ANÁLISE DE DISPOSITIVOS INFECTADOS POR CÓDIGOS MALICIOSOS (MALWARES)

Fernando Brito Campideli (PIC), Luciana Andréia Fondazzi Martimiano. E-mail: lafmartimiano@uem.br.

Universidade Estadual de Maringá, Centro de Ciências Exatas e da Terra, Maringá, PR.

Informática/Engenharia de Software

Palavras-chave: Análise Estática; Análise Dinâmica; Engenharia Reversa.

RESUMO

A crescente sofisticação dos códigos maliciosos (*malwares*) exige uma análise aprofundada para o desenvolvimento de defesas eficazes. Este trabalho apresenta um estudo comparativo de duas amostras de *malware* distintas, Maldal e Annabelle, utilizando uma abordagem combinada de análise estática e dinâmica em um ambiente de *sandbox*. A análise estática, com ferramentas como Detect It Easy e Ghidra, permitiu a identificação da arquitetura e das tecnologias de cada amostra, revelando que o Maldal era um executável não ofuscado em Visual Basic 6, enquanto o Annabelle era uma aplicação .NET protegida por múltiplas camadas de ofuscação. A análise dinâmica, utilizando dnSpy, Process Hacker e Process Monitor, foi essencial para observar o comportamento real e contornar proteções. Os resultados levaram à reclassificação do Maldal de *ransomware* para um *malware* não persistente com payload de Negação de Serviço (DoS) e funcionalidades de *Spyware*. Para o Annabelle, foi possível mapear sua cadeia de infecção completa, confirmando seu mecanismo de persistência via Registro do Windows e suas agressivas rotinas de autodefesa, como o sequestro de executáveis do sistema (IFEO), que resultam na ativação de seu *payload* de *screen locker*. A combinação de ambas as análises é fundamental para a correta classificação e compreensão das ameaças, uma vez que o comportamento dinâmico pode divergir significativamente das características observadas estaticamente.

INTRODUÇÃO

O cenário da cibercriminalidade tem crescido rapidamente, com os malwares se destacando como um dos principais instrumentos para a exploração de

vulnerabilidades em sistemas computacionais. A análise do comportamento desses códigos tornou-se uma área de pesquisa crucial para compreender a natureza dos ataques, identificar seus impactos e desenvolver estratégias de mitigação. Neste contexto, a análise estática examina o código sem executá-lo, enquanto a análise dinâmica observa o comportamento em tempo real dentro de um ambiente controlado. Este trabalho teve como objetivo aplicar ambas as metodologias para realizar uma análise aprofundada de duas amostras de malware, a fim de validar suas funcionalidades, compreender seus mecanismos de ataque e compará-los. As amostras selecionadas, Maldal e Annabelle, representam dois paradigmas distintos: um malware mais antigo e não ofuscado (KASPERSKY, 2021) e um ransomware moderno e protegido (PC RISK, 2024).

MATERIAIS E MÉTODOS

A pesquisa foi conduzida em um ambiente de análise isolado (sandbox), configurado com o software de virtualização Oracle VirtualBox. As amostras de malware, Maldal e Annabelle, foram obtidas de um repositório público no GitHub (https://github.com/Cybersight-Security/Malware-Samples/).

A análise estática foi iniciada com a ferramenta Detect It Easy (DIE) para a identificação da arquitetura, tecnologia e presença de ofuscadores em cada amostra. Para aprofundar a análise do Maldal, foi utilizada a ferramenta de engenharia reversa Ghidra para descompilar seu código e examinar sua lógica interna (MENTE BINÁRIA, 2024).

Para a análise dinâmica, foi utilizado um conjunto de ferramentas complementares. A ferramenta dnSpy foi empregada na análise interativa do Annabelle, permitindo a depuração e a edição de instruções IL (patching) para neutralizar suas rotinas anti-debug .

O Process Hacker foi utilizado para a inspeção em tempo real de ambos os processos, permitindo a análise de memória e a suspensão controlada da execução. Por fim, o Process Monitor (ProcMon) foi a principal ferramenta para registrar todas as interações das amostras com o sistema de arquivos e o Registro do Windows, fornecendo evidências forenses de seus comportamentos (MENTE BINÁRIA, 2024). A transferência segura dos logs foi garantida pela configuração de uma Pasta Compartilhada entre a máquina virtual e a hospedeira.

RESULTADOS E DISCUSSÃO

A investigação combinada revelou a verdadeira natureza de cada amostra, destacando a importância da análise dinâmica.

Para o Maldal, a análise dinâmica contradisse a classificação inicial de ransomware. Seu payload principal observado foi um ataque de Negação de Serviço (DoS) por exaustão de recursos, evidenciado pela execução de mais de 209.000 operações CreateFile para sobrecarregar a área de trabalho do usuário. A

funcionalidade de Spyware foi confirmada pela coleta ativa de dados do sistema e do usuário (KASPERSKY, 2021). Foi constatada a ausência de um mecanismo de persistência, classificando-o como um malware de execução única. As mensagens de Adware (*malware* projetado para exibir anúncios indesejados) encontradas na análise estática nunca foram exibidas, indicando que este código era não funcional ou uma herança de outra versão.

Para o Annabelle, a análise dinâmica confirmou seu comportamento como um ransomware do tipo screen locker. Após contornar sua proteção anti-debug, foi possível mapear sua cadeia de infecção: o malware estabelece persistência criando um valor na chave de registro HKCU\Software\Microsoft\Windows\CurrentVersion\Run; em seguida, executa rotinas agressivas de autodefesa, desabilitando ferramentas como o Gerenciador de Tarefas e utilizando a técnica de sequestro de executáveis via IFEO (Image File Execution Options) para impedir a execução de dezenas de aplicações de sistema e segurança; por fim, o código força um reinício do sistema para ativar sua tela de bloqueio, que exibe a nota de resgate e impede o acesso ao sistema (PC RISK, 2024).

CONCLUSÕES

Este trabalho mostrou a eficácia da aplicação combinada de técnicas de análises estática e dinâmica para a correta identificação e compreensão do comportamento de códigos maliciosos. A investigação das amostras Maldal e Annabelle provou que as características observadas no código estático podem ser incompletas, ressaltando a análise dinâmica como uma etapa indispensável para a validação de hipóteses e a descoberta do verdadeiro payload de uma ameaça. Os resultados permitiram reclassificar o Maldal como um malware não persistente de DoS e Spyware e detalhar a sofisticada cadeia de infecção e as táticas de autodefesa do ransomware Annabelle. Conclui-se que a combinação de diferentes metodologias de análise é essencial para um entendimento completo do funcionamento de um malware, contribuindo para o desenvolvimento de defesas mais eficazes.

REFERÊNCIAS

MENTE BINÁRIA. ***Engenharia Reversa: Ferramentas. 2024.*** *Disponível em: https://mentebinaria.gitbook.io/engenharia-reversa/apendices/ferramentas. Acesso em: 22/04/2025.*

KASPERSKY. ***Threat Encyclopedia: Email-Worm.Win32.Maldal.*** *Disponível em: https://threats.kaspersky.com/br/threat/Email-Worm.Win32.Maldal/. Acesso em: 15/07/2025.*

PC RISK. ***Como remover o ransomware Annabelle.*** *Disponível em: https://www.pcrisk.pt/guias-de-remocao/11599-annabelle-ransomware. Acesso em: 15/07/2025.*