THREATS IN VITRO

Construindo um ambiente de análise de malwares para detecção de ameaças desconhecidas (Zero Day).

Pedro Prudêncio
CISSP, CRISC, Morphus LABS

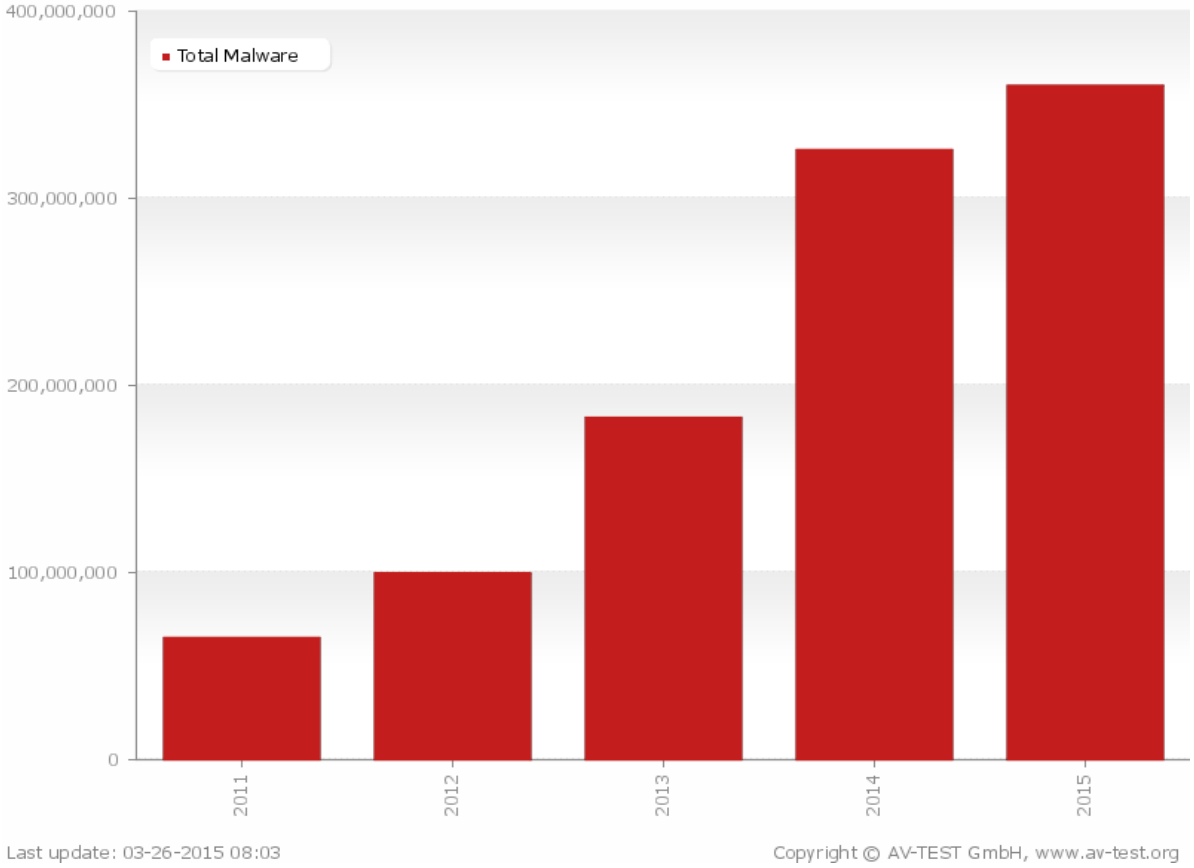
MORPHUS LABS

- Motivação;
- Malwares e Evolução;
- Advanced Persistent Threats;
- Análise de Malwares;
- TiV: Arquitetura da Plataforma;
- Classificação com Base Comportamental;
- Demonstração do Sistema.

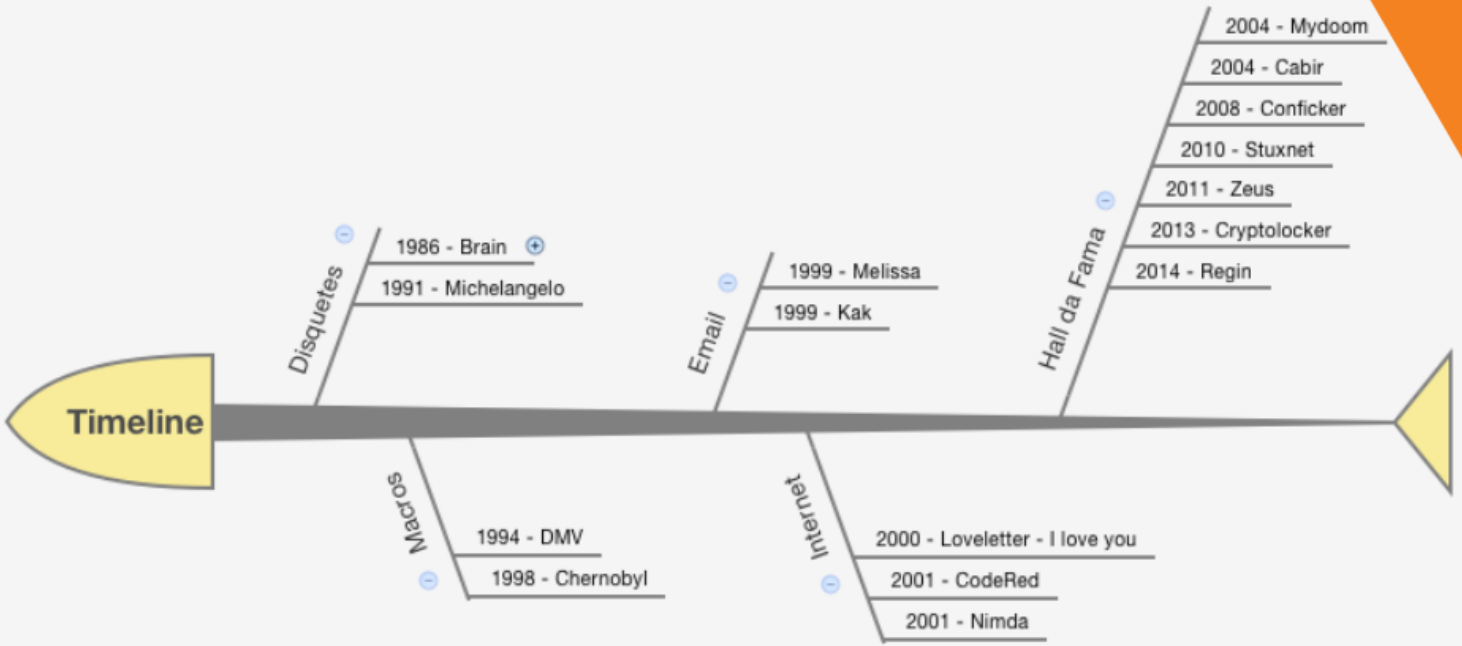
Malwares

“São programas destinados a se infiltrarem em um sistema digital alheio de forma ilícita, com o intuito de causar algum dano ou roubo de informações.”

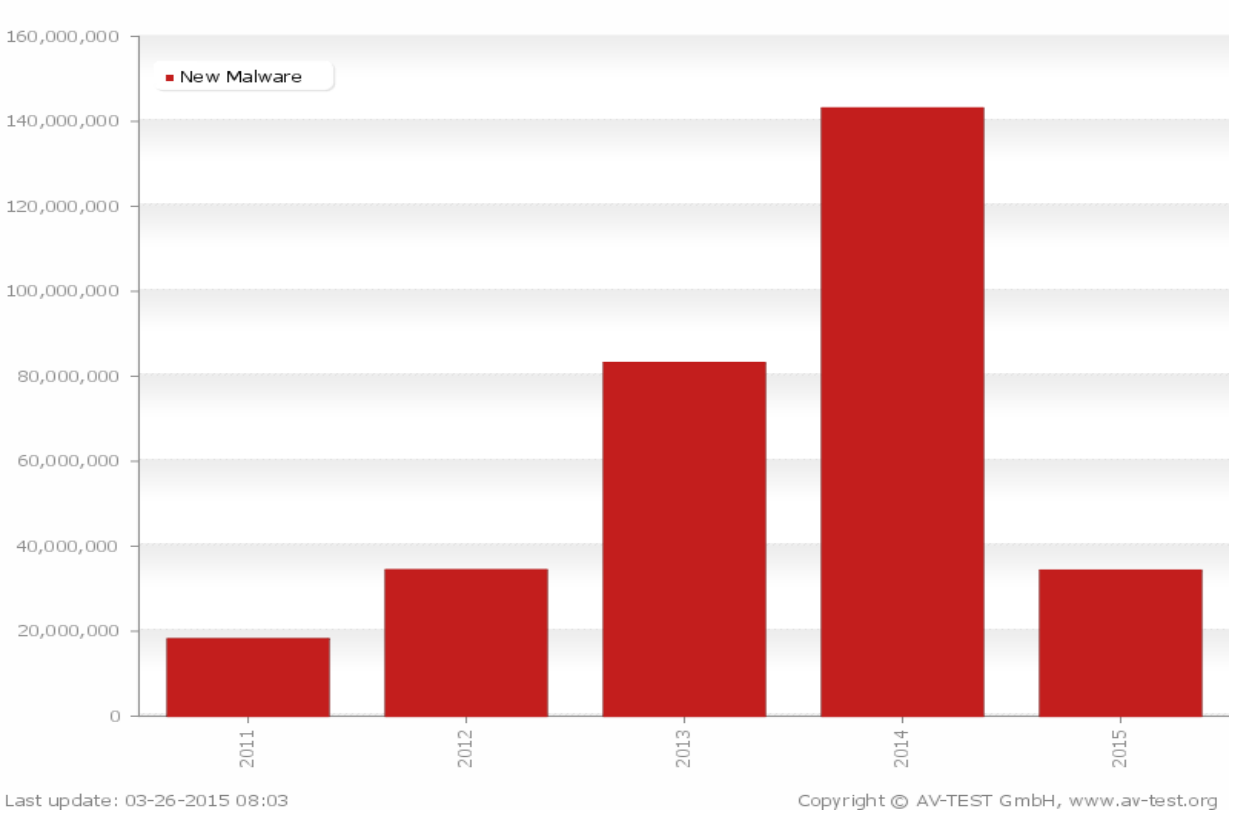
Malwares


400,000,000
300,000,000
200,000,000
100,000,000
0
Total Malware
2011
2012
2013
2014
2015
Last update: 03-26-2015 08:03
Copyright © AV-TEST GmbH, www.av-test.org

Evolução dos Malwares



Antivírus está morto?



Antivírus está morto?

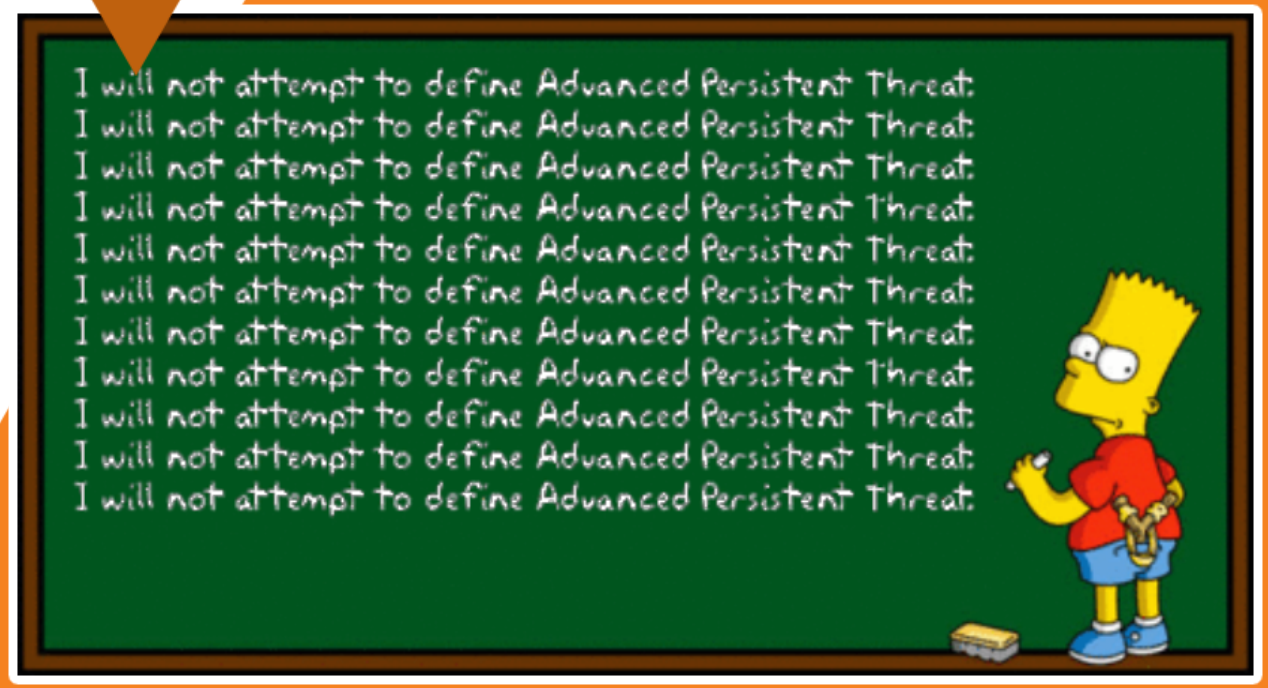
Direcionado

Avançado

Persistente

Advanced Persistent Threats

Como se proteger de um APT?



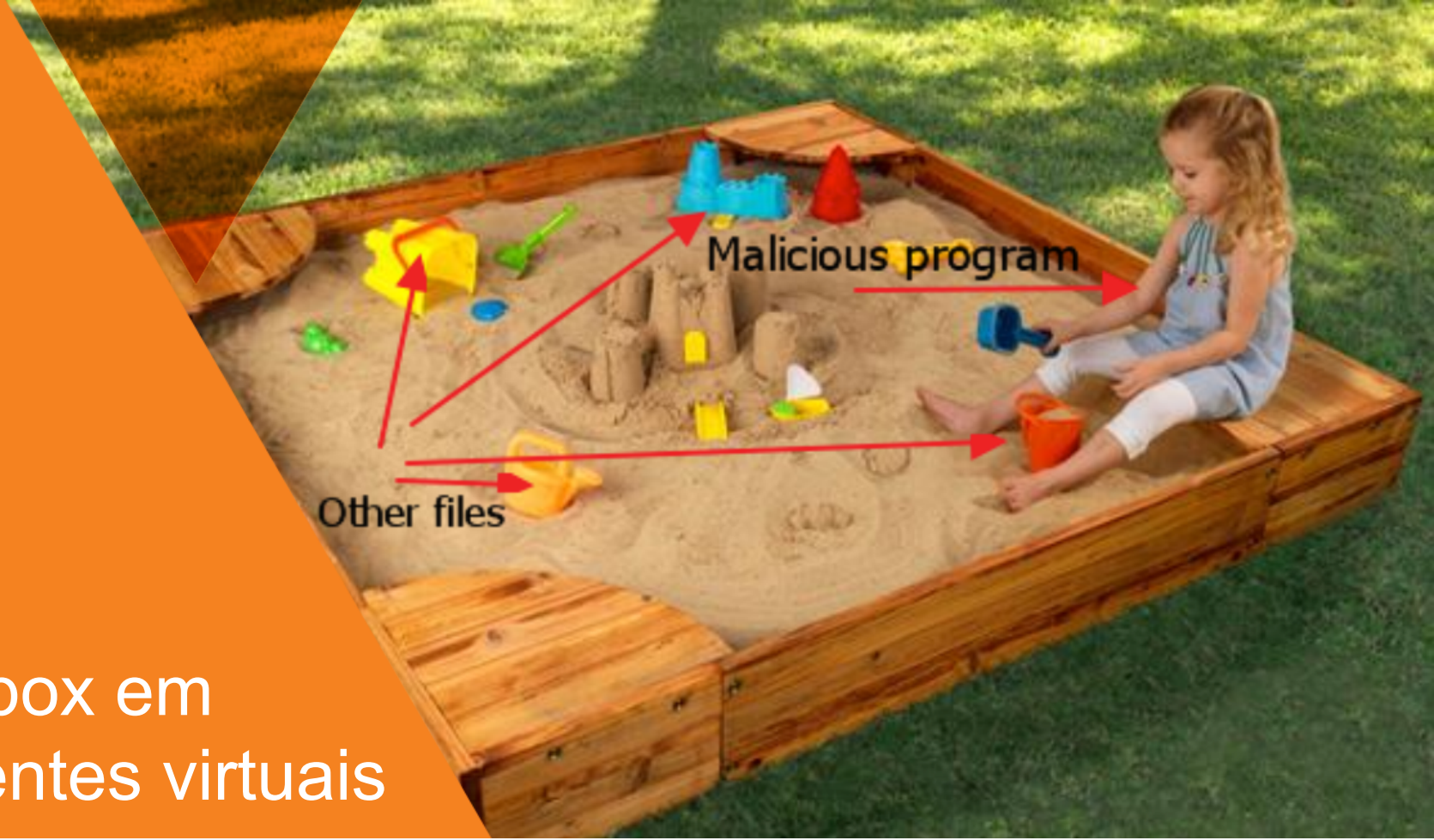
Análise Estática

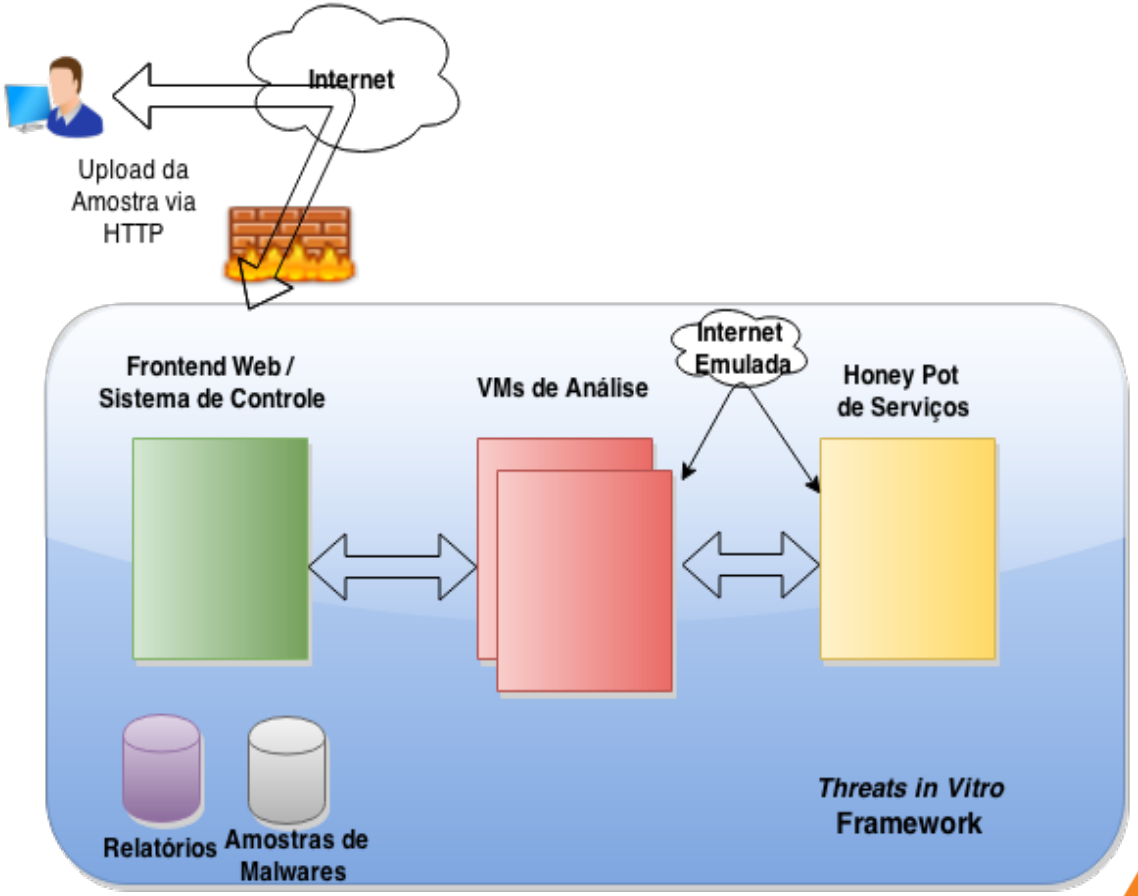
- Identificação única da amostra (HASHes)
- Identificação de funções importadas;
- Identificação de código ofuscado;
- Verificações de padrões do arquivo binário;
- Análise de código (disassembly);
- Metódo bastante preciso, pode demorar muito tempo e conhecimento.

Análise Dinâmica

- **Análise automatizada;**
- **Execução do binário;**
- **"Tracking" das mudanças realizadas pela amostra;**
- **Reconhecimentos de padrões maliciosos;**
- **Método rápido.**

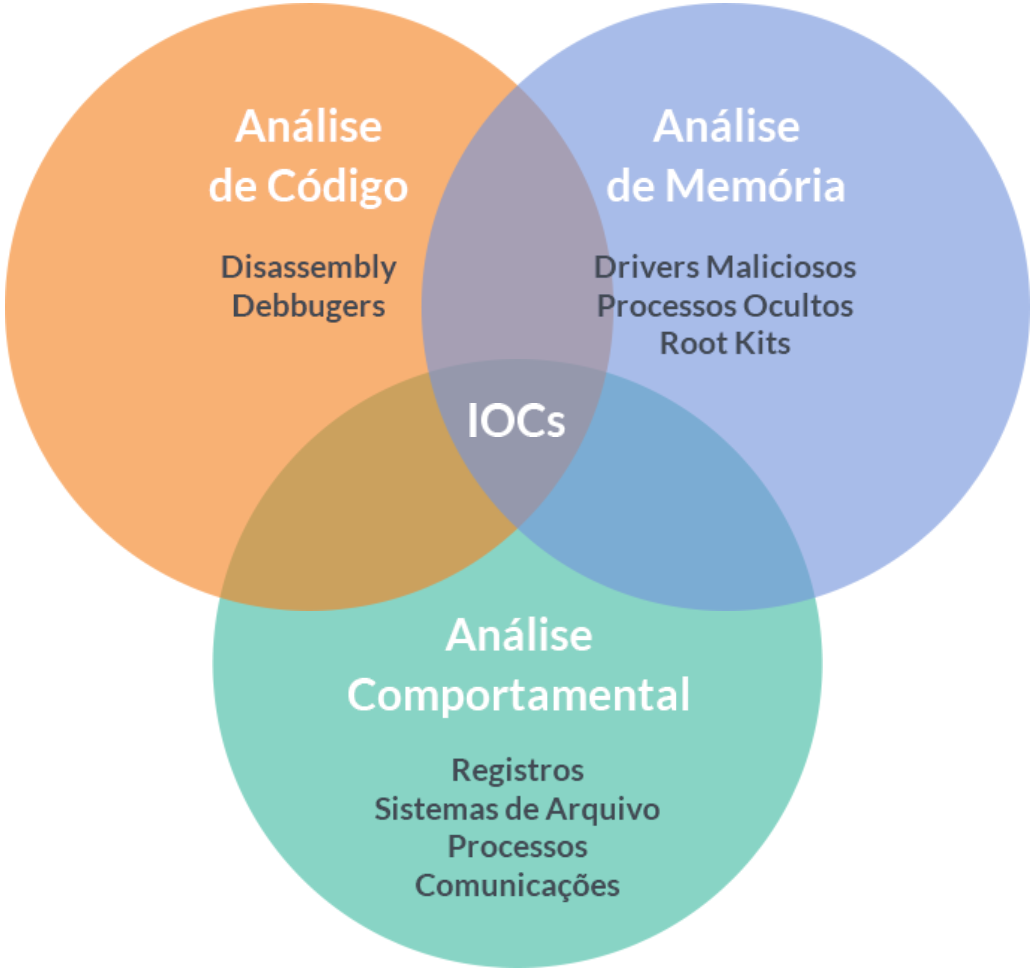
Sandbox em ambientes virtuais





Arquitetura Proposta: TiV

Análise do Sistema



TiV:
Classificação com base comportamental

Comportamento Observado	Risco
Autorreplicação via e-mail	Crítico
Instalação de novos certificados de segurança	Crítico
Persistência – Inicialização automática	Alto
Criação de arquivos no diretório de sistema (C:\Windows)	Alto
Modificação e/ou destruição de arquivos não temporários	Alto
Mudança das configurações dos navegadores Web	Médio
Criação de novos processos	Médio

THREATS IN VITRO

THREATS IN VITRO

Analise seus arquivos!

Lorem ipsum dolor sit amet, consecte tuer adipiscing elit, sed diam nonummy nibh euismod tincidunt ut laoreet dolore magna aliquam erat volutpat. Ut wisi enim ad minim veniam, quis nostrud exerci tation ullamcorper suscipit obortis nisl ut aliquip ex ea commodo quat.

1. Upload

Primeiro faça upload do arquivo

Upload

nome do arquivo.exe

CONTINUE

Uma solução MORPHUS LABS Apoio INSERT

THREATS IN VITRO

Analise seus arquivos!

Lorem ipsum dolor sit amet, consecte tuer adipiscing elit, sed diam nonummy nibh euismod tincidunt ut laoreet dolore magna aliquam erat volutpat. Ut wisi enim ad minim veniam, quis nostrud exerci tation ullamcorper suscipit obortis nisl ut aliquip ex ea commodo quat.

Opps...

O formato do arquivo enviado não é válido.
Formatos aceitos:
.pdf, .exe, .png.

Tentar novamente

Uma solução MORPHUS LABS Apoio INSERT

THREATS IN VITRO

Analise seus arquivos!

Lorem ipsum dolor sit amet, consecte tuer adipiscing elit, sed diam nonummy nibh euismod tincidunt ut laoreet dolore magna aliquam erat volutpat. Ut wisi enim ad minim veniam, quis nostrud exerci tation ullamcorper suscipit obortis nisl ut aliquip ex ea commodo quat.

Um instantinho!

Você é o 5º da fila.
em aproximadamente
2 minutos seu arquivo
será analisado.

Uma solução MORPHUS LABS Apoio INSERT

THREATS IN VITRO

Analise seus arquivos!

Lorem ipsum dolor sit amet, consecte tuer adipiscing elit, sed diam nonummy nibh euismod tincidunt ut laoreet dolore magna aliquam erat volutpat. Ut wisi enim ad minim veniam, quis nostrud exerci tation ullamcorper suscipit obortis nisl ut aliquip ex ea commodo quat.

2. Análise

Passo 1/4

Inicializando ambiente de análise.

Relatório

Uma solução MORPHUS LABS Apoio INSERT

THREATS IN VITRO

- **Serviço Online e Gratuito para análise de até X amostras / dia;**
- **Plataforma brasileira, relatórios em português;**
- **Combinação de técnicas de análises estáticas e dinâmicas e de memória;**
- **Possibilidade de download de sumário do relatório em PDF;**
- **Fonte de inteligência, novas tendências e técnicas de ameaças desconhecidas;**
- **Contribuição para comunidade.**

THREATS IN VITRO

Lançamento: 15/07/2015

Save the date!

http://threatsinvitro.morphuslabs.com

Em andamento …

- **Suporte a diferentes versões de sistema operacional, começando pelas versões do Microsoft Windows 8 (Powershell);**

- **Reconhecimento de padrões de forma automatizada, através de algoritmos de aprendizagem de máquina baseado em anomalias comportamentais;**

- **Melhoria nas técnicas de ofuscação do reconhecimento de ambientes virtualizados.**

THREATS IN VITRO

Obrigado!

Pedro Prudêncio
CISSP, CRISC, Morphus LABS