SEGURANÇA DA INFORMAÇÃO

Softwares Maliciosos

ROTEIRO

- O que é um código malicioso?
- Malware
  - Vírus. Worms, Trojans, Rootkit, Spyware, Ransoware
- Ataques internos
- Defesa contra ataques internos
- Proteção conta malware

SOFTWARES MALICIOSOS

O que é?

Um código de computador nocivo que tem como objetivo

- ✔ criar vulnerabilidades no sistema, gerando:
  - ✔ backdoors, violações de segurança, roubo de dados e informações, etc

MALWARE

Pode ser classificado em várias categorias, dependendo da propagação e ocultação.

Propagação

- ✔ **Vírus:** propagação assistida por humanos (por exemplo, anexo de e-mail aberto)
- ✔ **Worm:** propagação automática sem assistência humana

Ocultação

- ✔ **Rootkit:** modifica o sistema operacional para ocultar sua existência
- ✔ **Trojan:** fornece a funcionalidade desejável, mas oculta a operação maliciosa

MALWARE

Vírus

- ✔ Anexa-se a um host (geralmente um programa)
- ✔ Código autoreplicante
- ✔ Cavalos de Tróia autoreplicantes
- ✔ Altera o código normal com a versão “infectada”
  - ✔ Opera quando o código infectado é executado
  - ✔ Se a condição de propagação então

MALWARE

Worm

- ✔ Malware autorreplicante que não requer um programa host
- ✔ Propaga uma versão totalmente funcional de si mesmo para outras máquinas
- ✔ Carrega uma carga útil executando tarefas ocultas
  - ✔ Backdoors, retransmissores de spam, agentes DDoS; …

Fases

- ✔ Sondagem→Exploração→Replicação→Carga útil

MALWARE

Rootkit

É um software que permite acesso privilegiado e contínuo a um computador enquanto oculta ativamente sua presença dos administradores, subvertendo a funcionalidade padrão do sistema operacional ou outros aplicativos.

Objetivo: Ocultar as informações da visão dos administradores para que o *malware* não seja detectado

Exemplo: ***ocultar processos, arquivos, conexões de rede abertas, etc.***

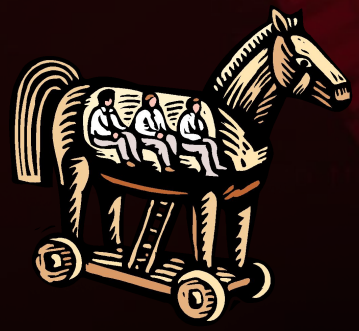
MALWARE

Trojan

- ✔ Software que parece desempenhar uma função desejável para o usuário antes de ser executado ou instalado, mas também pode roubar informações ou danificar o sistema

- ✔ Os cavalos de Tróia podem ser instalados como parte da carga útil de outro malware, mas geralmente são instalados por um usuário ou administrador, deliberada ou acidentalmente.

Exemplo: ***Lançar um keylogger***



MALWARE

Spyware

- ✔ Coleta, aos poucos, pequenas informações sobre os usuários sem o conhecimento deles
  Keyloggers: rastreamento furtivo e registro de pressionamentos de tecla
- ✔ Podem rastrear o hábito de navegação
- ✔ Podem redirecionar a navegação e exibir anúncios

MALWARE

Ransomware

- ✔ Mantém um sistema de computador, ou os dados que ele contém, refém contra seu usuário, exigindo um resgate.

O que faz?

- ✔ Desabilita um serviço essencial do sistema ou bloqueia a tela na inicialização do sistema
- ✔ Criptografa alguns dos arquivos pessoais do usuário, originalmente chamados de *criptovírus, criptotrojans* ou *criptoworms*

ATAQUES INTERNOS

É uma violação de segurança causada, ou facilitada, por alguém da própria organização que controla ou constrói o ativo que deve ser protegido.

No caso de *malware*, um ataque interno refere-se a uma falha de segurança criada em um sistema de software pelos seus programadores.

BACKDOORS

Também é chamado de alçapão, é um recurso ou comando oculto em um programa que permite que um usuário execute ações que ele normalmente não teria permissão para fazer.

Quando usado de maneira normal, este programa funciona completamente conforme o esperado e anunciado.

Mas se o recurso oculto estiver ativado, o programa fará algo inesperado, muitas vezes violando políticas de segurança, como realizar um escalonamento de privilégios.

BACKDOORS

- ✔ Alguns backdoors são colocados em um programa por seus programadores – **Não maliciosos**
- ✔ Finalidade de depuração
- ✔ Muitos jogos de computador têm backdoors
  - ✔ Código de chave secreta para alterar a função do jogo

BACKDOORS

- ✔ **Backdoors deliberados** inseridos por programadores maliciosos
  - ✔ Chantagem, privilégio secreto
- ✔ **Backdoor criado por malware em máquinas comprometidas**
  - ✔ Abre um serviço de escuta TCP
  - ✔ Qualquer pessoa pode ter uma conexão shell com a máquina sem conta e senha

BOMBA LÓGICA

- Programa que executa uma ação maliciosa como resultado de determinada condição lógica.

Exemplo:

1) Um programador que codifica o software para o sistema de folha de pagamento insere o código que faz o programa travar caso ele processe duas folhas de pagamento consecutivas sem pagá-lo.

- Combinar bomba lógica com um *backdoor*, onde um programador coloca uma bomba lógica que travará o programa em uma determinada data.

DEFESA CONTRA ATAQUES INTERNOS

- ✔ Evite pontos únicos de falha
- ✔ Use ferramentas de arquivamento e relatórios
- ✔ Limite a autoridade e as permissões
- ✔ Sistemas críticos devem ser fisicamente seguros
- ✔ Monitore o comportamento dos funcionários
- ✔ Controle as instalações de software na empresa ou no seu computador

CONTRAMEDIDAS CONTRA MALWARE

Assinatura

- *Scan* compara o objeto analisado com um banco de dados de assinaturas
  - Uma assinatura é uma impressão digital de vírus
    - Exemplo: uma *string* com uma sequência de instruções específicas para cada vírus
  - Diferente de uma assinatura digital
  - Um arquivo está infectado se houver uma assinatura dentro de seu código
  - Técnicas rápidas de correspondência de padrões para procurar assinaturas
  - Todas as assinaturas juntas criam o banco de dados de *malware* (em geral é proprietário)

PROTEÇÃO CONTRA MALWARE

Lista Branca/Negra

- ✔ Manter banco de dados de hashes criptográficos para
  - ✔ Arquivos do sistema operacional
  - ✔ Aplicativos populares

- ✔ Arquivos infectados conhecidos
- ✔ Calcule hash de cada arquivo em discos rígidos
- ✔ Procure no banco de dados para comparar
- ✔ Precisa proteger a integridade do banco de dados

- ✔ Exemplo: software TripWire

PROTEÇÃO CONTRA MALWARE

- **Análise heurística**

  Útil para identificar malware novo e de “dia zero”

- **Análise de código**

  Com base nas instruções, o antivírus pode determinar se o programa é malicioso ou não, ou seja, se o programa contém instruções para excluir arquivos do sistema

- **Emulação de execução**

  - ✔ **Executar código em ambiente de emulação isolado (em uma máquina virtual)**
  - ✔ **Monitora as ações que o arquivo de destino realiza**
    - ✔ **Se as ações forem prejudiciais, marque como vírus**
  - ✔ ***Métodos heurísticos podem acionar alarmes falsos***

PROTEÇÃO CONTRA MALWARE

Utilizar Barreiras

- ✔ Processo em segundo plano (serviço/daemon)
- ✔ Verifica cada vez que um arquivo é tocado (abrir, copiar, executar, etc.)

Análise sob demanda

- ✔ Digitalize a pedido explícito do usuário ou de acordo com a programação regular
- ✔ Em um arquivo suspeito, diretório, unidade, etc.

PROTEÇÃO CONTRA MALWARE

Análise On-line

- Plug-in de navegador gratuito
- Autenticação por meio de certificado de terceiros
- Atualização de software e assinaturas em cada varredura
- Configuração não adequada de fazer
- O escaneamento precisa de conexão com a Internet
- Relatório coletado pela empresa que oferece o serviço

PROTEÇÃO CONTRA MALWARE

Análise Off-line

- ✔ Assinatura anual paga
- ✔ Instalado no SO
- ✔ Software distribuído com segurança pelo fornecedor on-line ou por um varejista
- ✔ Atualizações agendadas de software e assinaturas
- ✔ Facilmente configurável
- ✔ Escaneamento sem conexão com a Internet
- ✔ Relatório coletado localmente e pode ser enviado ao fornecedor

PROTEÇÃO CONTRA MALWARE

Quarentena

- ✔ Um arquivo suspeito pode ser isolado em uma pasta chamada quarentena:
- ✔ O arquivo suspeito não é excluído, mas inofensivo: o usuário pode decidir quando removê-lo ou, eventualmente, restaurar para um falso positivo
- ✔ Interagir com um arquivo em quarentena só é possível através do programa antivírus
- ✔ O arquivo em quarentena é inofensivo porque está criptografado
- ✔ A técnica de quarentena é proprietária (em geral) e os detalhes são mantidos em segredo

PROTEÇÃO CONTRA MALWARE

Análises

Estática

- ✔ Verifica o código sem tentar executá-lo
- ✔ Verificação rápida na lista branca
- ✔ **Filtragem**: verifique com antivírus diferente e verifique se eles retornam o mesmo resultado com nome diferente
- ✔ **Remoção por partes:** remova a parte correta dos arquivos como lixo para identificar melhor o vírus
- ✔ **Análise de código:** verificar o código binário para entender se é um executável
- ✔ **Desmontagem:** verificar se o bytecode mostra algo incomum

CONTRAMEDIDAS CONTRA MALWARE

Análises

Dinâmica

- ✔ Verificar a execução de códigos (em uma sandbox virtual)
- ✔ Monitorar
  - ✔ Alterações de arquivo
  - ✔ Alterações no registro
  - ✔ Processo e threads
  - ✔ Porta de comunicação

REFERÊNCIAS

1. https://cartilha.cert.br/fasciculos/codigos-maliciosos/fasciculo-codigos-maliciosos-slides-notas.pdf
2. Introdução à segurança de computadores - Michael T. Goodrich e Roberto Tamassia
3. https://www.cs.purdue.edu/homes/clifton/cs526/

SEGURANÇA DA INFORMAÇÃO

Softwares Maliciosos