



# Modelagem

Identificação de atacantes



# Perfil - Fraudador/Carder

Grupos grandes, alguns agindo mundialmente, procurando **dados de cartões de crédito para venda**.

São bastante organizados, possuem grande ferramental tanto para identificar quanto para **explorar falhas técnicas e processuais para execução de seus ataques**.



Fraudador / Carder

# Perfil - Spammer

Grupos médios, quase em sua totalidade procurando **meios comprometidos ou com baixa rastreabilidade para envio de spams.**

São bastante organizados, possuem grande ferramental tanto para identificar quanto para **explorar falhas técnicas** para execução de seus ataques.



# Perfil - Troll

Grupos médios, quase sempre pouco focados, buscando **vítimas fáceis** para **propagar seu humor negro e qualquer tipo de humilhação** que possa ganhar **notoriedade pública**.

Pouco organizados e sem grande ferramental, ficam circunscritos a ataques às vítimas mais frágeis.



# Perfil - Ransomware Hacker

Grupos pequenos, muito focados, buscando vítimas aleatórias que permitam o **comprometimento dos acessos a seus ativos viabilizando a exigência de um resgate para recuperação do ativo.**

Pouco organizados e com grande ferramental técnico, quase sempre operando unicamente de forma automatizada e difusa, atacando quaisquer alvos que possam ser comprometidos.



# Perfil - Hacktivista

Grupos pequenos, muito focados, buscando vítimas que permitam com grande visibilidade na mídia para sua causa. **Esse grupo usa o hacking para atrair atenção para seu “ativismo”**, sendo muito comum vê-los associados a eventos esportivos, grandes eventos políticos e quaisquer outros fóruns que tenham ampla visibilidade na sociedade.



# Perfil - Fraudador Bancário

Grupos grandes, extremamente ativos no Brasil, armados de **amplo ferramental para identificação de falhas técnicas e processuais**, bem como de ferramental para abuso dessas falhas.

Seu grande objetivo é o abuso do sistema bancário para **obtenção de recursos financeiros (dinheiro)**.



Fraudador Bancário



# Perfil - Espião Governamental

Mundialmente bastante **ativos em países em guerra aberta ou em cenários relacionados a terrorismo**. Esse tipo de atacante é definido por pequenos grupos com apoio governamental, buscam obter vantagens para sua nação estado de origem. Grupos como o “**Fancy Bear**” (Russia), “**Equation Group**” (EUA), “**Syrian Electronic Army**” (Siria) etc. Quando falamos desse grupo nos referimos a coisas relacionadas a espionagem em massa e guerra cibernética como foi o caso do **STUXNET**





# Perfil - Espião Industrial

Mundialmente ativos em países que valorizam o ambiente cibernético como espaço de guerra, esse tipo de atacante está também **ligado às nações estado**, mas seu propósito maior é conseguir vantagens competitivas para suas nações.



Espião Industrial

# Perfil - Bot-Herder

São grupos interessados em encontrar **infraestruturas vulneráveis** para **vender o acesso a essas infraestruturas**, seja pelo poder de processamento, seja pela sua dispersão global de máquinas, seja pela concretização de ataques diretos de forma anônima, garantindo o anonimato do atacante que “aluga” dos Herders tais recursos computacionais.



# Perfil - Fraudador

São grupos que busca **operacionalizar fraudes** via de regra através do **comércio**. Eles buscam meios de obter as **commodities** (sem pagar por elas) para vendê-las no mercado informal (no qual raramente se pede algum tipo de confirmação de origem do produto como notas fiscais etc.). Algumas vezes esses grupos **usam apenas dados cadastrais de pessoas idôneas para abrir linhas de crédito**, contas, etc. e realizar compras que ficaram em nome da vítima.



# Perfil - Crime Organizado

São **grupos complexos e grandes** cujas **atividades permeiam vários domínios, inclusive o eletrônico**, mas dificilmente uma de suas atividades fica circunscrita ao mundo eletrônico. Com muitos membros especializados, seus crimes normalmente se desenvolvem de tal forma que os mandantes raramente são identificados, como aconteceu no Ceará no furto ao banco central.





# Perfil - Estelionatário

São grupos muito ativos, cujo principal insumo é **informação e conhecimento detalhado dos processos operacionais das empresas** para **aplicação de golpes contra os clientes** dessas empresas, via de regra obtendo **dinheiro** desses clientes.

