**Plump Spider: Uma Ameaça Persistente ao Setor Financeiro Brasileiro com Ênfase em Soluções BaaS**

**Resumo**

Este artigo analisa o grupo cibercriminoso Plump Spider, cuja atuação sofisticada e persistente tem como alvo instituições financeiras brasileiras, especialmente aquelas que operam com o modelo Banking as a Service (BaaS). A pesquisa descreve o modus operandi do grupo, suas táticas de engenharia social, exploração técnica e monetização ilícita, com base em evidências empíricas e indicadores de comprometimento (IOCs). A análise é fundamentada em literatura científica sobre segurança cibernética e crimes digitais no Brasil.

---

## 1. Introdução

A crescente digitalização dos serviços financeiros no Brasil, impulsionada por soluções BaaS, tem ampliado a superfície de ataque para agentes maliciosos. O Plump Spider representa um exemplo paradigmático de ameaça avançada persistente (APT), combinando engenharia social, exploração de vulnerabilidades e monetização estruturada. Conforme apontado por Nunes et al. (2022), a ausência de uma governança cibernética robusta no Brasil contribui para a vulnerabilidade de setores críticos [1].

---

## 2. Metodologia

A pesquisa baseia-se em análise documental de indicadores técnicos (hashes, domínios, ferramentas utilizadas), revisão bibliográfica e estudo de caso do ciclo de ataque do Plump Spider. A abordagem é qualitativa, com ênfase na descrição das táticas, técnicas e procedimentos (TTPs) do grupo.

---

## 3. Modus Operandi

### 3.1 Reconhecimento e Engenharia Social

O grupo inicia suas operações com campanhas de vishing altamente personalizadas, explorando falhas humanas em contact centers. Essa técnica é consistente com os achados de Silva e Souza (2023), que destacam a engenharia social como vetor primário de ataques no Brasil [2].

### 3.2 Distribuição de Ferramentas Maliciosas

A distribuição de RMMs e VPNs maliciosas ocorre por meio de domínios próprios e infraestruturas legítimas comprometidas, como sites governamentais. Essa tática de “Living off the Land” dificulta a detecção por soluções tradicionais de segurança.

### 3.3 Movimento Lateral e Coleta de Credenciais

Scripts automatizados realizam varreduras em file shares e Active Directory, extraindo credenciais e mapeando a estrutura organizacional. A construção de wordlists contextuais permite ataques de password spraying com alta taxa de sucesso.

### 3.4 Comprometimento de Sistemas Críticos

O foco do grupo são os sistemas de core banking, onde realizam escalonamento de privilégios e desenvolvem ferramentas "checker" personalizadas para validar acessos e permissões.

### 3.5 Execução de Fraudes Financeiras

Com acesso privilegiado, o grupo realiza majoração de limites de crédito e transações ilícitas em alta velocidade, utilizando canais como criptomoedas e contas de laranjas para lavagem de dinheiro.

### 3.6 Monetização como Serviço

A fase final envolve a comercialização de serviços fraudulentos em redes sociais e aplicativos de mensagens, caracterizando um modelo de "Fraud-as-a-Service" (FaaS), conforme discutido por autores como Brustolin (2019) no contexto da economia do cibercrime [1].

---

## 4. Indicadores Técnicos (IOCs)

O artigo apresenta uma tabela detalhada de hashes de arquivos maliciosos, domínios utilizados e ferramentas empregadas, contribuindo para a detecção e mitigação de ameaças.

---

## 5. Impactos e Riscos

As consequências para as instituições financeiras incluem perdas financeiras, danos reputacionais, riscos regulatórios e interrupções operacionais. A exposição de dados sensíveis também representa um risco significativo à conformidade com a LGPD.

---

## 6. Recomendações

Recomenda-se a adoção de medidas como:

- Treinamento contínuo em engenharia social;
- Implementação de EDR e SIEM;
- Segmentação de rede e MFA;
- Monitoramento de Active Directory;
- Participação em fóruns de threat intelligence.

## 7. Considerações Finais

O Plump Spider exemplifica a evolução do cibercrime no Brasil, com operações estruturadas e foco em monetização escalável. A resposta a essa ameaça exige uma abordagem integrada entre tecnologia, processos e cultura organizacional de segurança.

---

## Referencias


[1] Análise estrutural das estratégias de segurança cibernética do Brasil e ...

[2] Segurança cibernética: o cenário dos crimes virtuais no Brasil

[3] CRIMES CIBERNÉTICOS: ANÁLISE DO PROCESSO INVESTIGATÓRIO E OS DESAFIOS ...