Os atores de ameaças imitam marcas populares em novas campanhas de

Data: 2025-10-03 09:09:32

Autor: Inteligência Against Invaders

Em um ressurgimento sofisticado de campanhas de smishing, os cibercriminosos começaram a

incorporar nomes de marcas confiáveis ??em URLs enganosos e tópicos de mensagens em grupo

para atrair usuários desavisados ??a baixar malware.

Ao inserir um nome familiar de empresa antes do símbolo “@” nos links, os invasores exploram a confiança dos usuários em entidades estabelecidas como FedEx e Microsoft.

Juntamente com nomes de host de envelhecimento enganosamente e textos de grupo orquestrados, essa tática levou a um aumento em infecções bem -sucedidas no mês passado.

Os invasores criam URLs que parecem superficialmente legítimos, colocando o nome de uma marca bem conhecida imediatamente antes de um símbolo “@”, seguido por um domínio não afiliado.

Na realidade, o verdadeiro domínio – “Soogb[.]Xin ” – Hosts cargas úteis maliciosas. As vítimas que clicam nesses links são redirecionadas para baixar aplicativos ou instaladores trojanizados que instalam secretamente backdoors e colheitadeiras de credenciais.

Vários golpes de texto recentes em grupo têm endereçado Essa técnica enviando mensagens simultâneas para vários destinatários sob o disfarce de um atraso generalizado de remessa ou uma atualização de serviço urgente.

Os destinatários veem os números de telefone deles e de outras pessoas listados no tópico do grupo, conferindo um falso senso de legitimidade.

Um desses threads pretendemos ser “FedEx® Ground reageMule sua entrega de remessa”, pedindo aos usuários que cliquem em um link de rastreamento e confirme as datas de entrega remarcadas. Em vez disso, o link desencadeou o download de um Trojan de acesso remoto.

Nomes de host estrategicamente envelhecidos

Além da manipulação da URL, os atores de ameaças estão registrando nomes de domínio meses antecipadamente para contornar as defesas baseadas em reputação.

Esses nomes de host envelhecidos, às vezes registrados seis a oito meses antes do seu primeiro uso, parecem mais credíveis para filtros de spam e plataformas de proteção de terminais.

Ao encenar sua infraestrutura, os operadores garantem que, quando lançem a campanha, os domínios amadureceram o suficiente para evitar quedas automatizadas ou sinalização.

Em várias instâncias, os invasores usaram recursos de protocolo RCS (Rich Communication Services) para aprimorar a apresentação de mensagens em dispositivos Android, exibindo logotipos da empresa e interfaces de usuário higienizadas imitando aplicativos oficiais.

Os IDs do remetente do SMS são falsificados para refletir números corporativos genuínos, diminuindo ainda mais a suspeita entre os destinatários.

Mitigações

Depois que os usuários seguem o URL enganoso, eles são solicitados a baixar um instalador Android APK ou Windows, disfarçando como um aplicativo de confirmação de envio ou utilitário de suporte ao cliente.

Nos bastidores, esses instaladores implantam keyloggers e ferramentas de acesso remoto, como Orcus Rat e Cerberus Malware Androidcapaz de exfiltrar mensagens SMS, tokens de autenticação e listas de contatos.

A análise precoce indica que algumas cargas úteis também incluem módulos para interceptar códigos de autenticação de dois fatores e propagação através das listas de contatos das vítimas por meio de convites automáticos de mensagens em grupo.

Para se defender contra essa ameaça emergente, organizações e indivíduos devem:
Adote soluções de segurança móvel que executam profundamente Análise de URLincluindo detecção de “@”-ofuscation em estilo em links.
Implementar regras de filtragem de rede para bloquear o acesso a domínios recém -criados ou usados ??com pouca frequência.
Eduque os usuários sobre os indicadores sutis de URLs maliciosos, enfatizando que as mensagens legítimas nunca serão redirecionadas através de domínios não-marca.

À medida que esta campanha evolui, as equipes de segurança devem monitorar os indicadores de compromisso relacionados a esses links inteligentemente formatados e padrões de mensagens em grupo.

Bloquear nomes suspeitos de host no nível DNS e reforçar a filtragem de gateway SMS com feeds de inteligência de ameaças pode reduzir significativamente a exposição. A colaboração com transportadoras móveis para autenticar IDs do remetente e uma remoção rápida de infraestrutura maliciosa será fundamental para conter a maré desses ataques enganosos.