Os hackers implantam uma nova ferramenta EDR-Freeze para desativar o

Data: 2025-09-22 05:07:11

Autor: Inteligência Against Invaders

Um pesquisador de segurança divulgou uma nova ferramenta que pode desativar temporariamente os sistemas de detecção e resposta de terminais (EDR) e software antivírus sem exigir fatores vulneráveis, marcando uma evolução significativa nas técnicas de ataque direcionadas a soluções de segurança.

Evasão avançada através de componentes do Windows

A ferramenta, apelidada de congelamento e [desenvolvido](#) Pelo pesquisador TwosevenOnet, explora a funcionalidade de relatório de erro do Windows para suspender os processos de segurança por meio de um sofisticado ataque de condição de corrida.

Ao contrário do tradicional, traga suas próprias técnicas de driver vulnerável (BYOVD) que exigem que os invasores implantem drivers maliciosos, o EDR-Freeze opera inteiramente no modo de usuário usando componentes legítimos do Windows.

O ataque aproveita a função MinidumpWriteDump da biblioteca DBGHELP do Windows, que cria instantâneos de memória de processos de execução para fins de depuração.

Durante esta operação, a função suspende todos os threads no processo de destino para garantir a captura de memória consistente.

O EDR-Freeze explora esse comportamento, acionando o processo de despejo contra o software de segurança e suspendendo o próprio processo de dumping, deixando a solução de segurança de destino congelada indefinidamente.

A técnica tem como alvo especificamente o processo werfaultSecure.exe [Erro do Windows](#) Componente de relatório que pode ser executado com privilégios de luz de processo protegidos (PPL) no nível Wintcb.

Ao combinar isso com a ferramenta CreateProcessapl, os invasores podem ignorar os mecanismos de proteção de pessoas que normalmente protegem os processos de segurança do acesso não autorizado.

O pesquisador demonstrou o EDR-Freeze suspendendo com sucesso [Windows Defender's](#) Processo msmtp.exe no Windows 11 24h2 por uma duração especificada.

A ferramenta aceita dois parâmetros: o ID do processo do software de segurança de destino e a

duração da suspensão, permitindo que os invasores desativem temporariamente o monitoramento durante atividades maliciosas.

Essa abordagem aborda as principais limitações dos ataques BYOVD, que requerem implantação de drivers vulneráveis ??que podem desencadear alertas em sistemas monitorados. O EDR-Freeze usa apenas processos legítimos do Windows, tornando a detecção mais desafiadora para as equipes de segurança.

O lançamento da ferramenta destaca a dinâmica em andamento de gato e rato entre invasores e fornecedores de segurança.

À medida que as soluções EDR se tornam mais sofisticadas na detecção de técnicas BYOVD, os atores de ameaças estão desenvolvendo métodos alternativos para alcançar objetivos semelhantes usando a funcionalidade do sistema operacional interno.

As equipes de segurança podem monitorar o uso potencial do EDR-Freeze, examinando os parâmetros da linha de comando `werfaultSecure.exe`.

A atividade suspeita inclui os processos de sistema sensível ao processo, como LSASS, motores antivírus ou agentes EDR, o que pode indicar a tentativa de manipulação de software de segurança.

O pesquisador disponibilizou publicamente o código-fonte da EDR-Freeze no GitHub, enfatizando seu uso para pesquisas de segurança legítimas e exercícios da equipe vermelha.

No entanto, as capacidades da ferramenta levantam preocupações sobre potencial uso indevido por atores maliciosos que buscam evitar os controles de segurança durante os ataques.

As organizações devem revisar seus recursos de monitoramento de segurança para detectar a atividade incomum `werfaultSecure.exe` e considerar a implementação de mecanismos adicionais de proteção de processos além das salvaguardas padrão do PPL para se defender contra essa técnica de evasão emergente.

Encontre esta história interessante! Siga -nos [LinkedIn](#) X Para obter mais atualizações instantâneas.