Os hackers da Silver Fox usam a vulnerabilidade do motorista para evitar

Data: 2025-08-29 06:27:14

Autor: Inteligência Against Invaders

Uma campanha sofisticada do Silver Fox Apt Group, que explora um motorista vulnerável

anteriormente desconhecido para ignorar a detecção e a resposta do terminal (EDR) e as soluções

antivírus em sistemas Windows 10 e 11 totalmente atualizados.

O Check Point Research (RCP) revelou em 28 de agosto de 2025 que o grupo de ameaças persistentes avançado vem aproveitando o driver de antimalware do Watchdog (AMSDK.SYS versão 1.0.600) para encerrar processos protegidos e evitar soluções de segurança modernas.

Esse driver assinado pela Microsoft, construído no Zemana Anti-Malware SDK, não foi listado na lista de bloqueio de driver vulnerável da Microsoft e permaneceu sem ser detectado por projetos de segurança comunitária.

O Raposa prateada A APT empregou uma abordagem de motorista dupla para garantir a compatibilidade em diferentes versões do Windows.

Para sistemas herdados como o Windows 7, os invasores usaram o conhecido driver vulnerável Zemana que já está bloqueado por medidas de segurança.

No entanto, para moderno Windows 10 e 11 ambientes, eles implantaram o driver Watchdog não detectado, que manteve uma assinatura válida da Microsoft e ignorou os mecanismos de detecção tradicionais.

A campanha se concentra em amostras de carregadores all-in-one que combinam vários componentes maliciosos em um único executável.

Esses carregadores incorporam recursos anti-análises, dois drivers vulneráveis ??incorporados, lógica personalizada para encerrar processos de segurança e o módulo de download do Valleyrat.

Os atacantes projetaram essas ferramentas para funcionar perfeitamente no Windows 7 através do Windows 11, adaptando sua abordagem com base na versão do sistema de destino.

Implementação técnica

Após a execução, o malware realiza verificações abrangentes de anti-análise, incluindo detecção de máquinas virtuais, identificação de caixa de areia e reconhecimento de hipervisor.

Se essas verificações falharem, o malware abortará a execução e exibe mensagens de erro falsas do sistema para evitar a detecção.

Curiosamente, os pesquisadores descobriram exclusões para nomes específicos de computadores (Desktop-T3N3M3Q, Desktop-03Amf90 e Win-VMHH95J6C26) que permitem que a execução continue, prováveis ??sistemas usados ??durante o desenvolvimento de malware.

O mecanismo de persistência envolve a criação de uma pasta “tempo de execução” em C: Arquivos de Programas Runtime, onde o carregador e o driver vulnerável apropriado são armazenados como RuntTimeBroker.exe e AMSDK_Service.sys, respectivamente.

Dois serviços são estabelecidos: “Termontor” mantém a persistência do carregador, enquanto o “AMSDK_SERVICE” configura o registro para o carregamento do motorista.

A vulnerabilidade principal está na capacidade do driver de antimalware de vigilância de encerrar processos arbitrários sem verificar o status do processo protegido.

O driver usa iocreateviceSecure com uma forte DACL (lista de controle de acesso discricionário), mas não possui o sinalizador File_Device_Secure_Open, permitindo que até usuários não privilegiados se comuniquem com o dispositivo através da manipulação de namespace.

Os invasores exploram isso emitindo comandos de controle específico de entrada/saída (IOCTL): primeiro registrando seu processo com ioctl_register_process (0x80002010) e depois encerrar os processos de segurança de destino usando o IOCTL_terminate_process (0x80002048). Essa abordagem desativa efetivamente os produtos de proteção de terminais que normalmente são executados como processos protegidos.

O objetivo final da campanha está entregando Valleyrat (Também conhecido como Winos), um sofisticado acesso remoto de Trojan atribuído ao Silver Fox Apt.

O serviço nomeadoTermaintoré responsável por manter a persistência pela cópia previamente descartada do carregador all-in-one (RuntimeBroker.exe).

O malware se comunica com servidores de comando e controle hospedados na China usando canais criptografados com a criptografia XOR Cifra.

A Valleyrat fornece recursos abrangentes de vigilância remota, funcionalidade de execução de comandos e ferramentas de exfiltração de dados.

O padrão de segmentação sugere um foco nos mercados asiáticos, particularmente na China, como evidenciado pela lista de processos de segurança com codificação de segurança comumente usados ??nessa região.

O malware é normalmente entregue através de arquivos .rar contendo arquivos executáveis ??ou bibliotecas de link dinâmico que exploram técnicas legítimas de carregamento lateral do aplicativo.

Resposta do fornecedor e ameaças contínuas

Após a divulgação da CPR, o Watchdog lançou um driver corrigido (Wamsdk.sys versão 1.1.100) que abordava os vetores de escalação de privilégios locais.

No entanto, pesquisadores observado O fato de o patch não resolver completamente a vulnerabilidade arbitrária de terminação do processo, pois ainda não possuía verificações para

processos protegidos.

Demonstrando adaptabilidade notável, a Silver Fox Apt rapidamente incorporou uma versão modificada do driver corrigido em sua campanha em andamento.

Ao alterar um único byte no campo de data e hora não autenticado da assinatura do Microsoft Authenticode do motorista, os atacantes preservaram a assinatura válida do motorista enquanto geravam um novo hash de arquivo, ignorando efetivamente as listas de bloqueios de segurança baseadas em hash.

Esta campanha representa uma evolução significativa nas táticas de ameaças persistentes avançadas, destacando a tendência crescente de armas de armas assinadas, mas vulneráveis, para contornar as proteções dos pontos finais.

A técnica expõe limitações críticas nas abordagens de segurança atuais que dependem fortemente dos métodos de detecção baseados em assinatura e baseados em hash.

O ataque demonstra como os atores de ameaças estão indo além das vulnerabilidades conhecidas para explorar motoristas anteriormente não classificados, criando pontos cegos em muitos mecanismos de defesa.

O uso bem-sucedido de um driver assinado na Microsoft em sistemas totalmente atualizados ressalta a sofisticação das operações modernas do APT e sua capacidade de operar em ambientes de computação confiáveis.

Mitigações

Os especialistas em segurança recomendam a implementação de estratégias de defesa em camadas que se estendem além dos métodos tradicionais de detecção.

As organizações devem aplicar manualmente a mais recente lista de blocos de driver vulnerável da Microsoft, à medida que as atualizações automáticas ocorrem com pouca frequência. Os sistemas de detecção baseados em comportamento capazes de identificar padrões suspeitos de atividade do motorista são essenciais para capturar novas técnicas de exploração.

A campanha enfatiza a importância crítica da identificação proativa da vulnerabilidade e da rápida implantação de patches em toda a cadeia de suprimentos de software.

Os fornecedores e usuários de segurança devem manter uma vigilância aumentada contra o abuso emergente de motoristas legítimos, pois os limites entre código confiável e malicioso continuam a embaçar em operações sofisticadas de APT.

Esta campanha Silver Fox Apt serve como um lembrete gritante de que mesmo os sistemas modernos e modernos de Windows totalmente remendados permanecem vulneráveis ??a adversários determinados que exploram os relacionamentos fundamentais de confiança incorporados aos modelos de segurança do sistema operacional.

Encontre esta história interessante! Siga -nos LinkedIn**e**X**Para obter mais atualizações instantâneas**.