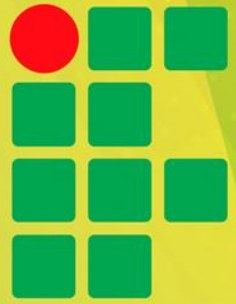
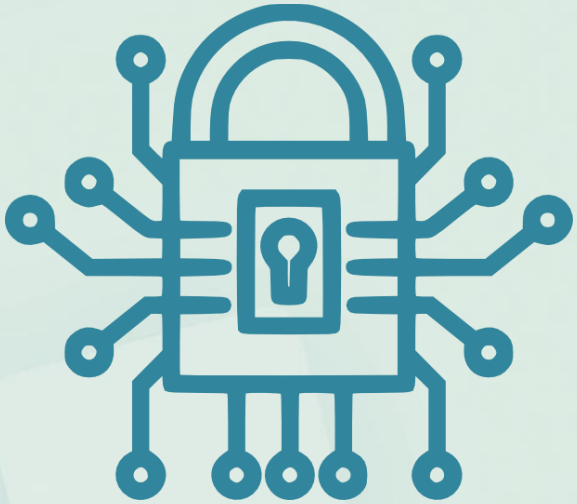


INSTITUTO FEDERAL

Sertão Pernambucano

Segurança da Informação



Códigos Maliciosos

Prof. Heraldo Gonçalves Lima Junior

INSTITUTO FEDERAL
Sertão Pernambucano

Worm

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

Worm

- Diferente do vírus, o worm não se propaga por meio da inclusão de cópias de si mesmo em outros programas ou arquivos, mas sim pela execução direta de suas cópias ou pela exploração automática de vulnerabilidades existentes em programas instalados em computadores.

Worm

- **São responsáveis por consumir muitos recursos**, devido à grande quantidade de cópias de si mesmo que costumam propagar.

Worm – Etapas de Infecção

1. **Identificação dos computadores alvos:** após infectar um computador, o worm tenta se propagar e continuar o processo de infecção. Identifica as vítimas:
   - efetuar varredura na rede e identificar computadores ativos;
   - utilizar informações contidas no computador infectado, como arquivos de configuração e listas de endereços de e-mail.

Worm – Etapas de Infecção

2. **Envio das cópias:** após identificar os alvos, o worm efetua cópias de si mesmo e tenta enviá-las para estes computadores, por uma ou mais das seguintes formas:
   - via programas de troca de mensagens instantâneas;
   - Incluídas em pastas compartilhadas em redes locais ou do tipo P2P (Peer to Peer).
   - anexadas a e-mails;

Worm – Etapas de Infecção

3. **Ativação das cópias:** após realizado o envio da cópia, o worm necessita ser executado para que a infecção ocorra:
   - imediatamente após ter sido transmitido, pela exploração de vulnerabilidades em programas sendo executados no computador alvo.
   - diretamente pelo usuário.
   - pela realização de uma ação específica do usuário, como por exemplo, a inserção de uma mídia removível.

Worm – Etapas de Infecção

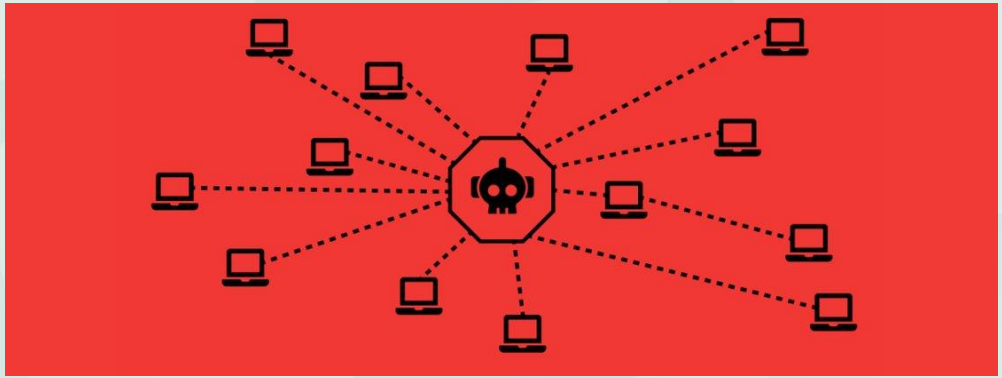
4. **Reinício do processo:** após o alvo ser infectado, o processo de propagação e infecção recomeça, sendo que, a partir de agora, o computador que antes era o alvo passa a ser também o computador originador dos ataques.

Bot e Botnet

- Bot é um programa que dispõe de mecanismos de comunicação com o invasor que permitem que ele seja controlado remotamente.

Bot e Botnet

- Processo de infecção e propagação similar ao do worm, sendo capaz de se propagar automaticamente, explorando vulnerabilidades existentes em computadores.



Bot e Botnet

- A comunicação entre o invasor e o computador infectado pelo bot pode ocorrer via canais de IRC, servidores Web e redes do tipo P2P, entre outros meios.

Bot e Botnet

- Um computador infectado por um bot costuma ser chamado de **zumbi** (zombie computer), pois pode ser controlado remotamente, sem o conhecimento do seu dono.

Bot e Botnet

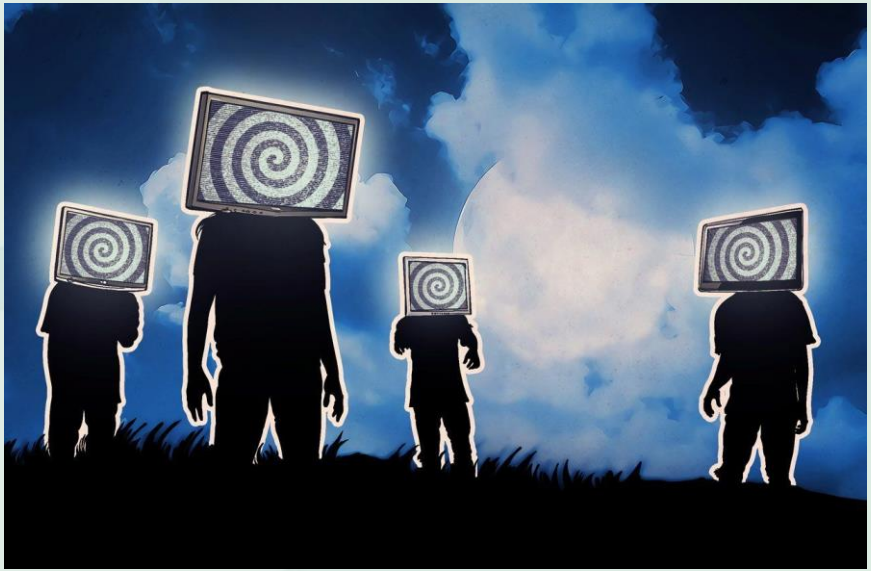
- **Botnet** é uma rede formada por centenas ou milhares de computadores zumbis e que permite potencializar as ações danosas executadas pelos bots.

Bot e Botnet

- Quanto mais zumbis participarem da botnet mais potente ela será. O atacante que a controlar, além de usá-la para seus próprios ataques, também pode alugá-la para outras pessoas ou grupos que desejem que uma ação maliciosa específica seja executada.

Bot e Botnet: Etapas de Infecção

1. Um atacante propaga um tipo específico de bot na esperança de infectar e conseguir a maior quantidade possível de zumbis;



Bot e Botnet: Etapas de Infecção

2. Os zumbis ficam então à disposição do atacante, agora seu controlador, à espera dos comandos a serem executados;
3. quando o controlador deseja que uma ação seja realizada, ele envia aos zumbis os comandos a serem executados;

Bot e Botnet: Etapas de Infecção

4. Os zumbis executam então os comandos recebidos, durante o período predeterminado pelo controlador;
5. Quando a ação se encerra, os zumbis voltam a ficar à espera dos próximos comandos a serem executados.

Spyware

- Spyware é um programa projetado para **monitorar as atividades** de um sistema e enviar as informações coletadas para terceiros.

Spyware

- **Legítimo:** quando instalado em um computador pessoal, pelo próprio dono ou com consentimento deste, com o objetivo de verificar se outras pessoas o estão utilizando de modo abusivo ou não autorizado.

Spyware

- **Malicioso:** quando executa ações que podem comprometer a privacidade do usuário e a segurança do computador, como monitorar e capturar informações referentes à navegação do usuário ou inseridas em outros programas (por exemplo, conta de usuário e senha).

Spyware

- **Malicioso:** quando executa ações que podem comprometer a privacidade do usuário e a segurança do computador, como monitorar e capturar informações referentes à navegação do usuário ou inseridas em outros programas (por exemplo, conta de usuário e senha).

Atividade

1. (1pt) Pesquise sobre os tipos de Spyware e apresente pelo menos 4 tipos, suas características e como se proteger.

Obrigado!
Vlw! Flw!

INSTITUTO FEDERAL
Sertão Pernambucano