O Google pede que os usuários de 2,5b do Gmail redefinam as senhas após

Data: 2025-08-30 12:50:41

Autor: Inteligência Against Invaders

Uma operação sofisticada de phishing de voz emergiu como uma ameaça significativa para organizações em todo o mundo, com os cibercriminosos infiltrando com sucesso ambientes de vendas para roubar dados confidenciais e exigir pagamentos de resgate.

O grupo de inteligência de ameaças do Google identificou esta campanha motivada financeiramente, designando o cluster de ameaças primárias como [UNC6040](#) que demonstrou sucesso alarmante na violação de redes corporativas por meio de ataques de engenharia social baseados em telefone.

Voice Phishing alvo de TI Suporte

O grupo cibercriminal UNC6040 aperfeiçoou uma estratégia enganosa que envolve a representação [Apoia](#) Pessoal durante telefonemas para funcionários desavisados.

Esses atacantes visam principalmente ramos de língua inglesa de corporações multinacionais, explorando os funcionários da confiança que colocam em aparente equipe de suporte técnico.

Durante essas chamadas fraudulentas, os criminosos orientam as vítimas através de um processo que parece legítimo, mas na verdade concede acesso não autorizado às instâncias do Salesforce de sua organização.

- **Autorização de aplicativos maliciosos:** Os invasores direcionam as vítimas para a página de configuração do aplicativo conectada do Salesforce para aprovar aplicativos falsos de carregador de dados.
- **Ferramentas modificadas:** Os criminosos usam versões alteradas do software legítimo do Salesforce Data Loader com nomes ou marcas diferentes.
- **Acesso extensivo:** Uma vez autorizado, esses aplicativos maliciosos fornecem amplos recursos para acessar, consultar e roubar dados organizacionais.
- **Exploração de confiança:** O esquema depende da confiança inerente dos funcionários em aparente pessoal de apoio de TI.

A metodologia dos atacantes centra -se em manipular as vítimas para autorizar aplicativos conectados maliciosos em seus portais do Salesforce.

Eles conseguem isso direcionando os funcionários para a página de configuração de aplicativos conectados do Salesforce e instruindo -os a aprovar o que parece ser um aplicativo legítimo do carregador de dados.

No entanto, esse aplicativo é na verdade uma versão modificada controlada pelos atores de

ameaças, com nomes diferentes ou marcas para evitar a detecção.

Uma vez autorizado, este aplicativo malicioso fornece aos criminosos extensos recursos para acessar, consultar e roubar dados organizacionais sensíveis diretamente dos ambientes comprometidos do Salesforce.

A própria instância corporativa do Salesforce do Google foi vítima de atividades semelhantes da UNC6040 em junho, afetando as informações de contato para pequenas e médias empresas.

Enquanto a empresa respondeu rapidamente e limitou a violação às informações básicas dos negócios, o incidente demonstra o amplo alcance e a eficácia da campanha contra organizações conscientes da segurança.

Após a exfiltração de dados bem-sucedidos, um grupo de ameaças secundário designado pela UNC6240 inicia atividades de extorsão, às vezes aguardando vários meses antes de fazer contato com as vítimas.

Essas tentativas de extorsão geralmente envolvem comunicação direta com os funcionários da organização direcionada, exigindo pagamentos de Bitcoin dentro de 72 horas de prazos.

Os extorsistas reivindicam consistentemente a afiliação ao notório grupo de hackers Shinyhunters, provavelmente como uma tática psicológica para aumentar a pressão sobre suas vítimas.

Google Intelligence [Relatórios](#) Sugira que esses atores de ameaças possam estar se preparando para escalar suas táticas lançando um site de vazamento de dados, que forneceria uma plataforma para liberar publicamente informações roubadas se as demandas de resgate não forem atendidas.

Esse desenvolvimento representa uma escalada significativa nas capacidades do grupo e demonstra seu compromisso de monetizar dados roubados através de vários pontos de pressão.

Fortalecer protocolos de segurança do Salesforce

Especialistas em segurança enfatizam que a defesa contra esses sofisticados ataques de engenharia social requer a implementação de estratégias abrangentes de proteção.

As organizações devem aderir estritamente ao princípio do menor privilégio, principalmente para ferramentas de acesso a dados como o carregador de dados, o que requer a permissão “ativada pela API” para a funcionalidade total.

Essa permissão poderosa permite amplos recursos de exportação de dados e deve ser cuidadosamente controlada e auditada regularmente.

As medidas críticas de segurança incluem gerenciamento rigoroso de aplicativos conectados, com as organizações que precisam controlar como aplicativos externos interagem com seus [Ambientes Salesforce](#).

O pessoal administrativo deve restringir permissões poderosas, como “Personalizar aplicativos” e “Gerenciar aplicativos conectados” apenas para pessoal confiável essencial.

Além disso, a implementação de restrições de acesso baseada em IP pode combater tentativas de

acesso não autorizadas de VPNs comerciais comumente usadas por esses atores de ameaças.

A campanha destaca a natureza em evolução do crime cibernético, onde as medidas de segurança tradicionais devem ser complementadas por educação abrangente do usuário e sistemas de monitoramento robustos para detectar padrões anômalos de acesso a dados e instalações de aplicativos não autorizados.

Encontre esta notícia interessante! Siga -nos [Google News](#) Assim, [LinkedIn](#) [X](#) Para obter atualizações instantâneas!