Worm da cadeia de suprimentos ronda npm para roubar centenas de segr

Data: 2025-09-17 10:20:00

Autor: Inteligência Against Invaders

Pela terceira vez em apenas algumas semanas, os especialistas estão alertando sobre uma ameaça

significativa ao ecossistema npm de código aberto, depois de descobrir um worm inédito projetado

para roubar segredos.

Na segunda-feira, versões maliciosas de vários pacotes npm populares com milhões de downloads semanais combinados começaram a aparecer, de acordo com o ReversingLabs. A empresa disse ontem que observou pelo menos 700 repositórios do GitHub afetados pela campanha.

O malware em si (3 MB + de JavaScript) foi apelidado de “Shai-Hulud” – o nome dos vermes gigantes do filme Duna.

“Depois que uma conta de desenvolvedor npm é comprometida, o worm procura outros pacotes que o desenvolvedor mantém. Em seguida, ele cria uma nova versão de cada um desses pacotes, injetando-se neles”, explicou ReversingLabs.

“Cada pacote recém-criado é modificado com um*pós-instalação*ação que executará o mal-intencionado*bundle.js*quando um usuário desavisado baixa o pacote comprometido. Isso se repete perpetuamente à medida que o worm encontra novos desenvolvedores para infectar e os usa para se espalhar ainda mais.”

Leia mais sobre ameaças npm: Código npm malicioso atingiu 10% dos ambientes de nuvem

Os pacotes publicados por contas npm comprometidas são atualizados automaticamente com o arquivo de bundle.js malicioso para acelerar a propagação do worm, acrescentou o fornecedor.

O script bundle.js foi projetado para roubar tokens npm, GitHub, AWS e GCP. Mas também instala o TruffleHog – uma ferramenta de código aberto que pode detectar até 800 segredos.

Se encontrar tokens do GitHub, o worm criará um novo repositório público do GitHub com o nome “Shai-Hulud” e despejará os segredos da vítima lá.

Ele também enviará um novo fluxo de trabalho do GitHub Actions para todos os repositórios acessíveis.

“A ação do GitHub tem uma ação executável acionada no evento PUSH que é projetada para exfiltrar os tokens acessíveis do ambiente de fluxo de trabalho para o hxxps://webhook.site/bb8ca5f6-4175-45d2-b042-fc9ebb8170b7 de URL. Esses dados também são

codificados em Base64 duplo”, disse a ReversingLabs.

Outra funcionalidade maliciosa do Shai-Hulud é migrar repositórios privados do GitHub pertencentes a uma conta comprometida do GitHub para os acessíveis ao público.

“Esta é provavelmente uma tentativa de obter acesso a segredos codificados nesses repositórios e, possivelmente, roubar o código-fonte que eles contêm”, continuou o relatório.

“Esse código roubado pode ser analisado em busca de vulnerabilidades que podem ser usadas em ataques posteriores ao software.”

Laboratórios de reversão ditoEle viu os repositórios privados de 700 vítimas expostos dessa maneira.

Links úteis S1ngularity

Vários fornecedores de segurança vincularam a campanha a um semelhante que teve como alvo os autores de um pacote popular chamado “Nx”.

“Com base na vitimologia, a Wiz Research avalia que essa atividade está ligada ao recente ataque à cadeia de suprimentos s1ngularity / Nx, onde o roubo inicial de tokens do GitHub permitiu a cadeia mais ampla de comprometimento e vazamento de repositórios anteriormente privados”, afirmou Wiz.

“Os pacotes npm iniciais que iniciaram essa reação em cadeia incluíram várias vítimas comprometidas conhecidas do ataque s1ngularity.”

JFrog alertou qualquer pessoa que tenha instalado um pacote comprometido por Shai-Hulud para assumir que os segredos foram exfiltrados.

Ele os instou a girar todos os tokens de acesso armazenados em uma máquina afetada que:

- Foram emitidos por um dos seguintes provedores – GitHub, npm, AWS, GCP, Azure
- Pode ser identificado por Porco Trufado