TLP:CLEAR

dec@tron®
30 anos

Conectando pessoas e negócios através de soluções inteligentes.

A ENGENHARIA REVERSA POTENCIALIZANDO A RESPOSTA A INCIDENTES CIBERNÉTICOS

MARCOS RABELLO - CISO

&

KENJI MINEI – Reverse Engineer

TLP:CLEAR

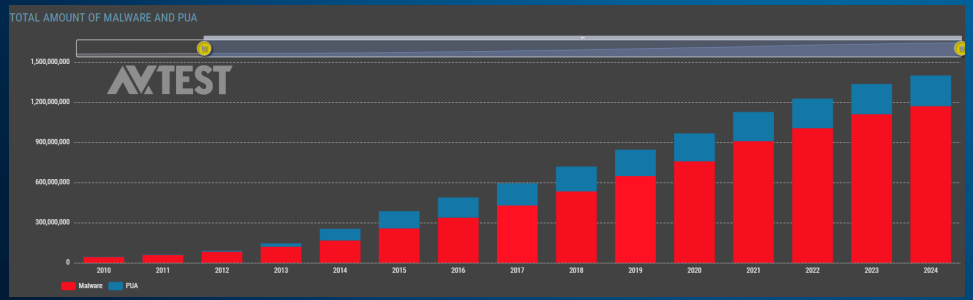
[Cenário Atual da Segurança Cibernética]

Crescente popularidade de Malwares

"O ransomware é uma das maiores ameaças em segurança cibernética e aumentou em 150% em 2020 devido à mudança repentina para o trabalho remoto"

"Em 2020, os ataques de ransomware direcionados a dispositivos de IoT aumentaram em 109% nos EUA"

Cisco Report 2021 – Proteção contra Ransonware



https://www.av-test.org/en/statistics/malware/

dec@tron®

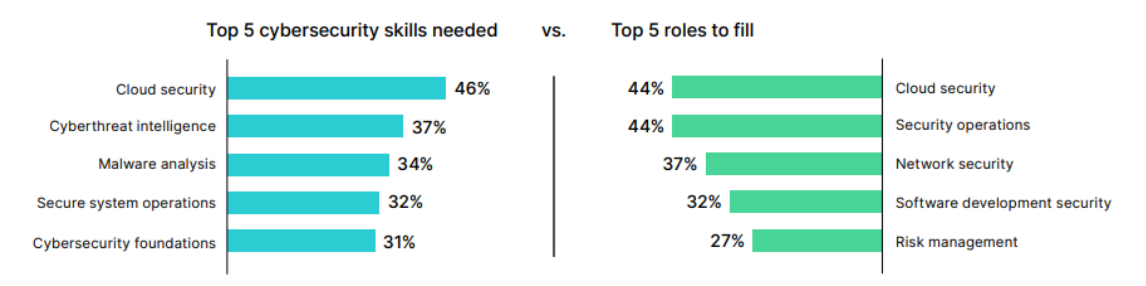
TLP:CLEAR

[Cenário Atual da Segurança Cibernética]

Crescente demanda por profissionais

“Estima-se que 3,14 milhões de profissionais sejam necessários para preencher a lacuna global da força de trabalho de segurança cibernética”

“68% das organizações indicam que enfrentam riscos cibernéticos adicionais devido a cargos de TI não preenchidos pela escassez de habilidades cibernéticas”



Fortinet Report 2023 - Cybersecurity Skills Gap

dec@tron®

TLP:CLEAR

[Cenário Atual da Segurança Cibernética]

ESTRATÉGIA

PROGRAMA CORPORATIVO DE TRANSIÇÃO DE CARREIRA

Outros áreas de atuação

Mentoria do RH

Cyber Security

TLP:CLEAR

[Cenário Atual da Segurança Cibernética]

ESTRATÉGIA

DIVERSIDADE DE TALENTOS NA FORMAÇÃO DE EQUIPES

- Socioemocionais, empatia, resiliência e etc

- Ensino Formal

- Artes, Esportes e etc

dec@tron®

TLP:CLEAR

[Desafios das Equipes de Resposta a Incidentes]

Arquitetura de Segurança

- Entendendo as capacidades de detectar e responder

dec@tron®

TLP:CLEAR

[Desafios das Equipes de Resposta a Incidentes]

Cenário da ameaça

- Atividade Suspeita

A detecção indica apenas um comportamento, sem informação clara da ameaça

Muitas aplicações internas, e automações, são detectadas como suspeitas

Ofuscação de código e aplicações compiladas requerem tempo adicional, além de conhecimento

Artefatos relacionados ao evento não identificados em bases de IOCs

SandBoxs que não revelam ações maliciosas ou não atuam.

TLP:CLEAR

[Desafios das Equipes de Resposta a Incidentes]

Cenário da Resposta

- Atividade Suspeita

É necessário expandir a analise para eventos correlatos ao Alerta

Montar a cadeia de interação com outros ativos relacionada ao evento detectado

Em alguns casos a legitimidade da ação ou processo precisa ser validada

verificar se o usuário ou gestor do ativo reconhecem a ação

Escalar para eventos com potencial de impacto, em áreas críticas ao negócio ou reincidentes (Persistentes)

Escalonamento Técnico

Escalação Executiva

TLP:CLEAR

[Desafios das Equipes de Resposta a Incidentes]

Escalonando a análise

Escalonar análise de malware para eventos

É preciso entender a completude da capacidade do malware e suas fragilidades para entender as ameaças e respostas possíveis

TLP:CLEAR

[Desafios das Equipes de Resposta a Incidentes]

Escalonado a Engenharia Reversa de Malware

TLP:CLEAR

A ENGENHARIA REVERSA DE MALWARE ESCALONADA

dec@tron®

TLP:CLEAR

[Analise de Incidente]

- **Métodos tradicionais de analise:**
  - **Analise de eventos**
  - **Analise via Sandbox**
  - **Analise de Reputação**

- **Problemas com os métodos acima;**
  - **Não Identificação das capacidades reais do artefato;**
  - **Métodos não determinísticos;**

TLP:CLEAR

[Analise de Incidente]

- **Analise de eventos**
  - **Verificar a sequência de execução e eventos do artefato.**
  - **Analisar conexões relacionadas com o artefato/máquina.**

[Analise de Incidente]

- **Analise de eventos (Deficiências)**
  - **Não identificação do artefato exato que causou o evento.**
  - **Exploração de softwares legítimos.**
    - **EX: VMNat.exe**

TLP:CLEAR

[Analise de Incidente]

- **Analise de eventos (Deficiências)**
  - **Fluxo de execução incompleto/Falta de logs da ferramenta.**
    - **O EDR vai registrar toda a execução?**
    - **HTTPs Based C2?**
    - **Aplicação funcional com Steganography?**
    - **Domain Fronting (Cloudflare/Azure/Discord...?)**

dec@tron®

TLP:CLEAR

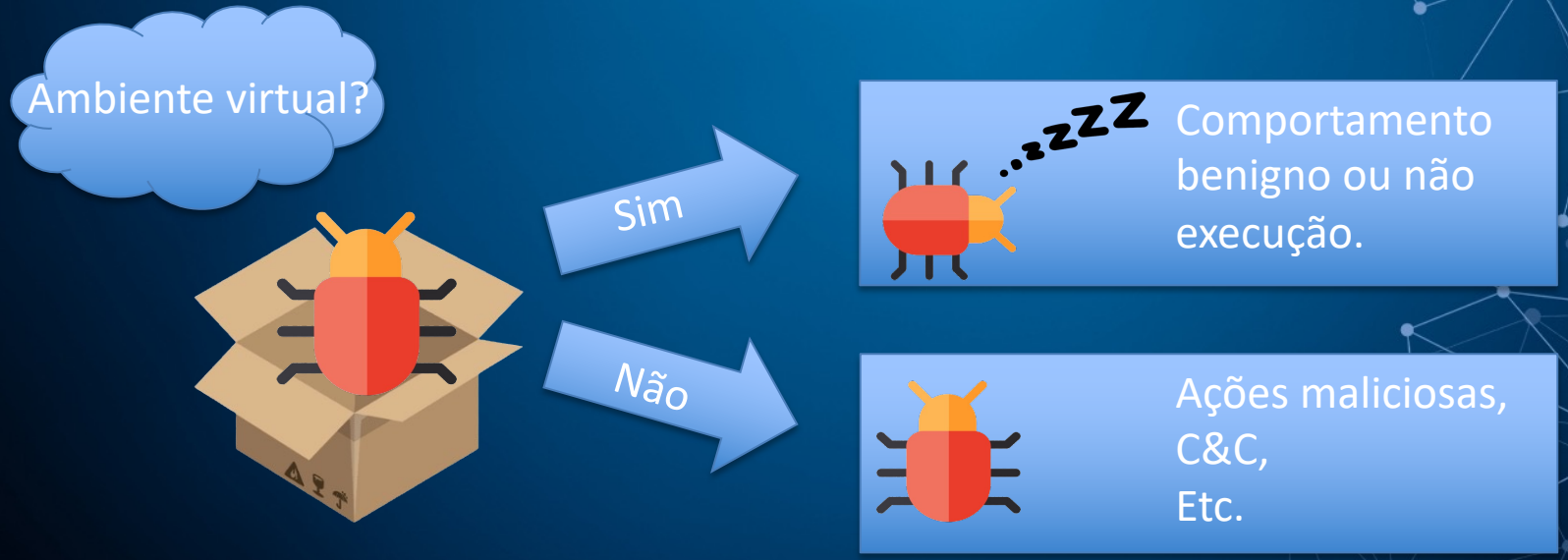
[Analise de Incidente]

- **Analise via Sandbox | Reputação**
  - **Verificar hash em ferramentas de sandbox.**
  - **Analise dinâmica usando sandbox online ou local.**

TLP:CLEAR

[Analise de Incidente]

- **Analise via Sandbox | Reputação (Deficiências)**
  - **Mudança de HASH ou não presença na DB da ferramenta.**
  - **Aquele é o comportamento real do artefato?**



TLP:CLEAR

[Engenharia Reversa]

OBJETIVO

- **Foco em identificar capacidades dos artefatos;**
  - **Analise e identificação de técnicas e objetivos do atacante.**
  - **Identificar ameaças e suas variações ao longo do tempo (Mapear grupos e atores maliciosos).**
  - **Analise independente dos métodos de proteção utilizados no software.**

Engenharia Reversa

Capacidades
Técnicas
Assinaturas
Objetivos

TLP:CLEAR

[Sandbox na visão do atacante]

Cenário do ataque

- Virtualização e Sandbox

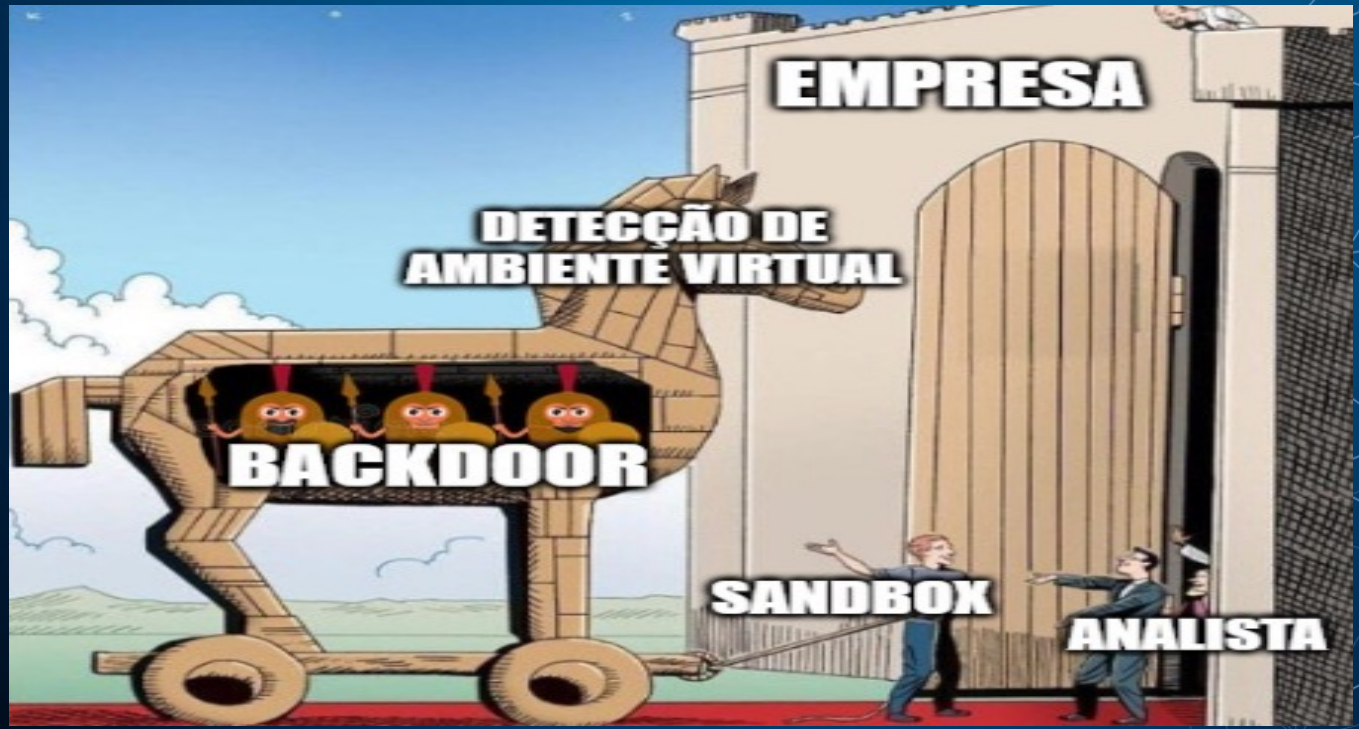
➢ **O uso de Sandbox está crescendo cada vez mais por times de segurança;**
  - **A simplicidade de verificar a sequência de execução na sandbox gera a falsa impressão da não necessidade do entendimento do binário.**

TLP:CLEAR

[Sandbox na visão do atacante]

Cenário do ataque

- Virtualização e Sandbox



TLP:CLEAR

[Sandbox na visão do atacante]

Cenário do ataque

- Virtualização e Sandbox

- **A sandbox usa a virtualização para executar e extrair informações sobre a execução de determinado artefato.**
- **Métodos mais populares de identificar o ambiente virtual;**
  - **Detecção de arquivos, processos e devices relacionados com ambientes virtuais.**
  - **Verificação de tamanho da tela, processador, interação do usuário, memoria etc...**

dec@tron®

Conectando pessoas e negócios através de soluções inteligentes.

MARCOS RABELLO
marcos.rabello@decatron.com.br

KENJI MINEI
kenji.minei@decatron.com.br

Estrada dos Bandeirantes, 7.000 – Bloco I - 3º andar
Rio de Janeiro – RJ – CEP 22780-084
(21) 3906-4000