Operação Boiúna

Agosto, 2017

Linha do Tempo:

1. Encerramento do Contrato:
   Data: 01/04/2017
   O banco FakeBank encerrou seu contrato com a Wicked S.A., optando por contratar uma empresa concorrente para desenvolver terminais de pagamento.

2. Início de desenvolvimento do Ransomware:
   Data:17/04/2017
   O time de inteligência competitiva iniciou o desenvolvimento de um protótipo de ransomware.

3. Desenvolvimento do Ransomware "Boiúna":
   Data: 02/07/2017
   O desenvolvimento do protótipo de ransomware, posteriormente apelidado de "Boiúna", foi concluído. O time de inteligência competitiva começou a procurar por um alvo a ser usado como prova de conceito para a eficácia do protótipo.

4. Colaboração com Operadores de Ransomware:
   Data: 09/07/2017
   A Wicked S.A. estabeleceu uma colaboração com um grupo de operadores de ransomware, referidos adiante como “equipe operacional”, para disseminação do "Boiúna".

5. Identificação do ponto de acesso
   Data: 11/08/2017
   O time de inteligência competitiva identificou um acesso RDP com credenciais fracas em um dos dispositivos da FakeBank que pode ser usado como ponto de partida do ataque.

6. Extração de Informações do FakeBank:
   Data: 13/08/2017
   A equipe operacional utilizou o "Boiúna" para extrair informações confidenciais do FakeBank, incluindo dados financeiros, registros de clientes e estratégias internas.

7. Criptografia dos Dados:
   Data: 14/08/2017
   A equipe operacional iniciou a fase de criptografia dos dados sensíveis, tornando-os inacessíveis para o FakeBank.

8. Pedido de Resgate:

Data: 16/08/2017
Foi enviado um pedido de resgate ao FakeBank, informando sobre os dados criptografados e as instruções para o pagamento por meio de Bitcoins.

9. Pagamento
   Data: 18/08/2017
   Após o pagamento de US$ 7.2 milhões em Bitcoin, as chaves de criptografia foram enviadas para o time de resposta a incidentes do FakeBank.

Justificativa do Ataque:

O ataque foi realizado como uma prova de conceito para evidenciar as possíveis consequências do encerramento do contrato pelo FakeBank e a contratação de uma empresa concorrente. O "Boiúna" foi utilizado como uma ferramenta para demonstrar a importância da segurança cibernética e para destacar as vulnerabilidades nos sistemas do FakeBank.

DISCLAIMER

Este relatório é fictício e faz parte de um cenário simulado para fins de treinamento no CTF. Todas as ações mencionadas são parte de uma narrativa criada exclusivamente para esse evento.