

Sobrescrita de MBR e MFT: Uma Revisão Bibliográfica sobre o Vetor de Sabotagem do Malware NotPetya

Léo Walker da Silva¹, Mayza Umbelina Fidelis da Silva¹, Melissa Behrends Rodrigues¹

¹Faculdade de Ciências Exatas e Tecnológicas (FACET) – Universidade do Estado do Mato Grosso (UNEMAT). Campus de Cáceres Av. São João, n. 563 – Cavallhada I – CEP: 78.216-060 – Cáceres – MT – Brasil

walker.leo@unemat.br, mayza.silva@unemat.br, melissa.rodrigues@unemat.br

Abstract. *The NotPetya cyberattack (2017), falsely classified as ransomware, operated as a systemic sabotage wiper. This article reviews the technical vector of this threat, detailing the replacement of the Master Boot Record (MBR) with a malicious microkernel and the encryption of the Master File Table (MFT) using a modified Salsa20 algorithm. Reverse engineering demonstrates the intentional discarding of the symmetric key, mathematically precluding the recovery of logical volumes. The study concludes that mitigating disk-level corruption threats requires transcending ransom negotiations, mandating the adoption of Zero Trust architectures and immutable offline backups.*

Resumo. *O ciberataque NotPetya (2017), falsamente tipificado como ransomware, operou como um wiper de sabotagem sistemática. Este artigo revisa o vetor técnico dessa ameaça, detalhando a substituição do Master Boot Record (MBR) por um microkernel malicioso e a encriptação da Master File Table (MFT) com o algoritmo Salsa20 modificado. A engenharia reversa demonstra o descarte intencional da chave simétrica, inviabilizando matematicamente a recuperação dos volumes lógicos. O estudo conclui que mitigar ameaças de corrupção em nível de disco exige transcender negociações de resgate, adotando obrigatoriamente arquiteturas Zero Trust e backups offline inutáveis.*

1. Introdução

Em junho de 2017, o *NotPetya* comprometeu infraestruturas críticas globais via movimentação lateral automatizada, utilizando o *exploit EternalBlue* e roubo de credenciais (CHIU et al., 2017; MICROSOFT SECURITY TEAM, 2017). Embora simulasse um *ransomware*, análises forenses o classificaram como um *wiper* voltado à destruição irreversível de ativos (KASPERSKY, 2017). Sua sofisticação iniciou no vetor de infecção: um ataque à cadeia de suprimentos via M.E.Doc. Segundo Albrecht et al. (2024), essa transição da finalidade financeira para destruição sistemática é um marco taxonômico: ao obter privilégios administrativos locais, o malware desceu da camada de aplicação para atingir diretamente os setores físicos do disco.

O vetor de sabotagem do *NotPetya* foca na sobrescrita do *Master Boot Record* (MBR) e na corrupção da *Master File Table* (MFT) através de um algoritmo Salsa20 modificado (CHECK POINT, 2017). Como detalhado por Greenberg (2018), essa estratégia causou danos globais devido à impossibilidade técnica de recuperação dos volumes afetados.

2. Fundamentação Teórica

2.1. O Master Boot Record (MBR)

O MBR, localizado no setor 0, armazena a organização das partições e o código inicial para carregar o sistema operacional. Por executar antes de qualquer software de segurança, sua manipulação permite que códigos maliciosos assumam o controle do sistema ainda na fase de boot (MICROSOFT SECURITY TEAM, 2017).

2.2. A Master File Table (MFT)

A MFT é o componente central do NTFS, funcionando como um banco de dados que indexa arquivos e diretórios. Contém metadados vitais e ponteiros lógicos para a localização física dos dados. Quando corrompida ou encriptada, essa estrutura inviabiliza o acesso lógico aos arquivos, tornando a recuperação extremamente complexa (CHECK POINT RESEARCH, 2017).

2.3. Cenário Atual

A evolução dessas técnicas observa-se no HybridPetya (2025-2026), que atua como um ransomware funcional acoplado a um bootkit avançado. O artefato explora vulnerabilidades para contornar o UEFI Secure Boot, instalando uma aplicação EFI maliciosa que encripta a MFT antes do carregamento do sistema. Isso demonstra que o sequestro do processo de inicialização continua sendo refinado para evadir defesas modernas.

3. Metodologia da Revisão

Esta revisão bibliográfica foi conduzida sob o modelo de Revisão Sistemática de Literatura (RSL), utilizando o protocolo estruturado de Kitchenham e Charters (2007) para garantir a reprodutibilidade. A pesquisa foi conduzida entre janeiro e abril de 2026, focando em publicações emitidas entre 2017 e 2024. O estudo foi norteado pela seguinte Questão de Pesquisa (QP): De que forma a manipulação estrutural do MBR e da MFT pelo NotPetya inviabiliza tecnicamente a recuperação de dados em comparação a ransomwares convencionais?

Para a busca, definiu-se a string: **("NotPetya" OR "Petya") AND ("MBR" OR "MFT" OR "Salsa20")**. Foram consultadas as bases IEEE Xplore, Google Scholar e os repositórios de inteligência da Microsoft, Kaspersky e Cisco Talos. O processo de seleção baseou-se em três critérios de inclusão (CI): (1) detalhamento da engenharia reversa do código-fonte; (2) análise de baixo nível das estruturas MBR/MFT; e (3) estudos de caso sobre o impacto em infraestruturas críticas. Como critérios de exclusão (CE), descartaram-se artigos focados estritamente em aspectos jurídicos ou geopolíticos sem fundamentação técnica em cibersegurança.

Do universo inicial de 24 trabalhos identificados, 14 foram pré-selecionados após leitura de resumos. Após aplicação dos critérios de rigor técnico e avaliação da qualidade das evidências de engenharia reversa, o corpus final consistiu em 6 fontes principais (4 relatórios de laboratórios de segurança e 2 artigos acadêmicos), que fundamentam a análise apresentada nas seções subsequentes.

4. Análise Técnica do Vetor de Sabotagem

A eficácia do NotPetya como ferramenta de destruição reside na sua capacidade de subverter processos legítimos do sistema operacional. A análise de engenharia reversa e os detalhes de baixo nível apresentados nas subseções a seguir são derivados diretamente do *corpus* primário selecionado na metodologia, com ênfase nas descobertas técnicas consolidadas por Microsoft Security Team (2017), Kaspersky Lab (2017), Check Point Research (2017) e Chiu et al. (2017).

4.1. A Camuflagem Criptográfica e a Falsa Fachada

A propagação inicial exigiu privilégios elevados. O artefato busca o SeDebugPrivilege para interagir com processos críticos (CHIU et al., 2017) e, uma vez garantida a persistência, agenda um reinício forçado do sistema.

Ao reiniciar, em vez do carregamento padrão do Windows, o código malicioso apresenta uma interface que simula a ferramenta nativa CHKDSK. Como demonstrado na Figura 1, esta tela informa falsamente que o sistema de arquivos está sendo reparado devido a erros no disco. Esta tática de engenharia social visa evitar que o utilizador interrompa o processo de escrita em baixo nível que ocorre em segundo plano. De acordo com a Microsoft Security Team (2017), enquanto o utilizador aguarda a "reparação", o *malware* está, na realidade, a executar a encriptação estrutural da partição. Ao final, é exibida a nota de resgate exigindo o pagamento em Bitcoin, embora o mecanismo de recuperação seja inexistente.

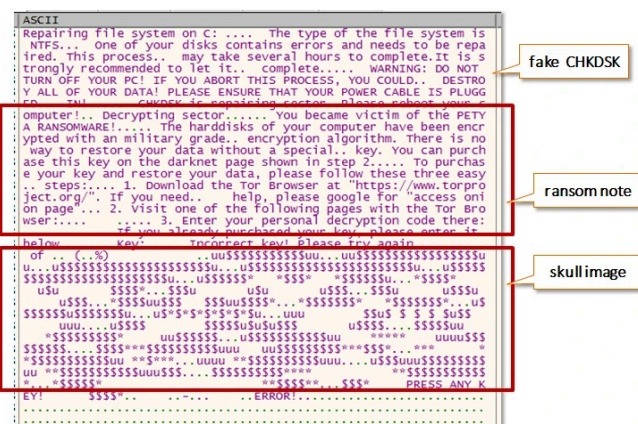


Figura 1. Sequência de boot adulterada pelo *NotPetya*, exibindo a simulação do utilitário de reparo de disco seguida pela notificação de cifragem. Fonte: Adaptado de Check Point Research (2017).

4.2. O Sequestro do Processo de Inicialização (Sobrescrita do MBR)

A execução do *NotPetya* antes do carregamento do *kernel* do Windows é garantida pela subscrição do *Master Boot Record*. O artefato substitui o código de inicialização original de 512 bytes por um microkernel malicioso customizado de 16-bits (MICROSOFT SECURITY TEAM, 2017).

Para garantir que a máquina torne-se inoperável sob o controle do sistema operacional legítimo, o *NotPetya* move o MBR original para o setor 34 do disco,

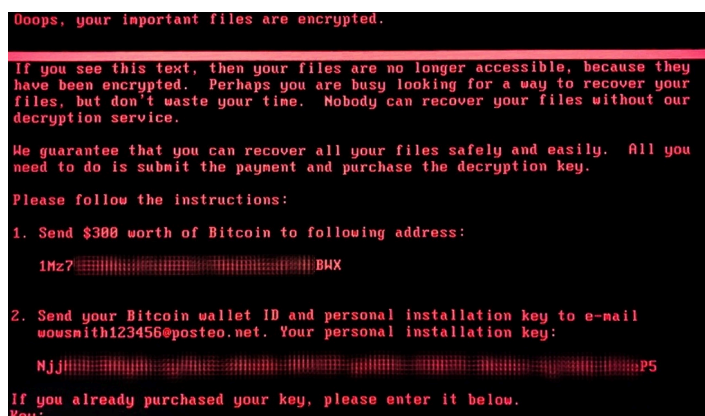
aplicando uma operação lógica XOR com o valor **0x07** para ofuscar os dados originais. Com o MBR comprometido, o controle do *hardware* no momento do *boot* é transferido diretamente para o código do atacante. Este microkernel é o responsável por gerir a exibição das mensagens falsas e por impedir que ferramentas de recuperação convencionais consigam restaurar a cadeia de inicialização sem a remoção física do código malicioso.

4.3. A Destruição da MFT e a Perda da Chave (O Comportamento Wiper)

A prova definitiva da natureza de *wiper* do *NotPetya* encontra-se na forma como a *Master File Table* (MFT) é manipulada. O *malware* utiliza uma implementação do algoritmo de criptografia simétrica Salsa20 para cifrar os registros da MFT, o que impossibilita o sistema operacional de localizar qualquer arquivo no volume NTFS (CHECK POINT RESEARCH, 2017).

Contudo, a análise de engenharia reversa conduzida pela Kaspersky Lab (2017) revelou uma falha crítica e deliberada no *design* criptográfico do artefato. Em ataques de *ransomware* legítimos, a chave simétrica utilizada para cifrar os dados é preservada e cifrada com uma chave pública do atacante para permitir uma posterior descryptografia. No caso do *NotPetya*, a chave Salsa20 é gerada, utilizada para corromper a MFT e imediatamente descartada da memória, sem nunca ser armazenada ou vinculada ao identificador exibido na tela da vítima.

Como pode ser observado na Figura 2, o sistema apresenta um "Personal Installation Key" ao utilizador, simulando um processo de recuperação padrão. Entretanto, análises técnicas comprovaram que este ID é, na verdade, uma sequência de caracteres aleatórios gerada localmente, sem qualquer relação matemática com a chave de cifragem utilizada (KASPERSKY LAB, 2017). Esta destruição intencional do material criptográfico torna a recuperação dos dados tecnicamente impossível, confirmando que o objetivo do ataque nunca foi o lucro, mas a sabotagem definitiva da infraestrutura afetada.



```
Oops, your important files are encrypted.

If you see this text, then your files are no longer accessible, because they
have been encrypted. Perhaps you are busy looking for a way to recover your
files, but don't waste your time. Nobody can recover your files without our
decryption service.

We guarantee that you can recover all your files safely and easily. All you
need to do is submit the payment and purchase the decryption key.

Please follow the instructions:

1. Send $300 worth of Bitcoin to following address:

1Mz7.....BMX

2. Send your Bitcoin wallet ID and personal installation key to e-mail
wousmith123456@posteo.net. Your personal installation key:

Njj.....PS

If you already purchased your key, please enter it below.
Key:
```

Figura 2. Nota de resgate exibida após a corrupção da MFT, apresentando um identificador de instalação sem validade criptográfica. Fonte: Kaspersky Lab (2017).

5. Discussão: Resiliência e Impacto na Infraestrutura

A análise técnica do *NotPetya* revela que estratégias tradicionais de defesa contra *ransomware* são insuficientes perante ataques de sabotagem em nível de disco. A destruição das estruturas MBR e MFT gera um cenário onde a recuperação de desastres depende exclusivamente da existência de cópias de segurança íntegras e isoladas.

5.1. Impacto em Infraestruturas de Grande Porte

O caso Maersk exemplifica o impacto operacional de um *wiper*. A inutilização de controladores de domínio e *endpoints* gerou um "apagão" logístico global imediato. A lição central é que a recuperação de sabotagens estruturais demanda semanas de reconstrução manual, superando os tempos previstos para *ransomwares* comuns.

5.2. Estratégias de Mitigação

Para mitigar os danos de ataques que operam sob o MBR, a literatura moderna aponta para duas frentes:

Segmentação de Rede e Zero Trust: Impedir que o *malware* utilize privilégios administrativos para se mover lateralmente (ALBRECHT et al., 2024). O *NotPetya* só consegue sobrescrever o MBR se obtiver privilégios de administrador local; restringir esses privilégios é a primeira linha de defesa.

Backups Imutáveis e Offline: Uma vez que o MFT é encriptado sem preservação de chave, a única forma de recuperar os dados é através de *backups* que não foram atingidos pela rede. Estratégias de *air-gapping* tornam-se, portanto, a única garantia de continuidade de negócios contra artefatos da classe *wiper*.

6. Conclusão

A análise técnica do *NotPetya* evidencia que o artefato utilizou a estética e os métodos de extorsão do *ransomware* como um vetor de negação de serviço e sabotagem. A substituição do código de inicialização mestre (MBR) e a cifragem deliberada da Master File Table (MFT) demonstram a intenção do artefato. A prova cabal que encerra o debate técnico sobre as motivações do ataque (sabotagem versus lucro) reside no descarte imediato da chave simétrica Salsa20 da memória. Este comportamento não apenas inviabiliza a recuperação lógica dos volumes, mas confirma definitivamente que o *ransomware* serviu estritamente como uma fachada para uma operação de sabotagem cibernética.

Este estudo reforça que, em um cenário de cibersegurança cada vez mais voltado para ataques de Estado e sabotagem industrial, a resiliência não pode depender de capacidades de descriptografia, mas sim de uma arquitetura de defesa profunda. A implementação de redes segmentadas, o controle rigoroso de privilégios de administrador e a manutenção de backups imutáveis e isolados (*air-gapped*) permanecem como as únicas contramedidas eficazes contra a classe de malwares *wiper* exemplificada pelo *NotPetya*.

Este trabalho apresenta limitações inerentes à sua natureza bibliográfica, uma vez que não contempla experimentação prática ou análise direta do código do *malware*. Ademais, a dependência de fontes secundárias, como relatórios de engenharia reversa, pode refletir vieses metodológicos das organizações que os produziram.

7. Referências Bibliográficas

- ALBRECHT, C. et al. Learning From the Past: Examining Ransomware Mitigations through a Systematic Literature Review. In: GI-Jahrestagung. Bonn: Gesellschaft für Informatik e.V., 2024. p. 1-15.
- CHECK POINT RESEARCH. NotPetya Ransomware Technical Analysis. Check Point Software Technologies, jul. 2017.
- CHIU, A. et al. New Ransomware Variant "Nyetya" Compromises Systems Worldwide. Cisco Talos Intelligence Group, 27 jun. 2017. Disponível em: <https://blog.talosintelligence.com/2017/06/worldwide-ransomware-variant.html>.
- ESET. Introducing HybridPetya: Petya/NotPetya copycat, UEFI Secure Boot bypass. WeLiveSecurity, 2026. Disponível em: <https://www.welivesecurity.com/en/eset-research/introducing-hybridpetya-petya-notpetya-copycat-uefi-secure-boot-bypass/>.
- GREENBERG, A. The Untold Story of NotPetya, the Most Devastating Cyberattack in History. Wired, 22 ago. 2018.
- KASPERSKY LAB. ExPetr/Petya/NotPetya is a Wiper, Not Ransomware. Kaspersky Securelist, 28 jun. 2017. Disponível em: <https://securelist.com/expetrpetyanotpetya-is-a-wiper-not-ransomware/78902/>.
- KITCHENHAM, B.; CHARTERS, S. Guidelines for performing Systematic Literature Reviews in Software Engineering. EBSE Technical Report EBSE-2007-01, Keele University and Lincoln University, 2007.
- MICROSOFT SECURITY TEAM. New ransomware, old techniques: Petya adds worm capabilities. Microsoft Security Blog, 27 jun. 2017. Disponível em: <https://www.microsoft.com/security/blog/2017/06/27/new-ransomware-old-technique-s-petya-adds-worm-capabilities/>.
- SOS RANSOMWARE. HybridPetya: When a new ransomware resurrects Petya/NotPetya techniques with advanced UEFI capabilities. SOS Ransomware, 2026. Disponível em: <https://sosransomware.com/en/cybersecurity/hybridpetya-when-a-new-ransomware-resurrects-petya-notpetya-techniques-with-advanced-uefi-capabilities/>. Acesso em: 12 maio. 2026.