O novo modstealista evita o antivírus, tem como alvo os usuários do macO

Data: 2025-09-29 09:06:36

Autor: Inteligência Against Invaders

Uma nova tensão sofisticada de malware direcionada aos usuários do MACOS surgiu, capaz de

ignorar as soluções antivírus tradicionais, enquanto direcionava especificamente desenvolvedores e

titulares de criptomoedas.

A ameaça de plataforma cruzada, dubbedmodstealer, representa a última evolução no cibercrime focado no MacOS, destacando os crescentes desafios de segurança enfrentados pelos usuários da Apple em 2024.

Modstealer foi o primeiro identificado pela empresa de segurança cibernética Mosyle e relatada até 9to5mac em 11 de setembro de 2024.

O malware surgiu inicialmente no Virustottal aproximadamente um mês antes de sua divulgação pública, indicando que estava operando no modo furtivo enquanto evita os sistemas de detecção.

Diferentemente das divulgações típicas de segurança cibernética, o Mosyle não lançou documentação técnica abrangente ou detalhes de análise forense por meio de canais oficiais.

Esse afastamento da prática padrão da indústria deixou os pesquisadores de segurança com detalhes técnicos limitados sobre o trabalho interno do malware.

Modstealer se distingue através da funcionalidade de sua plataforma, capaz de comprometer macos, janelas e Sistemas Linux.

Embora os mecanismos exatos que permitam essa versatilidade permaneçam incertos, as campanhas de plataforma cruzada geralmente implantam cargas úteis específicas do sistema operacional com base no perfil das vítimas.

O malware demonstra sofisticação particular em sua metodologia de segmentação, concentrando-se principalmente em dois grupos demográficos de alto valor:

Os desenvolvedores são direcionados através de anúncios falsos de emprego e golpes de recrutamento, explorando sua tendência a baixar ferramentas e recursos de desenvolvimento de várias fontes on -line.

O malware aproveita as táticas de engenharia social, com invasores representando recrutadores e empresas legítimas para estabelecer confiança antes de implantar cargas úteis maliciosas.

Holders de criptomoeda representar o segundo grupo de alvo primário, com o ModStealer projetado especificamente para comprometer as extensões de carteira baseadas em navegador no Chrome e

Safári plataformas.

Essa capacidade é particularmente digna de nota, pois os infostealistas visam as extensões da carteira de safári são relativamente incomuns na paisagem das ameaças.

Capacidades técnicas e exfiltração de dados

A ModStealer emprega um conjunto abrangente de técnicas de colheita de dados projetadas para maximizar o valor extraído de sistemas comprometidos:

Compromisso de extensão do navegador: O malware tem como alvo mais de 50 extensões diferentes do navegador, com foco particular nas extensões de carteira de criptomoeda nos navegadores Chrome/Chromium e Safari.

Monitoramento da área de transferência: O ladrão monitora continuamente o conteúdo da área de transferência para capturar informações confidenciais, como frases de sementes de criptomoeda e chaves privadas quando os usuários copiarem e colam essas credenciais.

Captura de captura de tela: ModStealer tira capturas de tela periódicas para capturar dados visíveis do usuário, potencialmente incluindo informações confidenciais exibidas na tela.

Colheita de dados do navegador: Os malware extraem sistematicamente dados do navegador salvo, incluindo armazenamento local, conteúdo, Conteúdo de LevelDB e IndexedDB, cookies e credenciais armazenadas.

Execução do comando remoto: O ladrão mantém a comunicação com servidores de comando e controle, permitindo que os invasores executem comandos adicionais para coleta de dados ou movimento lateral em redes comprometidas.

ModStealer demonstra recursos de persistência avançados em sistemas macos através do abuso de ferramentas legítimas do sistema de maçã.

O malware atinge a presença de longo prazo, explorando a propriedade da Apple, incorporando-se como um lancegent nos processos de inicialização do sistema.

Essa técnica envolve a instalação de mecanismos de persistência nos processos de lançamento e inicialização do macOS, permitindo que o malware sobreviva a reinicializações do sistema e mantenha o acesso contínuo a dispositivos comprometidos.

O ladrão oculta seus arquivos de carga útil usando nomes inócuos como “sysupdater.dat” para evitar a detecção durante a inspeção do sistema casual.

A capacidade do malware de evitar a detecção de antivírus sugere a implementação de técnicas avançadas de ofuscação e possivelmente zero dia Métodos de exploração que ainda não foram incorporados aos sistemas tradicionais de detecção baseados em assinatura.

Impacto nos grupos de usuários de alto risco

O direcionamento de desenvolvedores e titulares de criptomoedas reflete a tomada de decisões de

atores de ameaças estratégicas com base no retorno potencial do investimento.

Os desenvolvedores geralmente possuem privilégios elevados do sistema e acesso a uma propriedade intelectual valiosa, código -fonte e infraestrutura de desenvolvimento.

Os titulares de criptomoedas representam alvos de alto valor devido à natureza irreversível das transações de blockchain e aos ativos financeiros significativos normalmente armazenados em carteiras baseadas em navegador.

A adoção convencional da criptomoeda criou uma superfície de ataque maior, com muitos usuários armazenando ativos digitais substanciais em extensões de navegador que operam em ambientes digitais inerentemente arriscados.

Stephen Ajayi, Dapp e AI auditam o líder técnico da Hacken, enfatizou a importância de práticas de segurança aprimoradas para os desenvolvedores, afirmando: “Os desenvolvedores devem validar a legitimidade dos recrutadores e domínios associados”.

Mitigações

Os especialistas em segurança recomendam várias medidas defensivas para grupos de usuários de alto risco:

Para desenvolvedores:

- Verifique a legitimidade do recrutador por meio de canais oficiais da empresa antes de baixar qualquer arquivo ou concluir as avaliações técnicas.
- As atribuições de solicitação são compartilhadas por meio de repositórios públicos, em vez de downloads diretos de arquivos.
- Utilize máquinas virtuais descartáveis ??para testar código ou aplicativos de fontes desconhecidas.
- Mantenha sistemas separados e endurecidos para acessar carteiras de criptomoeda e recursos sensíveis de desenvolvimento.

Para usuários de criptomoeda:

- Considere migrar de carteiras baseadas em navegador para carteiras de hardware que armazenam teclas privadas offline.
- Implemente a verificação da carteira de hardware confirmando endereços de transações nos monitores do dispositivo, verificando pelo menos o primeiro e o último seis caracteres antes da aprovação.
- Estabeleça perfis de navegador separados e bloqueados dedicados exclusivamente às operações de criptomoeda.
- Habilitar Autenticação multifatorial com componentes biométricos para todas as contas relacionadas à criptomoeda.

Práticas de segurança gerais:

- Minimize a superfície de ataque digital, limitando a quantidade de dados sensíveis armazenados em plataformas on -line.
- Mantenha as soluções antivírus atualizadas e reconhecem suas limitações contra ameaças

de dia zero.
- Revise regularmente e audite extensões do navegador, removendo adições desnecessárias ou suspeitas
- Implementar a segmentação da rede para limitar o potencial movimento lateral em caso de compromisso.

O surgimento do ModStealer representa uma continuação da tendência preocupante na evolução de malware direcionada ao macOS ao longo de 2024.

A crescente sofisticação dessas ameaças desafia o equívoco comum de que os sistemas de Apple são inerentemente mais seguros do que outras plataformas.

A capacidade do malware de ignorar os mecanismos de segurança internos da Apple, incluindo o Gatekeeper, destaca possíveis fraquezas na arquitetura de segurança da empresa quando confrontados com ameaças persistentes avançadas. Esse desenvolvimento sugere que os usuários do MacOS não podem mais depender apenas de recursos de segurança internos para proteção contra atores determinados de ameaças.

O ModStealer representa uma escalada significativa na sofisticação e na precisão do MACOS malware. Seus recursos de plataforma cruzada, mecanismos avançados de persistência e foco específico em alvos de alto valor demonstram o cenário de ameaças em evolução que os usuários da Apple enfrentam.

A divulgação técnica limitada em torno dessa ameaça ressalta a importância da pesquisa de segurança independente e a necessidade de compartilhamento abrangente de inteligência de ameaças na comunidade de segurança cibernética.

À medida que as ameaças do MAC Infotealer continuam a se tornar mais prevalentes e eficazes, os usuários devem adotar medidas de segurança proativas, em vez de depender de mecanismos de proteção reativa.