INSTITUTO FEDERAL
PIAUÍ

Ameaças à Segurança da Informação

SEGURANÇA DA INFORMAÇÃO

Prof. Silvino Marques
silvinomarques@ifpi.edu.br

Introdução

- Para se garantir a proteção de uma rede ou sistema é importante conhecer as ameaças e **técnicas de ataque** utilizadas pelos invasores, para então aplicar as medidas e ferramentas necessárias para proteção desses recursos.

Introdução

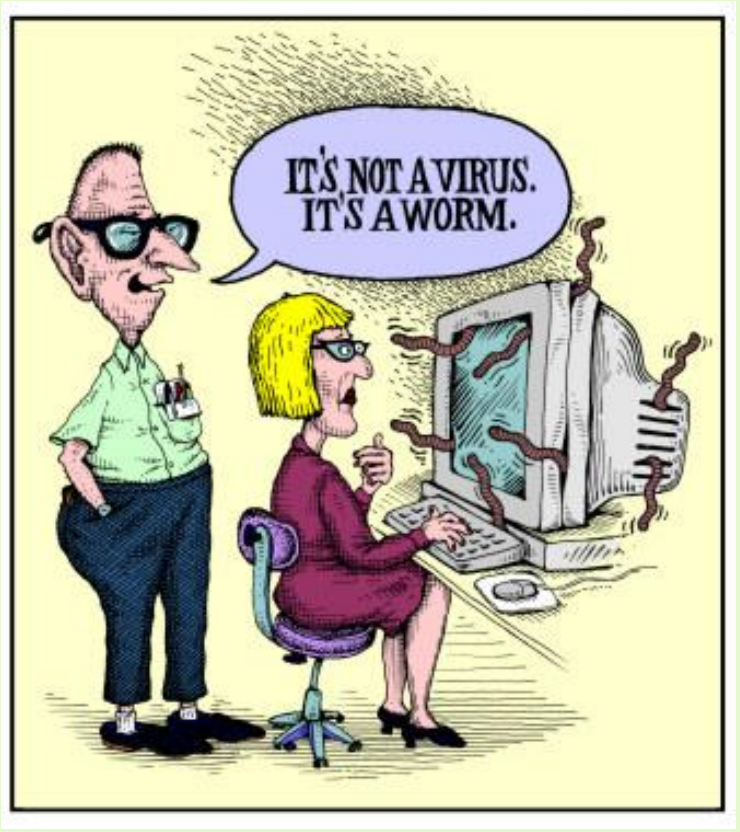
- Sem o conhecimento desses fatores, toda a aplicação de mecanismos de proteção pode ser anulada, pois se existir algum ponto vulnerável ou protegido de maneira incorreta, todo sistema estará comprometido.
  - Dessa maneira, vamos identificar as principais ameaças contra a segurança da informação.

Vírus

- São programas maliciosos, criados para se replicar automaticamente e danificar o sistema.
- A principal característica de um vírus é sua capacidade de se copiar sozinho e de se anexar a arquivos. Exemplos:
  - Vírus de Boot;
  - Vírus de Macro.

Worms

- Programa capaz de se propagar automaticamente através de redes, enviando cópias de si mesmo de computador para computador.
  - Não necessita ser explicitamente executado para se propagar.
  - Sua propagação se dá através da exploração de vulnerabilidades existentes ou falhas na configuração de softwares instalados em computadores.
  - Consomem muitos recursos;
  - Degradam sensivelmente o desempenho de redes.

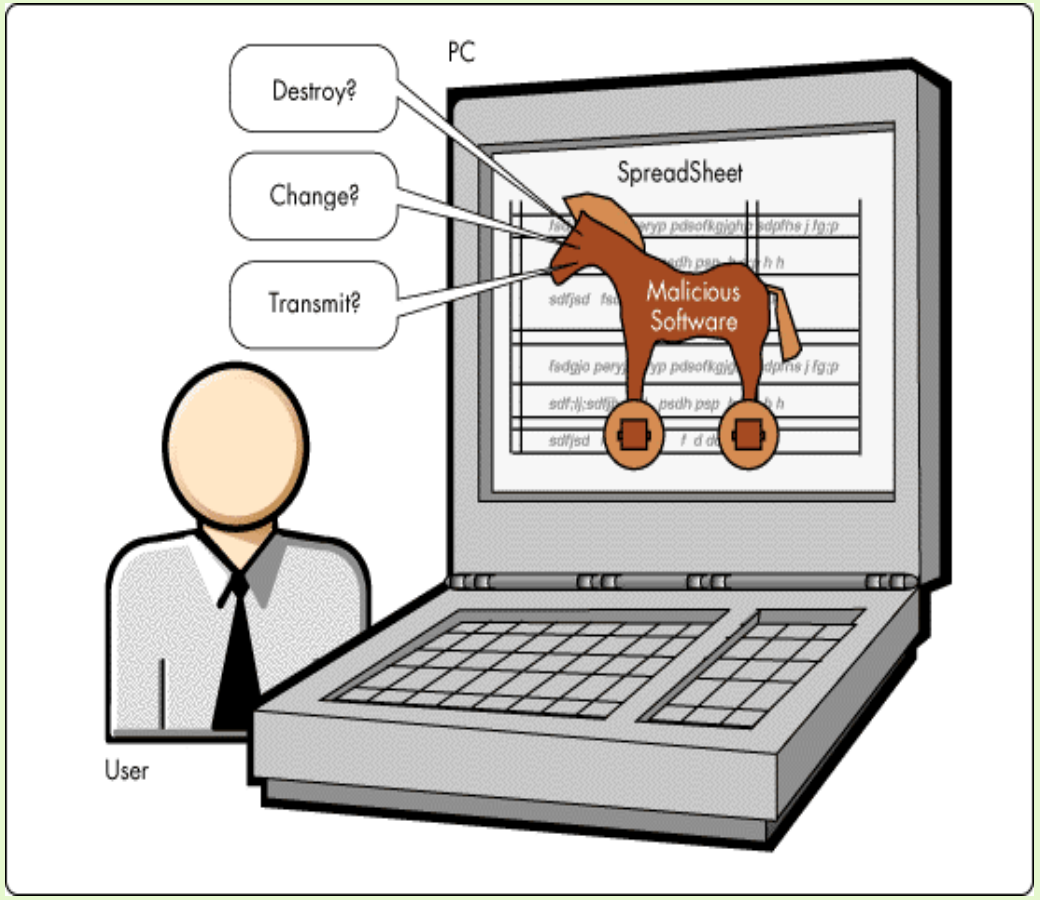


Bot

- Além de incluir funcionalidades de worms, dispõe 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, etc;
  - Botnets;

Cavalos de Tróia

- Também conhecidos como *Trojans*, são códigos maliciosos, geralmente camuflados como programas inofensivos que, uma vez instalados no computador da vítima, podem permitir que o criador da praga obtenha o controle completo sobre a máquina infectada, que passa a ser chamada de "zumbi".



Exploit

- Programa de computador, uma porção de dados ou uma seqüência de comandos que se aproveita das vulnerabilidades de um sistema computacional.
- São geralmente elaborados por hackers como programas de demonstração das vulnerabilidades, a fim de que as falhas sejam corrigidas, ou por crackers a fim de ganhar acesso não autorizado a sistemas.

Rootkits

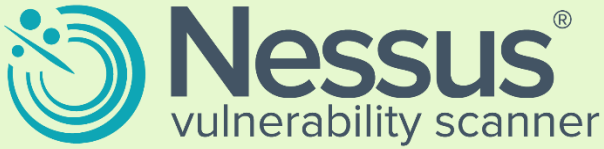
- Conjunto de programas com o fim de esconder e assegurar a presença de um invasor em um computador comprometido.
- Não diz respeito a obter acesso privilegiado;

Sniffers

- Os “farejadores” são programas que espionam a comunicação em uma rede.
- Eles exploram o fato do tráfego dos pacotes das aplicações TCP/IP não utilizar nenhum tipo de cifragem nos dados.
  - Dessa maneira um sniffer pode obter nomes de usuários, senhas ou qualquer outra informação transmitida que não esteja criptografada.

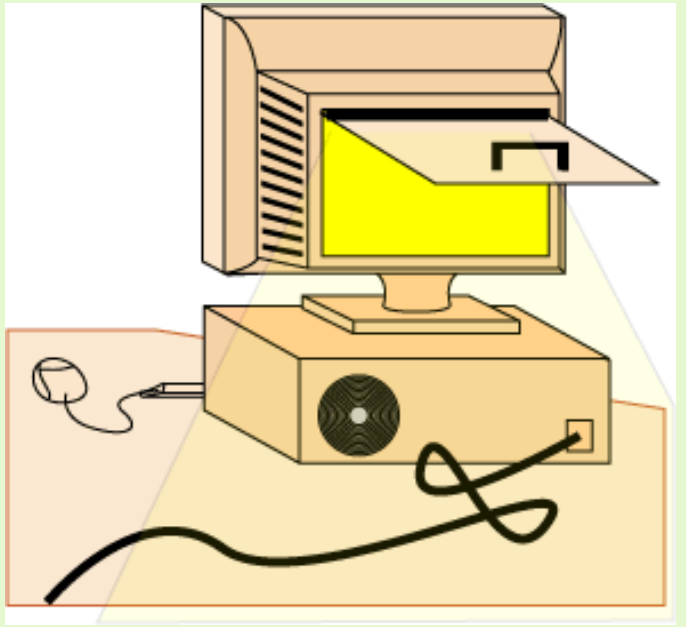
Port Scanners

- São programas que vasculham um computador a procura de portas de comunicação abertas.
- Esses programas ficam enviando vários pacotes seguidos para esse computador, em diferentes portas, apenas para receber a resposta de uma delas e, com isso, constatar a presença de portas abertas.



Backdoor

- Ou “porta dos fundos”, é uma brecha, normalmente colocada de forma intencional pelo programador, que permite a invasão do sistema por quem conhece a falha.



Spyware

- O Spyware é basicamente um programa, cuja função é a de coletar suas informações pessoais sem que você saiba o que está havendo.
- Você pode ser o alvo de um spyware se você faz download de músicas de programas de compartilhamento de arquivos, jogos gratuitos de sites, ou outros softwares de origem desconhecida.

Keylogger

- Programa capaz de capturar e armazenar as teclas digitadas pelo usuário no teclado de um computador.
- Normalmente, a ativação do keylogger é condicionada a uma ação prévia do usuário, como por exemplo, após o acesso a um site de comércio eletrônico ou Internet Banking, para a captura de senhas bancárias ou números de cartões de crédito.
  - ***Smart Keyloggers e Screenloggers***

Adware

- O Adware é um programa instalado no computador do usuário que realiza constantemente a abertura de janelas de anúncios de propagandas.
  - Alguns anunciantes podem instalar software Adware em seu sistema e gerar uma série de anúncios não solicitados que podem encher o seu desktop e afetar sua produtividade.

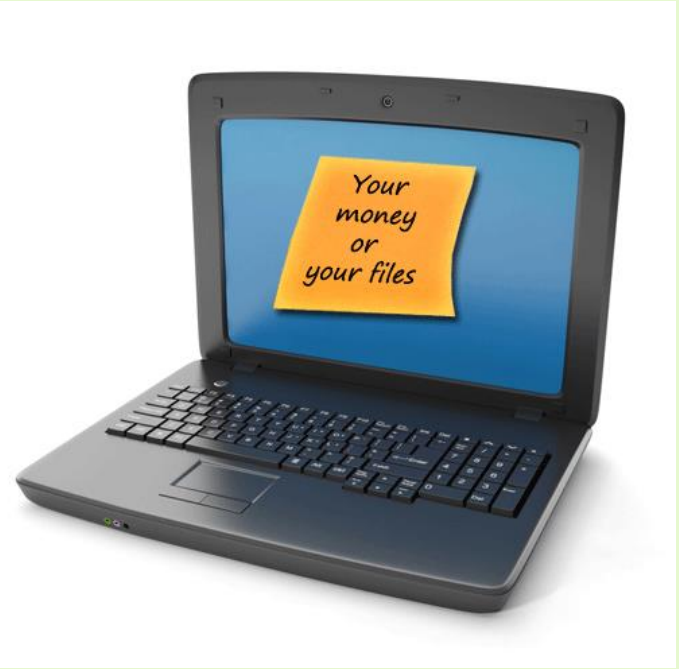
Stalkerwares

- São normalmente utilizados para rastrear violência doméstica, traição de cônjuges e suspeitos de crimes. Eles permitem, por exemplo, rastrear a localização em tempo real, acessar o registro de chamadas, ler mensagens, ter aceso a câmera e microfone do aparelho, etc.

Ransomware

- É um tipo de *malware* que restringe o acesso ao sistema infectado e cobra um valor de "resgate" para que o acesso possa ser reestabelecido.

Não permitem acesso externo ao computador infectado como os *trojans*, a maioria é criada com propósitos comerciais, geralmente são detectados pelos antivírus com uma certa facilidade pois costumam gerar arquivos criptografados grandes, embora alguns possuam opções que escolhem inteligentemente quais pastas criptografar, ou então, permitem que o atacante escolha quais as pastas de interesse.



Ransomware


Wana DecryptOr 2.0
Ooops, your files have been encrypted!
English
English
Bulgarian
Chinese (simplified)
Chinese (traditional)
Croatian
Czech
Danish
Dutch
Filipino
Finnish
French
German
Greek
Indonesian
Italian
Japanese
Korean
Latvian
Norwegian
Polish
Portuguese
Romanian
Russian
Slovak
Spanish
Swedish
Turkish
Vietnamese
What Happened to My Computer?
Your important files are encrypted.
Many of your documents, photos, videos, databases and other files are no long
because they have been encrypted. Maybe you are busy looking for a way to
files, but do not waste your time. Nobody can recover your files without our d
service.
Can I Recover My Files?
Sure. We guarantee that you can recover all your files safely and easily. But
enough time.
You can decrypt some of your files for free. Try now by clicking <Decrypt>.
But if you want to decrypt all your files, you need to pay.
You only have 3 days to submit the payment. After that the price will be doub
Also, if you don't pay in 7 days, you won't be able to recover your files forever
We will have free events for users who are so poor that they couldn't pay in 6
How Do I Pay?
Payment is accepted in Bitcoin only. For more information, click <About bitco
Please check the current price of Bitcoin and buy some bitcoins. For more inf
<How to buy bitcoins>.
And send the correct amount to the address specified in this window.
After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am GMT
Payment will be raised on
5/18/2017 11:04:00
Time Left
02:23:58:08
Your files will be lost on
5/22/2017 11:04:00
Time Left
06:23:58:08
About bitcoin
How to buy bitcoins?
Contact Us
bitcoin
ACCEPTED HERE
Send $300 worth of bitcoin to this address:
115p7UMMngoj1pMvkpHijcRdfJNXj6LrLn
Copy
Check Payment
Decrypt

Invasores

Hacker

- Originalmente, e para certos programadores, **hackers** são indivíduos que elaboram e modificam software e hardware de computadores, seja desenvolvendo funcionalidades novas, seja adaptando as antigas.
  - Os hackers utilizam todo o seu conhecimento para melhorar softwares de forma legal.
- A verdadeira expressão para invasores de computadores é denominada ***Cracker*** e o termo designa programadores maliciosos e ciberpiratas que agem com o intuito de violar ilegal ou imoralmente sistemas cibernéticos;

Tipos de Hackers

	Hackers de Chapéu Branco	Hackers de Chapéu Cinza	Hackers de Chapéu Preto
Motivação e objetivos	Aprender coisas novas, proteger a rede sob sua responsabilidade contra invasão ou danos, manter o *status quo*. Trabalhar com a sanção das organizações oficiais.	Fama, crédito por resolver quebra-cabeças de rede desafiadores. Mais interessados em danos do que em pilhagem. Os hacker-ativistas que alteram sites e redes de "malfeitores" alvo (p. ex., corporações envolvidas no comércio de peles, venda de tabaco, aborto) fazem parte desse grupo.	Pagamentos em dinheiro, ofensas. Podem roubar segredos comerciais, números de cartão de crédito, listas de clientes, listas de funcionários. Querem toda informação que puderem conseguir para gerar lucro. Trabalham sem a sanção de organizações oficiais ou extraoficiais.

Figura 1.1 Modelos dos Chapéus Branco e Preto.

Tipos de Hackers

- ***White hat*** (hacker ético), vem do inglês "chapéu branco" e indica um hacker interessado em segurança.
- Utiliza os seus conhecimentos na exploração e detecção de erros de concepção, dentro da lei.
  - Ministram palestras sobre segurança de sistemas, e até trabalham dentro de empresas para garantir a segurança dos dados.

Tipos de Hackers

- ***Gray hat*** - Tem as habilidades e intenções de um hacker de chapéu branco na maioria dos casos, mas por vezes utiliza seu conhecimento para propósitos menos nobres.
- Um hacker de chapéu cinza pode ser descrito como um hacker de chapéu branco que às vezes veste um chapéu preto para cumprir sua própria agenda.
  - Diz ser aceitável penetrar em sistemas desde que o hacker não cometa roubo, vandalismo ou infrinja a confidencialidade

Tipos de Hackers

- ***Black hat***, (*cracker* ou *dark-side hacker*), indica um hacker criminoso ou malicioso, comparável a um terrorista.
- Em geral são de perfil abusivo ou rebelde, muito bem descritos pelo termo "hacker do lado negro“ geralmente especializados em invasões maliciosas e silenciosas, são os hackers que não possuem ética.

Tipos de Hackers

- **Script Kiddies** - são os responsáveis pelas invasões em massa e por fazer barulho na mídia quando invadem sites importantes e alteram sua página inicial colocando frases de protesto ou quando tiram serviços do ar.
- Recebem esse nome por não saber o que estão fazendo. Eles simplesmente buscam ferramentas prontas, os chamados exploits;

Tipos de Hackers

- ***Newbie*** ou a sigla NB, vem do inglês "novato". Indica uma pessoa aprendiz na área, ainda sem muita habilidade, porém possui uma sede de conhecimento notável.
  - Pergunta muito, mas freqüentemente é ignorado ou ridicularizado por outros novatos que já saibam mais do que ele.
  - Hackers experientes normalmente não ridicularizam os novatos, por respeito ao desejo de aprender - no entanto, podem ignorá-los por falta de tempo ou paciência.

Tipos de Hackers

- O termo *Lamer* ou ***Lammer*** indica uma pessoa que acredita que é um hacker, demonstra grande arrogância, no entanto sabe pouco ou muito pouco e é geralmente malicioso.
  - Utilizam ferramentas criadas por *Crackers* para demonstrar sua suposta capacidade ou poder, na intenção de competir por reputação, no entanto são extremamente inconvenientes para convívio social, mesmo com outros hackers.
  - Lammer's geralmente atacam colegas de trabalho ou colegas de estudo, sempre com menos aprendizado, e estes se aterrorizam.

Tipos de Hackers

- **Cyberpunks**
  - *Hackers* dos “tempos românticos”;
  - Se dedicam à invasões de sistemas por divertimento e desafio;
  - Possuem grande conhecimento e são obcecados por privacidade de dados;
  - Grandes preocupações com o governo, devido à privacidade;
  - São responsáveis por encontrar novas vulnerabilidades em serviços, sistemas ou protocolos;

Tipos de Hackers

- **Insiders**
  - Ataques originados à partir da rede interna da organização;
  - Responsáveis por grande parte dos incidentes de segurança nas organizações;
  - Funcionários, ex-funcionários ou pessoas que conseguem infiltrar-se nas organizações;
  - Principais motivações: espionagem industrial e funcionários insatisfeitos;
  - A segurança é, muitas vezes, um problema social, e não apenas tecnológico.

Tipos de Hackers

- **Coders**
  - Hackers que resolveram compartilhar o conhecimento escrevendo livros ou ministrando palestras;
  - Motivação financeira;
    - Caso clássico: ***Kevin Mitnick***;
    - Após ser preso foi requisitado para dar palestras e seminários
    - sobre segurança;
    - Abriu uma empresa de segurança e lançou um livro sobre engenharia social;
    - “A arte de enganar” – Kevin Mitnick.

Outros Termos

- O termo ***Phreaker***, essencialmente significa a mesma coisa que o original "hacker", no entanto é um decifrador aplicado à área de telefonia (móvel ou fixa).
- No uso atual, entende-se que um Hacker modifica computadores, e um Phreaker modifica telefones
  - Os Phreakers também se enquadram no conceito de White hat ou Black hat.

Outros Termos

- O termo ***Cracker***, do inglês "quebrador", originalmente significa alguém que "quebra" sistemas.
- Hoje em dia, pode tanto significar alguém que quebra sistemas de segurança na intenção de obter proveito pessoal (como por exemplo modificar um programa para que ele não precise mais ser pago), como também pode ser um termo genérico para um Black Hat.

Outros Termos

- **Hacktivista**
  - Hackers que realizam seus ataques contra alvos selecionados cuidadosamente, com o objetivo de transmitir uma mensagem política ou religiosa;
  - Tipos de ataques: derrubar a infraestrutura de comunicações ou obter informações que podem comprometer a segurança de alguma nação;
  - *Nation State Professionals*
    - Afeganistão, Paquistão, Iraque, Índia, *cyberjihad.*

Outros Termos

- ***Carding*** – práticas envolvendo fraudes com cartões de crédito;
- ***Easter egg*** – mensagem, imagem ou som que o programador esconde em um software;
- ***Media whore*** – Hackers que buscam glória e fama;
- ***Suit*** – os “outros”, funcionários bem vestidos;
- ***Lap$us*** – codinomes utilizados pelos hackers;
- ***Warez*** – software pirata distribuído ilegalmente pela Internet.

Referências Bibliográficas

Segredos do Hacker Ético - Marcos Flávio Araújo Assunção. São Paulo, SP, Brasil. 2008.

Segurança de Computadores e Teste de Invasão. Alfred Basta; Nadine Basta; Mary Brown. 2ª Ed. - Cengage Learning, 2015.