Microsoft derruba mais de 300 sites atrás do Raccoono365 Phishing Sche

Data: 2025-09-17 09:22:49

Autor: Inteligência Against Invaders

A Unidade de Crimes Digitais (DCU) da Microsoft assumiu o controle de 338 sites que facilitam o

Raccoono365, a plataforma de phishing-como como serviço em rápida expansão que permite que

qualquer pessoa colhe as credenciais da Microsoft 365.

Atuando sob uma ordem judicial do Distrito Sul de Nova York, a DCU interrompeu a infraestrutura técnica da operação, negando o acesso dos cibercriminosos às vítimas e cortando seus fluxos de receita.

Essa ação ressalta como os kits de phishing baseados em assinatura prontamente disponíveis reduziram a barreira à entrada do cibercrime, colocando milhões de usuários em todo o mundo em risco aumentado.

Rastreado por Microsoft Como Storm-2246, o Raccoono365 oferece assinaturas em camadas, permitindo que os usuários-independentemente da experiência técnica-lançem ataques de phishing em larga escala.

Desde julho de 2024, seus clientes roubaram pelo menos 5.000 credenciais da Microsoft em 94 países. Apesar de muitos roubos de credenciais mitigados por recursos de segurança internos, o volume de ataques bem-sucedidos destaca a potência duradoura da engenharia social.

Em uma extensa campanha com temas fiscais, os invasores personificaram as autoridades fiscais oficiais a prender as metas e se infiltraram em mais de 2.300 organizações nos Estados Unidos.

Surpreendentemente, pelo menos 20 entidades de saúde dos EUA foram vítimas dessas campanhas, comprometendo o atendimento ao paciente, atrasando os serviços, corrompendo os resultados do laboratório e expondo dados sensíveis à saúde – os artigos que poderiam se traduzir em custos financeiros e humanos significativos.

Sofisticação técnica

Recurso rápido do Raccoono365 lançamentos acompanharam o ritmo da demanda do cliente. O serviço agora acomoda até 9.000 endereços-alvo por dia e inclui ferramentas para contornar os controles de autenticação de vários fatores, permitindo o acesso persistente assim que as credenciais forem capturadas.

A mais recente oferta da plataforma, a AI-Mailcheck, aproveita a IA generativa para criar e-mails mais convincentes em escala, ampliando ainda mais seu potencial de ameaça.

Os clientes podem escolher entre vários níveis de assinatura, cada um concedendo acesso a modelos de e -mail de phishing de marca, portais de login falsificados e sistemas de entrega automatizados.

A base desta operação é um canal de suporte simplificado hospedado no Telegram, onde mais de 850 membros se envolveram e pagaram pelo menos US $ 100.000 em criptomoeda – o suficiente para alimentar centenas de milhões de mensagens de phishing anualmente.

As investigações levaram os analistas da DCU ao desenvolvedor da Nigéria, Joshua Ogundipe, que escreveu a maior parte do código do Raccoono365 e registros de domínio orquestrados usando identidades fictícias.

Um deslize de segurança operacional – expondo um segredo criptomoeda Wallet – Microsoft habilitada para atribuir e rastrear fundos ilícitos.

Com uma indicação criminal agora enviada à aplicação da lei internacional, Ogundipe e seus associados enfrentam ações legais destinadas a desmantelar infraestrutura atual e futura.

A interrupção da Microsoft do Raccoono365 demonstra a eficácia de combinar autoridade legal com contramedidas técnicas.

Colaborando com o Cloudflare e a Health-ISAC, uma organização sem fins lucrativos focada na segurança cibernética da saúde, o DCU garantiu quedas e a inteligência compartilhada para proteger os setores críticos.

Para reforçar as investigações, a Microsoft está integrando Blockchain Ferramentas de análise, como reator de cadeia, aumentando sua capacidade de rastrear recursos criminais e construir evidências contra autores.

Fortalecimento das defesas

À medida que o cibercrime evolui, as ações legais são insuficientes. Os governos devem harmonizar as leis, acelerar processos transfronteiriços e próximos lacunas regulatórias que os cibercriminosos exploram.

Enquanto isso, organizações e indivíduos devem permanecer vigilantes, aplicando fortes autenticação de vários fatores, implantando soluções anti-phishing atualizadas e educando os usuários sobre táticas de ameaças emergentes.

Esta operação exemplifica o poder da cooperação multissetorial: empresas de tecnologia, fornecedores de segurança, organizações sem fins lucrativos e aplicação da lei que trabalham em concerto podem desmontar redes criminais sofisticadas.

Ao sustentar essas parcerias e avançar as iniciativas conjuntas, a comunidade global pode criar resiliência contra a próxima geração de ameaças cibernéticas acessíveis e aprimoradas.

Encontre esta história interessante! Siga -nosLinkedIneXPara obter mais atualizações instantâneas.