Novo malware Mac chamado "Jscorerunner" Site de conversão em PDF de

Data: 2025-08-29 07:28:28

Autor: Inteligência Against Invaders

Surgiu uma nova campanha de malware Mac Mac que explora a confiança dos usuários em

ferramentas gratuitas de conversão on -line em PDF, demonstrando como os cibercriminosos

continuam a evoluir suas táticas para ignorar as medidas modernas de segurança.

A empresa de segurança cibernética Mosyle tem exclusivamente divulgado A descoberta do Jscorerunner, uma linhagem de malware MAC anteriormente desconhecida que alcançou detecções zero no Virustottal no momento da descoberta.

O malware se propaga através de um site malicioso chamado FILERIPLE[.]com, que se disfarça como um serviço de conversão de PDF legítimo para trazer usuários desavisados ??para baixar o que parece ser um utilitário inofensivo.

Essa descoberta ocorre em meio a uma tendência mais ampla de cibercriminosos, explorando a popularidade dos serviços de conversão de arquivos gratuitos.

O Denver Field Office do FBI já emitiu avisos sobre o aumento do risco de malware e roubo de dados de tais sites, destacando como os invasores estão capitalizando a necessidade diária dos usuários de soluções de compatibilidade de formato rápido.

O JSCORERUNNER opera através de um processo de implantação de dois estágios orquestrado, projetado para evitar as proteções de segurança internas da Apple.

O estágio inicial envolve um pacote chamado FILERIPLE.PKG, que cria uma fachada convincente, exibindo uma visualização da Web falsa que mostra uma visualização de ferramentas em PDF de aparência legítima, enquanto atividades maliciosas são executadas silenciosamente em segundo plano.

Embora a Apple tenha revogado o certificado do desenvolvedor para esta primeira etapa, fazendo macos Bloqueie o pacote no lançamento, o verdadeiro perigo está no segundo estágio.

O pacote não assinado Safari14.1.2moJaveAuto.pkg ignora as proteções padrão do Gatekeeper, evitando o processo de validação de assinatura padrão, permitindo a instalação sem acionar avisos de segurança.

Operações de seqüestro de navegador e roubo de dados

Uma vez instalado com sucesso no sistema de uma vítima, o JSCORERUNNER demonstra seu objetivo principal: seqüestro abrangente do navegador focado especificamente no Google Chrome.

O malware atravessa metodicamente o diretório ~/biblioteca/aplicativo/Google/Chrome/diretório para identificar perfis de usuário padrão e adicionais.

O ataque envolve a criação de um objeto de modelo malicioso que redefine as configurações críticas do navegador, incluindo o URL de pesquisa, o novo URL da guia e o nome de exibição.

Essa manipulação redireciona efetivamente os usuários para mecanismos de pesquisa fraudulentos sem o seu conhecimento, a abertura de caminhos para o registro de chaves, redirecionamentos de sites de phishing e promoção de resultados de pesquisa maliciosa.

Para manter as operações furtivas, o malware emprega técnicas adicionais para ocultar sua presença, incluindo a passagem de argumentos ao Chrome de que suprimem os registros de falhas e desativam a bolha de notificação “Restaurar a última sessão”.

A equipe de pesquisa de segurança de Mosyle forneceu indicadores técnicos abrangentes para os profissionais de segurança cibernética identificar e mitigar essa ameaça.

As amostras de malware incluem vários componentes com assinaturas de hash distintas, variando do instalador inicial do FILERIPLE.PKG para ofuscar JavaScript Cargas úteis.

A infraestrutura de comando e controle segue protocolos de malware padrão, com a carga útil instalada primeiro confirmando a instalação bem-sucedida com servidores remotos antes de prosseguir com suas atividades de manipulação do navegador.

O malware também demonstra conhecimento sofisticado do sistema, identificando a conta de usuário real e removendo atributos de quarentena de aplicações maliciosas.

Paisagem crescente de ameaças

Essa descoberta representa parte de uma tendência preocupante em campanhas de malware direcionadas ao MAC. Os pesquisadores de segurança documentaram a crescente sofisticação em ataques direcionados aos sistemas de maçã, com atores de ameaças empregando linguagens de programação não convencionais e técnicas avançadas de evasão para contornar os métodos de detecção tradicionais.

A exploração de serviços legítimos de que sepultam, como conversores de PDF, reflete uma mudança mais ampla nas táticas cibernéticas.

Campanhas semelhantes foram documentadas usando sites falsos que clonam serviços populares, completos com telas de carregamento realistas e Captcha Verificações para estabelecer a confiança do usuário antes de implantar cargas úteis maliciosas.

O surgimento do JScorerunner ressalta a importância crítica de abordagens de segurança de várias camadas para ambientes MAC.

Embora as proteções internas da Apple, como Gatekeeper e XProtect, forneçam segurança na linha de base, o sucesso da implantação do segundo estágio desse malware demonstra a necessidade de medidas de segurança adicionais.

A detecção de Mosyle dessa ameaça de dia zero destaca o valor de soluções especializadas de

segurança da Apple que podem identificar novos vetores de ataque.

A equipe de pesquisa de segurança da empresa continua a monitorar ameaças em evolução especificamente Mac ambientes, fornecendo inteligência crucial para a comunidade mais ampla de segurança cibernética.

Recomendações de proteção

Especialistas em segurança cibernética enfatizam várias medidas de proteção importantes para usuários de Mac. As recomendações principais incluem evitar os resultados da pesquisa aleatória para ferramentas de conversão de arquivos on -line e usar exclusivamente sites oficiais verificados para esses serviços.

___Iframe_placeholder_0___

Além disso, as organizações devem implementar soluções abrangentes de detecção de terminais capazes de identificar novas famílias de malware.

Para os administradores do sistema, as assinaturas de hash fornecidas permitem o bloqueio proativo e a detecção de componentes Jscorerunner em ambientes MAC gerenciados.

O treinamento regular de conscientização sobre segurança deve enfatizar os riscos associados às ferramentas gratuitas de conversão on -line e a importância de verificar as fontes de software antes da instalação.

A campanha do JSCORERUNNER serve como um lembrete gritante de que os usuários de Mac não podem mais assumir a imunidade de ataques sofisticados de malware, principalmente porque os cibercriminosos continuam desenvolvendo táticas de engenharia social cada vez mais inteligentes para explorar as necessidades cotidianas de computação.

Encontre esta história interessante! Siga -nosLinkedIneXPara obter mais atualizações instantâneas.