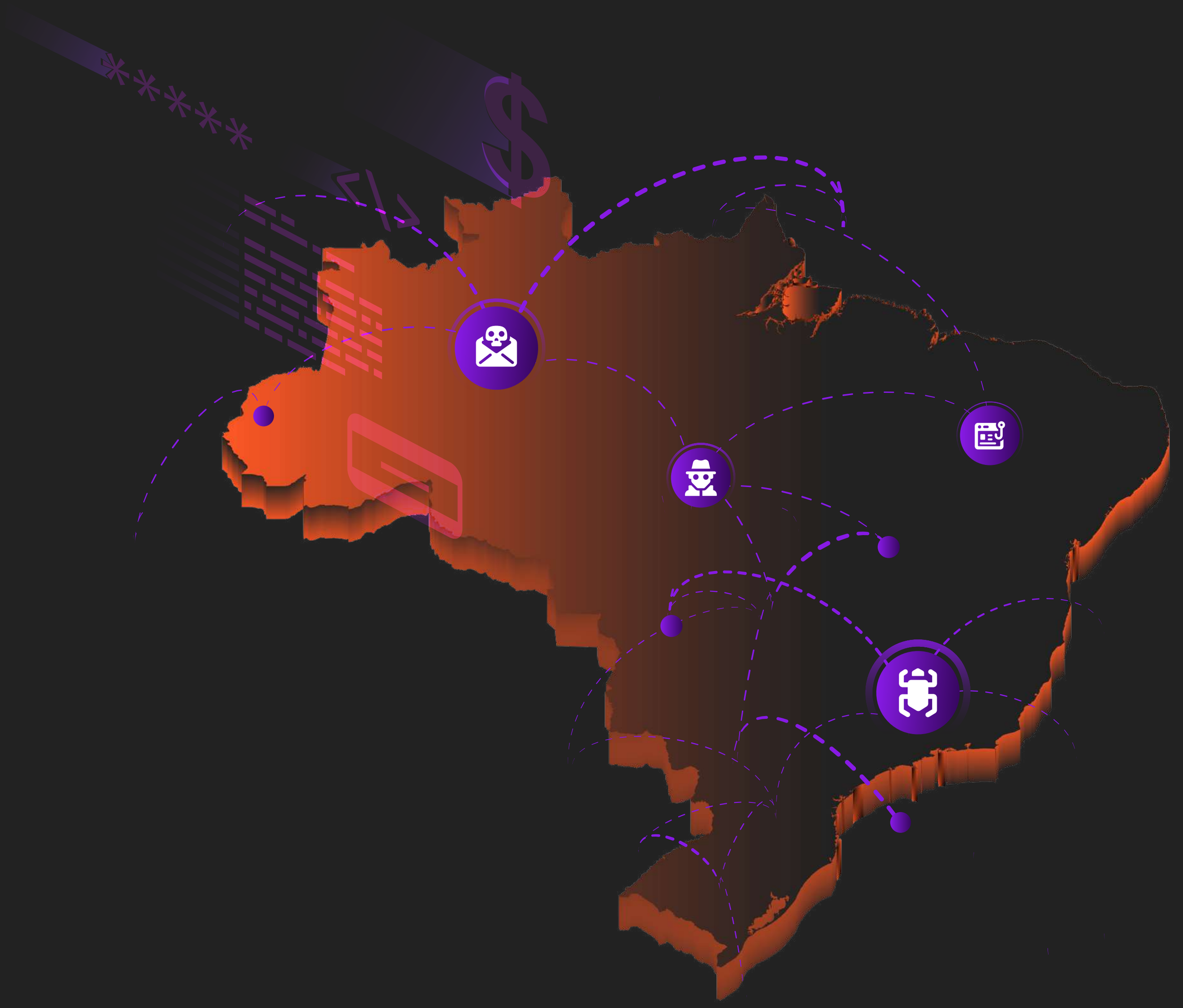
AXUR



E-BOOK

Made in Brazil: Decifrando as particularidades do cibercrime brasileiro

RESUMO EXECUTIVO

O Brasil conta com diversas particularidades no contexto da segurança da informação. A privacidade de dados, por exemplo, é um assunto muito mais recente do que em outras jurisdições, criando uma série de implicações para a conformidade com a legislação (a Lei Geral de Proteção de Dados) e para a própria segurança dos dados dos quais as empresas dependem em seus processos de trabalho.

Fatores culturais também tendem a influenciar a prevalência de ameaças internas (insiders), a necessidade de treinamentos e conscientização em segurança, e muitas outras questões. Isso vale para praticamente qualquer território, é claro.

Entretanto, não temos o objetivo de analisar todos esses aspectos culturais – embora isso seja importante para uma estratégia de cibersegurança eficaz.

Em vez disso, a proposta é **uma reflexão sobre o que é realmente "global" no contexto das ameaças cibernéticas.** Como a internet garante um passaporte para qualquer lugar, é tentador imaginar que as ameaças não têm nacionalidade – mas essa simplificação não dá conta de explicar os fatos e contribuir com a proteção dos dados.

Quando o assunto é inteligência de ameaças (cyber threat intelligence), deve-se aproveitar todo e qualquer instrumento que permita construir interpretações e intuições capazes de gerar valor dentro da análise. No dia a dia da segurança da informação, isso se reflete na priorização correta das ameaças e em uma atuação mais proativa, coerente com a missão da inteligência.

Questões como a linguagem, a influência de outros criminosos locais, as quadrilhas estabelecidas e os vícios de comportamento dos atacantes são algumas das várias características regionais que influem no caráter das ameaças. **O que veremos é de que forma a inteligência de ameaças se beneficia do conhecimento das características próprias dos agentes regionais que as realizam.**

Depois de entendermos o impacto da regionalização das ameaças na construção da inteligência e das soluções de segurança, temos uma visão geral das fraudes tipicamente brasileiras – aquelas que são realizadas por agentes locais e que, de uma forma ou de outra, se diferenciam do que é visto no contexto "global" das ameaças na internet.

Esperamos que fique evidente a influência que as fraudes regionais recebem de outros golpes e ameaças e das motivações dos criminosos – no caso brasileiro, a procura por ataques capazes de gerar ganhos rápidos e fáceis.

A FACE REGIONAL DAS AMEAÇAS CIBERNÉTICAS

As ameaças cibernéticas são normalmente tidas como globais. Ao contrário do que ocorre com outros tipos de ataques ou crimes, o agente malicioso que atua na internet não está confinado por qualquer barreira física ou geográfica. Mesmo que um site ou rede corporativa adote medidas de bloqueio gráfico (geo-blocking), o atacante pode recorrer a subterfúgios como o uso de redes privadas virtuais (VPNs), proxies e computadores já comprometidos em regiões específicas para mascarar a origem geográfica do ataque.

De fato, a Axur monitora continuamente diversos espaços em que criminosos vendem o acesso a computadores localizados em países ou até provedores específicos, permitindo que esses invasores estabeleçam um ponto de conexão próximo ao alvo para um ataque.

Apesar disso, ignorar o caráter nacional e geográfico das ameaças é um erro grave. Seja na análise uma operação sofisticada orquestrada por um estado ou de um crime cibernético qualquer, invariavelmente podem ser encontrados elementos que apontem para uma determinada origem. A atuação desses agentes é bastante influenciada por seus pares locais – outros criminosos, comparsas, cúmplices, ou até mentores.

Até onde uma fraude é 'global'?

Quando um invasor é bem-sucedido em seu ataque e consegue fraudar a vítima, a finalização do golpe ainda depende de trâmites rigorosamente regionais e comuns a diversos outros tipos de atividades ilícitas: lavagem de dinheiro, transferência de recursos, uso de laranjas e sistema bancário.

Esse vínculo do criminoso com sua realidade local é relativamente fácil de ser compreendido. Sendo o criminoso motivado pelo ganho financeiro, ele precisa passar por essas etapas para usufruir da receita ilícita.

O que pode passar despercebido é o caminho inverso desse processo. Para o criminoso, a preocupação com os desafios locais existe desde a concepção da fraude – ou seja, a influência local está presente em todos os aspectos da fraude, e não apenas nesses estágios finais.

Se um criminoso sabe que terá mais facilidade para usufruir de ganhos ilícitos obtidos com um certo tipo de fraude, isso serve de estímulo para que ele se interesse por ela. Da mesma forma, se já existe um esquema com outros criminosos, é mais fácil entrar na atividade organizada do que se arriscar criando uma modalidade de golpe e acabar sendo capturado pelas autoridades.

A legislação local e a capacidade de atuação das autoridades de investigar as atividades também influi na atuação dos criminosos. É notório, por exemplo, que muitos códigos maliciosos criados na Rússia evitam prejudicar sistemas que usem o idioma russo ou que tenham um teclado russo configurado. O objetivo é evitar uma atividade que acione as autoridades locais – que são as mais bem posicionadas para capturar o criminoso.

Por extensão desse raciocínio, a inexistência de legislação local para combater um certo tipo de fraude e a complacência das instituições locais diante de certos comportamentos pode contribuir para a prática de crimes envolvendo essas fraudes e comportamentos. A pirataria é um bom exemplo disso: embora seja tratada com muito rigor em alguns países, a lei raramente é aplicada à risca em países da América do Sul, na Rússia ou na China.

No limite, isso também se manifesta nas próprias iscas utilizadas para enganar as vítimas. Uma isca envolvendo um software ou conteúdo pirata tende a ser menos suspeita quando a vítima está inserida em uma cultura na qual esse tipo de conteúdo não causa estranheza.

Somando esse entendimento ao fato de que a maioria dos ataques cibernéticos envolve um fator humano, pode-se concluir que diversos componentes das fraudes – inclusive as mais "globais" – guardam alguma conexão com o contexto local ou regional de quem as pratica.

A ameaça local

Há fraudes que, por sua natureza, só podem atingir um público específico. Mesmo que a limitação não seja intencional, alguns elementos do ataque simplesmente não funcionariam fora de um contexto limitado. Um desses contextos costuma ser geográfico.

Uma fraude com cartão de crédito pode facilmente atingir um público amplo, mas golpes envolvendo meios de pagamento nacionais, como é o caso do Pix e de boletos bancários no Brasil, não podem atingir quem não tem acesso a esses mecanismos.

O mesmo ocorre com fraudes que envolvem documentos pessoais. Embora existam documentos internacionais como o passaporte, é comum que cada nação (e, às vezes, até estados ou províncias) emitam documentos de identificação próprios.

Raramente há equivalência direta entre os documentos de identificação. Por exemplo, um Social Security Number (SSN) dos Estados Unidos não equivale ao CPF brasileiro, ainda que eles sejam equiparados para facilitar o entendimento em certas circunstâncias. De fato, o Brasil conta com números de identificação exclusivos para o acesso à previdência social, para a identificação do cidadão no Sistema Único de Saúde, entre outros.

No âmbito das fraudes financeiras, muitas são direcionadas a clientes de instituições específicas, que atuam em apenas alguns mercados. Diversos códigos maliciosos projetados para roubar senhas acabam tendo essa limitação. Programas de roubo de senhas modernos (credential stealers) podem roubar diversas credenciais de maneira indiscriminada, mas um malware dedicado a roubar senhas bancárias (banker) abandona essa versatilidade em troca de uma maior efetividade na execução de fraudes bancárias.

É comum enxergar os golpes regionais como meras adaptações de golpes praticados ao redor do mundo. Contudo, assim como ocorre em fraudes de caráter global, normalmente a adaptação ganha contornos regionais decorrentes das práticas criminosas que já são comuns naquele local.

Especificidades técnicas também podem limitar ou direcionar um ataque. Foi o caso do malware NotPetya, de 2017. A ameaça foi inicialmente confundida com um ransomware (o Petya) que poderia atacar alvos globais, assim como o WannaCry descoberto um mês antes.

Posteriormente, ficou claro que o NotPetya era um malware diferente e destrutivo – sem um recurso funcional para recuperação de dados, como se

esperaria de um ransomware. O código também atingiu principalmente sistemas na Ucrânia, sendo distribuído como uma atualização adulterada do M.E. Doc, um software de contabilidade popular no país.

Aplicativos financeiros e contábeis são apenas dois exemplos de riscos locais aos quais uma empresa se expõe ao expandir suas operações para novos mercados. Também é preciso que se considere, dentre outros fatores, a cultura de informação ou compartilhamento de dados da região, a segurança pública, o nível de confiabilidade de prestadores de serviços e a qualidade dos softwares e serviços fornecidos por instituições do governo.

O combate às fraudes e aos ataques cibernéticos perde eficácia quando essas diferenças e influências locais são ignoradas. Da mesma forma, uma empresa pode colher muitos benefícios ao contar com especialistas que conhecem as características regionais das ameaças procedentes de cada mercado ou região onde atua.

COMO A INTELIGÊNCIA REGIONAL É MAIS EFICAZ

Partindo da compreensão de que até as ameaças mais "globais" normalmente possuem algum componente local, podemos olhar mais de perto para alguns fatores locais e sua influência na análise das ameaças e no preparo das informações para que elas tenham validade como inteligência de ameaças.

Linguagem

No contexto da inteligência de ameaças cibernéticas, a familiaridade com o idioma e o linguajar usado por adversários cibernéticos não serve apenas ao entendimento da comunicação entre eles. O conhecimento da linguagem tem um papel fundamental na análise dos sinais de inteligência.

No caso brasileiro, muitos criminosos adotam uma série de gírias, criando um linguajar conhecido como "tramponês". Mas não basta conhecer esses termos e a particularidade do emprego dessa linguagem. É a análise contextual da linguagem – como é usada, onde e por quem – que realmente agrega valor aos sinais coletados pela inteligência em ameaças.

ECLIPSE

O termo "eclipse" se popularizou entre criminosos brasileiros para indicar vulnerabilidades com alto potencial para ganhos e que, por sua natureza, seriam logo corrigidas. O monitoramento da Axur reconheceu o risco associado a este termo, permitindo que clientes respondam rapidamente aos "eclipses" em seus serviços.

Talvez o maior desafio ligado à coleta de sinais de inteligência em ameaças está na priorização dos dados e na separação das informações mais significativas ou que exigem ação imediata (actionable intelligence). O conhecimento apurado da linguagem dos adversários facilita e aprimora esse trabalho.

A capacidade de fazer uso do linguajar usado pelos agentes maliciosos também amplia as possibilidades para a investigação de alguns incidentes ou para a coleta de sinais de inteligência que estariam fora de alcance para quem não domina o idioma no mesmo nível.

Vale lembrar que, mesmo com a tecnologia atual e com o emprego de inteligência artificial, ainda é possível diferenciar um texto traduzido ou criado por máquina da comunicação nativa de um ser humano. É fundamental que o analista seja fluente e habituado ao uso do idioma no contexto de ameaças cibernéticas e que a ferramenta conte com uma base tecnológica adequada à tarefa.

Táticas, técnicas e procedimentos (TTPs)

Os threat actors muitas vezes se destacam pelo uso de táticas, técnicas e procedimentos (TTPs) recorrentes. Isso significa que um atacante (ou grupo de atacantes) tende a reutilizar a mesma "receita" em suas ações, permitindo que elas sejam vinculadas a eventos anteriores.

Não é raro que atores maliciosos provenientes de um mesmo contexto (inclusive regional) também demonstrem afinidades – inclusive porque, dada a existência de uma língua comum, esses criminosos também precisam de espaços compartilhados para oferecer "serviços" ou conhecimento. Em termos práticos, o que temos são fóruns, salas de bate-papo, aplicativos de mensagens e marketplaces dedicados a um tipo de fraude ou região.

Assim como no caso da linguagem, o conhecimento acerca dos TTPs locais aprimora a inteligência de ameaças, as técnicas de monitoramento e a resposta a incidentes.
Se os criminosos de um certo contexto tendem a discutir suas atividades por meio de um aplicativo de mensagens ou rede social, a coleta de inteligência em outros ambientes não terá a mesma efetividade. Da mesma forma, conhecer o OpSec desses agentes pode acelerar a identificação da atividade maliciosa em uma perícia.

Esse nivelamento das priorizações é constante. **Criminosos podem facilmente migrar de um espaço para outro e adotar novas técnicas. É importante que a inteligência local acompanhe esses movi**
mentos e ofereça a informação mais adequada e oportuna.
Desconsiderar essas tendências locais tende a gerar resultados abaixo do ideal. Coletar e priorizar inteligência de fontes menos relevantes pode gerar alertas desnecessários e criar ruído para a equipe de segurança. No longo prazo, o trabalho de inteligência pode começar a ser visto como ineficaz ou até descartável por causa de um fenômeno conhecido como alert overload ou alert fatigue ("sobrecarga de alertas").

É bastante difícil reconhecer uma fonte de inteligência de ameaças ineficaz em um contexto isolado, sem que ela seja comparada a outra fonte apropriada para o contexto da organização.

A inteligência em ameaças feita corretamente é valiosa. Se alertas estão sendo rotineiramente descartados, é preciso reavaliar a estratégia e passar a considerar fatores de risco, como as técnicas de agentes locais.

O MALWARE BRAZKING

A família de malwares BrazKing atinge dispositivos com Android e utiliza a função de acessibilidade do sistema para interferir no funcionamento de aplicativos financeiros. O malware é capaz de realizar transações financeiras por conta própria, sem a interferência do usuário. O malware se comunica com um servidor de comando e controle (C2) para realizar tarefas sob demanda no smartphone.

O "BrazKing" é um malware brasileiro que incorporou uma técnica de ataque conhecida como "Ghost Hand". Embora utilize uma técnica global, a existência de um malware dedicado a esses ataques no Brasil eleva o risco para as atividades mobile na região, pois evidencia o interesse dos criminosos nesse tipo de fraude.

Baixe o ebook sobre a técnica Ghost Hand

Atribuição

A atribuição de um ataque cibernético permite associá-lo a outras ações realizadas pelo mesmo grupo de invasores. Essa vinculação é útil para avaliar o risco que aquele grupo pode representar para uma empresa ou para seu ramo de negócios e, durante um processo de resposta a incidentes, ajuda a direcionar o trabalho de coleta e análise de evidências.

O processo de atribuição muitas vezes depende da intuição dos analistas. Não existe uma lista de evidências ou elementos que necessariamente devem ser avaliados em cada incidente ou ataque. Na prática, é o contato frequente com os incidentes e as atividades maliciosas que dá a um analista as condições de identificar semelhanças técnicas e operacionais em cada caso.

Considerando que certos grupos criminosos concentram suas atividades em algumas regiões – inclusive para facilitar os estágios subsequentes das fraudes que realizam, como já explicado –, uma equipe de especialistas familiarizada com os incidentes de uma região tende a ter mais contato com incidentes causados por esses grupos e, portanto, estará mais qualificada para realizar a atribuição do ataque corretamente.

UM RISO E UM INSIGHT

O relatório da Axur sobre o grupo **LAPSUS$** indicou que um dos membros do grupo era possivelmente brasileiro e não tinha o inglês como idioma nativo. Os apontamentos do relatório se basearam em chats interceptados que traziam risadas e vícios de linguagem comuns a falantes nativos do português brasileiro, bem como evidências do uso de ferramentas de tradução.

Meses após a disponibilização do relatório para os clientes da Axur, em outubro de 2022, a Polícia Federal do Brasil deflagou a operação Dark Cloud e prendeu um suspeito de integrar os ataques do LAPSUS$ em Feira de Santana, no estado da Bahia.

Na mesma linha, o analista precisa dessa sensibilidade para saber quando está diante de um ataque diferenciado, que não se enquadra no que é comum em um determinado contexto. Isso também exige um contato frequente com outros incidentes em contextos parecidos – seja na mesma região ou no mesmo ramo de atuação.

O conhecimento dos aspectos já mencionados (TTPs e linguagem) também desempenha um papel na atribuição, e ajuda a definir quais os grupos de criminosos e agentes maliciosos demandam uma atenção maior das empresas com presença em um determinado mercado.

Reconhecimento de tendências

O contato com incidentes diversos em um mesmo mercado, aliado aos conhecimentos sobre TTPs e linguagem, permite identificar tendências e semelhanças – ou seja, quais os novos tipos de golpes que estão sendo praticados por criminosos naquela região. **É a habilidade de perceber quais fraudes tendem a ser reproduzidas e reaproveitadas contra novos alvos, seja pelos mesmos criminosos ou por imitadores (copycats).**

Em algumas situações, essa linha de análise permite também antecipar como algum tipo de fraude pode ganhar novos contornos ou ser adaptada por diferentes grupos de criminosos já conhecidos. Na Axur, isso também ajuda a direcionar o desenvolvimento de novas soluções e funcionalidades nos produtos, garantindo sua eficácia.

O reconhecimento de tendências tem um valor fundamental para a inteligência de ameaças, pois reduz a janela de tempo que os atacantes têm para aproveitar o fator surpresa.

Criminosos buscam novas estratégias de ataque para contornar as camadas de defesa existentes. Um formato diferente de storytelling ou narrativa pode confundir até mesmo usuários que passaram por programas de conscientização em segurança, já que não houve treinamento específico para o novo golpe que foi inventado.

A agilidade na identificação de técnicas novas aumenta a capacidade de uma empresa para detectar atividades suspeitas, prevenir ataques e organizar sua estratégia de conscientização em segurança. É uma peça-chave para que a inteligência de ameaças entregue o valor que dela se espera.

O OPSEC DO CIBERCRIME BRASILEIRO

Os cibercriminosos utilizam uma infraestrutura de comunicação e negociação, criando uma comunidade do crime. Algumas dessas comunidades são construídas na Deep & Dark Web, mas outras se aproveitam das mesmas ferramentas disponíveis para qualquer usuário da internet – inclusive comunicadores como WhatsApp, Discord e Telegram. Os criminosos podem então empregar técnicas de OpSec (operation security) para limitar a quantidade de informação que pode ser extraída desses espaços e de artefatos maliciosos.

A Axur oferece coletores de inteligência e análises relevantes para o mercado brasileiro, em sintonia com as práticas de OpSec dos criminosos brasileiros e com os canais de interação mais usados pelos criminosos. Com esse monitoramento, nossos clientes podem ser os primeiros a saber quando uma atividade criminosa gera algum risco ao negócio.

Saiba mais no Relatório de Atividade Criminosa Online de 2022 da Axur

Sem o conhecimento da realidade regional para fundamentar essa análise, é bastante provável que sejam priorizados os riscos ligados aos ataques cibernéticos mais comuns em escala global, ficando subestimados os riscos provenientes de ameaças locais.

Em outras palavras, até ataques regionais muito comuns podem passar despercebidos sob um olhar global. **Ignorando-se a preponderância regional, pode haver um desalinhamento entre os maiores riscos considerados pela estratégia de cibersegurança e a realidade que a empresa e seus clientes enfrentam em cada mercado, comprometendo a eficácia da inteligência de ameaças.**

AS FRAUDES REGIONAIS NO BRASIL

A vasta experiência da Axur no mercado brasileiro e o trabalho de inteligência realizado por nossos analistas tendem a revelar um cenário bastante particular. Embora os brasileiros sejam ocasionalmente atingidos por ataques provenientes de agentes externos, existe um conjunto de ataques e fraudes frequentes de natureza local.
As fraudes praticadas por agentes locais costumam ter uma consistência interna – ou seja, elementos comuns entre si. Elas também normalmente conseguem explorar particularidades da realidade brasileira: os criminosos conhecem os serviços mais populares do Brasil e sabem como eles são usados.

São também essas fraudes locais que normalmente exploram fatos do noticiário ou características inerentes do sistema local de pagamentos, como é o caso dos boletos e do Pix. Analisar essas fraudes não é um trabalho intuitivo para quem não está acostumado com o modus operandi dos criminosos locais e com a conjuntura brasileira que eles exploram.

Para descrever o cenário local, vamos explorar algumas fraudes particulares do Brasil em duas categorias:

- Fraudes financeiras
- Fraudes contra o consumidor

Por fim, para caracterizar o golpista brasileiro neste capítulo, vamos falar dos golpes que não são comumente aplicados por golpistas brasileiros.

Fraudes financeiras

O e-commerce brasileiro lida com alguns dos mesmos desafios que as lojas digitais enfrentam em todo o mundo, incluindo compras ilegítimas feitas com cartões roubados (o que gera chargebacks). Contudo, as particularidades do cenário local influenciam e diferenciam certas fraudes realizadas no Brasil.

Um fato importante é a predominância do smartphone. As fintechs aumentaram de forma significativa o acesso do público brasileiro aos serviços financeiros, pois simplificaram a abertura de contas e diminuíram os custos para manter um relacionamento bancário. Segundo dados do Banco Central, 57% dos da população brasileira tinha uma conta corrente em 2017. Em 2022, esse número saltou para 82%.

A facilidade para criar contas e novos relacionamentos bancários também vem fazendo com que correntistas procurem serviços de outros bancos. Em 2012, cada correntista tinha em um média 2,1 "relacionamentos" (como contas bancárias ou semelhantes) com instituições financeiras, segundo o levantamento do Banco Central. Em 2022, essa proporção mais que dobrou, chegando a 5,2.

Como os brasileiros estão acostumados com essa relação digital com seus bancos, não é exatamente uma surpresa que o acesso via smartphone seja o mais popular no país. De acordo com a Pesquisa Febraban de Tecnologia Bancária 2023, **66% de todas as operações – transferências, pagamentos ou consultas de saldo – são realizadas a partir de dispositivos mobile.**

FRAUDE NA ABERTURA DE CONTAS

Muitos bancos brasileiros hoje adotam a identificação facial dos correntistas por meio digital, sem que o cliente precise se dirigir a uma agência.

No aplicativo oficial da instituição financeira, essa identificação exige o uso da câmera do smartphone. Para contornar essa medida de segurança, os criminosos utilizam "burladores de selfie", que simulam a operação da câmera do telefone com imagens previamente preparadas de acordo com os padrões solicitados pelo banco. Usando fotos e dados pessoais provenientes de vazamentos, além do aplicativo burlador, os criminosos muitas vezes conseguem realizar o cadastro de contas fantasma com sucesso

Na perspectiva do criminoso, atingir um único correntista significa ter acesso a possivelmente cinco contas diferentes – ou seja, o golpista é incentivado a adaptar uma mesma fraude a diferentes instituições.

Esse já era um cenário comum nos malwares direcionados para sistemas no Windows. **Enquanto o phishing tradicional leva a vítima a uma página clonada para roubar uma senha de uma instituição específica, os links no phishing brasileiro comumente leva as vítimas para pragas digitais (bankers) habilitados para roubar credenciais ou realizar transações em um grupo de instituições financeiras.** Somam-se a esse cenário as particularidades introduzidas pelo Sistema de Pagamentos Brasileiro (SPB), que rege a liquidação operações realizadas por vários instrumentos financeiros. Dois deles são bastante relevantes no contexto das fraudes: o Pix e o boleto.

Pix

O Pix é um sistema instantâneo e digital de transferências bancárias disponível 24 horas por dia. Esse instrumento tem diversos recursos, sendo um deles a possibilidade de associar contas bancárias a "chaves" (chamadas de "chaves Pix"). A chave pode ser um e-mail, um número de telefone ou um número do Cadastro de Pessoa Física (CPF), o número de identidade nacional brasileiro normalmente vinculado a questões financeiras e tributárias.

Embora esteja teoricamente disponível a partir de qualquer plataforma, 96% das transferências com o Pix são realizadas pelo smartphone.
Ao fornecer um método de pagamento pode ser acessado de praticamente qualquer smartphone e que está vinculado a dados pessoais, o Pix passou a protagonizar diversos incidentes de segurança:

- **Golpes de pagamento antecipado (advance-fee fraud)**

  > O Pix tem liquidação instantânea, o que favorece golpes que induzem o correntista a realizar uma transferência. O Banco Central adicionou ao Pix um Mecanismo Especial de Devolução para reduzir a incidência de fraudes, mas o estorno depende de um trabalho conjunto das instituições envolvidas na transação.

- **Transferências automatizadas por malware**

  > As credenciais necessárias para o envio de um Pix podem ser coletadas por malware e, em alguns casos, a própria função de transferência pode ser acionada por um código malicioso. É o que se observa em malwares como o PixStealer e o BrazKing.

- **Violência física**

  > Criminosos têm realizado sequestros e obrigado as vítimas a realizarem transferências via Pix para que sejam libertadas. Nesses casos, o meio de transferência digital substituiu o saque em caixas eletrônicos.

Os criminosos podem adaptar essas fraudes para diferentes contextos. No caso de pagamentos antecipados, há golpes envolvendo ofertas de emprego falsas, produtos fraudulentos e perfis falsos em redes sociais e comunicadores. Por exemplo, um criminoso pode entrar em contato com uma vítima se passando por um filho ou irmão e pedir dinheiro através do Pix, seja a pretexto de alguma ajuda financeira ou para quitar uma compra emergencial.

Há também uma variação do golpe de engenharia social que utiliza mensagens enviadas por SMS e números 0800 com centrais falsas. O golpe pode servir para que o criminoso obtenha dados ou para fazer uma solicitação de Pix (o golpe da central falsa está detalhado na seção sobre fraudes de atendimento).

Por conta de suas características, o Pix é bastante versátil e substitui outras formas de extorsão e roubo, o que adiciona uma camada única para diversas fraudes praticadas no território brasileiro.

O Pix também tem algumas implicações para a privacidade, já que usuários vinculam seus e-mails, telefones ou números de CPF às contas bancárias. No início, a consulta de uma chave Pix podia retornar diversos dados sobre o proprietário da chave; após alguns vazamentos e golpes, o Banco Central passou a recomendar que a maior parte das informações só fique visível após a confirmação da transferência.

Vale destacar que, embora o uso destas chaves seja opcional, é bastante comum que correntistas registrem ao menos uma delas. Muitas instituições financeiras ofereceram benefícios para correntistas que vinculavam as chaves Pix à sua conta corrente.

As fraudes no Pix têm potencial para impactar a relação entre empresas e consumidores. Como o uso do Pix é gratuito na maior parte das situações, empresas também recebem pagamentos via Pix para reduzir o risco de chargebacks e as taxas impostas por outros meios de pagamento.

BOLETO

O boleto de pagamento é uma fatura (invoice) que acompanha um código para liquidação. Esse código, que também aparece em forma de código de barra, é chamado de "linha digitável" e identifica o documento, o valor, a data de vencimento e o beneficiário.

Embora sejam normalmente chamados de "boletos", há também as faturas emitidas por convênio. Contas de serviços de telecomunicação e impostos muitas vezes são emitidos neste formato. Na perspectiva do consumidor, contudo, essa diferença é muito tênue, pois os aplicativos bancários tratam ambos da mesma forma – o tipo de documento é detectado e o consumidor será levado para a tela de confirmação de pagamento, independentemente do tipo de boleto.

As fraudes envolvendo boletos acabaram por exigir a criação de um registro, o que impede a alteração dos dados da linha digitável. A adoção do Pix também substituiu o boleto para pagamentos, já que a liquidação do Pix é muito mais ágil.

Por outro lado, o boleto ainda é um instrumento bastante utilizado em relações B2B. Criminosos podem adulterar documentos ou enviar faturas falsas, gerando cobranças indevidas e desviando o dinheiro de pagamentos para contas.

O termo "golpe do boleto" é usado de forma ampla para descrever todos os tipos de fraude em que alguém é levado a pagar um boleto falso ou adulterado. É possível dizer inclusive que a fraude conhecida como Business Email Compromise (BEC) muitas vezes se confunde com alguma variação do "golpe do boleto" no Brasil, já que o boleto, se adulterado, pode desviar o pagamento de um fornecedor – que é um cenário comum no BEC.

Fraudes contra o consumidor

Uma empresa tem muito a ganhar se estiver ciente das fraudes que atingem seu consumidor. A empresa pode orientar melhor seus clientes e parceiros, evitando prejuízos e melhorando a própria segurança de suas operações.

Contudo, mesmo que a fraude não represente um prejuízo direto para a marca, é importante considerar que criminosos se aproveitam de marcas conhecidas para aplicar golpes. Do ponto de vista do consumidor, a marca pode ficar associada à fraude ou, na pior dos casos, o consumidor pode nem sequer entender que foi vítima de uma fraude e culpar a empresa por um produto não entregue ou por uma promoção falsa.

E-COMMERCE E VAREJO

Os criminosos brasileiros realizam diversas fraudes no e-commerce, em especial por meio do uso de cartões de crédito roubados. Embora também existam casos comprovados de atuação de criminosos no varejo e de alta sofisticação técnica (a exemplo de uma gangue conhecida como "Prilex", que atua em sistemas de ponto de vida), o mais comum é que as fraudes sejam tecnicamente simples, apoiando-se em engenharia social e em dados roubados.

Um dos maiores riscos no caso do e-commerce é o abuso de marca. Criminosos se aproveitam de marcas de boa reputação para criar sites falsos ou ofertas falsas em marketplaces. Em algumas situações, **a marca pode ser usada indevidamente também em anúncios publicitários ilegítimos, induzindo o consumidor ao erro.**

Esse tipo de fraude causa constrangimento para as empresas e para o consumidor, que enxergará a situação como uma oferta ou compra não honrada pela empresa que teve sua marca utilizada pelos golpistas.

A Axur conta com um sistema de monitoramento avançado, que combina o uso de palavras-chave, inteligência artificial e filtros para aprimorar o reconhecimento da marca e detectar inconformidades em sua utilização. Além de evitar que o consumidor caia em golpes, esse trabalho reduz custos de atendimento e protege a relação da empresa com seus clientes.

Outra medida importante vinculada ao monitoramento é a de takedown, que derruba as páginas irregulares. Os criminosos tendem a desistir de usar marcas resguardadas por monitoramento e takedown, já que a fraude tende a ficar pouco tempo no ar. Como o criminoso se vê obrigado a repetir os passos de criação e disseminação da fraude sempre que um de seus golpes cai, é melhor utilizar uma marca que vai permitir que a fraude permaneça disponível por mais tempo.

Isso quer dizer que, embora o investimento no trabalho de monitoramento e takedown seja inicialmente reativo, ele passa a ter um caráter preventivo ao desencorajar a criação de fraudes com a marca protegida.

Fabricantes e fornecedores também costumam ter problemas com a pirataria. Novamente, o monitoramento de marca pode criar um diferencial nesse quesito, ajudando o consumidor a encontrar os produtos originais.

Ainda que seja mais raro, também há casos em que golpistas criam lojas on-line com marcas próprias. Esse tipo de incidente leva o consumidor brasileiro a ser mais desconfiado, especialmente quando lojas buscam oferecer descontos para pagamentos à vista – o que, como explicado na situação do Pix e do boleto, pode resultar em uma fraude em que o consumidor não consegue reaver o dinheiro pago depois que o produto não foi entregue.

Se por um lado essas lojas fraudulentas não exploram marcas consolidadas no mercado, elas acabam ajudando a corroer a confiança do consumidor. Para quem busca atuar com seriedade, é importante lembrar que o consumidor traz consigo essa bagagem de desconfiança construída por um cenário hostil.

MONITORAMENTO DA OSTENTAÇÃO

Os criminosos brasileiros muitas vezes "ostentam" os ganhos obtidos com as suas fraudes. Os valores nem precisam ser significativos: um único pedido de valor mais alto pago com um cartão roubado é suficiente para que o indivíduo "ostente" sua façanha perante os "colegas".

Esse comportamento cria uma oportunidade valiosa de inteligência. A Axur já ajudou lojistas a identificar e cancelar compras feitas de forma irregular que foram denunciadas pelos próprios criminosos – inclusive com situações em que o criminoso pretendia se dirigir à loja para fazer a retirada do pedido.

ATENDIMENTO FALSO E FRAUDES DE SUPORTE TÉCNICO

Embora criminosos possam facilmente criar sites falsos na internet e utilizar a marca de outras empresas, há uma variação dessa fraude que muitas vezes conta com uma sofisticação maior ou, pelo menos, um envolvimento maior do criminoso na interação com a vítima. É o atendimento falso, também chamado de "atendente impostor".

O golpe toma várias formas. Para crimes fora do mundo digital, assaltantes podem se aproveitar de uniformes de empresas conhecidas e prestadoras de serviços de água, energia e telecomunicações. No contexto das comunicações eletrônicas, temos os perfis falsos em redes sociais, centrais de atendimento falsas e a ligação do suporte técnico.

- ***Perfil falso em rede social***

  Os cibercriminosos criam um perfil em rede social que utiliza a marca de uma empresa. Em seguida, eles procuram vítimas – muitas vezes no perfil oficial da marca na mesma rede social – e entram em contato com as vítimas por mensagem direta. A mensagem traz alguma oferta, promoção ou prêmio, induzindo a vítima a fazer uma transferência bancária ou ceder informações.

- ***Central de atendimento (URA) fraudulenta***

  É preparada uma Unidade de Resposta Audível (URA) que imita a central de atendimento telefônica de uma empresa. Os golpistas então convencem a vítima a interagir com esta central, o que pode acontecer por meio de um contato telefônico prévio com a vítima ou por meio do envio de mensagens de SMS divulgando um número 0800 falso.

  Por acreditar que se trata do ambiente legítimo da empresa, o consumidor pode ser convencido a ceder informações (inclusive senhas). Em alguns casos, o golpe também evolui para outros tipos de fraudes, como o "golpe do motoboy", em que os criminosos criam um pretexto para enviar um motociclista para a residência da vítima com o intuito de coletar cartões de crédito e outros documentos.

  Esta fraude tem uma sofisticação considerável. A central falsa é configurada pelo criminoso com sons idênticos ao da verdadeira, de modo que a vítima pode navegar no menu eletrônico e receber as mesmas orientações e gravações que receberia no canal oficial.

  O uso de números telefônicos especiais também pode adicionar credibilidade ao golpe. Embora não seja uma prática universal, há diversos casos em que os golpistas enviam os SMSs falsos através de shortcodes (os números curtos de onde normalmente são enviadas mensagens legítimas), além da já citada utilização de números 0800 para receber as chamadas.

  As ferramentas e mecanismos para realizar essas fraudes são comercializados entre os criminosos, de modo que a execução do golpe nem sempre é realizada pelo mesmo agente malicioso que prepara a infraestrutura e o software utilizado.

- ***Ligação do suporte técnico***

  Essa é uma variação do tech support scam que também é observado em outros países. No Brasil, a fraude pode ser usada para convencer a vítima a instalar um programa de administração remota no celular. Diversas instituições financeiras no Brasil adotaram softwares de segurança obrigatório (normalmente chamados de "plug-ins de segurança") para acesso no computador e, por esta razão, usuários estão acostumados com a ideia de instalar programas de segurança vinculados aos serviços financeiros, dando credibilidade ao storytelling do golpe.

RAIO X DAS FRAUDES DIGITAIS BRASILEIRAS

AS ESPECIALIDADES DO CRIMINOSO BRASILEIRO

ENGENHARIA SOCIAL

A enganação com histórias e identidades falsas para atrair vítimas

GOLPES FINANCEIROS

Uso indevido de credenciais bancárias e cartões obtidos com malware

USO DE DADOS VAZADOS

Seja para um golpe de falsa extorsão ou para cadastrar contas e obter empréstimos indevidos em nome de outras pessoas, o golpista brasileiro emprega dados vazados e obtidos por outros criminosos.

POR ONDE CHEGAM OS GOLPES

- **WhatsApp** (Familiar Falso, Pedido De Dinheiro)
- **Telefone** (SMS Falso)
- **E-Mail** (Phishing, Malware)
- **Instagram** (Impostor Falso)
- **Publicidade Online** (Promoções Falsas)

O TRAJETO DO DINHEIRO

Boleto: Faturas Falsificadas No B2B E Compras Inexistentes No B2B

Computador: Uso De Malware Para Captura De Credenciais Financeiras

Pix: É O Caminho Por Onde O Dinheiro Vai Da Vítima Ao Criminoso Em Golpes Como O Falso Emprego E O Atendente Impostor Nas Redes Sociais

Smartphone: Por Meio Da Mão Fantasma – Ghost Hand – Os Criminosos Brasileiros Interferem Na Operação Dos Aplicativos.

A RELEVÂNCIA DO PIX

O Pix é usado por criminosos brasileiros inclusive em movimentações criminosas entre eles. Em outros lugares do mundo, golpistas recorrem a outros meios de pagamento, incluindo criptomoedas.

DO VIRTUAL AO REAL

A realidade da segurança pública no Brasil muitas vezes permite que um golpe virtual se estenda para o mundo real.

Um bom exemplo disso é o ***romance scam*** ("golpe do amor"). Globalmente, é comum que essa fraude permaneça no âmbito virtual – inclusive, é possível que quem realiza a fraude não esteja localizado no mesmo país da vítima.

No Brasil, há uma chance considerável de que o relacionamento avance para o mundo real. Neste caso, o golpista tende a sequestrar a vítima ou aplicar outro tipo de golpe, inclusive com o uso de drogas soníferas (conhecidas como "boa noite Cinderela") para realização de estupro ou de roubo (normalmente via Pix).

De fato, **os crimes comuns (como furto e ameaça à mão armada) podem representar um risco diferenciado para algumas operações digitais, pois oferecem risco à confidencialidade dos dados em dispositivos portáteis como celulares e notebooks.**

Fraudes de pagamento presencial também são comuns. Como já mencionado, há casos em que criminosos adulteram sistemas de ponto de venda (PdV, ou point of sale). Porém, são consideravelmente mais comuns em casos em que a fraude parte do próprio cobrador, como no caso do **golpe da maquininha,** em que a máquina usada para processar o pagamento no cartão de crédito foi adulterada e danificada para não permitir que o consumidor veja o valor real que está sendo pago por uma compra.

Esse cenário deve deixar em alerta as empresas que atuam com modelos de negócio híbridos (com presença virtual e física para cobrança ou retirada de produtos). Mesmo assim, o componente digital dessas fraudes gera uma oportunidade para que a inteligência de ameaças descubra mais informações sobre a operação desses criminosos.

O que não é comum no Brasil?

Há certos ataques cibernéticos que, no contexto atual, raramente são vistos no Brasil.

- **Ransomware**: o ransomware é uma fraude com impacto global, mas é bastante associada a criminosos do Leste Europeu, em especial da Rússia. Embora tenham sido registrado casos de brasileiros envolvidos com esse tipo de fraude, elas raramente são praticadas por agentes locais.

- **Alta sofisticação técnica:** muitos dos ataques e fraudes cibernéticas praticadas no Brasil guardam alguma semelhança ou relação com golpes e crimes que eram realizados antes da internet. Por esse motivo, o núcleo dos golpes normalmente é a engenharia social, enganando a vítima de alguma forma. Os malwares e instrumentos técnicos empregados na realização do crime normalmente não são sofisticados, inclusive porque várias das soluções são "caseiras", ou seja, são produzidas por outros criminosos locais. A adaptação e uso de malwares desenvolvidos fora do Brasil têm sido mais comuns nos últimos anos, mas permanece válida a noção de que a tecnologia do cibercrime local não é sofisticada.

- **Ataques de longo prazo:**Ataques de longo prazoos criminosos brasileiros buscam ganhos rápidos por meio da fraude. Os ataques de ransomware, que podem exigir alguns meses de preparação, já não satisfazem esse critério. Ataques ainda mais longos, que atingem a infraestrutura das empresas e coletam dados ao longo de vários meses ou até anos, são ainda menos comuns. Quando isso acontece, pode não ter sido de forma proposital ou planejada pelos invasores – pode acontecer de um malware simplesmente passar despercebido, mas isso não significa que os operadores do malware planejavam ficar todo esse tempo na rede da empresa.

Afirmar que algo é "incomum" não é o mesmo que afirmar que algo não acontece, evidentemente. Contudo, o formato e a frequência dos ataques são fatores a serem considerados na análise de ameaças e na produção de inteligência.

O GOLPE DE EXTORSÃO FALSA

Embora threat actors brasileiros raramente apliquem certos tipos de fraude, algumas delas (como o ransomware) foram adaptadas em golpes de engenharia social que simulam um ataque que não aconteceu de fato.

Na extorsão falsa, o criminoso utiliza dados já vazados para tentar convencer a vítima de que ela foi vítima de uma nova violação. O golpista solicita um pagamento para não divulgar a informação sigilosa pretensamente obtida por ele, mas isso não trará benefício nenhum para a vítima, pois não houve nenhuma violação nova e o conjunto de dados já circula na web.

Embora seja uma fraude simples e mais um exemplo do uso de engenharia social no crime brasileiro, nem sempre é fácil identificar que se trata de um caso de extorsão falsa. É preciso solicitar amostras dos dados e ter a capacidade de associar as informações a dados já vazados. O preparo prévio de bancos de dados com mecanismos de rastreamento (tokens) também pode ajudar. As soluções da Axur auxiliam na obtenção destas capacidades.

Assista ao webinar: Como parar e identificar um golpe de extorsão falsa

O DIFERENCIAL DA AXUR

A Axur construiu boa parte de sua história no mercado brasileiro, acompanhando de perto as ameaças locais e os desafios enfrentados pelas empresas que atuam no país. Entendendo que a segurança da informação requer capacidade de adaptação e agilidade, focamos nossos esforços em desenvolver tecnologias que atendem nossos clientes e priorizam as ameaças que são mais importantes para eles.

Monitoramento da Deep, Dark & Surface Web

A Plataforma Axur fornece visibilidade para que você encontre conteúdo relacionado à sua marca ou empresa em canais ligados ao cibercrime, inclusive em conversas realizadas através de serviços como Discord, Telegram e WhatsApp – sendo o WhatsApp um dos mais relevantes para as fraudes brasileiras.

- **Explore e monitore palavras-chave**

Monitore termos de relevância para a sua marca e para o seu negócio. Descubra o que criminosos estão falando e faça pesquisas usando a função Explorer para conhecer o contexto das conversas e o histórico de interações. Conte com os especialistas da Axur para ajudar você na triagem de detecções e encontrar os termos com maior impacto de risco para o seu negócio.

- **DeepChat**

Conte com o DeepChat, nosso modelo proprietário de inteligência artificial generativa, para obter um briefing diário com informações sobre os principais incidentes.

Inteligência e threat actor profiling

O Threat Actor Score e Profiling da Axur permite avaliar a relevância de cada ator malicioso, levando em consideração o histórico da atuação daquele atacante e suas interações com outros criminosos.

A inteligência de ameaças detecta e prioriza informações que podem antecipar ataques, motivar investigações ou acionar times de segurança para corrigir vulnerabilidades quando um ataque for iminente. A Axur tem uma equipe de especialistas pronta para apoiar sua empresa no processo de resposta a incidentes.

RECOMENDAÇÕES E ESTRATÉGIAS DE PREVENÇÃO

As melhores práticas de cibersegurança também ajudam as empresas a se protegerem das ameaças brasileiras. Contudo, certas medidas demandam alguns ajustes para dar conta das especificidades da ameaça:

- Deve ser realizado um monitoramento da superfície externa de ataque (External Attack Surface Management — EASM) para aprimorar a segurança da relação com parceiros e fornecedores (supply chain). Para empresas estrangeiras que atuam no Brasil, essa medida pode ajudar a encontrar desníveis nas práticas de segurança de cada organização. O monitoramento deve preferencialmente ser capaz de detectar credenciais vazadas, como aquelas obtidas por stealers, já que o uso desse tipo de malware é frequente na região.

- Utilizar um Malware Information Sharing Platform (MISP) e feeds de indicators of compromise (IoCs) de modo a expandir a capacidade das ferramentas já em uso no ambiente corporativo e viabilização a detecção de ameaças mais localizadas. A integração de soluções através de um modelo de Extended detection and response (XDR) pode facilitar esse trabalho.

- O treinamento e a conscientização dos usuários ajudam a defender a empresa das fraudes de engenharia social. É importante que a equipe de segurança (ou os responsáveis pelo programa de treinamento) conheçam os ataques mais recorrentes para supervisionar o programa de treinamento.

Veja a diferença na prática

Agente uma conversa com nossos especialistas e inicie um teste gratuito da Plataforma Axur.

AGENDE UMA DEMO