Alerta de Trojan DeliveryRAT: Hackers Roubam Dados e Dinheiro com Apl

Data: 2025-09-16 09:14:02

Autor: Inteligência Against Invaders

Redazione RHC**:16 setembro 2025 10:36**

Os especialistas da F6 e da RuStore relatam ter **Descobriu e bloqueou 604 domínios** que faziam parte da infraestrutura de hackers que infectaram dispositivos móveis com o **EntregaRAT** Troiano. O malware disfarçado de **Aplicativos de entrega de comida**, mercados, serviços bancários e serviços de rastreamento de pacotes.

No verão de 2024, os analistas da F6 descobriram um novo Trojan Android, chamado DeliveryRAT. Sua principal tarefa era *coletar dados confidenciais para processamento de empréstimos em organizações de microfinanças, bem como roubar dinheiro por meio de serviços bancários online.*

Posteriormente, foi descoberto o bot Telegram da equipe Bonvi, no qual o DeliveryRAT foi distribuído usando o **MaaS (Malware-as-a-Service)** esquema. Descobriu-se que, por meio do bot, os invasores *receberam uma amostra grátis do Trojan, após o que eles próprios tiveram que entregá-lo ao dispositivo da vítima.*

Os proprietários do bot ofereceram duas opções: *baixe o APK compilado ou obtenha um link para um site falso,* supostamente gerado separadamente para cada trabalhador.

Os dispositivos das vítimas foram infectados usando vários cenários comuns. *“Para atacar a vítima, os invasores usaram vários cenários engenhosos: eles criaram anúncios falsos de compra e venda ou anúncios de emprego remotos falsos com um salário alto”,* diz Evgeny Egorov, analista sênior do Departamento de Proteção de Riscos Digitais da F6. *“Em seguida, a conversa com a vítima é transferida para serviços de mensagens e a vítima é persuadida a instalar um aplicativo móvel, que acaba sendo malicioso.”*

Os invasores criam anúncios com produtos com desconto em marketplaces ou em lojas falsas. Fazendo-se passar por vendedor ou gerente, os criminosos entram em contato com a vítima via Telegram ou WhatsApp e, durante a conversa, **A vítima fornece seus dados pessoais (nome completo do destinatário, endereço de entrega do pedido e número de telefone).** Para rastrear o pedido falso, o operador pede para **Baixe um aplicativo malicioso.**

Os hackers também criam **anúncios de emprego remotos falsos com condições favoráveis e um bom salário.** A comunicação com a vítima também é transferida para *serviços de mensagens, onde eles coletam seus dados pela primeira vez: SNILS, número do cartão de crédito, número de telefone e data de nascimento.* Em seguida, os golpistas pedem para instalar um aplicativo malicioso, supostamente necessário para o trabalho.

Além disso, especialistas detectaram **a distribuição de postagens publicitárias no Telegram** Convidando pessoas a baixar um aplicativo infectado com **EntregaRAT**. Nesse caso, o malware geralmente era disfarçado como **aplicativos com descontos e códigos promocionais.**

O relatório enfatiza que *esse esquema fraudulento é generalizado porque a criação de links gerados em bots do Telegram não requer nenhum conhecimento técnico especial.* Os pesquisadores também afirmam que a principal característica do esquema é *o alto grau de automação de processos.*

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