Novo ransomware HybridPetya pode ignorar o UEFI Secure Boot - Against

Data: 2025-09-12 18:18:10

Autor: Inteligência Against Invaders

Uma variedade de ransomware descoberta recentemente chamada HybridPetya pode ignorar

oRecurso de inicialização segura UEFI para instalar um aplicativo malicioso na partição do sistema

EFI.

O HybridPetya parece inspirado no malware destrutivo Petya/NotPetya que criptografava computadores e impedia a inicialização do Windows em ataques em 2016 e 2017 mas não forneceu uma opção de recuperação.

Pesquisadores da empresa de segurança cibernética ESET encontraram uma amostra deHybridPetya no VirusTotal. Eles observam que isso pode ser um projeto de pesquisa, uma prova de conceito ou uma versão inicial de uma ferramenta de crime cibernético ainda em testes limitados.

Ainda assim, a ESET diz que sua presença é mais um exemplo (junto com Lótus Negro, BootKitty e Hyper-V Backdoor) que os bootkits UEFI com funcionalidade Secure Bypass são uma ameaça real.

O HybridPetya incorpora características do Petya e do NotPetya, incluindo o estilo visual e a cadeia de ataque dessas cepas de malware mais antigas.

No entanto, o desenvolvedor adicionou coisas novas, como a instalação na partição do sistema EFI e a capacidade de ignorar a inicialização segura explorando oCVE-2024-7344vulnerabilidade.

A ESET descobriu a falha em janeiro deste ano, O problema consiste emAplicativos assinados pela Microsoft que podem ser explorados para implantar bootkits mesmo com a proteção Secure Boot ativa no alvo.

[IMAGEM REMOVIDA]
[IMAGEM REMOVIDA]
[IMAGEM REMOVIDA]Repositório GitHub.

A Microsoft corrigiu o CVE-2024-7344 com o Atualização de janeiro de 2025, portanto, os sistemas Windows que aplicaram essa ou atualizações de segurança posteriores estão protegidos contra o HybridPetya.

Outra prática sólida contra ransomware é manter backups offline de seus dados mais importantes, permitindo a restauração fácil e gratuita do sistema.