Silver Fox explora drivers assinados para implantar o backdoor ValleyRAT

Data: 2025-09-04 08:26:19

Autor: Inteligência Against Invaders

Uma campanha cibernética recém-detectada está explorando drivers confiáveis, mas vulneráveis, do

Windows para contornar as proteções de segurança e instalar uma ferramenta de acesso remoto.

A operação, atribuída pela Check Point Research (CPR) ao Grupo APT Silver Fox, destaca os riscos de invasores explorarem drivers assinados pela Microsoft que antes eram considerados seguros.

Abusando de drivers assinados pela Microsoft

No centro do ataque está o driver WatchDog Antimalware (amsdk.sys, versão 1.0.600).

Embora assinado pela Microsoft e não listado anteriormente como vulnerável, o driver foi abusado para encerrar processos vinculados a ferramentas antivírus e EDR, abrindo caminho para a implantação de Vale-RATA–um backdoor modular capaz de vigilância, execução de comandos e exfiltração de dados.

A Silver Fox também contou com um driver mais antigo baseado em Zemana (*ZAM.exe*) para manter a compatibilidade entre sistemas que vão do Windows 7 ao Windows 11.

Ambos os drivers permitiam o encerramento arbitrário do processo, permitindo que os invasores desabilitassem até mesmo processos protegidos.

Leia mais sobre táticas de exploração de driver do Windows: Vulnerabilidade no driver do Windows leva a falhas no sistema

Os pesquisadores descobriram que o grupo empacotou todos os elementos em binários de carregadores independentes.

Cada amostra incluiu:

- Recursos anti-análise
- Mecanismos de persistência

- Dois drivers incorporados
- Uma lista codificada de processos de segurança a serem encerrados
- Um downloader do ValleyRAT

A campanha evoluiu rapidamente, produzindo variantes que usavam novos drivers ou versões alteradas de drivers corrigidos para evitar a detecção.

Evasão e Atribuição

Uma técnica envolvia modificar um driver WatchDog corrigido (wamsdk.sys, versão 1.1.100) alterando um único byte em seu campo de carimbo de data/hora. Como a assinatura digital da Microsoft não cobre esse campo, a assinatura do driver permaneceu válida ainda apareceu como um novo arquivo com um hash diferente.

A infraestrutura usada nos ataques foi rastreada até servidores na China, enquanto as configurações de malware visavam especificamente produtos de segurança populares no leste da Ásia. Esses detalhes, combinados com a carga útil do ValleyRAT, levaram à atribuição ao Silver Fox APT.

Embora o WatchDog tenha lançado uma atualização abordando falhas de escalonamento de privilégios locais, o encerramento arbitrário do processo continua sendo possíveldeixando os sistemas vulneráveis.

O Pesquisa de RCP enfatizou que as verificações de assinatura e hash por si só são insuficientes. As equipes de segurança são aconselhadas a aplicar a lista de bloqueio de driver mais recente da Microsoft, usar regras de detecção YARA e implementar monitoramento baseado em comportamento para detectar atividades anormais do driver.

“Nossa pesquisa reforça a necessidade de esforços contínuos de fornecedores e usuários de segurança para se manterem vigilantes contra o abuso emergente de motoristas legítimos”, escreveu a CPR.

“A identificação, a geração de relatórios e a correção proativa dessas vulnerabilidades são essenciais para fortalecer os sistemas Windows contra ameaças em evolução, aproveitando as técnicas de Bring Your Own Vulnerable Driver (BYOVD).”