Empresas & Negócios

Matéria de capa

khunkorn_CANVA

CIBERATAQUES

# PROGNÓSTICOS DE SEGURANÇA DE 2022 PARA A AMÉRICA LATINA

**Não é novidade que a pandemia acelerou a adoção de novas tecnologias nos últimos 18 meses e como as novas tendências impulsionaram a adaptação das táticas nos ataques dos cibercriminosos.**

No entanto, conforme as campanhas de vacinação avançaram na região e as atividades presenciais estão retornando, os especialistas da Kaspersky advertem que os cibercriminosos estão se adaptando novamente e focando em ferramentas e naquelas vítimas que maximizarão seus esforços e lucros.

"O cibercrime está em constante evolução, por isso nem as empresas, nem os consumidores, podem baixar a guarda. Os atacantes estão sempre atentos às últimas tendências e tecnologias para fisgar o maior número possível de vítimas.

No entanto, notamos que os ciberataques passaram de simples e massivos para mais complexos e direcionados, o que sugere que os cibercriminosos estão aperfeiçoando suas táticas e procedimentos para atirar à esmo", afirma Dmitry Bestuzhev, diretor da Equipe Global de Pesquisa e Análise da Kaspersky para a América Latina. Os prognósticos para 2022 são os seguintes:

1 **Haverá a consolidação do desenvolvimento de trojans bancários e trojans de acesso remoto (RATs) para Android.** Com o crescimento e maturidade dos serviços bancários móveis, é altamente provável que os grupos de cibercriminosos que tradicionalmente têm como alvo sistemas baseados em Microsoft Windows irão expandir seu portfólio para incluir golpes móveis. Em geral, esses Trojans e RATs serão mais sofisticados em termos de maturidade de código e mais diversificados em termos de alvos.

2 **Os InfoStealers (roubo de informações) vão criar um nicho no crime digital da região.** Devido ao baixo custo de licenciamento e ampla disponibilidade de versões crackeadas, bem como a facilidade de uso e eficácia na coleta e roubo de dados sensíveis de suas vítimas, os trojans infostealer se tornarão uma das ferramentas de ataque preferidas na região.

Os cibercriminosos procuram um equilíbrio entre os seus esforços e os lucros, sendo que os infostealers vão preencher essa necessidade. Veremos um "boom" em sua utilização, independentemente das motivações finais. Sejam elas financeiras ou para o planejamento de ataques futuros mais complexos.

3 **O ransomware dirigido será ainda mais seletivo.** A cultura da região impede que os cibercriminosos latinos consigam persuadir as vítimas a pagar o resgate para recuperar os dados. Por este motivo, os ataques de ransomware se tornam menos atraentes para os pares internacionais, pois seu objetivo final é receber o pagamento.

Frente a esta situação, os grupos que detém o ransomware (programa) serão cada vez mais seletivos, visando vítimas que estão sob uma legislação que prevê multas pesadas para empresas que tenham informações pessoais de clientes vazadas.

4 **Venda de dados roubados em plataforma internacionais.** Os cibercriminosos latino-americanos aprenderam que é mais lucrativo roubar dados pessoais e vendê-los em plataformas internacionais que atraem criminosos que querem comprar essas informações.

Por isso, alguns grupos regionais estão se especializando neste processo de comprometimento de redes das vítimas, roubo de informações sensíveis e venda direta em mercados internacionais, seja em inglês ou em outra língua.

5 **Exploração e monetização do mercado de PoS.** O retomar das atividades econômicas aumentará as transações financeiras realizadas por meio de pontos de pagamento PoS (sigla em inglês para ponto de venda). É um mercado em crescimento e com diversos fabricantes de tecnologia.

Por mais que haja opções, todos os PoS compartilham algo em comum: a falta de segurança contra malware - e esta é a vulnerabilidade que os criminosos continuarão a explorar. Além disso, os cibercrimonosos continuarão a buscar novas oportunidades para explorar os pagamentos digitais feitos nos celulares.

6 **Intensificação dos web skimmers estrangeiros na região.** Durante a pandemia, os consumidores da América Latina se acostumaram a fazer compras online, incluindo mantimentos e outros itens essenciais. Vários sites de comércio eletrônico que oferecem roupas, bebidas, aparelhos eletrônicos e outros itens, serão comprometidos por ações externas para inserir um programa web skimmer (Magecart) para roubar dados de cartões de créditos dos internautas enquanto eles realizam compras nesses sites comprometidos.

Este é um desafio para os administradores online, pois sua detecção requer conhecimento de como esse código malicioso funciona e de suas técnicas de ocultação.

7 **Ataques avançados direcionados, principalmente de origem estrangeira, para obter informações de terceiros e países aliados.** Olhando para a polarização global que existe atualmente, antecipamos ataques avançados do tipo APT (sigla inglês para advanced persistent threat) visando infraestruturas críticas de vários países aliados do mundo ocidental. Tais ataques terão como objetivo extrair informações de interesse para os atacantes, bem como para rivais em países aliados da América Latina.

8 **Fábricas de trolls em redes sociais.** Prevemos uma espécie de legitimação no uso de contas dos tipos troll ou zumbi por diferentes atores políticos no poder e por aqueles que procuram o poder. Esse uso se intensificará durante períodos eleitorais e momentos críticos nas sociedades, como as comoções nacionais devido a grandes eventos.

9 **Golpes com criptomoedas.** Com o aumento da pobreza e a desvalorização das moedas nacionais, mais pessoas estarão à procura de formas de sobreviver ou de assegurar seu dinheiro investindo em criptomoedas.

Infelizmente, por não serem especialistas neste mercado e por motivos culturais, muitas delas acabaram confiando em empresas que anunciavam opções de investimentos fáceis, mas acabam perdendo todo ou parcialmente seu dinheiro - pois estas empresas captam os fundos e depois somem, seja imediatamente ou após alguns envios das comissões prometidas.

10 **Ataques usando códigos QR.** Em 2021, foram identificados vários ataques usando códigos QR, algo que está se tornando cada vez mais comum devido às suas diferentes utilizações, incluindo publicidade em transportes públicos, cardápios de restaurantes, promoções ou localização de lojas.

Este método de ataque combina engenharia social com a facilidade que essa tecnologia oferece às pessoas para que, a partir dos seus dispositivos móveis, possam acessar imediatamente algum site. No entanto, pode haver códigos QR maliciosos que irão instalar aplicações no dispositivo da vítima ou redirecioná-las para sites que irão solicitar informações confidenciais, como credenciais de login.

"Como nossas vidas, o ambiente digital também está se preparando para o mundo 'híbrido'. Neste sentido, em 2022, vamos testemunhar novos tipos de ataques, como infecções por códigos QR e trojans RATs, mas também veremos ameaças que se tornaram famosas neste ano, como ataques a criptomoedas e ransomware", destaca Bestuzhev.

"À medida que se tornam mais seletivos e complexos, estes ciberataques tornam-se mais perigosos, o que aumenta a probabilidade de perdas financeiras grandes e maiores danos à reputação das empresas. Se aprendemos algo durante esses últimos 18 meses de transformação digital, é que tanto as empresas, quanto as pessoas devem ter um conhecimento básico de cibersegurança e praticar bons hábitos digitais.

No caso das empresas, elas também devem conhecer as técnicas e procedimentos dos grupos de cibercriminosos e contar também com visibilidade técnica em suas redes para identificar os atacantes com antecedência, bem como ter acesso a relatórios de inteligência para prevenir problemas (actionable intelligence)". - Fonte e  mais informações, acesse: (www.kaspersky.com.br).

blackdovfx_CANVA