UNESPAR - APUCARANA

Trabalho 3º Bimestre - Redes e Sistemas Distribuídos
Professora: Lailla Bine

Computação Forense em Redes de Computadores

Guilherme Fortunato da Silva, Paloma de Castro Leite

08 de Outubro de 2025

1 Introdução

A segurança cibernética no Brasil enfrenta desafios principalmente em organizações, sejam elas públicas ou privadas, que são confrontadas diariamente com um volume massivo e uma sofisticação crescente de ciberataques. Ameaças como ransomware, que paralisam infraestruturas críticas, e Trojans de Acesso Remoto (RATs), projetados para a espionagem silenciosa e o roubo de dados financeiros e estratégicos, tornaram-se ocorrências comuns, exigindo uma evolução constante nas estratégias de defesa digital. Surge, portanto, a necessidade crítica de desenvolver e aplicar metodologias de análise forense robustas, capazes de investigar incidentes de rede a fundo para compreender a verdadeira natureza e o impacto de uma violação de segurança. O presente trabalho tem como objetivo demonstrar o processo metodológico da análise forense em redes de computadores, por meio de um estudo de caso prático. A investigação parte de um alerta de segurança gerado na rede, progride através da validação de Indicadores de Comprometimento (IOCs) e finaliza na análise comportamental e classificação detalhada de um artefato malicioso, ilustrando a jornada da detecção à inteligência acionável.

2 Computação Forense Digital

2.1 Conceito e Processo no Brasil

A computação forense surgiu em resposta à escalada de crimes cometidos pelo uso de sistemas computacionais, seja como objeto de crime, instrumento ou repositório de evidências. Dessa forma, a perícia forense digital foi definida como o uso de métodos cientificamente derivados e comprovados para a preservação, coleta, validação, identificação, análise, interpretação e apresentação de evidências digitais com o propósito de reconstruir eventos criminosos ou antecipar ações não autorizadas.

No Brasil, o processo forense, embora alinhado a padrões como a ISO/IEC 27037, tem sua validade jurídica vinculada ao Código de Processo Penal (CPP). A Lei nº 13.964/2019 (Pacote Anticrime) foi um marco ao inserir no CPP os artigos 158-A a 158-F, que regulamentam a **Cadeia de Custódia**. Legalmente, ela é o "conjunto de todos os procedimentos utilizados para manter e documentar a história cronológica do vestígio", garantindo sua **integridade, autenticidade e rastreabilidade**.

O Art. 158-B do CPP detalha as etapas formais da Cadeia de Custódia, aplicáveis tanto a vestígios físicos quanto digitais. O processo inicia-se com o **Reconhecimento** da fonte de evidência, seguido pelo **Isolamento** para evitar alteração (ex: uso de bloqueadores de escrita). A **Fixação** descreve detalhadamente o vestígio, enquanto a **Coleta** envolve a criação de uma imagem forense (cópia bit a bit). O material é então acondicionado em embalagens adequadas (**Acondicionamento**), seguido pelo **Transporte** e **Recebimento** formais. A análise pericial (**Processamento**) é realizada sobre a cópia, e o material original é mantido em **Armazenamento** seguro até seu eventual **Descarte**. A falha em documentar qualquer uma dessas etapas pode levar à inadmissibilidade da prova em um processo judicial.

3 As Fases do Processo Forense Digital

O processo técnico da análise forense é dividido em quatro fases sequenciais, sempre seguindo a Cadeia de Custódia para garantir a validade jurídica das evidências.

3.1 Coleta e Preservação (Identificação e Aquisição)

Esta fase é crítica para não comprometer a investigação. O objetivo é adquirir uma cópia exata da evidência sem alterar a fonte original. Envolve a **Identificação e Isolamento** das fontes de dados (HDs, servidores, logs), a **Aquisição Forense** através da criação de uma imagem bit a bit com o uso de bloqueadores de escrita (*write-blockers*), e a **Verificação de Integridade**, onde um cálculo de hash (como SHA-256) é realizado no original e na cópia. Os hashes devem ser idênticos, provando matematicamente a integridade da cópia.

3.2 Exame

Trabalhando exclusivamente sobre a cópia forense, esta fase processa os dados brutos para revelar informações ocultas. Os procedimentos incluem a **Recuperação de Dados** deletados, a **Extração de Artefatos** do sistema (como registros, históricos e metadados) e a **Indexação** de toda a massa de dados para permitir buscas rápidas e eficientes.

3.3 Análise

Nesta fase investigativa, o perito interpreta os dados para construir linhas do tempo, correlacionar eventos e responder aos quesitos da perícia. O analista **constrói linhas do tempo** com base nos metadados de tempo (MAC times), **correlaciona evidências** de diferentes fontes, **busca por padrões** de atividade maliciosa e **formula e testa hipóteses** para chegar a uma conclusão tecnicamente fundamentada.

3.4 Laudo Pericial (Relatório)

A fase final é a comunicação dos resultados em um Laudo Pericial. O documento deve ser **objetivo e imparcial**, baseado estritamente nas evidências; **tecnicamente fundamentado**, com cada conclusão suportada por dados; e **reprodutível**, permitindo que outro perito possa seguir a mesma metodologia e alcançar os mesmos resultados.

4 Metodologia e Ferramentas

A metodologia deste estudo de caso simula o fluxo de trabalho de uma equipe de resposta a incidentes, progredindo da detecção à inteligência acionável. O fluxo investigativo seguiu quatro etapas: **1) Detecção do Incidente**, iniciada por um alerta de um Sistema de Prevenção de Intrusão (IPS); **2) Coleta e Validação do IOC**, verificando o hash do arquivo suspeito em bases de conhecimento; **3) Análise Comportamental Dinâmica**, executando o artefato em um ambiente seguro (sandbox) para registrar suas interações; e **4) Classificação da Ameaça**, mapeando o comportamento observado no framework MITRE ATT&CK para identificar as Táticas, Técnicas e Procedimentos (TTPs) do adversário.

Para isso, foram utilizadas as seguintes ferramentas: um **Sistema de Prevenção de Intrusão (IPS)** como sensor de rede; a plataforma **ANY.RUN** como ambiente de sandbox para a análise dinâmica; e o **Framework MITRE ATT&CK** como base de conhecimento para a classificação da ameaça.

5 Estudo de Caso: Análise do Artefato

5.1 Validação do Hash e Análise da Execução

A investigação partiu do hash MD5 `2F3D3624E271EC70B49CE56BF3B8F563B`, obtido de um alerta do IPS. A consulta na plataforma ANY.RUN retornou um veredito imediato de "Atividade Maliciosa"para o arquivo `wireframe.exe`, validando a ameaça.

Ao ser executado no sandbox, o `wireframe.exe` iniciou um processo `cmd.exe` para rodar um script em lote (`.bat`), uma tática de "Living off the Land". Simultaneamente, abriu um documento RTF com o `WINWORD.EXE` como isca para o usuário. Para evasão, invocou o `timeout.exe`, atrasando sua execução para contornar sandboxes automatizadas. A ação mais notável foi a criação e execução de `nvidiagpu.exe`, uma tentativa de mascarar o processo malicioso como um componente de driver de vídeo legítimo da NVIDIA.

5.2 Análise de Rede e Perfil da Ameaça

A análise de rede registrou requisições DNS para `google.com` (teste de conectividade) e, crucialmente, para o domínio malicioso `tasteless-minister.auto.playit.gg`. Essa atividade de "phone home"é a marca de um Trojan de Acesso Remoto (RAT). Conclui-se que o `wireframe.exe` é um RAT da família AsyncRAT, cujo objetivo é obter controle remoto e persistência no sistema da vítima usando táticas de engano, evasão e mascaramento.

5.3 Classificação MITRE ATT&CK

O mapeamento do comportamento do malware no framework MITRE ATT&CK permitiu a classificação de suas ações em quatro táticas principais: **Execução, Persistência, Escalação de Privilégio** e **Descoberta**. Essa classificação é fundamental para entender a estratégia do adversário de forma padronizada.

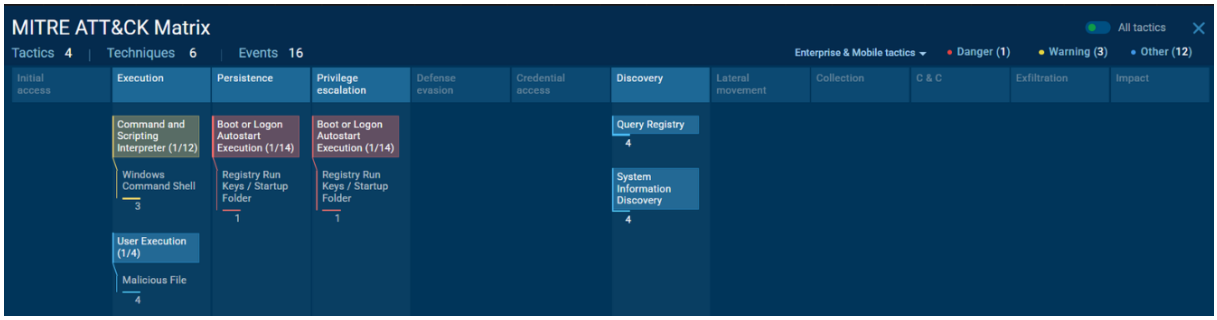

Figura 1: Mapeamento do comportamento do `wireframe.exe` na Matriz MITRE ATT&CK.

Dentre as técnicas observadas, a mais crítica e perigosa foi a de **"Boot or Logon Autostart Execution"(T1547.001)**, dentro da tática de **Persistência**. Essa técnica, que consiste em modificar chaves de registro para garantir que o malware seja executado a cada inicialização do sistema, representa o pilar da estratégia do atacante. Ela transforma uma infecção temporária em uma violação permanente e de difícil remediação, permitindo ao adversário manter o acesso ao sistema indefinidamente, mesmo após reinicializações, para realizar espionagem ou escalar o ataque no futuro.

6 Recomendações

Com base na análise, recomenda-se um plano de ação em três fases. Primeiramente, a **Contenção** imediata, bloqueando os IOCs descobertos (o hash `2F3D3624...` no EDR e o domínio `tasteless-minister...` no firewall/DNS). Em seguida, a **Remediação**, que envolve isolar o sistema infectado e, idealmente, formatá-lo e restaurar os dados de um backup limpo. Por fim, a **Prevenção** futura, que inclui reforçar o monitoramento de processos legítimos do sistema (*security hardening*) e investir em treinamento contínuo de usuários para identificar phishing e táticas de engenharia social, o vetor de entrada mais comum para este tipo de ameaça.

7 Conclusão

Este estudo de caso demonstrou que a aplicação de uma metodologia forense sistemática é crucial para converter dados brutos de segurança em conhecimento estratégico. A investigação avança na identificação de um Indicador de Comprometimento (IOC), aprofundando-se na análise comportamental para desvendar as Táticas, Técnicas e Procedimentos (TTPs) de um Trojan de Acesso Remoto (RAT). O principal achado foi a implementação de mecanismos de persistência pelo malware, uma ameaça muito mais significativa do que o evento de infecção isolado. Conclui-se que a resiliência cibernética não se constrói apenas com a defesa de perímetro, mas com a capacidade de dissecar a estratégia do atacante, para a qual a análise forense se apresenta como disciplina fundamental.

Referências

SUPERIOR TRIBUNAL DE JUSTIÇA (STJ). **A cadeia de custódia no processo penal: do Pacote Anticrime à jurisprudência do STJ**. 2023. Disponível em: `https://www.stj.jus.br/sites/portalp/Paginas/Comunicacao/Noticias/2023/23042023-A-cadeia-de-custodia-no-processo-penal-do-Pacote-Anticrime-a-jurisprudencia.aspx`. Acesso em: out. 2025.

ACADEMIA DE FORENSE DIGITAL. **Computação Forense: o que é e para que serve?**. Disponível em: `https://academiadeforensedigital.com.br/computacao-forense-o-que-e-e-para-que-serve`. Acesso em: out. 2025.

IBM. **O que é computação forense?**. Disponível em: `https://www.ibm.com/br-pt/think/topics/computer-forensics`. Acesso em: out. 2025.

PROOFPOINT. **O que é Forense Digital?**. Disponível em: `https://www.proofpoint.com/us/threat-reference/digital-forensics`. Acesso em: out. 2025.

AMERICAN PUBLIC UNIVERSITY. **O que é Forense Digital?**. Disponível em: `https://www.apu.apus.edu/area-of-study/information-technology/resources/what-is-digital-forensics/`. Acesso em: out. 2025.

AGARWAL, R. K.; VYAS, O. P.; GUPTA, M. L. **Systematic Digital Forensic Investigation Model**. International Journal of Computer Science and Security (IJCSS), v. 3, n. 6, p. 498-510, 2009. Disponível em: `https://www.researchgate.net/profile/Yatendra-Gupta/publication/228410430_Systematic_`

Digital_Forensic_Investigation_Model/links/56ea8cd208ae95bddc2bcc6b/Systematic-Digital-Forensic-Investigation-Model.pdf. Acesso em: out. 2025.