

# Análise de Malware em Sistemas Windows

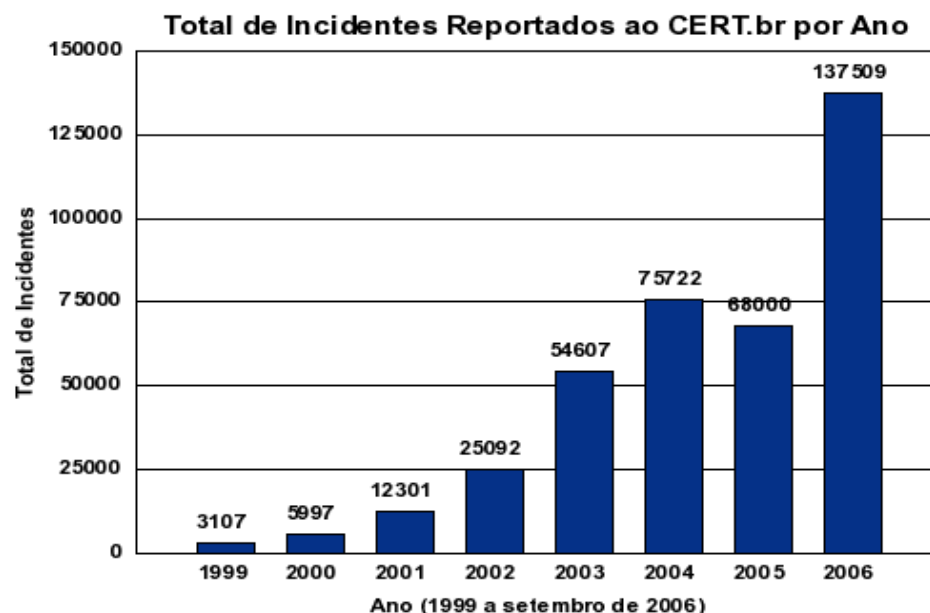
*Rafael Siqueira*  
*Samuel Macedo*

# Malware

- Software designado a se infiltrar em um sistema de computador alheio de forma ilícita com o intuito de causar algum dano ou roubo de informações.
- Exemplos:
  - Vírus, Worms, Trojans, Bots, Spywares e outras variantes

# Curiosidade estatística

- Dados do Cert.br
  - 77.933 incidentes reportados em 2006
  - 59% algum tipo de uso de Malwares



# Novidades

- Rootkits:
  - Capacidade de ocultar processos, arquivos e dados do sistema.
  - Dificuldade de detecção
  - Variações:
    - Kernel, Aplicações, Virtualised

# Motivação para se realizar uma Análise de Malware

- Aumento do número de Malwares
- Recuperação do sistema infectado
  - Cálculo da extensão dos danos causados pelo Malware
- Desenvolvimento de novas técnicas de proteção
- Pesquisa sobre novos tipos de ataque
- Curiosidade, diversão...

# Análise de Malware

- Processo de análise de um código malicioso para descoberta de suas funcionalidades básicas.
- Tipos de análise:
  - Análise de Código
  - Execução e Análise Comportamental

# Análise de Código

- Leitura do código
- Uso de disassemblers e debuggers
- Vantagens:
  - Maior conhecimento sobre o Malware e seu funcionamento
- Desvantagens:
  - Elevado conhecimento de linguagens de programação
  - Tempo dedicado e paciência

# Análise Comportamental

- Ambiente Controlado
- Informações iniciais de um ambiente sadio
- Execução e análise dos “passos de execução” do Malware
- Análise forense comparativa

# Ambiente Controlado

- Máquina isolada ou máquina virtual
- Confiança no conjunto de ferramentas a serem utilizadas:
  - [www.sleuthkit.org](http://www.sleuthkit.org)
- VMware:
  - Acesso à rede seja praticamente nulo (host-only)
  - Sistemas operacionais distintos
    - Dificultar comprometimento da máquina host
  - Uso de snapshots

# Dados iniciais sobre o sistema

- Arquivos, processos em execução, portas abertas, cópia do registro, informações sobre usuários e grupos.
- Ferramentas:
  - Winalysis:
    - Utiliza snapshots para realizar uma análise comparativa
  - Netstat e fport
    - Informações sobre portas abertas
  - Nmap
    - Scan de portas

# Análise Estática

- Analisar o Malware antes de sua execução
- Ferramentas:
  - Strings:
    - Analisar as seqüências de caracteres
  - PEid:
    - Obter informações sobre a ferramenta utilizada na compactação do malware
  - Resource hacker:
    - Visualizar imagens, menus, tabelas de strings, e outras informações que seriam exibidas pelo executável analisado

# Análise Dinâmica

- Execução do Malware dentro de um ambiente controlado
- Análise comparativa do sistema
- É finalizada quando o Malware termina sua execução ou entra em execução estacionária
- Ferramentas:
  - Regmon:
    - Alterações no registro do Windows em tempo real
  - Filemon:
    - Monitora o sistema de arquivos possibilitando visualizar a criação de arquivos, remoção e modificação

# Análise Dinâmica

- Ferramentas (cont.):
  - Wireshark:
    - Tráfego de rede
  - Process Explorer:
    - Processos em execução no sistema

# Análise Comparativa

- Analisar as mudanças que ocorreram devido a execução do Malware
- Análise forense com informações iniciais do sistema
- Ferramenta Winanalysis.

# Documentação

- Relatório da análise realizada:
  - MD5sum ou Sha1
  - Arquivos alterados
  - Alterações no registro
  - Acesso à rede
  - Processos executados
  - Strings

# Conclusão

- A Análise de Malwares deve seguir conceitos de Análise Forense como imparcialidade, troca de informações entre a equipe, paciência e atenção.
- Os resultados podem ser pouco conclusivos, o que obrigaria o analista a realizar uma Análise de Código.
- A utilização de máquinas virtuais não é totalmente segura devido a evolução dos Malwares na detecção destas máquinas.

# Perguntas

- Dúvidas antes de iniciar as demonstrações?

**Computer Security Incident Response Team - PoP-MG**

**[www.csirt.pop-mg.rnp.br](http://www.csirt.pop-mg.rnp.br)**

**[seguranca@csirt.pop-mg.rnp.br](mailto:seguranca@csirt.pop-mg.rnp.br)**