Ataque a NPM

Data do ataque

8 de setembro de 2025 (ataque inicial detectado).

Tipo de ataque

Ataque de cadeia de suprimentos (supply chain) com injeção de malware em pacotes npm, combinado com phishing para comprometer contas de mantenedores.

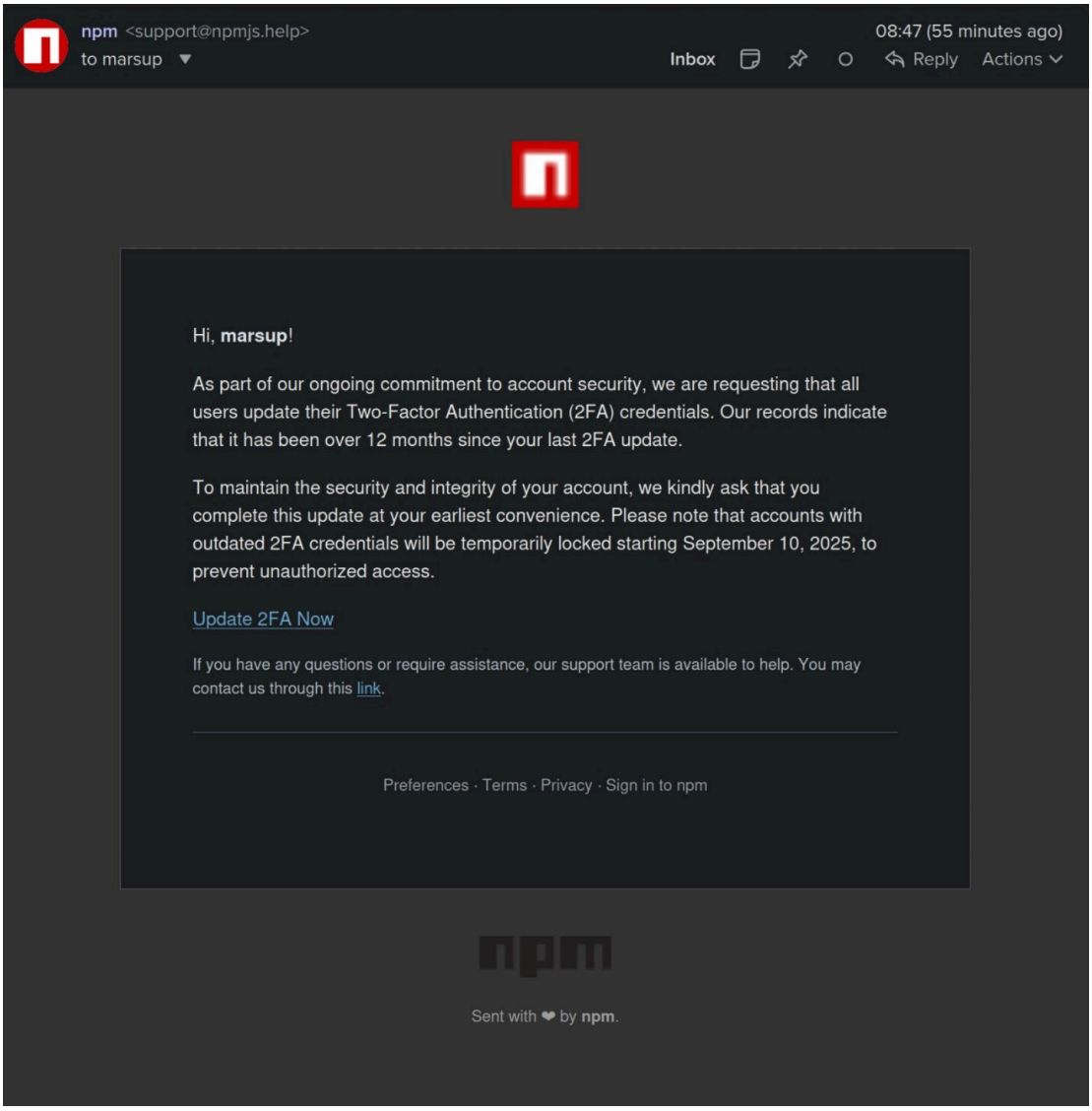
Descrição

O maior ataque a cadeida de suprimentos da história do npm, gerenciador de pacotes do JavaScript, comprometeu 18 pacotes fundamentais do JavaScript, como o chalk, debug e ansi-styles, que represetam mais de 2.6 bilhoẽs de downloands semanais.

Josh Junon, responsável por manter esses pacotes, teve sua conta npm comprometida através de um ataque de phishing em seu email.

O ataque iniciou quando Junon recebeu um e-mail fraudulento que ameaçava bloquear contas de mantenedores em 10 de setembro, solicitando atualização das credenciais 2FA para induzir o clique no link malicioso.

Nos e-mails, os invasores ameaçaram que as contas dos mantenedores visados seriam bloqueadas em 10 de setembro de 2025, como uma tática de intimidação para fazê-los clicar no link que os redirecionaria para os sites de phishing.



Ao clicar no link malicioso, os mantenedores foram redirecionados para uma página de phishing que roubou suas credenciais e tokens de autenticação.

Com o acesso às contas, os invasores publicaram versões maliciosas de alguns pacotes que totalizam 2,6 bilhões de downloads semanais. O código injetado era altamente ofuscado e atuava como um interceptador no navegador, projetado para:

- Monitorar transações de criptomoedas (Ethereum, Bitcoin, Solana, Tron, Litecoin e Bitcoin Cash).
- Substituir endereços de carteira legítimos por endereços controlados pelos invasores em tempo real.

O malware operava silenciosamente, alterando transações antes da assinatura pelo usuário, sem deixar sinais evidentes de comprometimento.

Vunerabilidade explorada

Engenharia social e phishing: Exploração da confiança ao se utilizar comunicações aparentemente legítimas.

Falha na autenticação de dois fatores (2FA): O 2FA foi contornado pois as vitimas forneceram voluntariamente os tokens no site de phishing.

Falta de verificações adicionais para publicações em pacotes críticos: A plataforma npm não exigia confirmações adicionais, como a aprovação de múltiplos colaboradores, para atualizações em pacotes de alto impacto.

Impactos e/ou prejuízo

- Pacotes com 2,6 bilhões de downloads semanais foram comprometidos, afetando milhares de aplicações em todo o mundo, desde startups até grandes empresas.
- Transações de criptomoedas foram redirecionadas para carteiras controladas pelos invasores. O prejuízo potencial é difícil de estimar pois não existem dados ainda sobre quais clientes foram afetados, mas pode chegar a milhões de dólares.
- Danos à confiança no ecossistema de código aberto: O incidente expõe a fragilidade de dependências críticas mantidas por voluntários, que são alvos frequentes de ataques.

Tipo de proteção que poderia ter sido aplicada

Treinamento contra phishing para mantenedores de projetos críticos.

Revisão por pares para atualizações em pacotes de alto impacto.

Integração de verificações automatizadas no pipeline de CI/CD para bloquear dependências maliciosas.

Fonte

https://www.bleepingcomputer.com/news/security/hackers-hijack-npm-packages-with-2-billion-weekly-downloads-in-supply-chain-attack/

https://sek.io/comunicado-emergencial-maior-ataque-a-cadeia-de-suprimentos-npm-da-historia-atinge-pacotes-com-26-bilhoes-de-downloads-semanais/

Ataque a Kaseya

Data do ataque

O ataque foi iniciado em 2 de julho de 2021.

Tipo do Ataque

Ataque de Cadeia de Suprimentos (Supply Chain) seguido de Ransomware.

Descrição

O grupo de ransomware REvil explorou uma vulnerabilidade zero-day no software de gerenciamento de TI da Kaseya, chamado Kaseya VSA (Virtual System/Server Administrator), programa que permite às empresa administrar redes de computadores.

Os atacantes comprometeram os servidores da Kaseya e usaram o mecanismo de atualização legítimo da empresa para distribuir uma versão maliciosa de um pacote de software para os clientes da Kaseya (que são principalmente MSPs - Provedores de Serviços Gerenciados). Quando os clientes instalaram a atualização, o ransomware foi implantado em suas redes e, subsequentemente, se espalhou para os sistemas de seus clientes (empresas finais). Estima-se que entre cerca de 1.500 empresas tenham sido afetadas indiretamente.

Vunerabilidade explorada

CVE-2021-30116: Vulnerabilidade de bypass de autenticação que permitia que um atacante não autenticado executasse comandos arbitrários no servidor VSA.

Como fuciona essa vunerabilidade:

- Quando um invasor baixa um cliente do Kaseya VSA é gerando em seu SO um Agent_Guid e AgentPassword.
- Com o Agente_Guid e AgentPassword o atacante podia fazer login no site que baixava o VSA e obtia um cookie sessionld que podia ser usada em ataque aos sitemas da empresa sem a necessidade de realizar autenticação.

Vunerabilidades encontradas:

- Página de download do VSA vaza credenciais sem necessidade de autenticação.
- Credencias do sofware podem ser usadadas para obter cookie que pode ser usados para outros serviços fora do objetivo do VSA
- As credenciais do VSA dava ao invasor acesso a informações para penetrar na instalação do Kaseya e em seus clientes.

Impactos e/ou prejuízo

Alcance em Cascata: O ataque não atingiu apenas a Kaseya, mas explodiu através de sua cadeia de suprimentos, afetando dezenas de seus clientes e, por sua vez, centenas de clientes das empresas clientes. Por exemplo: A rede de supermercados sueca Coop foi uma das vítimas indiretas do ciberataque. A empresa ficou alguns dias sem conseguir usar sua rede de caixas registradoras, já que a empresa para a qual terceirizou o serviço de informática, a Visma Esscom, foi vítima do ataque.

Paralisação de Negócios: Supermercados, escolas, creches e empresas de diversos setores em pelo menos 17 países tiveram suas operações paralisadas.

Demanda de Resgate Extorsivo: O grupo REvil inicialmente demandou um resgate de US$ 70 milhões em Bitcoin para fornecer o decryptor universal para todas as vítimas.

Custo Financeiro: A Kaseya estimou que os custos relacionados ao ataque foram de aproximadamente 6 a 8 milhões de doláres em gastos diretos com a resposta ao incidente, além dos danos incalculáveis à reputação e aos negócios dos clientes afetados.

Tipo de proteção que poderia ter sido aplicada

Segmentação de Rede Rigorosa: Isolar os servidores VSA da internet e de outras partes críticas da rede poderia ter contido o avanço do ataque.

Aplicação Imediata de Patches: A Kaseya estava ciente das vulnerabilidades e havia preparado um patch, que estava programado para ser lançado no fim de semana do

ataque. Um processo mais ágil de teste e implantação de patches críticos poderia ter fechado a janela de oportunidade.

Monitoramento de Comportamento de Rede: Ferramentas de detecção poderiam ter identificado a comunicação anômala dos servidores VSA com os servidores dos atacantes.

Princípio do Menor Privilégio: Restringir ao máximo as permissões dos sistemas e usuários para dificultar a movimentação lateral dos invasores.

Backups Imutáveis e Offline: Manter cópias de backups regulares que não possam ser alteradas ou criptografadas pelo ransomware, permitindo a recuperação sem pagar resgate.

Fonte

CVE

https://g1.globo.com/economia/tecnologia/noticia/2021/07/06/empresa-de-ti-vitima-de-ciberataque-nos-eua-calcula-que-outras-1500-companhias-foram-afetadas.ghtml

https://vaultone.com/pt-br/ataque-kaseya-entenda-tudo-sobre-o-incidente/

https://www.ksecurity.com.br/criminosos-exigem-pagamento-de-us-70-milhoes-apos-ataque-cibernetico-a-kaseya/

https://www.watchguard.com/br/wgrd-news/blog/msp-principais-vitimas-do-ataque-de-ransomware-kaseya