ANÁLISE DA EVOLUÇÃO E DO COMPORTAMENTO DE CÓDIGOS MALICIOSOS DO TIPO *TROJAN*

Caio Garcia (PIC/CNPq/UEM), Luciana Andréia Fondazzi Martimiano (Orientadora).
E-mail: lafmartimiano@uem.br

Universidade Estadual de Maringá, Centro de Tecnologia, Maringá, PR.

Área e subárea do conhecimento: Ciência da Computação, Metodologia e Técnicas da Computação

Palavras-chave: Códigos Maliciosos; *Malwares*; Segurança; *Trojans*.

RESUMO

Códigos maliciosos, ou *malwares*, são programas que podem ser utilizados para que indivíduos mal-intencionados realizem ataques com o intuito de comprometer pessoas e sistemas, obtendo vantagens financeiras ou acessando dados pessoais e sensíveis indevidamente. Os códigos do tipo *Trojan*, ou cavalo de troia, são programas que, além de executarem as funções para as quais foram aparentemente projetados, também executam outras funções, normalmente maliciosas, sem o conhecimento do usuário. Eles têm sido usados em grande escala para a realização de ataques, inclusive para implantação e disseminação de outros tipos de códigos maliciosos, como *ransomwares* e *worms*. Entender como eles evoluem, como funcionam e como podem comprometer um ambiente computacional é importante para definir estratégias de proteção, tornando o ambiente mais seguro. Nesse contexto, este projeto tem como objetivo principal realizar a análise da evolução e do comportamento de códigos maliciosos do tipo *Trojan*, procurando entender seus impactos na segurança dos ambientes computacionais.

INTRODUÇÃO

O cenário da cibercriminalidade tem crescido, representando uma ameaça constante para pessoas e organizações. Segundo dados do CERT.br (Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil) sobre incidentes de segurança no Brasil, houve um total de 2.901.506 notificações entre 2021 e julho de 2026 (https://stats.cert.br/incidentes/). Dentre os diversos tipos de incidentes de segurança descritos pelo CERT.br, aqueles que usam os códigos maliciosos, ou *malwares*, têm se destacado.

Segundo dados do relatório do FortiGuard Labs (2026), o Brasil registrou 753,8 bilhões de tentativas de ataques cibernéticos em 2025. O relatório ainda revela que parte dos ataques usaram algum tipo de código malicioso, principalmente *ransomwares* e *trojans*. Este cenário crescente do uso dos códigos maliciosos faz com que a análise do seu comportamento seja uma área de pesquisa crucial para

compreender a natureza dos ataques, identificar pontos de entrada, entender os impactos, contribuir para a elucidação de crimes cibernéticos e mitigar ataques.

MATERIAIS E MÉTODOS

O estudo foi desenvolvido por meio de uma pesquisa bibliográfica para construir uma linha do tempo sobre *trojans*, a fim de avaliar sua evolução, partindo de sua origem como conceito em 1972 (ADMONI, 2025) até a década de 2020. Além disso, para entender a natureza desse tipo de *malware*, foi necessário realizar a análise estática, consistindo da avaliação de *strings* e chamadas de funções presentes em códigos maliciosos (BERRUETA et al., 2019), e a análise dinâmica, baseada em analisar o código em execução, monitorando-o por meio de emuladores, *debuggers*, ferramentas de processos, registros, arquivos e *tracers* de chamada de sistema, com execução do código em ambiente controlado e protegido (AL-RIMY; MAAROF; SHAID, 2018).

Neste projeto, a fim de tornar viável a prática das análises estática e dinâmica em ambiente controlado, foi usado um computador com sistema operacional *Kali Linux* para reduzir o consumo padrão de memória principal; a máquina virtual (VM) *Oracle VirtualBox* com sistema operacional *Windows 7* para execução do *trojan* escolhido; a ferramenta *PeStudio* para a análise estática; *Process Monitor*, *Process Hacker, FakeNet-NG, RegsitryChangeView* e *WireShark* para a análise dinâmica, visando realizar a análise de atividade de rede, processos, registros e arquivos. O objeto de estudo foi uma variante do *Zeus*, um *trojan* bancário elaborado em 2007[1].

Com o intuito de utilizar todas as ferramentas disponíveis para a análise estática, a máquina virtual ainda estava com acesso a rede para permitir que o *PeStudio* pudesse fazer uso do *VirusTotal*, um serviço gratuito *online* responsável por inspecionar arquivos e *sites* suspeitos. Adiante, com a finalidade de realizar a análise dinâmica, isolou-se a rede da máquina para evitar que o *trojan* se espalhasse para outros computadores. O protocolo IPv4 do sistema *Windows* instalado também foi modificado, permitindo que o *FakeNet-NG* pudesse simular uma rede.

RESULTADOS E DISCUSSÃO

Em relação à linha do tempo desenvolvida, foi possível identificar, além de observar uma evolução técnica dos *trojans*, como métodos de infecção, espionagem e ataque, quais tendências e tecnologias de cada época esses códigos conseguiam se aproveitar, como protocolos de rede, limitações de sistemas operacionais e *software* de segurança, e nível de conhecimento computacional da população.

Considerando a análise estática do *Zeus*, por meio da Figura 1, pode-se verificar algumas importações de funcionalidades do *Windows* utilizadas pelo executável, as quais foram sinalizadas como suspeitas pelo *PeStudio*, sendo elas

[1] Amostra da variante do malware obtida no projeto theZoo, via GitHub. Disponível em: https://github.com/ytisf/theZoo. Acesso em: 27 ago. 2026.

respectivamente: *VirtualQueryEx*; *WriteFile*; *WinExec* e *GetClipboardOwner*. Dentre estas importações citadas, se destaca a *GetClipboardOwner*, usada para verificar qual janela possui a área de transferência mais recente, indicando o caráter de espionagem do código malicioso.

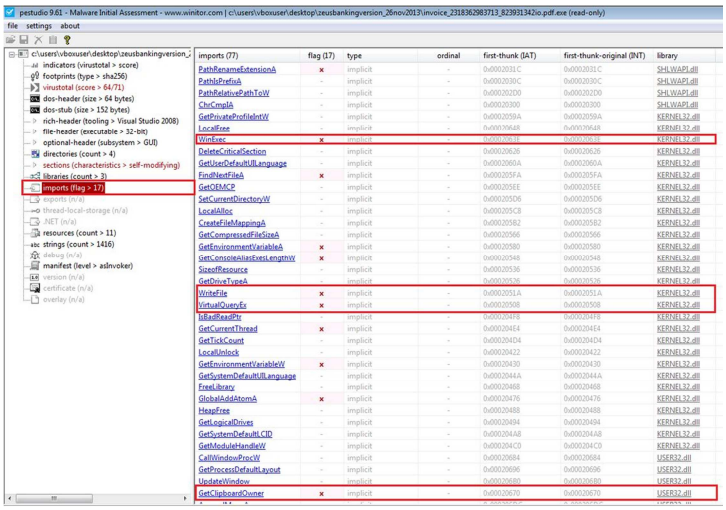


Figura 1 - Tabela de importações do *Zeus*

Considerando a análise dinâmica, a Figura 2 mostra as ações em arquivos e em registros capturadas pelo *Process Monitor*. Tais ações indicam a tentativa do *trojan*, identificado como *"zeus.exe"*, de garantir sua persistência no sistema após reinicialização da máquina, como a criação, escrita e fechamento de um mesmo arquivo (*Create, Write* e *CloseFile*) e operações denominadas *RegSetValue*, associadas ao salvamento de dados no sistema.

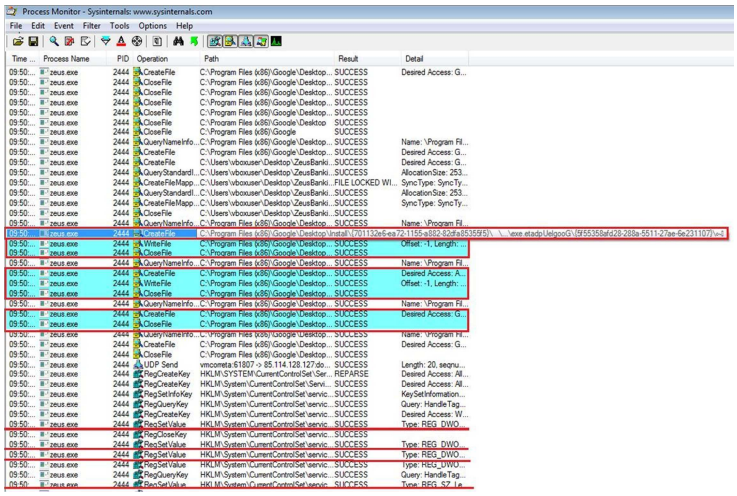


Figura 2 - Ações em arquivos e registros efetuadas pelo *Zeus*

CONCLUSÕES

Este trabalho envolveu uma investigação dos principais *trojans* criados, durante seu período conceitual ao período atual, além da execução de duas das principais análises em códigos maliciosos. Os resultados indicam alguns comportamentos fundamentais de *trojans* no funcionamento da amostra do *Zeus* e em outros programas dessa família. As principais contribuições deste estudo foram a criação e a análise da evolução dos *trojans* e as tecnologias usadas por estes *malwares*, majoritariamente em nível de redes e de sistemas operacionais, e a execução das análises estática e dinâmica em uma amostra de um *trojan*, com uso de ferramentas que permitem o estudo de atributos e ações de *malwares* no geral.

REFERÊNCIAS

ADMONI, A. "A horse with no name": the role of Trojan horse in cyber warfare during its' first decade (1972-1983). **HISTORICAL: Journal of History and Social Sciences**, [S. l.], v. 4, n. 3, p. 293-306, set. 2025. Disponível em: https://doi.org/10.58355/historical.v4i3.197. Acesso em: 2 fev. 2026.

AL-RIMY, B. A. S.; MAAROF, M. A.; SHAID, S. Z. M. Ransomware threat success factors, taxonomy, and countermeasures: a survey and research directions. **Computer & Security**, [S. l.], v. 74, p. 144-166, 2018. Disponível em: https://doi.org/10.1016/j.cose.2018.01.001.

BERRUETA, E.; MORATO, D.; MAGAÑA, E.; IZAL, M. A survey on detection techniques for cryptographic ransomware. **IEEE Access**, [S. l.], v. 7, p. 144925-144944, 2019. DOI: https://doi.org/10.1109/ACCESS.2019.2945839.

CERT.BR. **Cartilha de segurança para internet**: fascículo códigos maliciosos. São Paulo: CERT.br, [s. d.]. Disponível em: https://cartilha.cert.br/fasciculos/#codigos-maliciosos. Acesso em: maio 2025.

FORTIGUARD LABS. **Global threat landscape report**. [S. l.]: Fortinet, 2026. Disponível em: https://www.fortinet.com/library/soc-dgt/global-threat-landscape-report. Acesso em: 24 ago. 2026.