O ransomware HybridPetya ignora o UEFI Secure Boot ecoando o Petya/N

Data: 2025-09-13 14:46:49

Autor: Inteligência Against Invaders

O ransomware HybridPetya ignora o UEFI Secure Boot ecoando o Petya/NotPetya

O ransomware HybridPetya ignora o UEFI Secure Boot para infectar partições EFI, ecoando os infames ataques Petya/NotPetya de 2016–2017.

Os pesquisadores da ESET descobriram um novo ransomware chamado HybridPetya na plataforma VirusTotal. O malware ecoa o infame Petya/NãoPetya malware, suportando recursos adicionais, como comprometer sistemas baseados em UEFI e explorarCVE-2024-7344para contornar Inicialização segura UEFI em sistemas desatualizados.

“Curiosamente, o código responsável por gerar as chaves de instalação pessoal das vítimas parece ser inspirado noRedPetyaOpenSSLPoC.” lê o relatório publicado pela ESET. “Estamos cientes de pelo menos uma outra reescrita de PoC compatível com UEFI do NotPetya, apelidada deNãoPetyaNovamente, que está escrito emFerrugem; no entanto, esse código não está relacionado ao HybridPetya.”

Ao contrário do NotPetya, o HybridPetya atua como um verdadeiro ransomware como o Petya, permitindo a descriptografia. Os pesquisadores suspeitam que a amostra possa estar ligada a um UEFI Petya PoC que foi o primeiro Discutido em 9 de setembro de 2025, sugerindo que o HybridPetya pode ser um projeto de pesquisa.

Os pesquisadores da ESET publicaram uma análise técnica dos componentes do HybridPetya, o bootkit e o instalador.

O bootkit UEFI tem duas versões semelhantes. Na execução, ele verifica o sinalizador de criptografia no arquivo de configuração: 0 (pronto), 1 (criptografado) ou 2 (descriptografado).

Se definido como 0, ele extrai uma chave Salsa20 e nonce, zera a chave do arquivo de configuração, define o sinalizador como 1, criptografa o sinalizador *‘verificar’* e cria um arquivo de contador. O bootkit procura partições NTFS e criptografa a Tabela de Arquivos Mestre. Em seguida, o código malicioso atualiza o arquivo do contador com o número de clusters criptografados e exibe um status CHKDSK falso. Após a criptografia, o malware é reiniciado. Se o disco já estiver criptografado (sinalizador 1), ele mostrará uma nota de resgate e aceitará uma chave de 32 caracteres.

O malware verifica a chave descriptografando o *verificar* arquivo e, se correto, define o sinalizador como 2 (descriptografado), recupera os carregadores de inicialização e solicita a reinicialização.

Os instaladores do HybridPetya localizam a partição do sistema EFI em discos GPT, removem o carregador de fallback (EFIBootBootx64.efi) e descartam uma configuração de criptografia (EFIMicrosoftBootconfig) contendo a chave Salsa20, nonce e chave vítima, além de um blob de verificação de 0x200 bytes (EFIMicrosoftBootverify) que o bootkit descriptografa posteriormente para validar as chaves inseridas. O instalador faz backup de bootmgfw.efi para bootmgfw.efi.old e, em seguida, força um BSOD (NtRaiseHardError) para que o sistema seja reinicializado no fluxo de inicialização substituído e execute o kit de inicialização.

O HybridPetya é o quarto bootkit UEFI conhecido com bypass Secure Boot, depois de Lótus Negro, BootKitty e o Hyper-V Backdoor PoC (exploração CVE-2020-26200), mostrando que esses ataques estão se tornando mais comuns.

"Embora o HybridPetya não esteja se espalhando ativamente, seus recursos técnicos – especialmente criptografia MFT, compatibilidade com sistema UEFI e desvio de inicialização segura – o tornam notável para monitoramento de ameaças futuras." conclui o relatório.

Siga-me no Twitter: @securityaffairs e Linkedin e Mastodonte

PierluigiPaganini

(Assuntos de Segurança – hacking, UEFI)