Análise de Malware com Software Livre

17º GTS - 2011

Apresentação

Luiz Vieira

- Construtor 4Linux
- Consultor de Segurança
- 16 anos de experiência em TI
- Pen-Tester, Perito Forense (CHFI)
- Articulista sobre Segurança de vários sites: VivaOLinux, SegurançaLinux, Imasters, HackProofing e etc
- Entusiasta do Software Livre
- Filósofo e Psicoterapeuta
- Blog: http://hackproofing.blogspot.com

4LINUX
FREE SOFTWARE SOLUTIONS

Tópicos de hoje

- Definição
- Por que analisar?
- O que procurar?
- Processo investigativo
- Ferramentas
- Sandboxes
- TRUMAN
- TWMAN
- Cuckoo
- Demo

Definição

Malware = Malicious + Software

- **Vírus**
- **Worms**
- **Trojans**
- **Spyware**
- **Adware**
- **Rootkits**

Por que analisar?

- Desenvolver regras para NIDS
- Desenvolver vacinas
- Entender o comportamento e funcionamento
- Realizar resposta a incidentes mais efetivamente
- Desenvolver patchs de correção
- Ganhar o controle do código malicioso e utilizá-lo para outros fins

Fases da análise:

- Fase 1: Preservação e análise de dados voláteis
- Fase 2: Análise de memória
- Fase 3: Análise de discos
- Fase 4: Análise estática de malware
- Fase 5: Análise dinâmica de malware

O que procurar?

Ao analisar um programa suspeito, há uma série de perguntas que o pesquisador deve considerar:

- Qual é a natureza e a finalidade do programa?
- Como funciona o programa para cumprir a sua finalidade?
- Como funciona o programa ao interagir com o sistema vítima?
- Como o programa interage com a rede?
- O que o programa sugere sobre o nível de sofisticação do atacante?
- Há um vetor de ataque identificável que o programa usa para infectar um hospedeiro?
- Qual é a extensão da infecção ou comprometimento do sistema ou rede?

Processo investigativo

Alguns dos preceitos básicos que precisamos explorar incluem:

- Estabelecer a linha de base do ambiente
- Preparação pré-execução: monitoramento do sistema e da rede
- Execução do binário suspeito
- Observação do processo: monitoramento de bibliotecas e system calls
- Avaliação do processo: análise dos processos em execução
- Análise das portas abertas e conexões de rede
- Análise de arquivos abertos e sockets
- Exploração do diretório /proc
- Quebra de ofuscação: remoção da proteção do malware
- Ajustes de ambiente
- Ganhando controle do malware
- Interagindo e manipulando o malware
- Explorando e verificando as funcionalidades do malware
- Reconstrução de eventos: capturar tráfego de rede, integridade de arquivos e logs de IDS
- Varredura de portas/vulnerabilidades do host comprometido
- Verificação de rootkits

Ferramentas

Análise de Binários

- hexdump, ghex2, bless, radare, elfsh, binutils (readelf, objdump, strings), file, dissy, elfutils, pev, RDG Packer Detector (via wine), E2A (via wine)

Packing

- upx, ImpRec (via wine)

Debugging

- gdb, edb, ddd, eresi, ollydbg (via wine)

Tracing

- strace, ltrace

Kernel debugging

- kgdb, ftrace, systemtap

Network

- wireshark, tcpdump, nmap, zenmap, telnet, ettercap, netcat, snort, xplico

Sistema

- AIDE, OSSEC

Sandboxes

- Anubis
- **Malware Analyzer**
- **Truman**
- **TWMAN**
- **Cuckoo**
- GFI Sandbox
- CWSandbox
- Norman Sandbox
- JoeBox
- Idefender Sysanalyzer
- Threat Expert
- Malwarepunk

TRUMAN

Análise de Tráfego de Rede

- ipaudit
- tshark
- ngrep
- tcptrace
- fauxservers –IRC, DNS, SMB, SMTP

Análise de Imagem de Disco

- AIDE
- Alternate Data Streams
- Registry analysis – dumphive, regdiff.pl, regripper

Análise de Imagem de Memória

- pmodump.pl
- Volatility

Análise Estática de Binário

- A/V
- objdump
- binhash
- ssdeep
- packerid.py

TWMAN

Development

- Truman, The Reusable Unknown Malware Analysis Net
- NCHC Clonezilla
- INetSim, Internet Services Simulation Suite

Co-operation

- Honeynet
  - *Nepenthes*
  - *Dionaea*
- Search engine
  - *Splunk*
- Virus Scanner
  - *Virus Total*

4LINUX
FREE SOFTWARE SOLUTIONS

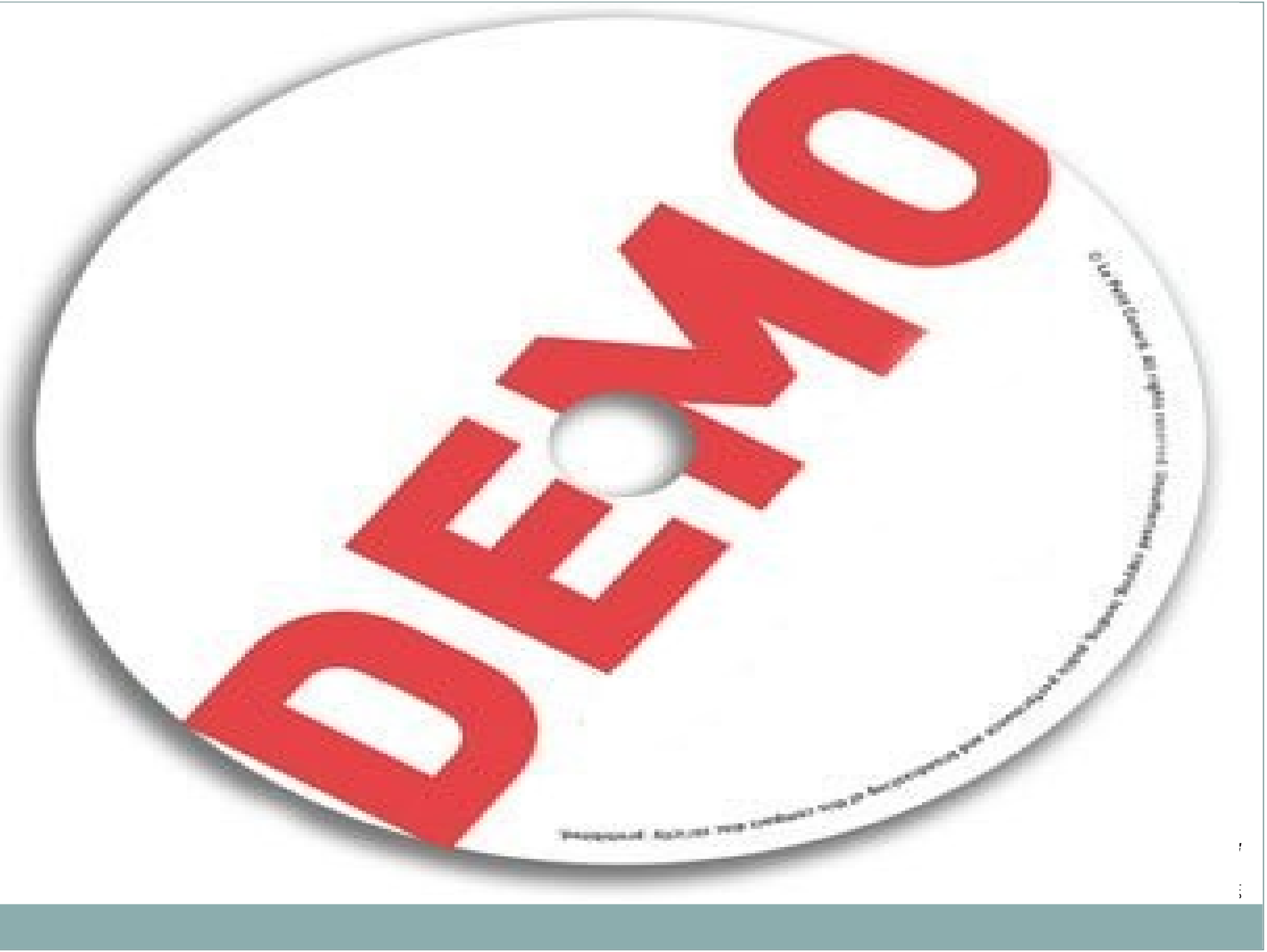
http://sourceforge.net/projects/twman/

Cuckoo

http://www.cuckoobox.org/

```
root@laptop:/home/luiz/cuckoo-0.1.0-beta/cuckoo# ./cuckoo.sh
   .---.                    _
  /   6_6                  | |
  \_  (__\    ____ _   _   ____| |  _ ___   ___
  //   \\    / __) | | |/ __) |_/ ) _ \ /_ \
 ((     ))  ( (___| |_| ( (___|  _ ( |_| | |_| |
==""===""==  \____)___/ \____)_| \_)___/ \___/
    |||            www.cuckoobox.org
     |

[2011-05-13 23:07:30] [Start Up] Starting Cuckoo TCP Server...
[2011-05-13 23:07:30] [Start Up] Cuckoo TCP Server running on address 192.168.1.101 and port 7777.
[2011-05-13 23:08:39] [TCP] [192.168.1.101] Received start analysis request: "START|LOCAL:/home/luiz/cuckoo-0.1.0-beta/cuckoo/Sac_Serasa.exe".
[2011-05-13 23:08:39] [TCP] [NOTICE] [192.168.1.101] No custom package specified, using default.
[2011-05-13 23:08:39] [QUEUE] [NOTICE] Analyses Queue size: 1.
[2011-05-13 23:08:39] [CORE] Acquired and locked Virtual Machine with IP "192.168.1.106" to analyze "/home/luiz/cuckoo-0.1.0-beta/cuckoo/Sac_Serasa.exe".
[2011-05-13 23:08:39] [Start Analysis] Starting analysis of file "Sac_Serasa.exe" on virtual machine "192.168.1.106".
[2011-05-13 23:08:39] [Start Analysis] Loaded package "/home/luiz/cuckoo-0.1.0-beta/cuckoo/packages/exe.au3".
[2011-05-13 23:08:39] [Start Analysis] Selected virtual machine "192.168.1.106" with label "WinXP".
[2011-05-13 23:08:39] [Start Analysis] Copied file "/home/luiz/cuckoo-0.1.0-beta/cuckoo/Sac_Serasa.exe" to path "/home/luiz/cuckoo-0.1.0-beta/cuckoo/shares/1
92.168.1.106/bin/24291eb061dc38a2b9314c11ef8f22c3.exe".
[2011-05-13 23:08:39] [Start Analysis] Generated AutoIt3 Analysis package at path "/home/luiz/cuckoo-0.1.0-beta/cuckoo/shares/192.168.1.106/run.au3".
[2011-05-13 23:08:39] [Start Sniffer] Sniffer started monitoring IP "192.168.1.106".
[2011-05-13 23:08:39] [Start Analysis] Launched analysis of file "24291eb061dc38a2b9314c11ef8f22c3.exe" on "WinXP".
tcpdump: listening on wlan0, link-type EN10MB (Ethernet), capture size 1515 bytes
```


DEMO

4LINUX
FREE SOFTWARE SOLUTIONS