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

Fabricio Raposo da Silva Bonifacio (PIBIC/CNPq/FA/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: Ciências Exatas e da Terra/Ciência da Computação.

Palavras-chave: *ransomware*; análise de *malware*; segurança da informação.

RESUMO

O *ransomware* consolidou-se como a ameaça cibernética mais destrutiva e lucrativa da última década, exigindo estudos que contemplem simultaneamente sua dimensão histórica, técnica e comportamental. Este trabalho analisou a evolução e o comportamento de códigos maliciosos do tipo *ransomware*, combinando pesquisa bibliográfica sobre a trajetória, os impactos econômicos e os principais grupos operadores, com análise experimental de amostras representativas de diferentes gerações. A metodologia empregou ambiente virtual isolado, sobre o qual foram submetidas às análises estática e dinâmica as amostras AIDS Trojan, CryptoLocker e LockBit 4.0. Os resultados evidenciaram o salto evolutivo da ameaça, desde a intimidação psicológica do AIDS Trojan, passando pela criptografia e persistência via Registro do CryptoLocker, até as sofisticadas técnicas de evasão e a dupla extorsão do LockBit 4.0. Conclui-se que o monitoramento contínuo das táticas, técnicas e procedimentos desses grupos é indispensável para a prospecção de defesas adequadas.

INTRODUÇÃO

A digitalização de processos, dados e comunicações expôs indivíduos e organizações a riscos cibernéticos cada vez mais sofisticados, no âmbito dos quais o *ransomware* se mantém no núcleo operacional das ameaças (ENISA, 2024). Trata-se de um código malicioso que sequestra dados ou sistemas inteiros, geralmente por meio de criptografia forte, exigindo um resgate para a restauração do acesso. Os danos globais associados à ameaça saltaram de US$ 325 milhões em 2015 para estimativas superiores a US$ 265 bilhões até 2031 (CYBERSECURITY VENTURES, 2021), enquanto os pagamentos de resgate confirmados em criptomoedas alcançaram o recorde histórico de mais de US$ 1,1 bilhão em 2023 (CHAINALYSIS, 2024).

Essa trajetória é marcada por uma rápida e constante evolução: conforme detalhado por Oz et al. (2022), a progressão partiu de ataques oportunistas e rudimentares

para modelos de negócio complexos e profissionais, impulsionados pela popularização do *Ransomware-as-a-Service* (RaaS) e pela adoção da dupla extorsão, em que os atacantes exfiltram os dados e ameaçam divulgá-los publicamente. Diante desse cenário, este trabalho se propôs a analisar a evolução e o comportamento de códigos maliciosos do tipo ransomware, por meio de uma pesquisa teórico-bibliográfica sobre a trajetória, os impactos e os principais grupos operadores, e a realizar uma pesquisa experimental de análise estática e dinâmica de amostras representativas de diferentes gerações.

MATERIAIS E MÉTODOS

A metodologia foi estruturada em duas frentes. A primeira consiste em uma pesquisa teórica, documental e bibliográfica, voltada a traçar o progresso histórico, técnico e econômico dos ataques de ransomware, abrangendo conceitos de segurança da informação, criptografia, evolução da ameaça e os principais grupos operadores. A segunda frente é uma pesquisa prática e experimental, realizada de forma conteinerizada em máquinas virtuais para garantir o isolamento e a segurança necessários à experimentação de códigos maliciosos, sem expor a infraestrutura física.

O ambiente computacional de contenção baseia-se no ecossistema Linux, com as distribuições Kali Linux e REMnux executadas no Oracle VirtualBox, interligadas por uma rede no modo *host-only* e complementadas pelo utilitário INetSim, que fornece serviços falsos de DNS e HTTP para simular a conectividade de forma controlada. As amostras selecionadas foram o AIDS Trojan, o CryptoLocker e o LockBit 4.0, escolhidas por suas relevâncias na linha do tempo evolutiva. Sobre essas amostras foram aplicadas técnicas de análise estática, com as ferramentas file, sha256sum, strings, rabin2, FLOSS e Ghidra, e de análise dinâmica, com o Process Monitor e o Wireshark, em *sandbox*, para extrair indicadores de comprometimento e mapear o comportamento em tempo de execução.

RESULTADOS E DISCUSSÃO

A análise do AIDS Trojan revelou um executável de 16 bits para MS-DOS, desprovido de empacotamento ou ofuscação, cujas *strings* expõem diretamente o propósito extorsivo, confirmando que as estratégias iniciais de extorsão baseavam-se na intimidação psicológica e na alteração do AUTOEXEC.BAT, em vez da criptografia robusta. O CryptoLocker representou o ponto de virada histórico: a biblioteca advapi32.dll indicou o uso malicioso da Microsoft CryptoAPI para gerar chaves, enquanto a kernel32.dll evidenciou a varredura e reescrita em disco com *multithreading* (*CreateThread*), e a manipulação do Registro (HKCU) assegurou a persistência. Na análise dinâmica, o Wireshark identificou tentativas persistentes de comunicação com um servidor de Comando e Controle (C2), com requisições TCP [SYN] ao IP público 184.164.136.134:80 seguidas de retransmissões pelo isolamento da rede *host-only*. Contudo, a amostra não criptografou arquivos em um

Windows 10 atualizado, possivelmente por anti-análise ou incompatibilidade de arquitetura.

O LockBit 4.0 mostrou o estado da arte das operações de RaaS. A análise estática revelou empacotamento de aproximadamente 90% e alta entropia, com ofuscação por API *Hashing* contornada pelo FLOSS, que evidenciou a descarga de carga em %SystemRoot%\Temp e a elevação furtiva de privilégios via UAC *Bypass* (interface CMSTPLUA), além da destruição de cópias de sombra por WMI (SELECT * FROM Win32_ShadowCopy). Na análise dinâmica, o *ransomware* criptografou os arquivos (extensão .QAJXKFWok), modificou o papel de parede e deixou nota de resgate confirmando a dupla extorsão, com ameaça de vazamento via .onion. O monitoramento de desempenho revelou esgotamento do disco (100% de atividade, gravação superior a 500 MB/s) por um processo temporário ofuscado (F9A2.tmp), tática de evasão por injeção em processos disfarçados. Observou-se que arquivos .bin grandes (250MB, 512MB e 1GB) permaneceram intactos, evidenciando algoritmos de filtragem e otimização de tempo, provavelmente baseados em listas de exclusão ou limite de tamanho, priorizando a criptografia rápida de dados críticos antes da intervenção de defesas.

A Tabela 1 sintetiza as características principais das três amostras analisadas, evidenciando o salto evolutivo da ameaça ao longo das gerações.

Tabela 1: Síntese comparativa das amostras de *ransomware* analisadas

Característica	AIDS Trojan	CryptoLocker	LockBit 4.0
Aparição	1989	2013	2024
Arquitetura	16 bits (MS-DOS COM)	32 bits (PE/Windows)	64 bits (PE/Windows)
Ofuscação/Empacotamento	Ausente	~68%	~90% (alta entropia)
Criptografia	Ausente	Microsoft CryptoAPI	ChaCha20/RSA /Curva Elíptica
Persistência	AUTOEXEC.BAT	Registro (HKCU)	Temp + UAC Bypass
Anti-análise	Nenhuma	Limitada	API Hashing, packing
Tática de extorsão	Intimidação psicológica	Criptografia + resgate	Dupla extorsão

CONCLUSÕES

A dissecação das três amostras evidenciou o salto evolutivo do *ransomware*: de um código rudimentar de 16 bits, baseado em intimidação psicológica e alteração do AUTOEXEC.BAT (AIDS Trojan), passou-se à adoção de criptografia robusta,

persistência via Registro e multithreading (CryptoLocker), até alcançar o estado da arte em evasão e destruição, com empacotamento denso, UAC *Bypass*, remoção de cópias de sombra via WMI e dupla extorsão (LockBit 4.0). O ambiente virtual isolado, composto por Kali Linux, REMnux, VirtualBox e INetSim mostrou-se eficaz e seguro para dissecar os artefatos sem expor a infraestrutura física.

Conclui-se que o monitoramento contínuo das táticas, técnicas e procedimentos (TTPs) adotados pelos grupos criminosos é indispensável para a prospecção de defesas adequadas. Como trabalhos futuros, apontam-se o aprofundamento da engenharia reversa para isolar algoritmos criptográficos em *Assembly*, a elaboração de regras de detecção automatizadas (YARA e Sigma) baseadas em indicadores de comprometimento e padrões de chamadas de sistema, e a expansão do laboratório para incluir *ransomwares* voltados a servidores Linux e hipervisores VMware ESXi.

AGRADECIMENTOS

À Universidade Estadual de Maringá (UEM) pelo financiamento da bolsa de Iniciação Científica (PIBIC), e à orientadora Luciana Andréia Fondazzi Martimiano pelo apoio.

REFERÊNCIAS

CHAINALYSIS. **The 2024 Crypto Crime Report. New York**: Chainalysis, 2024. Disponível em: https://go.chainalysis.com/crypto-crime-2024.html.

CYBERSECURITY VENTURES. **Global Ransomware Damage Costs Predicted To Exceed $275 Billion By 2031.** Cybercrime Magazine, 2 abr. 2025. Disponível em: https://cybersecurityventures.com/global-ransomware-damage-costs-predicted-to-reach-250-billion-usd-by-2031/.

ENISA. **ENISA Threat Landscape 2024-2025.** Atenas: European Union Agency for Cybersecurity, 2024. Disponível em: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2025.

OZ, H. et al. **A Survey on Ransomware: Evolution, Taxonomy, and Defense Solutions.** ACM Computing Surveys, v. 54, n. 11s, p. 1-37, 2022.