Vírus de Computador

Instituto Federal de Educação, Ciência e Tecnologia do Triângulo Mineiro

Prof. Edwar Saliba Júnior

Introdução

- O que é Vírus de Computador para você?

Conceito

- Vírus:
  - é um programa ou pedaço de código que é carregado ao seu computador sem seu conhecimento ou permissão. Alguns vírus são meramente irritantes, mas a maioria dos vírus são destrutivos e designados a infectar e controlar sistemas vulneráveis. Um vírus pode se alastrar a vários computadores e redes ao criar cópias de si, assim como um vírus biológico passa de uma pessoa para a outra. (Avast, 2017)

Formas de Contaminação

- Vírus são geralmente escondidos em um programa usado em comum com outras pessoas, como um *game* ou PDF, ou você pode receber um arquivo infectado anexado ao seu e-mail ou de um outro arquivo baixado da Internet.
- Assim que você começa a interagir com o arquivo (roda o programa, clica em um anexo ou abre um arquivo), o vírus é executado automaticamente. O vírus pode se copiar para outros arquivos e fazer mudanças em seu computador. (Avast, 2017)

Outras Formas de Contaminação

- Cópia de arquivos de ou para *pendrives*. Ou de ou para qualquer outro tipo de dispositivo ou mídia de armazenamento de dados (HD externo, CD's, DVD's e etc.);
- acesso a sites de origem duvidosa;
- download de *softwares* de origem duvidosa ou jogos de computador (principalmente);
- sistema operacional desatualizado;
- sistema operacional sem *firewall*;
- sistema operacional sem antivírus e
- etc.

Como Reconhecer um Vírus

- A sua conexão à internet pode estar devagar ou nem se quer existir;
- é comum o seu antivírus e/ou *firewall* desaparecerem ou ficarem desativados e
- computadores infectados com vírus são capazes de agirem sozinhos, executando ações sem você solicitar ou mesmo sem você saber. (Avast, 2017)

Como Remover um Vírus

- Remova todos os arquivos temporários e execute um escaneamento de vírus usando um *software* antivírus. Se algum vírus for detectado, então, apague-o.

  (Avast, 2017)

Como Se Prevenir de Vírus

- Evite programas originado em fontes desconhecidas;
- não abra anexos contidos em *e-mail* que não foram solicitados ou no Facebook;
- somente baixe aplicativos que estão no mercado oficial ou de empresas que são conhecidas no mercado (Avast, 2017) e
- proteja seu telefone e/ou computador com um antivírus de boa procedência.

Malware

- Abreviação do termo em Inglês: ***Malicious Software*** (em Português, **Programa Malicioso**); (WIKIPÉDIA, 2017)
- *Malware* refere-se a qualquer tipo de software malicioso que tenta infectar um computador, telefone ou *tablet*. Hackers usam *malwares* para vários motivos, na maioria das vezes com o intuito de extrair informações pessoais, roubar dinheiro e propriedade intelectual ou impedir que usuários acessem seus próprios computadores. (AVAST, 2017)

De onde vêm os *malwares*?

- Geralmente os *malwares* acessam o seu dispositivo através da Internet e via *e-mail*, embora ele possa fazer isso através de *sites* hackeados, demos de *games*, arquivos de música, barras de ferramentas, software, assinaturas gratuitas ou qualquer outra coisa que você baixa na Internet. (AVAST, 2017)

Como reconhecer um malware?

- Um computador lento é geralmente um sinal de que a sua máquina pode ter sido infectada com *malware*, assim como *pop-ups*, *spam* e panes frequentes. (AVAST, 2017)

Principais Tipos de *Malwares* Conhecidos

- **Vírus**: propaga-se infectando com cópias de si mesmo e se tornando parte de outros programas e arquivos de um computador. O vírus depende da execução dos arquivos hospedeiros para que possa se tornar ativo e continuar o processo de infecção;
- ***Worm***: 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 executado para se propagar. A sua propagação dá-se através da exploração de vulnerabilidades existentes ou falhas na configuração de *softwares* instalados em computadores. (WIKIPÉDIA, 2017)

Principais Tipos de *Malwares* Conhecidos

- **Trojan** ou em Português, Cavalo de Troia: passa-se por "presente"; cartões virtuais, álbum de fotos, protetor de tela, jogo e etc.; que, além de executar funções às quais foi aparentemente projetado, também executa outras funções, normalmente maliciosas e sem o conhecimento do usuário;
- ***Keylogger***: captura e armazena as teclas digitadas pelo usuário no teclado do computador. Normalmente, a ativação é condicionada a uma ação prévia do usuário, por exemplo, após o acesso a um *e-commerce* ou *Internet Banking*, para captura de senhas bancárias e/ou números de cartões de crédito com o código de segurança. (WIKIPÉDIA, 2017)

Principais Tipos de *Malwares* Conhecidos

- ***Screenlogger***: forma avançada de *keylogger*, capaz de armazenar a posição do cursor e a tela apresentada no monitor, nos momentos em que o *mouse* é clicado;
- ***Spyware***: tem objetivo de monitorar atividades de um sistema e enviar as informações a terceiros;
- ***Adware***: projetado para apresentar propagandas. É comum aparecerem na hora de instalar um programa;
- ***Backdoor***, em Português, “Porta dos Fundos”: permite a entrada de um invasor por meio das portas virtuais existentes no computador. Normalmente, este programa é colocado de forma a não ser notado. (WIKIPÉDIA, 2017)

Principais Tipos de *Malwares* Conhecidos

- ***Exploits***: projetado para explorar uma vulnerabilidade existente em um *software* de computador;
- ***Sniffers***: usados para capturar e armazenar dados trafegando em uma rede de computadores, principalmente onde não se faz uso de criptografia. Deixa a placa de rede em modo promíscuo;
- ***Port Scanners***: fazem varreduras em redes de computadores, com o intuito de identificar quais computadores estão ativos e quais serviços estão sendo disponibilizados por eles. Amplamente usados para identificar potenciais alvos, pois permite associar possíveis vulnerabilidades aos serviços habilitados em um computador;
- ***Bot***: além de incluir funcionalidades de *worms*, dispõem de mecanismos de comunicação com o invasor, permitindo que o programa seja controlado remotamente. O invasor, ao se comunicar com o bot, pode orientá-lo a desferir ataques contra outros computadores, furtar dados, enviar spam e etc. (WIKIPÉDIA, 2017)

Principais Tipos de *Malwares* Conhecidos

- ***Rootkit***: conjunto de programas com o fim de esconder e assegurar a presença de um invasor em um computador comprometido. Apesar do nome "*rootkit*", não é usado para obter acesso privilegiado (root ou administrador) em um computador, mas sim para manter o acesso privilegiado em um computador previamente comprometido;
- ***Quantum***: cria *site* falso para implantar sistemas e obter informações - usado pelo GCHQ (*Government Communications Headquarters* – serviço de inteligência britânico) na vigilância de computadores e Redes. (WIKIPÉDIA, 2017)

Antivírus

- Existem diversos no mercado:
  - Avast,
  - AVG,
  - Avira,
  - Bitdefender,
  - Kaspersky,
  - McAfee,
  - Norton,
  - Panda e
  - Etc.
- Qual é o melhor?
- É gratuito ou é pago?
- Reportagens:
  - Os 5 melhores antivírus gratuitos de 2016 (PAYÃO, 2016)
  - Os melhores antivírus gratuítos e pagos (CIRIACO, [2015?])

Pra terminar!

- Se você usa Windows, então, é bom ter instalado:
  - *firewall*:
    - para proteger o computador contra tentativas de invasão e ameaças oriundas da Internet e eventualmente de redes locais;
    - o *firewall* checa todos os pacotes de dados que trafegam pela rede, filtrando aqueles que não satisfazem as regras de segurança que foram estabelecidas em sua configuração e
    - um *firewall* já vem pré-configurado, ou seja, vem com algumas regras de segurança básicas já definida, mas você pode alterar as regras pré-existentes e/ou acrescentar novas, de acordo com suas necessidades;
  - antivírus:
    - para se proteger contra os diversos tipos de pragas virtuais existentes no mercado;
  - *sandbox* e
    - o conceito do Sandbox é bem semelhante ao de criar uma máquina virtual – de fato, esse método é considerado um tipo de virtualização. São softwares que permitem que você faça testes em uma área especial, reservada do computador. De modo que não prejudique o SO e seus arquivos;
  - Anti-spyware
    - software que tem por finalidade combater os vírus que, quando instalados, têm o objetivo de roubar senhas e/ou arquivos pessoais.

Trabalho

- Em equipe:
  - Antivírus

Referências

- AVAST SOFTWARE S.R.O. **Vírus de Computador**. Disponível em: <https://www.avast.com/pt-br/c-computer-virus>. Acesso em: 04 fev. 2017.
- AVAST SOFTWARE S.R.O. **Malware**. Disponível em: <https://www.avast.com/pt-br/c-malware>. Acesso em: 05 fev. 2017.
- CIRIACO, D. Os melhores antivírus gratuítos e pagos. **Canaltech**. [2015?]. Disponível em: <https://canaltech.com.br/dica/antivirus/os-melhores-antivirus/>. Acesso em: 04 fev. 2017.
- GUILHERME, P. O que é Sandbox?. **Techmundo**. 05 jul. 2012. Disponível em: <https://www.tecmundo.com.br/spyware/1172-o-que-e-sandbox-.htm>. Acesso em: 07 mar. 2017.
- PAYÃO, F. Os 5 melhores antivírus gratuitos de 2016. **Techmundo**. 18 abr. 2016. Disponível em: <https://pt.wikipedia.org/wiki/Sistema_operativo>. Acesso em: 02 fev. 2017.
- WIKIPÉDIA. **Malware**. Disponível em: <https://pt.wikipedia.org/wiki/Malware>. Acesso em: 05 fev. 2017.
- WIKIPÉDIA. **Government Communications Headquarters**. Disponível em: <https://pt.wikipedia.org/wiki/Government_Communications_Headquarters>. Acesso em: 05 fev. 2017.