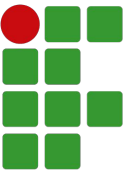
Códigos Malicioso (Malware)

Prof. Gustavo neves



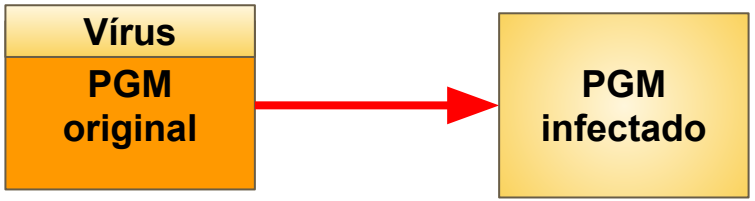
INSTITUTO FEDERAL
Sul de Minas Gerais
Campus Muzambinho

Malware

- Os códigos maliciosos, conhecidos como *Malware*, são programas que tem a intenção de causar algum dano nos dispositivos, computadores, *modems, switches,* roteadores, smartphones, etc.
- Os dispositivos são infectados quando:
  - acessamos páginas *WEB* maliciosa através de navegadores vulneráveis
  - acesso à mídias removíveis infectadas (pen-drives)
  - ao executar arquivos infectados
  - o atacante invade o computador e incluem arquivos contendo códigos maliciosos
- Após o código ser instalado passa a ter acesso aos dados armazenados no computador e podem executar ações em nome do usuário, de acordo com suas permissões.

Funcionamento dos Malware

- Vírus
  - uma parte de software que infecta programas
    - modifica programa ou arquivo com suporte script



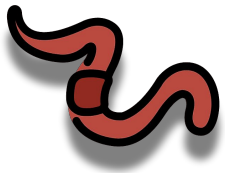

```
Programa X:{
xxxxxxxxxxxxxxx;
xxxxxxxxxxxxx;
9999// marcador do vírus
instruções de infecções
wwwwwwwwwwwwwwwwww;
yyyyyyyyyyyyyyyyy;
```

Vírus

- Vírus é um programa ou parte de um programa de computador que se propaga inserindo cópias de si mesmo e tornando parte de outros programas e arquivos
- Ele se instala através de um hospedeiro, ou seja, um programa já infectado é executado
- Seu principal meio de propagação são as mídias. Também ocorrem nos e-mails.
- Há diferentes tipos de vírus. Uns ficam ocultos infectando arquivos de disco e executando várias atividades. Outros ficam inativos por um determinado período.
    - **Propagado por e-mail:** anexos que o usuário clica, envia cópias de si mesmo para e-mails da lista de contatos
    - ***Script***: Linguagens *VBScript* e *JavaScript,* recebido ao acessar uma WEB ou e-mail, podendo ser automaticamente executado
    - **Macro:** escrito em linguagem de macro. Office (Excel, Word, Powerpoint)
    - **Celular:** por meio de mensagens recebidas por Bluetooth. Realiza ligações, drena a bateria e tenta se propagar a outros celulares

Worm (”vermes”)

- *Worm* é um programa capaz de se propagar de forma automática, enviando cópias de si mesmo entre os dispositivos
- Se difere do vírus, o *worm* não se propaga por meio de inclusão de cópias em programas ou arquivos, mas sim pela execução direta de suas cópias ou exploração automática de vulnerabilidade existentes
- Devido à grande quantidade de cópias propagadas, são responsáveis por consumir muitos recursos, afetando o desempenho de redes e computadores.
- O processo de infecção dos *worms* ocorre da seguinte maneira:
    - **identificação dos alvos:** após infectar um computador, o *worm* tenta se propagar e continuar o processo de infecção. Ele busca identificar seus possíveis alvos, fazendo varredura na rede, aguardar que outros computadores contate o infectado, utilizar de listas predefinidas na internet, informações contidas no computador infectado, etc.



Worm (”vermes”)

- **envio e ativação de cópias:** após identificar os alvos, o *worm* tenta enviar suas cópias:
  - anexadas a e-mails
  - programas de troca de mensagens instantâneas
  - pastas compartilhadas em rede locais ou P2P
  - a infecção ocorre apenas quando o usuário carrega o software ou insere uma mídia infectada
- **reinício do processo:** após o alvo ser infectado, o processo de propagação e infecção recomeça

Bot

- *Bot* é um programa que dispõe de mecanismos de comunicação com o invasor
- Permite que a máquina seja controlada à distância
- A comunicação entre o invasor e o computador infectado pelo *bot* pode ocorrer através de mensagens instantâneas, servidores *Web*, redes do tipo P2P, dentre outros.
- O processo de infecção é similar ao *worm*
- O computador infectado por um *bot* é chamado de zumbi (*zombie computer*)
- *Botnet* é uma rede formada por milhares de computadores zumbi
- Alguns ações maliciosas:
    - DDoS
    - envio de *spam*
    - camuflagem da identidade do atacante

Spyware

- *Spyware* é um programa que monitora atividades de um sistema e envia-as a terceiros
- Pode ser utilizado de forma legítima ou maliciosa
  - **Legítimo:** instalado pelo próprio usuário com objetivo de monitorar de qual modo máquina está sendo utilizada pelos demais usuários
  - **Malicioso:** corrompe a privacidade do usuário e sua segurança. Coleta dados do usuário como: toques no teclado (*keyloggers*), cliques de mouse e capturas de telas (*screenloggers*), dados trafegados na rede, e dados em arquivos locais

***Adware*:** software de propaganda, aparece muitas vezes embutidos em um programa útil. Busca de retorno financeiro

Backdoor

- *Backdoor* (*trapdoor)* é um programa que permite o acesso remoto por um usuário desautorizado
- Se instala através de outros códigos maliciosos, cuja máquina já estava infectada, por atacantes, exploração de vulnerabilidades
- Uma vez instalado não necessita mais de recorrer aos métodos utilizados na invasão ou infecção
- Programas de acesso remoto BackOrifice, NetBus, VNC, Radmin, se mal configurados podem ser classificados como *backdoors*

Cavalo de Troia (*trojan*)

- Cavalo de troia é um programa que executa funções maliciosa sem o conhecimento do usuário
- programa que faz algo útil, mas tem um código malicioso adicional
- São obtidos através de programas gratuítos, versões piratas, sites na Internet que parecem ser apenas cartões virtuais animados, fotos, jogos, protetores de tela
- Precisam da ação do usuário para executar o programa

Rootkit

- *Rootkit* é um conjunto de ferramentas para ganhar acesso de administrador (*root*) em uma máquina, sem que seja percebido e assegurar sua presença de um invasor ou de outro código malicioso