"Mic-e-mouse" O ataque permite que hackers roubam dados c

Data: 2025-10-08 05:52:31

Autor: Inteligência Against Invaders

Uma vulnerabilidade inovadora de segurança cibernética foi descoberta que transforma os ratos do

computador diário em ferramentas sofisticadas de escutas.

Os pesquisadores têm técnicas para reconstruir o discurso inteligível.

O ataque alcança resultados notáveis, apesar desses desafios técnicos. Os testes de sensores de nível de consumo usando conjuntos de dados de fala VCTK e audiomnista demonstraram um aumento de SI-SNR de +19DB, precisão do reconhecimento de alto-falante de 80% em testes automatizados e uma taxa de erro de palavras de apenas 16,79% em estudos em humanos.

O oleoduto captura com sucesso as frequências de fala humana entre 200Hz e 2000Hz, cobrindo a maioria do áudio de conversação.

___Iframe_placeholder_0___

A vulnerabilidade se torna mais preocupante à medida que os ratos de alto desempenho se tornam cada vez mais acessíveis aos consumidores.

Os dispositivos de entrada avançados com sensores vulneráveis ??estão agora disponíveis por menos de US $ 50, tornando o vetor de ataque generalizado entre os ambientes de consumidores, corporativos e governamentais.

À medida que os custos de fabricação continuam diminuindo devido a melhorias tecnológicas, a superfície de ataque para estes Vulnerabilidades continua expandindo.

O modelo de ameaças tem como alvo aplicativos de código aberto, onde a coleta de dados de ratos de alta frequência parece legítima.

Software criativo, videogames e outros aplicativos de alto desempenho servem como veículos de entrega ideais para injetar a exploração sem levantar suspeitas.

Muitos videogames contêm código de rede que os invasores podem redirecionar para extrair dados coletados do mouse dos computadores de vítimas discretamente.

O pipeline Mic-E-Mouse opera totalmente invisivelmente para usuários em média durante as fases de coleta de dados.

Os invasores precisam apenas de acesso a um mouse vulnerável e software comprometido no computador da vítima, incluindo aplicativos potencialmente benignos baseados na Web.

Depois que a coleta de dados é concluída, todo o processamento e análise de sinal podem ocorrer offline conforme a conveniência do invasor.

O ataque demonstra que a vigilância auditiva através de sensores ópticos de alto desempenho agora é tecnicamente viável, eficaz e com desempenho.

Essa descoberta destaca um vetor de ataque anteriormente desconhecido que transforma os periféricos comuns de computadores em dispositivos de vigilância secretos, levantando preocupações significativas de privacidade para indivíduos e organizações usando dispositivos de entrada modernos com sensores ópticos avançados.