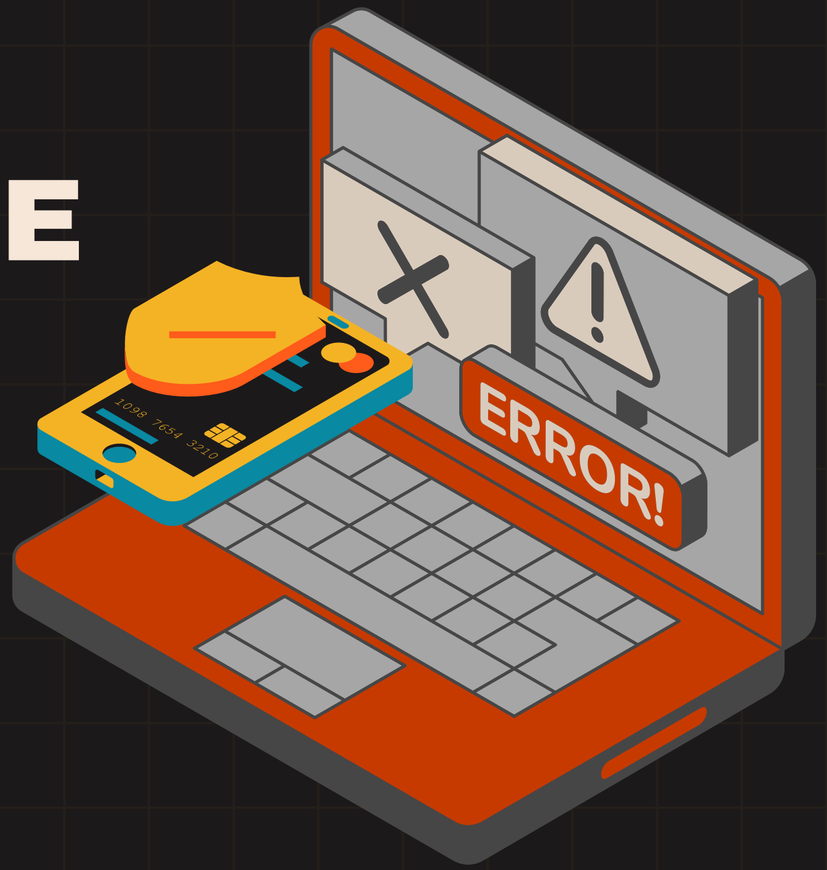
COMPUTAÇÃO FORENSE EM REDES DE COMPUTADORES



Guilherme Fortunato da Silva, Paloma de Castro Leite
REDES - UNESPAR - CCOMP

1. O QUE É COMPUTAÇÃO FORENSE DIGITAL?

COMPUTAÇÃO FORENSE DIGITAL

- A perícia digital é a recuperação e investigação de informações encontradas em dispositivos digitais no que diz respeito a atividades criminosas. Indicadores de comprometimento são a evidência de que ocorreu um incidente de segurança cibernética. Essas informações podem ser dados em dispositivos de armazenamento, na memória volátil do computador ou vestígios de cibercrime que são preservados em dados de rede, como pcaps e logs. É essencial que todos os indicadores de compromisso sejam preservados para análise futura e atribuição de ataques.

2. PROCESSO FORENSE DE EVIDÊNCIAS DIGITAIS

O QUE É?

- No Brasil, o Processo Forense de Evidências Digitais segue um rigoroso conjunto de etapas e procedimentos, fortemente influenciado por boas práticas internacionais, mas, fundamentalmente, regulado pelo Código de Processo Penal (CPP), especialmente após as alterações introduzidas pela Lei nº 13.964/2019 (Pacote Anticrime), que formalizou a Cadeia de Custódia para todos os tipos de vestígios, incluindo os digitais.

- O objetivo principal é garantir a integridade, a autenticidade e a rastreabilidade da evidência digital, desde sua coleta até sua apresentação em juízo, para que ela seja considerada uma prova lícita e válida. O processo pode ser dividido em quatro etapas principais.

ETAPAS

1.Coleta e Preservação (Identificação e Aquisição): O objetivo é identificar, isolar e coletar os dados de interesse de forma a preservar o estado original da evidência, evitando qualquer tipo de alteração.

2.Exame: Uso sobre a imagem forense (a cópia). O objetivo é processar os dados brutos coletados e prepará-los para a análise, recuperando informações que não estão diretamente visíveis.

3.Análise: Interpretação os dados examinados para construir uma narrativa, responder às perguntas da investigação (quesitos) e correlacionar as evidências digitais com os fatos do caso.

ETAPAS

4.Laudo Pericial (Relatório): É a fase final, onde todo o trabalho técnico é traduzido em um documento formal, o Laudo Pericial de Informática ou Relatório Técnico. Este documento deve ser claro, objetivo, imparcial e tecnicamente fundamentado para ser compreendido por um público não técnico, como advogados, promotores e juízes.

A Cadeia de Custódia é o pilar que sustenta todo o processo. Conforme definido nos Artigos 158-A a 158-F do Código de Processo Penal, ela é "o conjunto de todos os procedimentos utilizados para manter e documentar a história cronológica do vestígio, para rastrear sua posse e manuseio a partir de seu reconhecimento até o descarte". A quebra da cadeia de custódia pode levar à inadmissibilidade da prova, ou seja, a evidência digital pode ser invalidada e desconsiderada no processo judicial.

3. ANÁLISE FORENSE DE ALERTA DE REDE

CENÁRIO

- **Gatilho do Incidente**: Alerta gerado por um Sistema de Prevenção de Intrusão (IPS).
- **Evidência Inicial:** Valores de hash de arquivos suspeitos identificados no tráfego de rede.
- **Objetivo Principal:** Validar a ameaça e analisar o comportamento do artefato digital.

METODOLOGIA DE ANÁLISE

1. Análise Dinâmica (Sandbox):

- Execução do artefato em ambiente seguro e controlado.
- Observação em tempo real de suas ações: Processos criados, conexões de rede, alterações em arquivos e no sistema

2. Classificação e Contexto (Framework):

- Mapeamento do comportamento na matriz MITRE ATT&CK.
- Identificação das Táticas, Técnicas e Procedimentos (TTPs) do atacante.

FLUXO DA INVESTIGAÇÃO

ALERTA DO IPS

EXTRAÇÃO DO HASH (IOC)

ANÁLISE

MAPEAMENTO

CONLUSÃO

4. INVESTIGAÇÃO DE INDICADORES DE COMPROMETIMENTO (IOCS) A PARTIR DE ALERTAS DE UM IPS

O QUE É

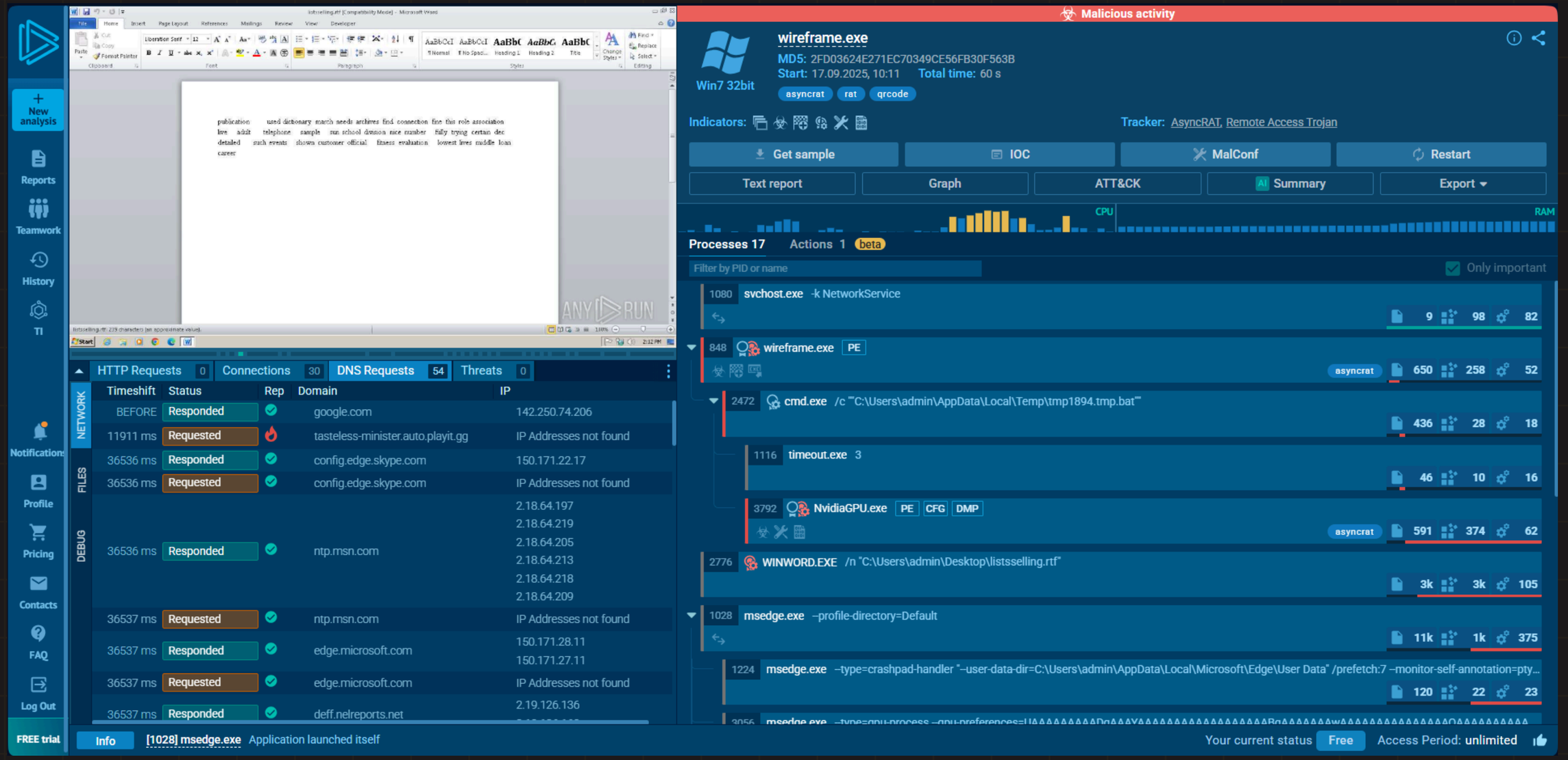
1.Sistema de Prevenção de Intrusão (IPS): Um IPS é um dispositivo de segurança de rede, sua função é inspecionar pacotes de dados que trafegam pela infraestrutura de rede em tempo real. Isso pode ter ocorrido durante qualquer forma de transferência de dados entre dois pontos da rede.

2.Evidência Hash: hash (MD5) é a "impressão digital" de um arquivo que o IPS suspeita ser malicioso. Isso demonstra um alerta de rede e implica que ele foi transmitido através de um protocolo de rede, nesse contexto, ele é um Indicador de Comprometimento (IOC) que representa um objeto que viajou pela rede e que pode ter chegado a um ou mais computadores da organização.

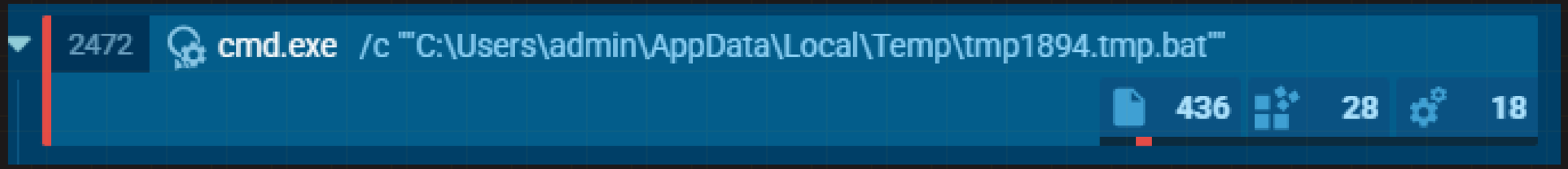
VALIDAÇÃO DO HASH ATRÁVES DO ANY.RUN

- Valor do hash MD5 do IOC: 2fd03624e271ec70349ce56fb30f563b

ÁRVORE DE PROCESSOS

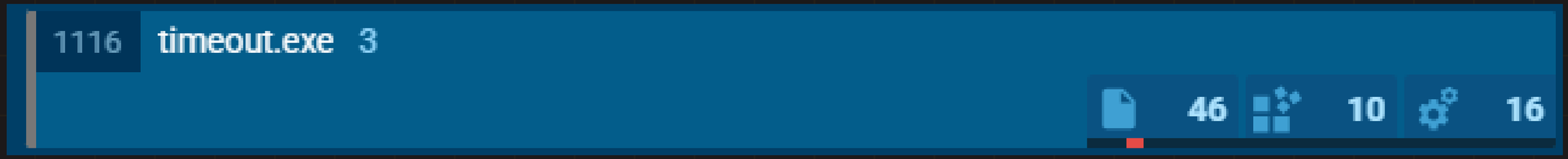


ÁRVORE DE PROCESSOS



- **cmd.exe:** uso do 'Living off the Land' (Vivendo da Terra), onde o malware usa ferramentas legítimas do próprio Windows para realizar suas ações e se camuflar. Ele usou o prompt de comando para executar um script (1994.tmp.bat), que provavelmente continha as instruções para os próximos estágios do ataque.

ÁRVORE DE PROCESSOS

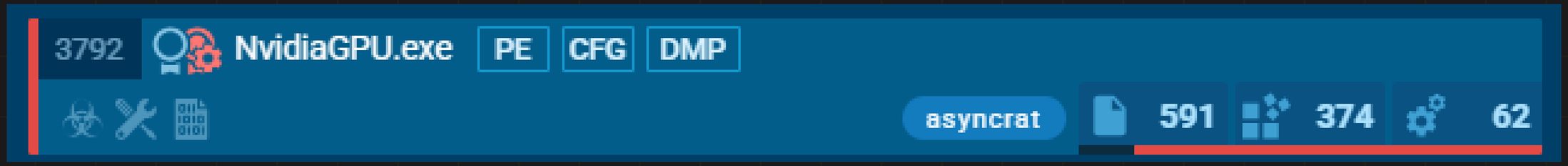


- **timeout.exe:** Esta é uma técnica de evasão, ao usar o 'timeout', o malware atrasa suas ações mais maliciosas, na esperança de que a análise seja encerrada antes que ele revele seu verdadeiro objetivo.

ÁRVORE DE PROCESSOS

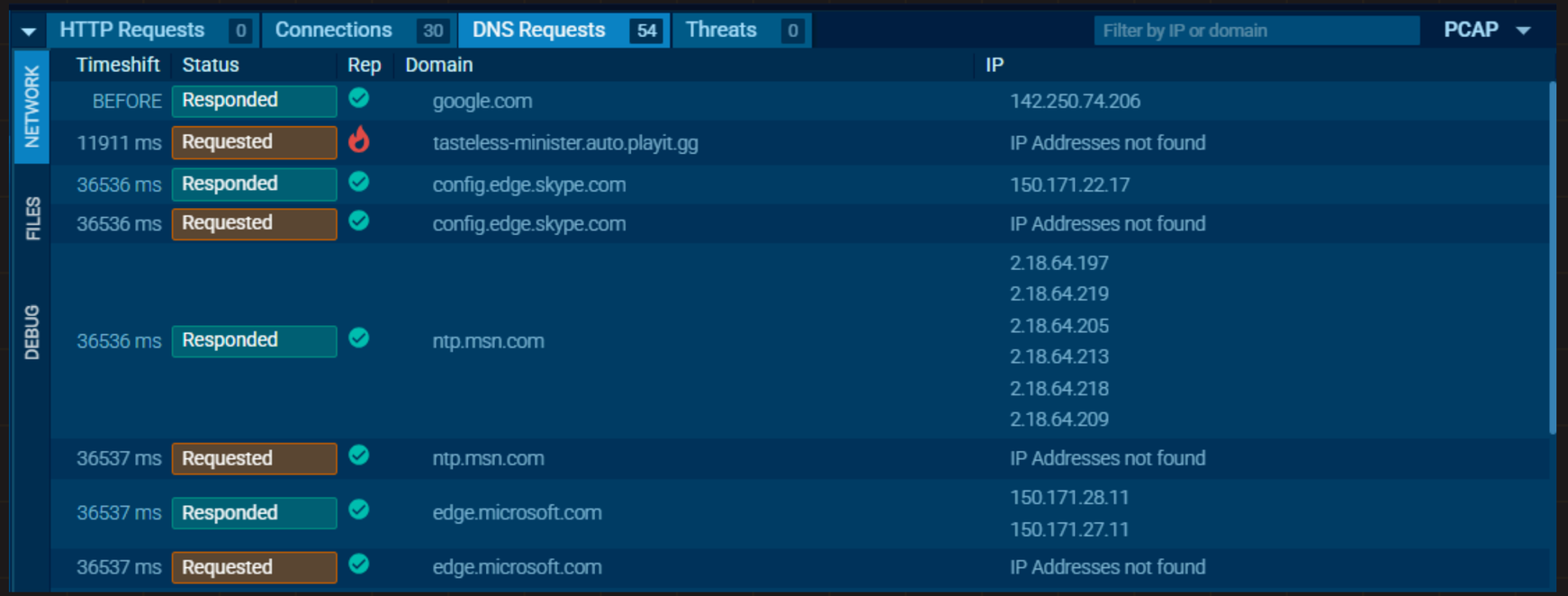
- **WINWORD.EXE (Microsoft Word):** Tática de distração e engano, onde o malware abre o Microsoft Word para carregar um documento (bestselling.rtf). Para o usuário, parece que ele apenas abriu um documento normal, mas a infecção continua a se espalhar.

ÁRVORE DE PROCESSOS



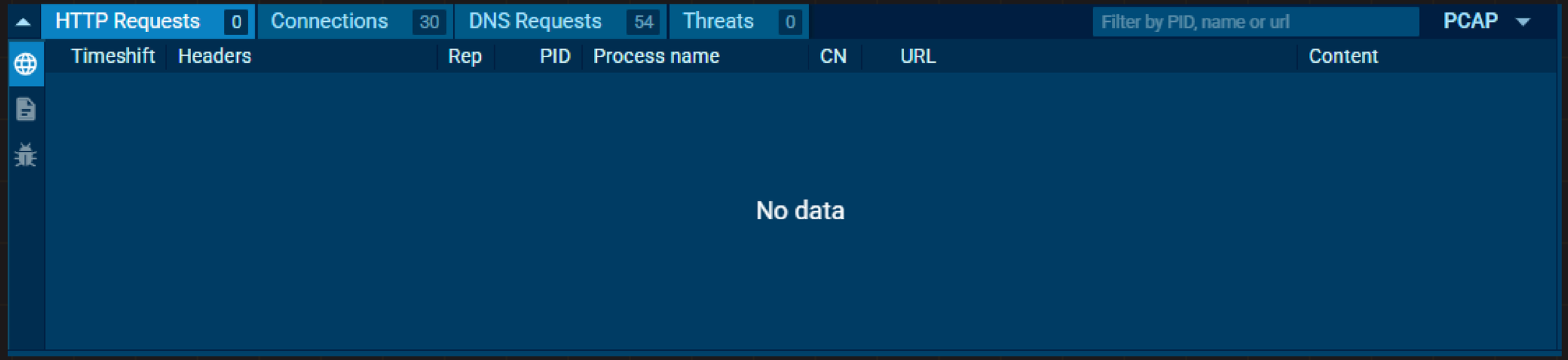
- **NVvGDE.GPU.exe:** O processo tenta se mascarar como um componente de driver de vídeo da NVIDIA para parecer legítimo. É muito provável que este seja outro componente do próprio malware, renomeado para não levantar suspeitas enquanto executa tarefas maliciosas em segundo plano.

ÁRVORE DE PROCESSOS



- **DNS Requests:** Antes de se conectar a um servidor, o malware precisa descobrir o endereço IP desse servidor. Ele primeiro checa se a máquina tem acesso à internet resolvendo um domínio legítimo. Se funcionar, ele sabe que pode tentar se conectar ao seu próprio servidor malicioso.

ÁRVORE DE PROCESSOS



- **HTTP Requests:** Esta aba mostraria o tráfego web real. Se houvesse requisições HTTP, seria exibido o malware tentando baixar um arquivo (ex: GET /payload.exe) ou enviar dados roubados (ex: POST /dados.php). É aqui que o conteúdo da comunicação com o atacante ficaria visíve**l.**

ÁRVORE DE PROCESSOS

- **Connections:** Esta aba mostra as conexões de rede diretas (TCP/UDP) que o malware estabeleceu com os endereços IP. Ela nos demonstra os endereços IP exatos dos servidores do atacante.

RELATÓRIO GERAL

General Info

Add for printing

File name:	wireframe.exe
Full analysis:	https://app.any.run/tasks/40844662-acf1-42f8-a78b-4337ae61ab26
Verdict:	Malicious activity
Threats:	**AsyncRAT** Remote Access Trojan

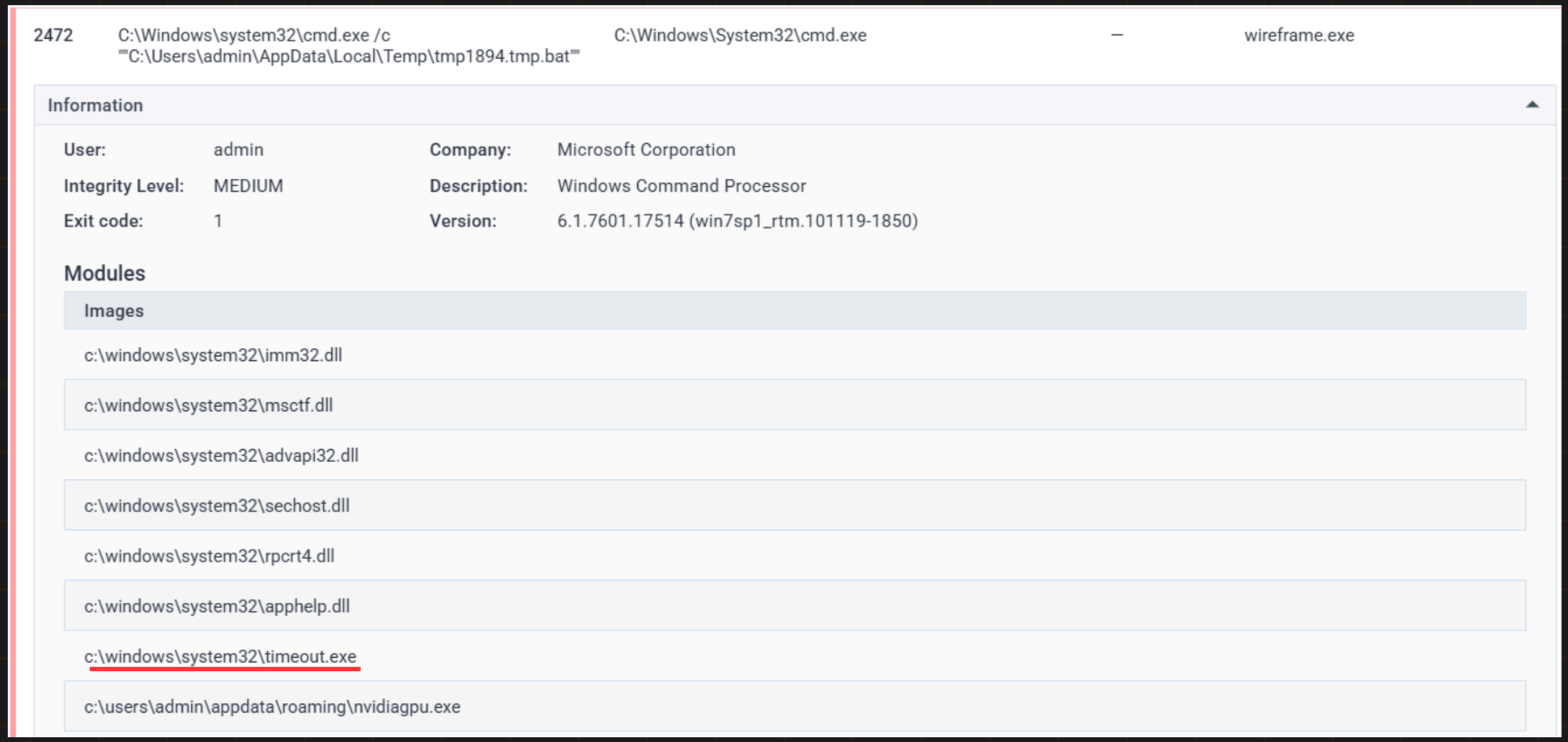
AsyncRAT is a RAT that can monitor and remotely control infected systems. This malware was introduced on Github as a legitimate open-source remote administration software, but hackers use it for its many powerful malicious functions.

Malware Trends Tracker >>>

Analysis date:	September 17, 2025 at 10:11:55
OS:	Windows 7 Professional Service Pack 1 (build: 7601, 32 bit)
Tags:	asyncrat rat qrcode
Indicators:	
MIME:	application/vnd.microsoft.portable-executable
File info:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows, 3 sections
MD5:	2FD03624E271EC70349CE56FB30F563B
SHA1:	7ED2E38DECB996A7F695BF7B80E0C102F4D01F10
SHA256:	9C83A89EA0E56D5AF9AA37D2DABED20B2412DB8C9694A13128EA173A73557487
SSDEEP:	1536:DCWYHwZU0YIv/bzdHIn2UpeOGBLPH73bTXSAgLni3Rimmx:DCWYHwZU0YI1HI8b73bTfBOx

- Tags como backdoor ou rat (Remote Access Trojan) confirmam que o objetivo do malware é permitir o acesso remoto ao sistema.

RELATÓRIO GERAL



2472	C:\Windows\system32\cmd.exe /c ""C:\Users\admin\AppData\Local\Temp\tmp1894.tmp.bat""	C:\Windows\System32\cmd.exe	–	wireframe.exe

Information

User:	admin	**Company:**	Microsoft Corporation
Integrity Level:	MEDIUM	**Description:**	Windows Command Processor
Exit code:	1	**Version:**	6.1.7601.17514 (win7sp1_rtm.101119-1850)

Modules

Images

- c:\windows\system32\imm32.dll
- c:\windows\system32\msctf.dll
- c:\windows\system32\advapi32.dll
- c:\windows\system32\sechost.dll
- c:\windows\system32\rpcrt4.dll
- c:\windows\system32\apphelp.dll
- c:\windows\system32\timeout.exe
- c:\users\admin\appdata\roaming\nvidiagpu.exe

- O relatório confirma que o malware usou o comando 'timeout.exe' intencionalmente para atrasar sua execução, uma tática para enganar sistemas de análise automática.

RELATÓRIO GERAL

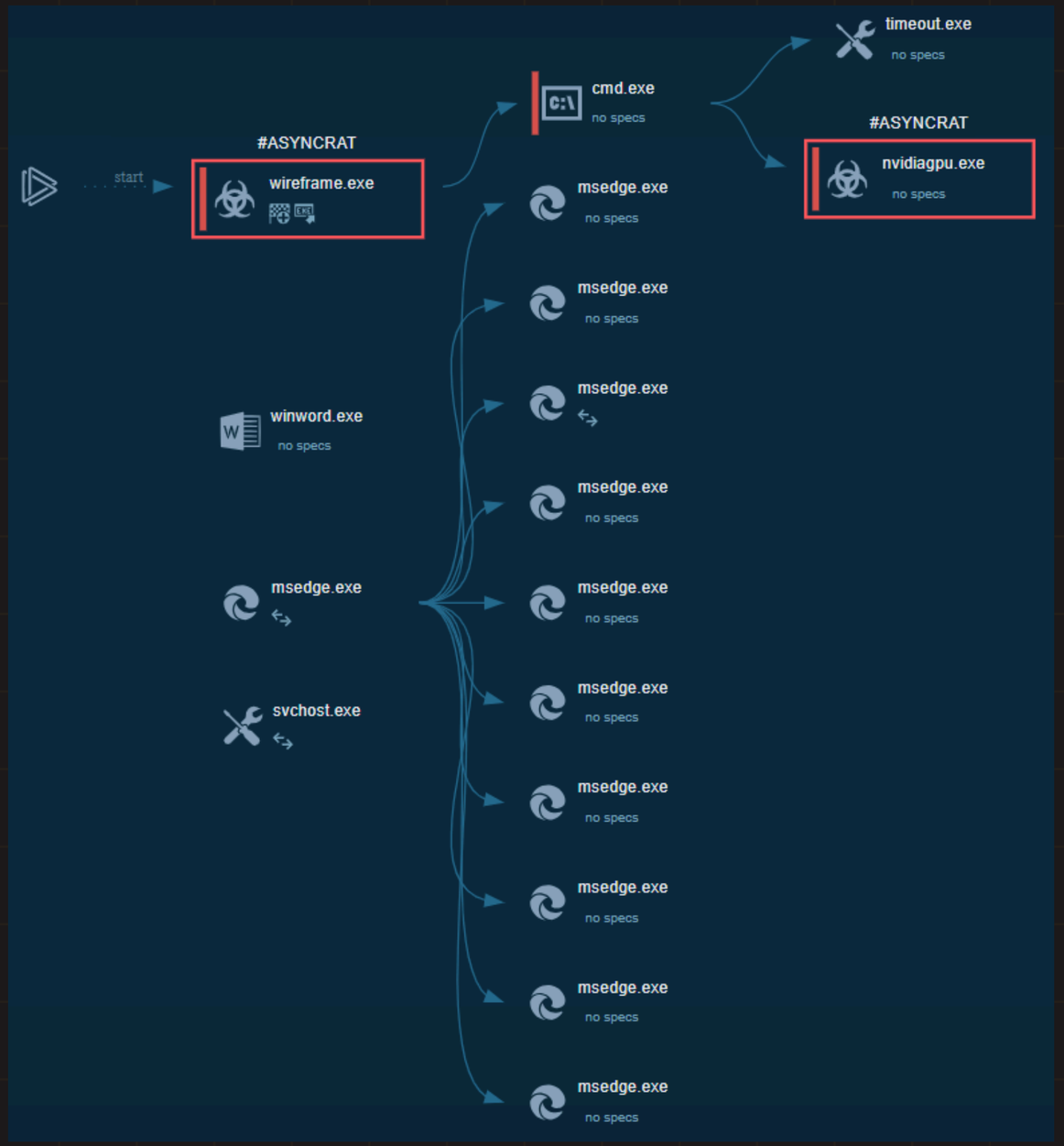
DNS requests

Domain	IP	Reputation
google.com	142.250.74.206	whitelisted
tasteless-minister.auto.playit.gg	–	malicious

- Ele fornece o domínio exato (tasteless-minister.auto.playit.gg) com o qual o malware tentou se comunicar.

GRÁFICO DE PROCESSOS

- **wireframe.exe:** O arquivo malicioso inicial que foi executado.
- **nvidiagpu.exe:** Um segundo componente malicioso, criado durante o ataque.
- **AsyncRAT (Cavalo de Troia de Acesso Remoto):** ele entrega ao invasor o controle total e remoto sobre o computador infectado

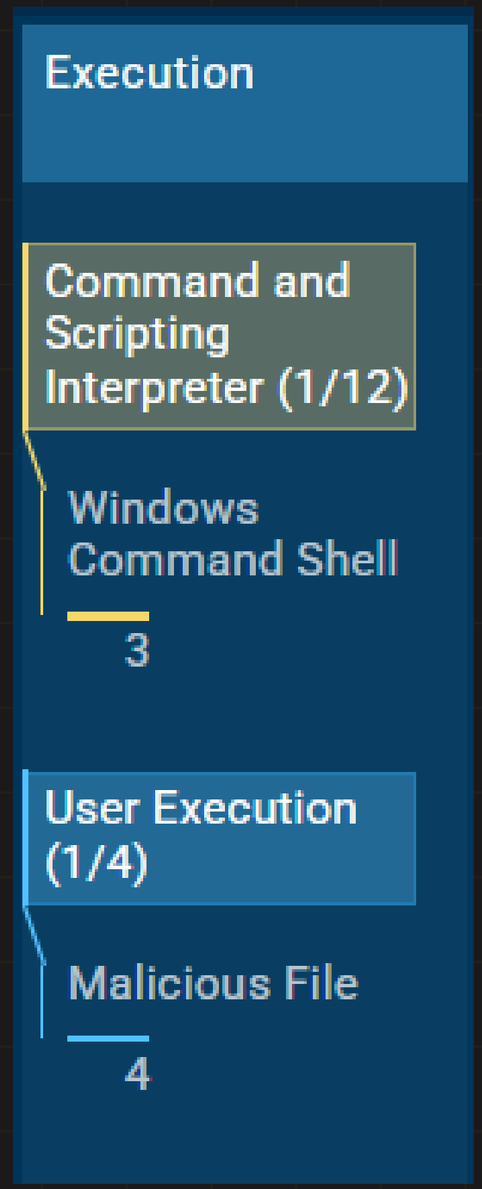


MATRIZ MITRE ATT&CK

TÁTICAS: EXECUÇÃO

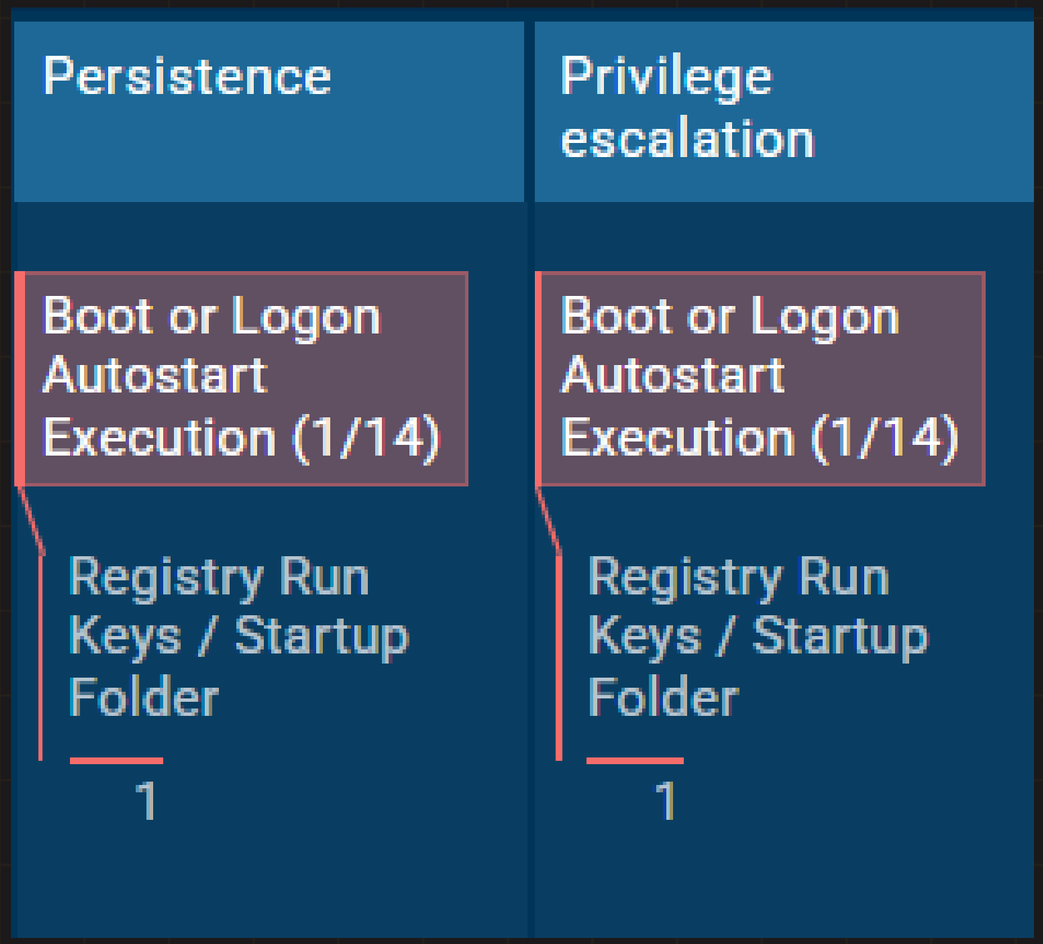
- **User Execution (Execução pelo Usuário):** um usuário foi enganado e clicou ou abriu o arquivo malicioso wireframe.exe.

- **Command and Scripting Interpreter (Intérprete de Comando):** Assim que foi executado, o malware usou o Prompt de Comando (cmd.exe), para executar seus scripts e comandos. É uma forma de se camuflar e parecer uma atividade normal do sistema.



TÁTICAS: PERSISTÊNCIA E ESCALAÇÃO DE PRIVILÉGIO

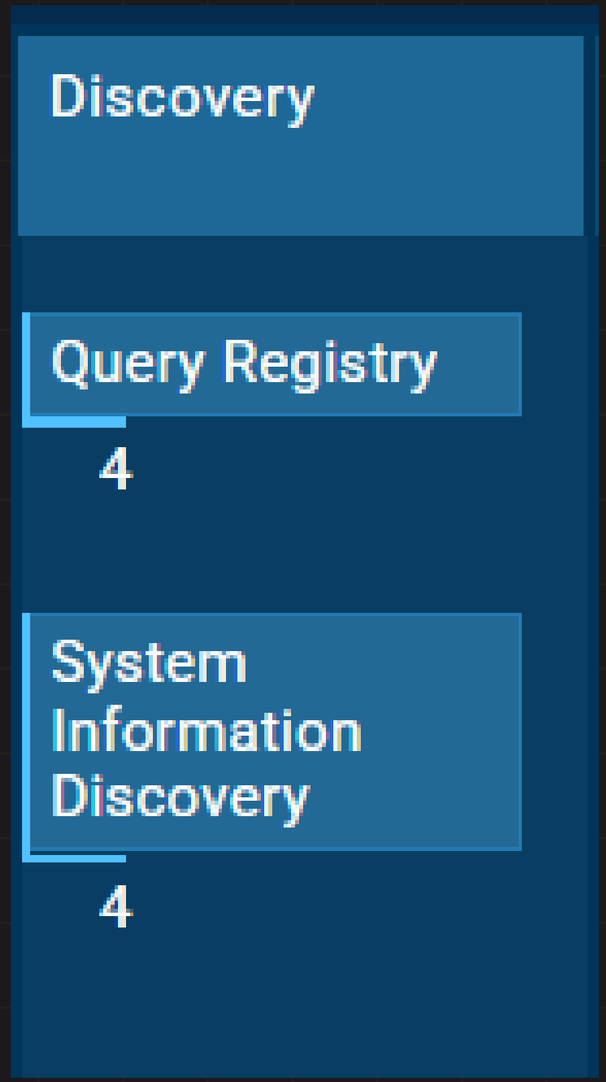
- **Boot or Logon Autostart Execution** (Execução Automática na Inicialização ou Logon).
- **Sub-técnica específica:** Registry Run Keys / Startup Folder (Chaves de Registro de Execução / Pasta de Inicialização).



TÁTICAS: DESCOBERTA

- **System Information Discovery (Descoberta de Informações do Sistema):** O malware coletou informações básicas sobre o computador: nome do usuário, versão do Windows, etc.

- **Query Registry (Consulta ao Registro):** Ele fez buscas no Registro do Windows. Ele pode estar procurando por softwares de segurança instalados, senhas salvas ou outras informações valiosas.



4. RESUMO DA ANÁLISE

PERFIL DA AMEAÇA

- **Tipo de Ameaça:** RAT (Remote Access Trojan) da família AsyncRAT.
- **Vetor de Entrada:** Tráfego de Rede (detectado pelo IPS).
- **Comportamento Principal:**
  - Usa ferramentas legítimas do sistema (cmd.exe) para se camuflar.
  - Cria persistência no sistema para sobreviver a reinicializações.
  - Tenta se comunicar com um servidor de Comando e Controle (C2) na internet.
- **Objetivo Provável:** Controle remoto total do sistema para espionagem, roubo de dados ou para servir como ponto de partida para ataques mais graves.

IMPACTO POTENCIAL E RECOMENDAÇÕES

Impacto Potencial para a Organização:

- Vazamento de dados sensíveis (credenciais de usuários, informações de clientes).
- Comprometimento de outros sistemas na rede.
- Porta de entrada para ataques de Ransomware.
- Perda financeira e dano à reputação.

IMPACTO POTENCIAL E RECOMENDAÇÕES

Recomendações (Plano de Ação):

- Isolar a(s) máquina(s) infectada(s) da rede.
- Bloquear o domínio/IP do servidor C2 no firewall.
- Bloquear o hash do wireframe.exe no antivírus/EDR da empresa.

Longo Prazo (Prevenção):

- Reforçar o treinamento de usuários contra phishing e downloads suspeitos.
- Monitorar o uso de ferramentas como cmd.exe e timeout.exe em estações de trabalho.

5. CONCLUSÃO

CONCLUSÃO

A análise forense demonstra na prática como um alerta de rede – um dado isolado – é transformado em inteligência acionável. O hash inicial mostra "o quê", mas a análise de comportamento revela "o como" e "o porquê" da ameaça. O processo expõe um RAT, cujo principal perigo não é o ataque imediato, mas sua capacidade de permanecer oculto no sistema. Isso reforça que a defesa não está em apenas bloquear ameaças, mas em entender a estratégia do atacante, e a metodologia forense é a ferramenta essencial para garantir que esses ataques não ocorram novamente.

OBRIGADO!