Cuidado: repositórios GitHub distribuindo Atomic Infostealer no macOS

Data: 2025-09-22 06:57:13

Autor: Inteligência Against Invaders

Cuidado: repositórios GitHub distribuindo Atomic Infostealer no macOS

O LastPass avisa os usuários do macOS sobre repositórios falsos do GitHub que distribuem malware infostealer atômico disfarçado de ferramentas legítimas.

O LastPass avisa os usuários do macOS sobre repositórios falsos do GitHub que espalham malware disfarçado de ferramentas legítimas, redirecionando as vítimas para baixar o Atómico Infostealer do macOS.

“A equipe de Inteligência, Mitigação e Escalonamento de Ameaças (TIME) do LastPass está rastreando uma campanha de infostealer generalizada e contínua direcionada a usuários de Mac por meio de repositórios fraudulentos do GitHub projetados para induzir vítimas em potencial a instalar o que é apresentado como software de várias empresas para MacOS.” lê o relatório publicado pelo LastPass. “No caso do LastPass, os repositórios fraudulentos redirecionaram as vítimas em potencial para um repositório que baixa o malware infostealer Atômico.”

A campanha de malware ainda está em andamento, os agentes de ameaças usam SEO para colocar sites maliciosos no topo dos resultados do Google e do Bing, visando empresas de tecnologia, bancos e gerenciadores de senhas. As equipes de segurança compartilham IoCs para detectar e mitigar a campanha.

O LastPass identificou dois repositórios fraudulentos do GitHub que foram prontamente rotulados para remoção e agora estão inativos.

“Notavelmente, as páginas do GitHub parecem ter sido criadas por vários nomes de usuário do GitHub para contornar as remoções.” continua o relatório. “Os títulos da página do GitHub incluem “nome da empresa” e terminologia relacionada ao Mac (ou seja, MacOS, Mac, Premium no Macbook), já que é isso que eles estão visando.”

A página do GitHub engana os usuários para que sigam as instruções no estilo ClickFix no Terminal, que instala o malware Atomic Stealer.

A campanha também tem como alvo usuários do macOS, fazendo-se passar por ferramentas populares como 1Password, Dropbox, Notion, Shopify e outras.

Os pesquisadores também compartilharam Indicadores de Comprometimento (IoCs) para esta campanha.

Siga-me no Twitter:@securityaffairseLinkedineMastodonte

PierluigiPaganini

(Assuntos de Segurança–hacking,macOS)