Cadeia de suprimentos wormable? Chegam os Pacotes NPM com Malware

Data: 2025-09-18 15:14:54

Autor: Inteligência Against Invaders

Redazione RHC**:18 Setembro 2025 16:26**

Pesquisadores de segurança **descobriram o comprometimento de mais de 180 pacotes npm**, infectado com um *Malware de autopropagação projetado para infectar outros pacotes*. A campanha, apelidada de **Shai-Hulud,** provavelmente começou com o hack do **@ctrl/tinycolor** pacote, que é baixado por **2 milhões de vezes por semana.**

O nome Shai-Hulud vem dos arquivos shai-hulud.yaml usados pelo malware. **É uma referência aos vermes gigantes da areia de Duna de Frank Herbert**. A questão foi levada ao conhecimento do desenvolvedor Daniel Pereira Daniel Pereira, que alertou a comunidade para **um ataque à cadeia de suprimentos em larga escala.**

> *“No momento, enquanto você lê isso, o malware está sendo distribuído no npm”,* Pereira disse, pedindo a todos que não instalem as versões mais recentes do @ctrl/tinycolor.

O desenvolvedor tentou para notificar a equipe de segurança do GitHub por meio de canais privados, como os invasores **eles tinham como alvo “vários repositórios”** e divulgar publicamente o ataque poderia ter criado mais riscos. *No entanto, entrar em contato com o GitHub se mostrou muito difícil, então Pereira relatou publicamente o problema.*

Pesquisadores na Soquete e Aikido estão atualmente investigando o incidente e descobriram que pelo menos **187 pacotes foram comprometidos.** Entre os pacotes afetados, vários são publicados pela conta npmjs da empresa de segurança cibernética CrowdStrike.

> *“Depois de descobrir vários pacotes maliciosos no registro público npm (um repositório de código aberto de terceiros), nós os removemos rapidamente e atualizamos preventivamente nossas chaves”, disseram representantes da CrowdStrike.“Esses pacotes não são usados pela Falcon, nossa plataforma não é afetada e os clientes permanecem protegidos. Estamos trabalhando com o npm e conduzindo uma investigação completa.”*

Laboratórios de reversão, por sua vez, descreve este incidente como **“O primeiro de seu tipo, um worm auto-replicante que infecta pacotes NPM e rouba tokens de nuvem.”** Os pesquisadores acreditam que o ataque se originou no **rxnt-authentication, uma versão maliciosa do qual foi publicada no npm em 14 de setembro de 2025.**

De acordo com a ReversingLabs, a pessoa responsável por **suporte técnico** podem ser considerados **paciente zero.** A chave para descobrir a origem do ataque está exatamente em como a conta techsupportrxnt foi comprometida. Pode ter começado com um e-mail de phishing ou a exploração de um *Ação do GitHub.*

As versões comprometidas dos pacotes são equipadas com um mecanismo de autopropagação de malware, visando outros pacotes dos mantenedores afetados. De acordo com os pesquisadores do Socket, o malware baixou cada pacote do mantenedor, modificou seu **package.json**, injetou o **bundle.js** script, reempacotou o arquivo e o republicou, *“garantindo assim a Trojanização automática de pacotes downstream.”*

O bundle.js script usa **Porco Trufado**, um scanner secreto legítimo projetado para desenvolvedores e profissionais de segurança. O TruffleHog ajuda a detectar informações confidenciais vazadas acidentalmente, como chaves de API, senhas e tokens, de repositórios e outras fontes. O script malicioso abusou da ferramenta para encontrar tokens e credenciais de nuvem.

Redação
A equipe editorial da Red Hot Cyber é composta por um grupo de indivíduos e fontes anônimas que colaboram ativamente para fornecer informações e notícias antecipadas sobre segurança cibernética e computação em geral.

Lista degli articoli