Pacote popular npm 'ctrl/tinycolor' com downloads semanais de 2m e mais

Data: 2025-09-16 06:17:18

Autor: Inteligência Against Invaders

O ecossistema do NPM está sob ataque mais uma vez, com uma sofisticada cadeia de suprimentos

comprometida com o objetivo do pacote @ctrl/tinycolor amplamente utilizado e mais de 40 outros

pacotes JavaScript.

Este último incidente representa uma escalada significativa nas ameaças da cadeia de suprimentos, com malware autopropagante que se espalha automaticamente pelo ecossistema.

Diagrama mostrando como os e-mails de phishing com URLs maliciosos ou anexos HTML levam a uma infecção por malware baseada em JavaScript no dispositivo de um usuário

O compromisso malicioso foi o primeiro descoberto pelo pesquisador de segurança@Franky47, que prontamente relatou a questão através de um alerta do GitHub.

O ataque direcionado às versões @ctrl/tinycolor 4.1.1 e 4.1.2, pacotes que recebem coletivamente mais de 2 milhões de downloads semanais de desenvolvedores em todo o mundo.

O que torna esse incidente particularmente perigoso é a capacidade do malware de propagar automaticamente para outros pacotes mantidos pelos mesmos autores ou acessíveis por meio de credenciais comprometidas.

O Socket.Dev forneceu uma análise técnica abrangente do ataque, revelando uma cadeia de infecção em vários estágios que demonstra a sofisticação.

Os pacotes comprometidos foram removidos do registro da NPM, mas os danos se estendem muito além do alvo inicial.

Malware autopropagante

O ataque emprega uma abordagem sofisticada de vários estágios que o diferencia dos compromissos típicos da cadeia de suprimentos.

Ao introduzir um curto período de espera antes de permitir novas dependências, as equipes podem reduzir sua exposição a novos ataques, mantendo suas dependências atualizadas.

O malware utiliza uma função chamadaNpmModule.updatePackagepara se espalhar automaticamente para pacotes adicionais sem intervenção manual. Esse recurso de autopropagação transforma um único compromisso de pacote em uma ameaça em todo o ecossistema em cascata.

Diagrama mostrando a propagação de malware por meio de sites comprometidos e ataques de phishing que afetam usuários e servidores

Os downloads e reaproveitados de código maliciosos e reaproveitados, uma ferramenta de varredura de segredos legítimos, para colheita de credenciais.

O malware tem como alvo sistematicamente tokens de autenticação NPM, tokens de acesso pessoal do github, chaves de acesso da AWS, Google Cloud Credenciais da plataforma e detalhes de autenticação do Azure.

Além disso, ele tenta acessar pontos de extremidade dos metadados em nuvem para extrair informações mais sensíveis.

Para manter a persistência, o ataque cria um arquivo de fluxo de trabalho de ações do GitHub malicioso em.github/workflows/shai-hulud-workflow.yml. Este fluxo de trabalho pode ser acionado remotamente para reasgar repositórios ou extrair dados adicionais muito após o compromisso inicial.

Impacto abrangente do pacote

O ataque afetou vários pacotes de alto nível em vários mantenedores. Além do @Ctrl/Tinycolor, os pacotes comprometidos incluem o angulararticts2 (versão 14.1.2), vários pacotes de namespace @ctrl, @nativescript-community pacotes e várias bibliotecas reagentes e angulares. A amplitude dos pacotes afetados demonstra a abordagem sistemática do ataque ao compromisso do ecossistema.

Cada pacote comprometido continha o arquivo malicioso Bundle.js com hash sha-25646faab8ab153fae6e80e7cca38eab363075bb524edd79e42269217a083628f09. Todas as credenciais colhidas e dados sensíveis foram exfiltrados parawebhook.site/bb8ca5f6-4175-45d2-b042-fc9ebb8170b7.

As organizações que usam quaisquer pacotes afetados devem tomar medidas imediatas. Primeiro, identifique e remova ou faça o downgrade de todos os pacotes comprometidos de ambientes de desenvolvimento e sistemas de produção.

Verifique a presença de arquivos maliciosos de fluxo de trabalho e audite as recentes atividades de publicação do NPM para modificações não autorizadas.

Vulnerabilidades da cadeia de suprimentos e vetores de ataque no processo de desenvolvimento de software visualizado em um infográfico detalhado pelo Atlantic Council

Todas as credenciais potencialmente expostas a ambientes comprometidos requerem rotação imediata. Isso inclui tokens npm, tokens de acesso pessoal do github, credenciais da AWS IAM, chaves da conta de serviço do Google Cloud e chaves Azure diretores de serviço.

Dada a natureza abrangente da colheita de credenciais, suponha que quaisquer segredos acessíveis aos sistemas afetados tenham sido comprometidos.

Soluções de segurança corporativa, como o StepSecurity, fornecem várias camadas de proteção contra tais ataques.

O pacote NPM Recooldown Check bloqueia automaticamente os pacotes lançados dentro de um

período de espera configurado, normalmente impedindo a adoção de pacotes recém -comprometidos antes que a detecção ocorra.

A corredora Harden-Runner do StephEcurity adiciona monitoramento de tempo de execução para Github Ações de fluxos de trabalho, fornecendo visibilidade em chamadas de rede e execuções de processos durante as execuções de CI/CD.

Seu monitor de artefato rastreia continuamente os lançamentos de pacotes para detectar publicações não autorizadas fora dos pipelines aprovados.

O incidente destaca as lacunas críticas nos atuais modelos de segurança do NPM e a necessidade de mecanismos aprimorados de proteção da cadeia de suprimentos.

Embora a ameaça imediata tenha sido contida através da remoção de pacotes, a natureza autopropagadora desse ataque representa uma evolução preocupante nas ameaças da cadeia de suprimentos que exigem atenção em todo o setor e estratégias defensivas aprimoradas.

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