O APT41 vinculado à China tem como alvo governos, think tanks e acadêm

Data: 2025-09-17 20:54:18

Autor: Inteligência Against Invaders

O APT41 vinculado à China tem como alvo governos, think tanks e acadêmicos vinculados ao comércio e à política EUA-China

O grupo APT41, ligado à China, se passou por um legislador dos EUA em ataques de phishing ao governo, think tanks e acadêmicos ligados ao comércio e à política EUA-China.

A Proofpoint observou o grupo de espionagem cibernética APT41 ligado à China se passando por um legislador dos EUA em uma campanha de phishing direcionada ao governo, think tanks e acadêmicos ligados ao comércio e à política EUA-China.

APT41, conhecido também como ameba, bário, atlas de bronze, exportação de bronze, mosca negra, tufão de bronze, terra Baku, G0044, G0096, Grayfly, HOODOO, CHUMBO, Kelpie vermelho, TA415,PANDA PERVERSOe WICKED SPIDER originário da China (com possíveis laços com o governo), é conhecido por suas campanhas complexas e variedade de setores-alvo, sua motivação varia de exfiltração de dados sensatos a ganhos financeiros.

“Ao longo de julho e agosto de 2025, o TA415 conduziu campanhas de spearphishing direcionadas ao governo dos Estados Unidos, think tank e organizações acadêmicas utilizando iscas com temas econômicos EUA-China.” diz o relatório *publicado pela Proofpoint. “Nesta atividade, o grupo se disfarçou como o atual presidente do Comitê Seleto de Competição Estratégica entre os Estados Unidos e o Partido Comunista Chinês (PCC), bem como o Conselho Empresarial EUA-China, para atingir uma série de indivíduos e organizações predominantemente focados nas relações, comércio e política econômica EUA-China.”*

O TA415 executa campanhas de phishing que usam túneis remotos do VS Code e serviços legítimos como Planilhas Google e Agenda para obter acesso remoto persistente. Ao combinar com o tráfego normal, os invasores evitam a detecção. Essas operações visam coletar informações sobre as relações econômicas EUA-China em meio às negociações comerciais em andamento, refletindo o foco do TA415 no monitoramento de políticas e desenvolvimentos econômicos.

Em julho e agosto de 2025, o TA415 lançou ataques de phishing se passando pelo representante dos EUA John Moolenaar, presidente do Comitê Seleto de Competição Estratégica com a China. Eles criaram e-mails convincentes usando informações de código aberto, pedindo aos alvos que revisassem projetos de legislação falsos sobre sanções contra a China. Os e-mails incluíam links para arquivos protegidos por senha hospedados em serviços em nuvem como Zoho e Dropbox, enquanto o grupo mascarava sua atividade com o Cloudflare WARP VPN.

O arquivo protegido por senha contém um LNK que é executado logon.bat a partir de um arquivo

oculto *MACOS* e mostra um PDF corrompido como isca. O lote inicia um carregador Python incorporado (WhirlCoil) via pythonw.exe. O WhirlCoil instala a CLI do VSCode em %LOCALAPPDATA%MicrosoftVSCode, verifica os direitos de administrador e cria uma tarefa agendada para manter a persistência (por exemplo, GoogleUpdate). O script WhirlCoil é executado code.exe tunnel user login --provider github --name , salva o código de verificação, coleta informações do sistema e arquivos do usuário e, em seguida, exfiltra tudo para um serviço gratuito de registro de solicitações. Com o código de verificação, os invasores autenticam remotamente o túnel remoto do VS Code para acessar o sistema de arquivos e o terminal do host.

As acusações dos EUA dizem que o TA415 opera em Chengdu como Chengdu 404 Network Technology, um empreiteiro privado vinculado ao ecossistema de ciberespionagem da China. O grupo trabalhou com outros empreiteiros como i-Soon, e alguns membros alegaram ligações com o Ministério da Segurança do Estado. A Proofpoint atribui a atividade recente e histórica de backdoor da Voldemort ao TA415 com alta confiança com base em sobreposições de infraestrutura, táticas e direcionamentos que se alinham com os interesses do estado chinês.

“muitas das entidades visadas são consistentes com as prioridades conhecidas de coleta de inteligência chinesa. No entanto, o momento do pivô do TA415 em direção a esses alvos é particularmente notável, dada a complexa evolução contínua das relações econômicas e de política externa entre a China e os Estados Unidos”, conclui o relatório.

Siga-me no Twitter:@securityaffairseLinkedineMastodonte

PierluigiPaganini

(Assuntos de Segurança–hacking,APT41)