Mobile Phishers direciona clientes de corretagem no esquema de caixa 'ra

Data: 2025-08-19 18:18:30

Autor: Inteligência Against Invaders

Grupos cibercriminais especializados em kits avançados de phishing móvel desenvolveram suas

operações além de roubar dados do cartão de pagamento para a inscrição em carteira móvel, agora

girando para explorar contas de corretagem em esquemas sofisticados de ‘rampa e dump’.

Essa mudança, conforme detalhada em pesquisas recentes de especialistas em segurança, aproveita as credenciais do usuário para manipular os preços das ações estrangeiras, contornando os controles de segurança tradicionais que impedem transferências diretas de fundos.

Diferentemente das fraudes convencionais de bomba e despejo que dependem do hype das mídias sociais para aumentar os valores de estoque de centavos, as operações de rampa e despejo usam negociações coordenadas em várias contas seqüestradas para aumentar artificialmente os preços das ações sem promoção externa.

Evolução das táticas de phishing

De acordo com a Krebson Security, uma vez que as ações direcionadas atinjam um limiar predeterminado, os autores vendem participações, deixando investidores legítimos com ativos desvalorizados e perdas substanciais.

A Autoridade Reguladora da Indústria Financeira (FINRA) emitiu avisos destacando como essa manipulação decorre de negociações controladas por atores maliciosos, resultando em colapsos do preço das ações catastróficas que refletem os golpes tradicionais, mas operam através da dinâmica interna do mercado.

A Ford Merrill, pesquisadora de segurança da Secalliance, acompanhou essa atividade às comunidades de telegrama em língua chinesa, vendendo abertamente essas ferramentas de phishing.

Esses kits, refinados nos últimos três anos, permitem que os invasores se preponham em ações de baixa liquidez, como ofertas públicas iniciais chinesas (IPOs) ou estoques de centavos, liquidando as posições existentes das vítimas e os fundos reais.

Os autores coordenam as compras cronometradas em contas phished para aumentar os preços e depois despejar ações com lucro.

Este método explora vulnerabilidades na corretora Autenticação multifatorial (MFA) Sistemas, particularmente aqueles que dependem de códigos de senha (OTPs) Phishable (OTPs) entregues por SMS ou chamadas automatizadas.

Por exemplo, plataformas como Schwab e Fidelity oferecem opções de OTP que podem ser interceptadas durante os ataques de phishing, onde as vítimas são atraídas por meio de mensagens falsificadas que reivindicam a suspensão da conta e solicitadas a inserir credenciais e códigos de verificação.

Mesmo as notificações push baseadas em aplicativos permanecem suscetíveis se os invasores iniciarem logins com dados roubados, levando a aprovação dos usuários.

Fundamentos técnicos

Os kits de phishing, frequentemente demonstrados em vídeos de fornecedores no Telegram, incluem modelos personalizáveis imitando grandes corretoras, enviadas pelo IMessage da Apple ou pelo RCS do Google por maior legitimidade.

Um fornecedor notável, conhecido como “Outsider” (anteriormente “Chenlun”), fornece kits que colhem nomes de usuário, senhas e OTPs, adaptando -se facilmente a alvos como Schwab, enquanto expansíveis para outras pessoas.

Isso se baseia em ondas de phishing anteriores de 2022-2024, que falsificaram entidades como o Serviço Postal dos EUA para inscrever cartões em carteiras móveis usando OTPs phished.

À medida que as instituições financeiras reforçavam o provisionamento de carteira, exigindo fraudadores de inscrição baseados em aplicativos, redireciam os esforços para corretoras com MFA mais fraco, como as opções de Schwab para SMS, chamadas ou notificações de aplicativos, todas vulneráveis a Engenharia Social.

Merrill Notas A ingenuidade do esquema na dissociação de traços de fraude: os atacantes podem comprar ações em trocas chinesas legítimas, beneficiando-se da inflação de preços impulsionada por contas comprometidas com sede nos EUA sem vínculos diretos.

A coordenação pode envolver contas de phishing em tempo real ou pré-armazenadas, suportadas por operadores humanos que gerenciam bancos de dispositivos para distribuição de isca e captura de OTP.

Inteligência artificial, incluindo grandes modelos de idiomas, acelera o desenvolvimento de kits, reduzindo as barreiras para criminosos cibernéticos e permitir iterações rápidas.

Enquanto algumas corretoras como a Vanguard oferecem alternativas robustas, como as teclas de hardware do 2º fator universal (U2F) que resistem ao phishing, exigindo lags de adoção generalizada de interação física.

O pedido de fevereiro de 2025 do FBI para as informações da vítima ressalta a escala do esquema, com a FINRA enfatizando ameaças em todo o setor.

A mitigação requer a mudança para o MFA não fisicável, o monitoramento aprimorado de transações para padrões anômalos e a educação do usuário em vetores emergentes de fraude.

À medida que os ecossistemas de phishing amadurecem, a integração de defesas orientadas pela IA e supervisão regulatória será crucial para combater essas ameaças adaptativas, impedindo uma erosão de confiança nos mercados financeiros.

Encontre esta notícia interessante! Siga -nosGoogle NewsAssim,LinkedIneXPara obter atualizações instantâneas!