Os hackers abusam de páginas do github para espalhar malware de ladrilh

Data: 2025-09-22 07:11:41

Autor: Inteligência Against Invaders

Uma campanha sofisticada de malware está visando usuários de Mac através de repositórios fraudulentos do GitHub que se disfarçam de downloads legítimos de software, com atores de ameaças explorando táticas de otimização de mecanismos de pesquisa para fornecer links maliciosos diretamente a vítimas inocentes.

A equipe do LastPassapPeat Ameans Intelligence, Mitigation and Escalation tem identificado Uma operação infetealista generalizada contínua que tem como alvo especificamente os usuários do MacOS por meio de páginas enganosas do GitHub projetadas para distribuir o notório malware de roubos atômicos.

A manipulação do mecanismo de pesquisa leva o tráfego para sites maliciosos

A campanha demonstra técnicas avançadas de engenharia social, alavancando o envenenamento por SEO para garantir Github malicioso Os repositórios aparecem no topo dos resultados da pesquisa nas principais plataformas, incluindo Google e Bing.

Quando os usuários pesquisam downloads legítimos de software, eles encontram o que parece ser repositórios oficiais da empresa, mas são fachadas elaboradas criadas pelos cibercriminosos.

Os atores de ameaças lançaram uma ampla rede, visando inúmeras organizações de alto nível em vários setores, incluindo empresas de tecnologia, instituições financeiras e serviços de gerenciamento de senhas.

Exemplo de um email de phishing que se vende LastPass para roubar informações do usuário, instando a verificação de dados pessoais

Os pesquisadores do LastPass descobriram dois sites fraudulentos do Github se passando por seu serviço, ambos criados pelo usuário “Modhopmduck476” em 16 de setembro.

Esses repositórios apresentaram manchetes convincentes incorporando nomes de empresas e terminologia específica para Mac, como “MacOS”, “Mac” e “Premium no MacBook”, para maximizar seu apelo à demografia alvo.

As páginas maliciosas incluíam links que afirmam oferecer “Instalar o LastPass no MacBook” que redirecionaram as vítimas para um local de estadiamento secundário em “Ahoastock825[.]Github[.]io/.github/lastPass. ”

O ataque emprega um sofisticado mecanismo de entrega em várias etapas que começa quando as vítimas visitam a página fraudulenta do github e são redirecionadas para “MacPrograms-Pro[.]com/mac-git-2-download.html. ”

Este site secundário instrui os usuários a copiar e colar um comando de terminal que inicia uma solicitação de CLO a uma URL codificada por Base64.

O URL codificado decodifica para “Bonoud[.]com/get3/install.sh ”, que depois baixará uma carga útil disfarçada de um arquivo” atualização “no diretório temporário do sistema.

Relatório de detecção de malware mostrando vários fornecedores de segurança identificando um malware suspenso MacOS Trojan, consistente com Ladrão atômico análise

As equipes de segurança de todo o setor agora estão monitorando ativamente os indicadores de compromisso relacionados a esta campanha, com os esforços líderes do LastPass liderando contra os repositórios fraudulentos direcionados a seus clientes.

A empresa removeu com sucesso os sites maliciosos identificados e continua a realizar atividades de interrupção, compartilhando a inteligência de ameaças com outras organizações de segurança para combater esse cenário de ameaças em evolução.

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