EDR-Freeze: uma ferramenta que coloca EDRs e antivírus em estado de co

Data: 2025-09-21 16:54:15

Autor: Inteligência Against Invaders

Uma nova ferramenta de prova de conceito chamada EDR-Freeze foi desenvolvida, capaz de

colocar Endpoint Detection and Response (EDR) e soluções antivírus em um estado de “coma”

suspenso.

A técnica do Zero Salarium usa um recurso integrado do Windows, fornecendo uma opção furtiva em comparação com a tendência crescente de ataques Bring Your Own Vulnerable Driver (BYOVD) que os hackers empregam para desativar o software de segurança.

Esse método elimina a necessidade de drivers de terceiros, diminuindo o risco de problemas e detecção do sistema. Ele opera inteiramente no modo de usuário, desativando de forma eficaz e discreta o monitoramento de segurança.

O exploit MiniDumpWriteDump:

A técnica EDR-Freeze envolve principalmente a manipulação da função MiniDumpWriteDump, que é da biblioteca Windows DbgHelp e é usada para criar um minidespejo, um instantâneo de memória de um processo de depuração.

Para garantir um instantâneo consistente e não corrompido, a função suspende todos os threads dentro do processo de destino enquanto o despejo é criado.

Normalmente, essa suspensão é breve. No entanto, o desenvolvedor do EDR-Freeze desenvolveu um método para prolongar esse estado suspenso indefinidamente.

Os principais desafios foram estender o tempo de execução rápida da função MiniDumpWriteDump e obter past o recurso de segurança Protected Process Light (PPL) que protege os processos de EDR e antivírus contra interferências.

Para superar a proteção PPL, a técnica utiliza WerFaultSecure.exe, um componente do serviço WER (Relatório de Erros do Windows). WerFaultSecure.exe pode ser executado com proteção de nível WinTCB, um dos níveis de privilégio mais altos, permitindo que ele interaja com processos protegidos.

WerFaultSecure.exe pode ser configurado para executar a função MiniDumpWriteDump em qualquer processo, mesmo aqueles de EDR protegido e software antivírus, usando os parâmetros corretos.

Um ataque de condição de corrida pode transformar uma breve pausa em um congelamento duradouro, ocorrendo em uma sequência rápida e exata:

1. *WerFaultSecure.exe é iniciado com parâmetros que o direcionam para criar um despejo de memória do processo de EDR ou antivírus de destino.*

2. A ferramenta EDR-Freeze monitora continuamente o processo de destino.

3. No momento em que o processo de destino entra em um estado suspenso (quando MiniDumpWriteDump começa seu trabalho), a ferramenta EDR-Freeze suspende imediatamente o próprio processo WerFaultSecure.exe.

Como WerFaultSecure.exe agora está suspenso, ele nunca pode concluir a operação de despejo de memória e, crucialmente, nunca pode retomar os threads do processo EDR de destino.

A Zero Salarium afirmou que o software de segurança permanece permanentemente suspenso e ineficaz até que o processo de WerFaultSecure.exe seja encerrado.

Processo de eliminação da ferramenta EDR-Freeze:

O desenvolvedor ***Lançado*** a ferramenta EDR-Freeze para mostrar essa técnica. Ele requer dois parâmetros: o ID do processo (PID) do destino e a duração da suspensão em milissegundos.

Um invasor pode desativar ferramentas de segurança, realizar ações prejudiciais e restaurar o software de segurança ao normal como se nada tivesse acontecido.

Um teste no Windows 11 24H2 suspendeu com sucesso o processo MsMpEng.exe do Windows Defender.

Durante ***Defensores***, a detecção dessa técnica envolve o monitoramento de execuções incomuns de WerFaultSecure.exe.

Se o programa for observado visando os PIDs de processos confidenciais, como agentes lsass.exe ou EDR, ele deverá ser tratado como um alerta de segurança de alta prioridade que requer investigação imediata.

Fonte: *Zerosalarium, Notícias de segurança cibernética*