Nova ferramenta EDR-Freeze usa o Windows WER para suspender softwa

Data: 2025-09-22 17:31:30

Autor: Inteligência Against Invaders

Um novo método e ferramenta de prova de conceito chamado EDR-Freeze demonstra que é

possível evitar soluções de segurança no modo de usuário com o sistema Windows Error Reporting

(WER) da Microsoft.

A técnica elimina a necessidade de um driver vulnerável e coloca agentes de segurança como ferramentas de detecção e resposta de endpoint (EDR) em um estado de hibernação.

Usando a estrutura do WER junto com a API MiniDumpWriteDump, o pesquisador de segurança TwoSevenOneThree (Salarium Zero)encontrou uma maneira desuspender indefinidamente a atividade de processos de EDR e antivírus indefinidamente.

Os métodos de desativação de EDR existentes operam com base na técnica “Bring Your Own Vulnerable Driver” (BYOVD), em que os invasores pegam um driver de kernel legítimo, mas vulnerável, e o exploram para escalonamento de privilégios.

As principais desvantagens nos ataques BYOVD incluem a necessidade de contrabandear o driver para o sistema de destino, ignorar as proteções de execução e limpar artefatos no nível do kernel que podem expor a operação.

O EDR-Freeze é descrito como um método muito mais furtivo que não requer driver de kernel, funciona inteiramente no modo de usuário e aproveita componentes legítimos do Windows que estão presentes por padrão no sistema operacional.

Como funciona o EDR-Freeze

WerFaultSecure é um componente de Relatório de Erros do Windows que é executado com privilégios PPL (Protected Process Light), projetado para coletar despejos de memória de processos confidenciais do sistema para fins de depuração e diagnóstico.

MiniDumpWriteDump é uma API na biblioteca DbgHelp que gera um instantâneo (“minidump”) da memória e do estado de um processo. Ao fazer isso, ele suspende todos os threads do processo de destino e os retoma após a conclusão do trabalho.

O EDR-Freeze aproveita o WerFaultSecure para disparar MiniDumpWriteDump, que suspende temporariamente todos os threads no processo de destino enquanto o despejo é gravado.

Durante esse processo, o invasor suspende o próprio processo WerFaultSecure, para que o dumper nunca retome o destino, deixando o processo AV em um estado de “coma”.

O pesquisador descreve isso como um ataque de condição de corrida que pode ser reproduzido em quatro etapas:

1. Gere WerFaultSecure como uma PPL.
2. Passe argumentos para WerFaultSecure para que ele chame MiniDumpWriteDump no PID de destino.
3. Sonde o destino até que ele seja suspenso pela operação de despejo.
4. Abra imediatamente WerFaultSecure (PROCESS_SUSPEND_RESUME) e chame NtSuspendProcess para congelar o dumper.

O pesquisador também publicou uma ferramenta que executa essas ações e testou no Windows 11 24H2, congelando com sucesso o processo do Windows Defender.

[IMAGEM REMOVIDA]Steven Lim desenvolveu uma ferramenta que mapeiaWerFaultSecure para processos do Microsoft Defender Endpoint.

Ainda assim, a Microsoft poderia tomar medidas para proteger esses componentes do Windows contra abusos, como bloquear invocações suspeitas, permitir apenas determinados PIDs ou restringir os parâmetros possíveis.

O BleepingComputer entrou em contato com a Microsoft para comentar sobre como se defender contra essa técnica e atualizaremos esta postagem assim que recebermos uma resposta.

[IMAGEM REMOVIDA]