60 gems Ruby maliciosos baixados 275.000 vezes roubam credenciais - Ag

Data: 2025-08-09 20:17:59

Autor: Inteligência Against Invaders

Sessenta gems Ruby maliciosas contendo código de roubo de credenciais foram baixadas mais de

275.000 vezes desde março de 2023, visando contas de desenvolvedores.

As gemas Ruby maliciosas foram descobertas pela Socket, que relata que visavam principalmente usuários sul-coreanos de ferramentas de automação para Instagram, TikTok, Twitter/X, Telegram, Naver, WordPress e Kakao.

RubyGems é o gerenciador de pacotes oficial para a linguagem de programação Ruby, permitindo a distribuição, instalação e gerenciamento de bibliotecas Ruby, conhecidas como gems, muito parecidas com npm para JavaScript ou PyPI para Python.

As joias maliciosas desta campanha foram publicadas em RubyGems.org sob vários pseudônimos ao longo dos anos. Os editores ofensivos são zon, nowon, kwonsoonje e soonje, espalhando a atividade por várias contas para dificultar o rastreamento e o bloqueio.

A lista completa dos pacotes maliciosos pode ser encontrada em Relatório do soquete, mas abaixo estão alguns casos notáveis de pacotes com nomes enganosos ou typosquatted:

- Automatizadores no estilo WordPress: wp_posting_duo, wp_posting_zon
- Bots no estilo Telegram: tg_send_duo, tg_send_zon
- Ferramentas de SEO/backlink: backlink_zon, back_duo
- A plataforma de blog imita: nblog_duo, nblog_zon, tblog_duopack, tblog_zon
- Ferramentas de interação do Naver Café: cafe_basics[_duo], cafe_buy[_duo], cafe_bey, *_blog_comment, *_cafe_comment

Todas as 60 gemas destacadas no relatório Socket apresentam uma interface gráfica do usuário (GUI) que parece legítima, bem como a funcionalidade anunciada.

Na prática, no entanto, eles atuam como ferramentas de phishing que exfiltram as credenciais que os usuários inserem no formulário de login para os invasores em um endereço de comando e controle (C2) codificado (programzon[.]com, appspace[.]KR, MarketingDuo[.]co[.]kr).

[IMAGEM REMOVIDA]
[IMAGEM REMOVIDA]há vários anos.

Em junho, a Socket relatou outro caso de gemas Ruby maliciosas que digitaram o Fastlane, um plug-in legítimo de código aberto que serve como uma ferramenta de automação para desenvolvedores

de aplicativos móveis, visando especificamente os desenvolvedores de bots do Telegram.

Os desenvolvedores devem examinar as bibliotecas que obtêm de repositórios de código aberto em busca de sinais de código suspeito, como partes ofuscadas, considerar a reputação e o histórico de lançamentos do editor e bloquear dependências para versões “conhecidas por serem seguras”.