Malwares **VS** Antivírus

Wendel Guglielmetti Henrique
wendel at security dot org dot br

Security OpenSource (http://www.security.org.br/)
Intruders Tiger Team Security (http://www.intruders.com.br/)

H2HC Fourth Edition - 06, 07, 08 e 09 de Novembro.

Malwares: Vírus, Worms, Spywares, Keyloggers e Rootkits **VS** Antivírus

Agenda

- Definições:
  - Malwares.
  - Vírus.
  - Worms
  - Spywares.
  - Keyloggers.
  - Rootkits
- Antivírus:
  - Definição.
  - Como funciona?
- Exemplos de métodos de Evasão:
  - Assinaturas malfeitas.
  - Packers, Binders, Encryptação, etc.
  - Antivírus Killer.
- Rootkit Hooking:
  - Exemplo de Processos Ocultos.
  - Exemplo de detecção.
- Dicas.
- Dúvidas?
- Links.

Nota

Esta palestra e todos os seus exemplos (Proof Of Concept) foram criados em 2006 para o Unsecurity Day.

A ausência de atualizações na palestra e nos exemplos é proposital para demonstrar como os POCs (Proof Of Concept) criados e compilados a mais de 1 ano se mostram efetivos contra os antivírus atuais (com todas as suas atualizações).

Durante o H2HC 2007 todos os exemplos foram demonstrados ao vivo e com diversos antivírus com as últimas atualizações.

As técnicas apresentadas nesta palestra são efetivas contra vários antivírus e não apenas contra os antivírus apresentados nos vídeos.

Malwares: Vírus, Worms, Spywares, Keyloggers e Rootkits **VS** Antivírus

Definições:

- Não existe um órgão ou instituição que regulamente a definição dos termos Malwares, Vírus, Worms, Spywares, Keyloggers, Rootkits, etc.

- Conseqüentemente existem algumas divergências de opiniões sobre as definições dos mesmos.

- Utilizaremos a linha de definição que a maioria dos experts do seguimento adotam.

- A única definição 100% correta é: “Malwares, Vírus, Worms, Spywares, Keyloggers e Rootkits são simplesmente programas de computador.”

Malwares: Vírus, Worms, Spywares, Keyloggers e Rootkits **VS** Antivírus

Definições: Malwares

- **Malwares** são programas de computadores criados com a intenção de infiltrar e/ou roubar dados e/ou espionar e/ou danificar e/ou esconder evidências em um sistema computacional.

- Vírus, Worms, Spywares, Keyloggers, Rootkits, Backdoors, Trojan Horses, etc, são considerados **Malwares**.

- Como o próprio nome sugeri, a palavra **Malware** foi criada a partir da junção de duas palavras em inglês ”**Mal**icious” e “Soft**ware**”.

Malwares: Vírus, Worms, Spywares, Keyloggers e Rootkits **VS** Antivírus

Definições: Vírus

- **Vírus** de computador agem de forma parecida com os vírus biológicos, que se proliferam através da inserção em células. **Vírus** de computador tem como principal característica se proliferam através da sua rotina de auto replicação, que visa inserir o mesmo em outros arquivos (executáveis, scripts, documentos, etc) do sistema computacional.

- Os **vírus** antigamente se replicavam pelos meios existentes (como disquetes) e conseqüentemente precisavam de interação do usuário para ser executado, com o advento das redes de computadores e a Internet os **vírus** passaram a se replicar através de compartilhamentos de arquivos, e-mail, redes p2p, etc. Considerar que a interação do usuário faz parte da definição de um **vírus** é um erro!

Malwares: Vírus, Worms, Spywares, Keyloggers e Rootkits **VS** Antivírus

Definições: Vírus

- Em 1982 foi encontrado em ambiente real (“in the wild”) o primeiro **vírus** de computador, que foi criado por Rich Skrenta e nomeado de Elk Cloner, o mesmo infectava o sistema operacional DOS 3.3 do Apple II e se proliferava através de disquetes.

- Fred Cohen em 1984 escreveu um artigo entitulado “Experiments with Computer Viruses”, que pela primeira vez utilizou computacionalmente o termo **vírus** em um artigo.

- Exemplos de **vírus** que ficaram mundialmente conhecidos são Mydoom, Ninda, Zmist, ILOVEYOU, etc.

Malwares: Vírus, Worms, Spywares, Keyloggers e Rootkits **VS** Antivírus

Definições: Worms

- Worms se replicam de forma similar aos vírus, as duas principais características de um **Worm** são:

· Não necessita infectar arquivos (executável, script, documento, etc) como os vírus para se proliferam.

· Se prolifera com maior velocidade que os vírus, pois explorara vulnerabilidades em sistemas e as utiliza para se replicar, pode utilizar os mesmos métodos de replicação dos vírus como compartilhamentos de arquivos, e-mail, redes p2p, etc.

- Robert Tappan Morris em 1988 criou o primeiro **Worm** que se proliferava pela Internet, explorando vulnerabilidades (Sendmail, Finger e logins/senhas fracas em rsh/rexec) em sistemas Unix BSD, afetando cerca de 6,000 máquinas (aproximadamente 10% da Internet da época).

Malwares: Vírus, Worms, Spywares, Keyloggers e Rootkits **VS** Antivírus

Definições: Spywares

- Como o próprio nome sugere **Spyware** é a junção das palavras "**SPY**" e "Soft**ware**", ou seja software espião.

- **Spywares** não se auto-replicam como vírus e worms, porém podem explorar vulnerabilidades (geralmente em browsers como Internet Explorer, Firefox, etc) nós computadores dos usuários para se instalar.

- A criação de Spywares tem como objetivo principal o lucro financeiro, pois entre suas atividades estão o marketing em geral (propagandas não solicitadas) e o furto de informações pessoais e sigilosas.

Malwares: Vírus, Worms, Spywares, Keyloggers e Rootkits **VS** Antivírus

Definições: Spywares

- Em 2000 Gregor Freund (Zone Labs) utilizou computacionalmente pela primeira vez o termo **Spyware** em um documento (press release).

- Exemplos de Spywares abrangentemente conhecidos são 180 Solutions, Internet Optimizer, CoolWebSearch, etc.

Malwares: Vírus, Worms, Spywares, Keyloggers e Rootkits **VS** Antivírus

Definições: Keyloggers

- **Keyloggers** também chamados de Keystroke logging são programas que capturam as teclas pressionadas (incluindo senhas).

- **Keyloggers** podem ser utilizados para vários fins como espionagem, fraudes eletrônicas, monitoramento permitido de usuários, etc.

- Existem **Keyloggers** em hardware (como eu mostrei no Secomp 2005) e software.

- Existe uma variação chamada de ScreenLoggers que captura (screenshot) as telas ao invés das teclas, geralmente é utilizado para obter dados de teclados virtuais (como os utilizados em bancos).

Malwares: Vírus, Worms, Spywares, Keyloggers e Rootkits **VS** Antivírus

Definições: Rootkits

- **Rootkit** é um software geralmente utilizado por invasores após comprometer um sistema, sua característica principal é auxiliar o invasor a manter acesso ao sistema sem conhecimento de outros usuários (incluindo o Administrador).

- Os primeiros **Rootkits** foram feitos para Unix e continham um conjunto (**Kit**) de ferramentas (ps, ls, netstat, etc) modificadas com objetivo de esconder o invasor, e conseqüentemente manter acesso de Administrador (**Root**) no sistema sem que outros usuários percebam (incluindo o Administrador).

Malwares: Vírus, Worms, Spywares, Keyloggers e Rootkits **VS** Antivírus

Definições: Rootkits

- Existem basicamente 3 tipos de **Rootkits**:

· Kernel Space = modifica estruturas internas do Kernel.

· Bibliotecas e APIs = intercepta e modifica o fluxo de execução das Bibliotecas/APIs.

· Aplicativos = modifica o próprio aplicativo por exemplo ps, ls, netstat, etc.

- Atualmente existem **Rootkits** para diversos sistemas operacionais como Windows, Linux, Solaris, BSD-Like, HP-UX, etc.

- Exemplos de Rootkits abrangentemente conhecidos são SuckIT, Adore, NT Rootkit, FU rootkit, AFX Rootkit, Vanquish, etc.

Malwares: Vírus, Worms, Spywares, Keyloggers e Rootkits **VS** Antivírus

Antivírus: definição

- **Antivírus** são softwares que tentam identificar, tratar e eliminar vírus (atualmente malwares).

- Softwares Antivírus utilizam basicamente duas linhas de identificação:

• Assinatura é um bloco (geralmente armazenado em hexadecimal) de dados que identifica o vírus, esse bloco pode ser uma seqüência de instruções ou texto (string).

• Análise Heurística é baseado em analisar e/ou monitorar os executáveis e procurar (através de regras) por comportamentos similares aos de malwares.

Antivírus: Como funciona?

- A análise heurística é um recurso que muda muito de fabricante para fabricante de **Antivírus**, de forma geral ela é implementada superficialmente e acaba tornando-se pouco eficiente.

- Assinaturas ficão em um arquivo (geralmente formato proprietário) indexado e muitas vezes encriptados e assinados digitalmente que contem as informações dos vírus, as mais comuns são:

• Name é o nome pelo qual o vírus é identificado, costuma seguir um padrão de nomes onde se identifica se é um vírus, worm, backdoor, etc.

Antivírus: Como funciona?

- Signature é o bloco (geralmente representado em hexadecimal) que contém o fragmento viral para identificar o vírus.

- FileType é o tipo do arquivo (pode ser nulo), exemplos PE, ELF, HTLM, VBS, etc.

- Offset é o endereço (pode ser nulo) no arquivo de onde comparar com a "Signature". Exemplo compare a "Signature" no arquivo começando no byte 0xb6.

Exemplos de métodos de Evasão: Assinaturas Malfeitas

- Um problema na detecção baseada em assinaturas é a qualidade das mesmas, como foi dito a assinatura pode ser um conjunto de instruções ou texto.

- A utilização de texto como assinatura é ruim pois pode gerar vários falsos positivos e facilita a evasão (utilize um editor hexadecimal e substitua o texto utilizado como assinatura e o malware não será mais detectado).

Exemplos de métodos de Evasão: Assinaturas Malfeitas

DEMONSTRAÇÃO

(Veja o vídeo acessando o arquivo “Videos\BadSignature\index.htm”)

Como detectar a assinatura de um Malware?

- A assinatura pode ser detectada de várias formas, a mais simples é através do método file split (fragmentação de arquivo).

- O método consiste em dividir o arquivo detectado pelo antivírus em diversas partes começando a partir do zero e incrementando em blocos de tamanho pré definidos.

- Posteriormente os arquivos fragmentados são analisados pelo antivírus, a diferença entre o último arquivo não detectado e o primeiro detectado é a assinatura utilizada pelo antivírus para detectar o malware.

Como detectar a assinatura de um Malware?

DEMONSTRAÇÃO

(Veja o vídeo acessando o arquivo “Videos\HowToDetectAVSignatures\index.htm”)

Malwares: Vírus, Worms, Spywares, Keyloggers e Rootkits **VS** Antivírus

Exemplos de métodos de Evasão: Packers, Binders, Encryptação, etc.

- **Packers** são softwares que comprimem (alguns também encriptam) um arquivo executável, esse código comprimido é adicionado em um novo arquivo binário que também conterá as rotinas de descompressão (e decriptação caso necessário).

- **Binders** também conhecidos como **Joiners** são softwares que comprimem vários executáveis em um único arquivo executável.

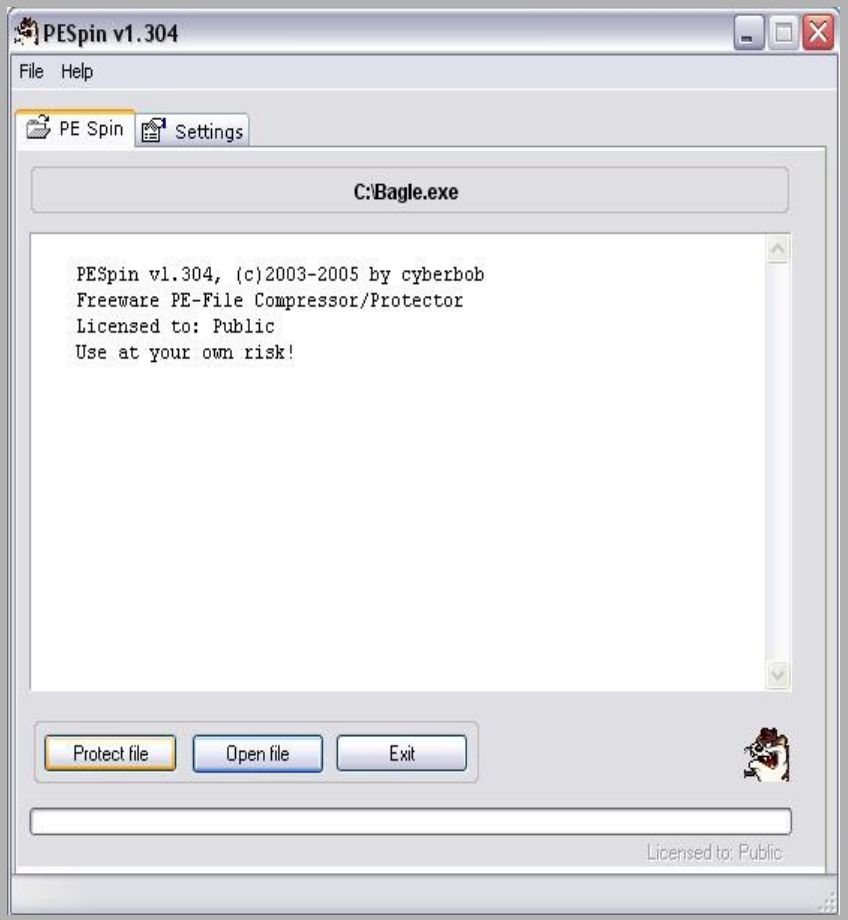
- Muitos Packers, Binders, etc tem rotinas para dificultar engenharia reversa (Anti-Dump, Disassembler Detection, etc).

- Binders, Packers, etc conseqüentemente são utilizados para inviabilizar a detecção de Malwares pelos softwares antivírus.

Malwares: Vírus, Worms, Spywares, Keyloggers e Rootkits **VS** Antivírus

Exemplos de métodos de Evasão: Packers, Binders, Encryptação, etc.

Passo 1 (Packing)



Passo 2 (Scrambing)

C:\> PEspinScramb bagle-new.exe bagle-packed.exe

PEspin Private Scrambler – by Dr. Spy

Analyzing bagle-new.exe...
Scrumbling...
Generated bagle-packed.exe

Malwares: Vírus, Worms, Spywares, Keyloggers e Rootkits **VS** Antivírus

Exemplos de métodos de Evasão: Packers, Binders, Encryptação, etc.

Teste **antes de utilizar o Packer (PEspin + Scramber)** utilizando o Antivírus F-Prot:

/usr/bin/f-prot Bagle.exe -ai -archive -dumb -list -packed
F-prot 3.16c/20060217 **found**: **W32/Bagle.AM.worm**

Teste **depois de utilizar o Packer (PEspin + Scramber)** utilizando o Antivírus F-Prot:

./f-prot Bagle-packed.exe -ai -archive -dumb -list -packed
F-Prot 3.16c/20060217 **found nothing**

Malwares: Vírus, Worms, Spywares, Keyloggers e Rootkits **VS** Antivírus

Exemplos de métodos de Evasão: Antivírus Killer

- **Antivírus Killer** é outro método extremamente difundido para inviabilizar as detecções dos antivírus.

- A técnica consiste em terminar o processo do antivírus, parar o serviço do antivírus, danificar a base de assinatura, etc.

- Essa técnica funciona:

➔ Devido aos usuários que utilizam o sistema operacional como Administrador, root, etc.

➔ Devido a falta de implementação de métodos de segurança para prevenir a finalização indevida de softwares antivírus.

Exemplos de métodos de Evasão: Antivírus Killer

```
for(p=Process32First(proc,&entry); p; p=Process32Next(proc,&entry)) {
wsprintf(nproc,"%s", entry.szExeFile, sizeof(sproc));
WSstring2low(nproc);

  if ((strstr(nproc, "avgamsrv.exe" )) == NULL){  // avgamsrv.exe é AVG Alert Manager.

     PID =  entry.th32ProcessID;
     GetPrivilegie();
     hProc = OpenProcess(SYNCHRONIZE|PROCESS_TERMINATE, FALSE, PID);
     TerminateProcess(hProc,0);
     BackPrivilegie();
  }
}
// Do bad stuff (Extract and execute a Malware, etc).
//Restart AV software
```

Malwares: Vírus, Worms, Spywares, Keyloggers e Rootkits **VS** Antivírus

Exemplos de métodos de Evasão: Antivírus Killers

DEMONSTRAÇÃO

(Veja o vídeo acessando o arquivo “Videos\Kill&Launch\index.htm”)

Exemplos de métodos de Evasão: Rootkits

Conteúdo removido para a apresentação no H2HC por questões de tempo.

Exemplos de métodos de Evasão: Rootkits

Conteúdo removido para a apresentação no H2HC por questões de tempo.

Rootkit Hooking: Exemplo de Processos Ocultos.

Conteúdo removido para a apresentação no H2HC por questões de tempo.

Rootkit Hooking: Exemplo de detecção.

Conteúdo removido para a apresentação no H2HC por questões de tempo.

Malwares: Vírus, Worms, Spywares, Keyloggers e Rootkits **VS** Antivírus

Dicas de segurança.

Conteúdo removido por não ser o foco do evento. ;)

Dúvidas?

Malwares: Vírus, Worms, Spywares, Keyloggers e Rootkits **VS** Antivírus

Links

http://en.wikipedia.org/

http://www.intruders.com.br/

http://www.security.org.br/

http://www.h2hc.org.br/

http://www.hackaholic.org/

http://ws.hackaholic.org/