# Raven Stealer tem como alvo os usuários do Google Chrome para exfiltrar

Data: 2025-09-18 05:49:00

Autor: Inteligência Against Invaders

Raven Stealer, um sofisticado malware que rouba informações que causou estragos nos dados

confidenciais dos usuários.

Esse malware contemporâneo representa uma evolução preocupante na tecnologia de roubo de credenciais, combinando técnicas avançadas de evasão com recursos de exfiltração de dados simplificados.

Raven Stealer se destaca como um malware leve, mas altamente eficaz, desenvolvido principalmente em Delphi e C ++.

Os pesquisadores de segurança cibernética têm identificado Uma ameaça significativa direcionada ao Google Chrome e outros navegadores baseados em cromo.

Projetado para furtividade e eficiência, este software malicioso opera com a interação mínima do usuário, mantendo recursos excepcionais de ocultação operacional.

O malware tem como alvo especificamente os navegadores baseados em cromo, incluindo Chrome, Edge e Brave, colhendo sistematicamente senhas, cookies, dados de pagamento e entradas de preenchimento automático de sistemas infectados.

A abordagem sofisticada do malware envolve o acesso a caminhos de armazenamento local e cofres de credenciais nesses navegadores, permitindo que os invasores roubem credenciais de login para compromisso potencial de conta e exfiltração de dados.

O que torna o ladrão de Raven particularmente perigoso é sua capacidade de descriptografar dados sensíveis ao navegador, acessando as teclas de criptografia AES armazenadas nos arquivos estaduais locais dos navegadores, convertendo credenciais criptografadas em formato de texto simples para roubar fácil.

Quatro estágios principais da análise de malware: análise de propriedades estáticas, análise de comportamento interativo, análise totalmente automatizada e reversão de código manual

A Raven Stealer emprega recursos técnicos avançados que o diferenciam dos malware convencional.

O malware utiliza um design modular com um editor de recursos embutido, permitindo que os atacantes incorporem detalhes de configuração, como Telegrama Tokens de bot diretamente na carga útil.

Essa abordagem simplificada torna a implantação acessível mesmo para atores de ameaças com baixo qualificação, expandindo seu alcance potencial significativamente.

A integração do telegrama para operações de comando e controle (C2), combinadas com uma interface de usuário simplificada.

A distribuição geralmente ocorre através de fóruns subterrâneos e agrupada com software rachado, tornando -o uma ameaça persistente a ambientes pessoais e corporativos.

O malware é promovido ativamente por meio de canais de telegrama dedicados, onde cibercriminosos pode acessar ferramentas do construtor e recursos de suporte.

Essa comercialização de ferramentas de malware demonstra o cenário em evolução do crime cibernético, onde ataques sofisticados se tornam cada vez mais acessíveis.

A estratégia de execução do malware envolve recursos incorporados armazenados na seção .RSRC, uma prática comum Delphi para agrupar módulos externos.

Esses recursos são extraídos e carregados na memória durante a execução, permitindo que o malware opere sem soltar arquivos no disco, aumentando significativamente seus recursos furtivos e potencial de evasão.

## Exfiltração de dados e comunicação

Um dos recursos mais preocupantes do Raven Stoualer é sua capacidade de exfiltração de dados em tempo real através da integração do Telegram Bot.

Os malware consolidam credenciais roubadas e informações do sistema dentro de uma hierarquia de pastas estruturada sob % %local Ravenstealer, organizando dados coletados para transmissão eficiente para os atacantes.

As malware incorporam credenciais sensíveis ao telegrama, textão específica de thechat_idandbot_tokenas dentro de sua seção de recursos, usando o recurso IDS 102 e 103, respectivamente.

O New Backdoor Malware usa a API do Telegram Bot para controle remoto, descoberto pelos pesquisadores do Netskope Threat Labs

Os dados roubados incluem vários tipos de informações confidenciais organizadas sistematicamente em arquivos separados.

Os cookies do navegador são agregados de vários navegadores baseados em cromo e armazenados em arquivos cookies.txt, permitindo seqüestro de sessão e representação do usuário.

Descriptografado credenciais Incluindo nomes de usuário e senhas são compilados em senha.txt arquivos, facilitando o acesso à conta não autorizada em várias plataformas.

Talvez os detalhes mais preocupantes do cartão de crédito e débito armazenados, juntamente com as informações de cobrança, sejam extraídos dos navegadores e salvos em arquivos de pagamento.txt, criando oportunidades de fraude financeira e roubo de identidade.

O malware também captura capturas de tela dos desktops das vítimas e comprime todos os artefatos coletados em arquivos de zip para transmissão.

Esses arquivos são enviados aos atacantes via telegrama usando o terminal da API, fornecendo ao cibercriminal acesso abrangente às vidas digitais e informações financeiras das vítimas.

Raven Stealer demonstra recursos sofisticados de evasão por meio de sua implementação de injeção de carga útil criptografada e técnicas de vazamento de processos.

O malware incorpora sua carga útil de DLL principal usando a criptografia chacha20, mantendo -a oculta em seu próprio binário, evitando a detecção por medidas tradicionais de segurança.

Durante a execução, o malware emprega um processo reflexivo oco, lançando novas instâncias do navegador de cromo em estados suspensos e injetando DLLs descriptografados nesses processos legítimos.

Essa técnica permite que o malware seja executado sob identidade de software confiável, ignorando efetivamente os sistemas de detecção comportamentais e baseados em assinatura que dependem da reputação do processo e assinaturas maliciosas conhecidas.

A abordagem de execução na memória garante que o código malicioso nunca toque o disco em sua forma descriptografada, tornando a análise e detecção forenses significativamente mais desafiadora para profissionais de segurança e sistemas automatizados.

## Mitigações

Organizações e usuários individuais podem implementar várias medidas defensivas para proteger contra o ladrão de Raven e ameaças semelhantes.

Os sistemas de detecção de ameaças baseados em comportamento são mais eficazes contra esse tipo de malware, pois podem identificar atividades suspeitas, independentemente das técnicas de evasão do malware.

O monitoramento regular do tráfego de telegrama pode ajudar a detectar possíveis tentativas de exfiltração de dados, principalmente em ambientes corporativos.

A educação do usuário permanece crucial na prevenção de infecções iniciais, pois o malware geralmente se espalha através de táticas de phishing e downloads maliciosos de software.

As organizações devem implementar programas abrangentes de conscientização sobre segurança, com foco nos riscos de baixar software quebrado e clicar em links ou anexos suspeitos.

As defesas técnicas devem incluir soluções antivírus atualizadas com proteção em tempo real ativada, de preferência aqueles que utilizam recursos avançados de análise comportamental.

O monitoramento regular de desempenho do sistema através do gerenciador de tarefas pode ajudar a identificar processos incomuns ou padrões de consumo de recursos que podem indicar presença de malware. Mais importante, o patch de software consistente ajuda a fechar vulnerabilidades que o malware pode explorar para o acesso inicial ao sistema.

O surgimento do ladrão de Raven representa uma evolução significativa em malware para roubar informações, combinando recursos técnicos sofisticados com ferramentas de implantação amigáveis ??que democratizam ataques cibernéticos avançados.

À medida que essa ameaça continua a evoluir, usuários e organizações individuais devem permanecer vigilantes e implementar medidas abrangentes de segurança para proteger dados confidenciais dessas ameaças cada vez mais sofisticadas.

## Indicadores de compromisso

| **Indicador de arquivos – SHA256** | **Contexto** |
|---|---|
| 2B24885942253784E0F6617B26F5E6A05B8AD4 5F092D2856473439FA6E095CE4 | Raven Stealer |
| 65CA89993F2EE21B95362E151A7CFC50B8718 3BF0E9C5B753C5E5E17B46F8C24 | 65a16km1.69n.exe |

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