Golpe usa boletos falsos para espalhar malware e roubar dados de brasileiros[1]

Os brasileiros precisam ficar atentos na hora de abrir e-mails. A Unit 42, uma unidade de pesquisa da Palo Alto Networks, identificou uma campanha de spam que usa boletos falsos para distribuir malware e roubar dados da vítima.

O golpe já foi responsável pela distribuição de mais de 260 mil e-mails desde junho de 2017 e as mensagens continham títulos como "***Envio de Boleto – URGENTE***". No conteúdo dos e-mails tem um hiperlink ou um arquivo PDF disfarçado que cria a conexão entre o computador da vítima e um servidor usado pelos criminosos.

Ao clicar, é iniciado o download de um malware do tipo Trojan, sendo que os hosts do Windows infectados por esta campanha geram tráfego de texto simples em IRC (protocolo de comunicação utilizado para chats, bate-papo, e troca de arquivo).

No caso dos anexos PDF, eles não têm exploits, mas incluem um link com a mensagem "***Ocorreu um erro inesperado. Clique para abrir o arquivo PDF***", como o link no corpo do e-mail que direciona para uma URL que instala o malware.

A orientação para evitar cair nesse tipo de golpe é não clicar em links ou baixar arquivos suspeitos, principalmente quando enviados por desconhecidos. Além disso, instale uma antivírus e mantenha-o atualizado.

[1] Juliana Américo 07/12/2017 16h57 malware Spam