊNCIAS BIBLIOGRÁFICAS

Taxonomia de Malwares: Uma Avaliação dos Malwares Automaticamente Propagados na Rede.
http://www.ufrgs.br/tri/files/sbseg2009.pdf

Principais Ameaças e Vulnerabilidades.
https://edisciplinas.usp.br/pluginfile.php/4591628/mod_resource/content/1/2019-03-Aula%20Malware_2019.pdf

Prevenção de Ataques Causados por Malwares. https://cutt.ly/FRJS5Di

O que é um trojan e que danos eles podem causar?. https://www.kaspersky.com.br/resource-center/threats/trojans

Slideshare - Malwares(Breno Damasceno). https://pt.slideshare.net/BrenoDamasceno1/malware-33777497

Criado por: Fabrício Luis de Sousa Santos & Wanderson Amorim dos Santos, 2021, IFBA.