Eles estão oferecendo € 55.000 para acesso à sua conta do escritório. O q

Data: 2025-10-03 10:12:23

Autor: Inteligência Against Invaders

Redazione RHC**:3 Outubro 2025 11:54**

Jornalista da BBC Joe Tidy encontrou-se em uma situação geralmente escondida nas sombras do crime cibernético. Em julho, **ele recebeu uma mensagem inesperada no aplicativo de mensagens Signal** de uma pessoa desconhecida que se identificou como ” **Sindicato** .”

A pessoa se ofereceu para participar de um esquema criminoso: **se Tidy desistisse do acesso ao seu computador, ele receberia uma parte do resgate exigido pela empresa** . Inicialmente, a oferta era *15% do valor disponível, mas depois aumentou para 25%, com a promessa de que este “negócio” seria suficiente para viver confortavelmente.*

Os criminosos explicaram seu interesse na colaboração **citando os benefícios que receberam no passado de acordos semelhantes.** O sindicato, que até mudou de nome durante as comunicações, afirmou que *Os funcionários da empresa geralmente concordam em ajudar os hackers.*

Eles citaram como evidência ataques a **uma organização de saúde britânica e uma agência americana de serviços de emergência.** Além disso, poucos dias antes, um especialista em TI havia sido preso no Brasil por vender suas credenciais a hackers. De acordo com a polícia, *O banco sofreu perdas de aproximadamente US$ 100 milhões, uma história que reforçou o senso de urgência.*

A fonte se identificou como um **“gerente de comunicações” do grupo Medusa** , conhecida como uma das organizações mais ativas que operam sob o modelo “ransomware-as-a-service”. Qualquer criminoso afiliado pode usar a plataforma Medusa para ataques. De acordo com a CheckPoint, o núcleo do grupo opera a partir da Rússia ou de países aliados e evita ataques dentro da CEI. *concentrando-se em empresas estrangeiras.* Em um anúncio oficial, as autoridades dos EUA informaram que **A Medusa atacou mais de 300 organizações em quatro anos. O site darknet do grupo lista dezenas de empresas afetadas, mas seus nomes foram redigidos.**

Durante as negociações, o Sindicato continuou a aumentar a pressão. Eles alegaram **sabem que os salários na BBC não eram particularmente altos** e ofereceu a *“aposentar-se nas Bahamas”* após um hack bem-sucedido. Como um *“garantia de honestidade”,* **os hackers prometeram um depósito de 0,5 Bitcoin, aproximadamente US$ 55.000.**

Eles solicitaram um login, um código de autenticação de dois fatores e até enviaram um trecho de código complexo com a solicitação para executá-lo em um laptop da empresa e relatar os resultados. Isso permitiria que eles avaliassem seu nível de acesso e planejassem novas

intervenções na infraestrutura.

Sindicato **insistiu que a conversa fosse transferida para Tox,** um mensageiro usado ativamente por cibercriminosos e postou links para páginas do Medusa em fóruns fechados.

Quando o jornalista, consultando colegas, começou a ganhar tempo, a outra pessoa perdeu a paciência. Ele estabeleceu um prazo e logo mudou para uma tática diferente. **O telefone de Tidy foi bombardeado com notificações pop-up pedindo que ele confirmasse o acesso à sua conta na BBC.** Este método é conhecido como **Bombardeio MFA:** a vítima recebe dezenas ou centenas de notificações push e *pode eventualmente tocar em "confirmar", acidentalmente ou por cansaço.* O Uber foi hackeado de maneira semelhante em 2022, por exemplo.

Tidy não respondeu e entrou em contato com urgência com a equipe de segurança cibernética da BBC. Para mitigar o risco, ele foi temporariamente desconectado dos sistemas da empresa: sem e-mail, sem serviços internos, sem ferramentas de login. Naquela mesma noite, uma mensagem inesperadamente calma do Syndicate pediu desculpas: *"A equipe pede desculpas. Estávamos testando a página de login da BBC e pedimos desculpas se isso causou algum problema."* Apesar da pressão, o hacker continuou a oferecer um acordo, mas não recebendo resposta, ele excluiu sua conta do Signal e desapareceu.

O acesso do jornalista aos sistemas foi posteriormente restaurado e a segurança de sua conta foi reforçada. Essa experiência demonstrou **que as ameaças reais vêm não apenas de ataques técnicos sofisticados, mas também de ataques direcionados a funcionários.**

Mesmo aqueles sem direitos privilegiados na rede corporativa podem ser alvos de recrutamento. A história de Tidy se tornou um exemplo claro de como crimiOs grupos NAIS usam uma combinação de promessas, manipulação e técnicas para contornar a segurança interna e forçar as organizações a pagar um resgate.

Redação
A equipe editorial da Red Hot Cyber é composta por um grupo de indivíduos e fontes anônimas que colaboram ativamente para fornecer informações e notícias antecipadas sobre segurança cibernética e computação em geral.

Lista degli articoli