

OPINIÃO

Boom do ransomware não mostra sinais de desaceleração no mundo

Felipe Guimarães (*)

O ano de 2025 vem confirmando os piores temores de especialistas em segurança digital: a epidemia de ransomware continua em expansão, sem indícios de arrefecimento.

Nos primeiros meses de 2025, o volume global de ataques de ransomware deu um salto impressionante com um aumento de 126% em relação ao ano anterior, segundo dados da SonicWall. Entre janeiro e junho, 4.198 casos de ataques foram expostos em fóruns da dark web, quase 50% acima do registrado no mesmo período de 2024.

Os criminosos estão lucrando e reinvestindo nessas ofensivas digitais, tornando-as cada vez mais frequentes e sofisticadas. Apesar de afetar organizações de todos os portes, alguns setores e perfis de empresas têm sofrido com mais intensidade. Os impactos têm sido agravados pela dificuldade de proteger operações distribuídas geograficamente e pela persistência de sistemas legados sem correções de segurança.

Além disso, pequenas e médias empresas não ficam ílesas: organizações entre 50 e 200 funcionários lideraram as estatísticas no mundo todo. Estudos indicam que essa vulnerabilidade das empresas médias se deve, em parte, à dependência de fornecedores terceiros de TI e à falta de medidas abrangentes de cibersegurança.

Escalada global e grupos mais ativos de 2025

Em meio a essa onda global de ataques, alguns grupos de ransomware se destacam pela agressividade e volume de incidentes causados. No segundo trimestre de 2025, por exemplo, três gangues encabeçaram o ranking de atividade criminosa: o grupo Qilin foi responsável por 214 ataques no período, seguido de perto pelo SafePay (com 201 incidentes) e pelo Akira (200 ataques). Esses nomes relativamente novos juntam-se às fileiras dos já conhecidos conglomerados do crime digital.

Grupos veteranos como LockBit 3.0, BlackCat (ALPHV) e Cl0p continuam entre os mais temidos e atuantes do mundo – para se ter ideia, apenas o LockBit foi atribuído a mais de 1.400 ataques nos três primeiros meses de 2025. Essa capacidade de operação em larga escala faz do LockBit e similares uma ameaça onipresente em diversos continentes. Os Estados Unidos seguem liderando em quantidade de vítimas, concentrando cerca de metade dos casos reportados mundialmente no início de 2025.

Mas a atuação desses grupos é verdadeiramente global: empresas na Europa, Ásia e outras regiões também estão na mira, incluindo mercados emergentes menos preparados. Na prática, os criminosos miram onde há dinheiro e vulnerabilidades. Setores críticos como indústrias, serviços financeiros, saúde e até educação já foram atingidos por diferentes variantes de ransomware. No Brasil e na América Latina o cenário não é diferente, com ataques paralisando desde fábricas até órgãos governamentais. Para as organizações vítimas, o prejuízo vai muito além do resgate financeiro: há interrupção de operações essenciais, perda de dados sensíveis e danos reputacionais potencialmente devastadores.

América Latina na mira: setores críticos e respostas estratégicas

Se alguém ainda vê a América Latina como coadjuvante no cenário de ciberameaças, os números recentes

tratam de desfazer esse equívoco. A região se tornou um alvo estratégico tanto para gangues financeiras quanto para outros atores maliciosos. Segundo relatório da CrowdStrike, os ataques de ransomware cresceram 15% na América Latina no último ano, com destaque de incidência em Brasil, México e Argentina.

O Brasil, em particular, é o país mais visado por cibercriminosos na região, não só liderando em quantidade de incidentes, mas também em volume de dados roubados expostos em vazamentos na dark web.

Um levantamento da SonicWall reforça esse panorama: a América Latina apresentou o maior aumento proporcional de ataques de ransomware em 2025, com o Brasil registrando mais de 4 mil ataques apenas no primeiro trimestre do ano. Em fevereiro de 2025, o país atingiu um pico histórico, com mais de 960 ataques de ransomware em um único mês.

Essas estatísticas ressaltam que a região entrou definitivamente na mira dos grupos de ransomware globais. Vários fatores explicam essa tendência. A infraestrutura digital heterogênea, a maturidade ainda baixa em governança de segurança e mesmo leis em evolução tornam muitos países latino-americanos alvos vulneráveis, na avaliação de especialistas.

Para os criminosos, mercados como o Brasil oferecem um ótimo custo-benefício do crime: as chances de sucesso são altas e, muitas vezes, os valores de resgate pagos localmente podem se aproximar dos praticados em países mais ricos. Com isso, há uma migração do foco de ataques: gangues que antes miravam prioritariamente a Europa ou os EUA agora expandiram suas campanhas para a América Latina.

Com isso, setores críticos não estão sendo poupados. Relatórios indicam que indústria, governo, agricultura, energia e varejo estão entre os alvos preferenciais dos ataques na região. Ou seja, tanto infraestruturas essenciais, quanto serviços públicos e negócios estratégicos têm sofrido interrupções e vazamentos de dados.

Diante desse cenário, a realidade é clara: não há mais espaço para improvisos ou negligência. Empresas latino-americanas precisam abandonar a postura reativa, assumindo uma estratégia pró-ativa e integrada que combine tecnologia robusta, processos rigorosos e conscientização constante das equipes. Os ataques de ransomware não vão desaparecer em breve, e aqueles que demorarem para reagir provavelmente enfrentarão crises maiores e mais frequentes.

Cabe agora aos líderes empresariais reconhecerem que a segurança cibernética não é mais apenas um desafio tecnológico, mas uma questão de sobrevivência estratégica para os negócios. Investir em medidas preventivas sólidas, fortalecer planos de resposta e priorizar a segurança digital como pilar fundamental é o único caminho viável para proteger a continuidade dos negócios.

A questão não é mais "se" uma organização será atacada, mas sim "quando". Portanto, estar um passo à frente dos criminosos, com uma postura assertiva e defensiva, será o diferencial entre empresas que sucumbirão aos ataques e aquelas que prosperarão, mesmo diante da ameaça constante do ransomware.

(*) Chief Information Security Officer - CISO da Solo Iron.

Shein abre lojas físicas na França

A Shein, varejista online de fast fashion, planeja abrir suas primeiras lojas físicas na França.

Vivaldo José Breternitz (*)

Isso deve acontecer em novembro, por meio de um acordo com a Société des Grands Magasins (SGM), empresa dona de grandes lojas de departamento como as da marca BHV em Paris e que tem lojas franqueadas da Galeries Lafayette em cinco outras cidades francesas – essas lojas tem um padrão bastante elevado em relação aos produtos vendidos pela Shein.

Em meio a críticas partidas de varejistas locais, o presidente da SGM, Frédéric Merlin, afirmou que a novidade atrairá um público jovem, destacando que um cliente poderá ir do popular ao sofisticado, ao adquirir um produto Shein e uma bolsa de grife no mesmo local.

No entanto, a Galeries Lafayette se posicionou contra a ação, alegando que ela viola o contrato de franquia e pretende impedir sua concretização.

Em comunicado, o grupo disse: “A Galeries Lafayette discorda profundamente dessa decisão, devido ao posicionamento e às práticas dessa marca de ultra fast fashion, que contrariam seus valores.”

A prefeita de Paris, Anne Hidalgo também criticou a abertura, afirmando que o modus operandi da Shein contraria os objetivos do



Gagliardi_Photohraphy_CANVA

governo no sentido promover o “comércio local sustentável”, incentivando negócios e produtos locais.

A Shein, conhecida por vender vestidos a 12 euros e jeans a 20 euros, enfrenta pressão de outros varejistas, políticos e reguladores na França- um projeto de lei em discussão visa regular o fast fashion e pode proibir a publicidade da Shein no país.

O chefe da Federação Francesa do Pret-à-Porter, Yann Rivoallan, declarou que a Shein, após destruir dezenas de marcas

francesas, pretende inundar o mercado nacional com produtos importados descartáveis.

Os varejistas franceses já enfrentavam dificuldades para competir com a espanhola Zara e com a sueca H&M; agora, com a chegada da chinesa Shein, atrairdo consumidores focados em preços baixos, devem passar a enfrentar dificuldades ainda maiores...

(*) Doutor em Ciências pela Universidade de São Paulo, é professor, consultor e diretor do Fórum Brasileiro de Internet das Coisas – vjntz@gmail.com.

Empresa brasileira lança cartão de criptomoedas com integração global e conversão direta na conta do usuário

A OnilX, exchange brasileira focada em soluções de pagamento com ativos digitais, assessoria e educação financeira, anuncia o lançamento do Crypto Card OnilX, produto exclusivo desenvolvido com tecnologia 100% própria. A novidade chega ao mercado com a proposta de integrar de forma prática a jornada do cliente cripto, levando os ativos digitais para o uso direto e facilitado no cotidiano, com a conversão de criptomoedas para reais automaticamente na conta do usuário, sem que o lojista precise lidar diretamente com criptomoedas.

O movimento acompanha uma tendência global. Segundo relatório da Boston Consulting Group (BCG), o mercado de pagamentos com criptoativos deve ultrapassar os US\$ 3 trilhões até 2030, impulsionado pela busca por soluções financeiras mais ágeis e descentralizadas. No Brasil, estima-se que, dos 59 milhões de investidores nacionais, cerca de 11% alocam parte dos seus recursos em criptoativos. Este número representa cerca de 6,5 milhões de pessoas – 3% da população do país –, especialmente homens na faixa dos 30 anos, que já operam ativos digitais, conforme pesquisa realizada pela Associação Brasileira das Entidades dos Mercados Financeiro e de Capitais (Anbima).

“O lançamento do cartão é um marco estratégico para a OnilX. Nosso objetivo é conectar a confiança dos nossos clientes no universo cripto ao uso direto no dia a dia. Queremos eliminar



Divulgado

barreiras, mostrar que o dinheiro digital já é realidade e oferecer uma solução completa para quem busca praticidade e liberdade financeira”, afirma Fabio Lino, presidente da OnilX.

Assim como um cartão tradicional, o Crypto Card OnilX permite o pagamento de qualquer compra no Brasil e no exterior em poucos segundos, com segurança e muita agilidade. Além disso, ele facilita a conversão do saldo em reais (R\$) da conta no OnilX Bank em Tether

Dólar (USDT), conhecido como “dólar digital”, stablecoin atrelada ao dólar estadunidense; e agiliza a transferência do USDT de qualquer exchange para a conta OnilX Bank. “Vale destacar que, além de toda sua funcionalidade, o grande diferencial do Crypto Card está em sua tecnologia, desenvolvida com exclusividade pela OnilX”, destaca Fabio Lino.

De acordo com Lino, enquanto outras soluções internacionais operam de forma limitada no Brasil, a OnilX desenvolveu uma estrutura pensada para o mercado local, com compliance regulatório, integração bancária e atendimento direto em português. “Construímos nossa própria tecnologia para oferecer mais segurança, velocidade e flexibilidade. Isso nos permite adaptar o produto às demandas do cliente brasileiro e ampliar as funcionalidades de forma contínua, sem depender de terceiros”, explica o presidente da OnilX.

O lançamento marca também uma evolução no posicionamento da OnilX como ecossistema de soluções financeiras digitais. “Além da exchange, o cartão entra como peça-chave para consolidar a empresa como referência em inovação no setor”, ressalta Lino. O Crypto Card OnilX poderá ser solicitado com exclusividade pelos clientes OnilX, via aplicativo oficial (OnilX Bank), até o próximo dia 27 de outubro. Na sequência, o cartão será liberado para o público geral (www.onilx.com.br).



News @TI

ricardosouza@netjen.com.br

Programa de pós em Estatística da USP e da UFSCar abre inscrições para ingresso em 2026

@ Como seria poder estudar em duas universidades ao mesmo tempo, usufruindo da infraestrutura e do corpo docente de ambas? Essa é a proposta do Programa Interinstitucional de Pós-Graduação em Estatística (PIPGEs), que reúne o Instituto de Ciências Matemáticas e de Computação (ICMC) da USP, em São Carlos, e o Departamento de Estatística da Universidade Federal de São Carlos (UFSCar). As inscrições para os processos seletivos de ingresso em 2026 já estão abertas e podem ser feitas gratuitamente até às 17 horas do dia 20 de outubro de 2025 em <http://bit.ly/3KweEiw> (mestrado) e Inscrições ao Processo Seletivo de Doutorado - 01/2026 (doutorado). No momento da inscrição os candidatos deverão enviar uma carta de apresentação relatando os motivos para ingressar no programa, experiências prévias na área e, se for o caso, pesquisas já realizadas.

ABCOMM muda para ABIACOM e reforça aposta na inteligência artificial

@ A ABCOMM, Associação Brasileira de Comércio Eletrônico, anunciou oficialmente sua mudança de nome para ABIACOM, Associação Brasileira de Inteligência Artificial e E-commerce. A alteração reflete o novo posicionamento da entidade diante do rápido avanço da inteligência artificial e de sua influência direta sobre o futuro dos negócios digitais. Nos últimos anos, a IA deixou de ser apenas uma tendência distante e se tornou realidade concreta, capaz de transformar processos, otimizar resultados e abrir novas oportunidades para empresas e consumidores. Segundo a entidade, o setor de e-commerce já consolidou sua trajetória como ponte entre tecnologia e negócios, mas agora a missão é expandir esse papel para assumir protagonismo também no campo da inteligência artificial (<http://www.abiacom.org/>).

Editorias

Economia/Política: J. L. Lobato (lobato@netjen.com.br); Ciência/Tecnologia: Ricardo Souza (ricardosouza@netjen.com.br); Livros: Ralph Peter (ralphpeter@agenteliterarioph.com.br);

Comercial: comercial@netjen.com.br

Publicidade Legal: lilian@netjen.com.br

Webmaster/TI: Fabio Nader; Edição Eletrônica: Ricardo Souza.

Revisão: Maria Cecília Camargo; Serviço Informativo: Agências Brasil, Senado, Câmara, EBC, ANSA.

Artigos e colunas são de inteira responsabilidade de seus autores, que não recebem remuneração direta do jornal.

Jornal Empresas & Negócios Ltda

Administração, Publicidade e Redação: Rua Joel Jorge de Melo, 468, cj. 71 – Vila Mariana – São Paulo – SP – CEP: 04128-080

Telefone: (11) 3106-4171 – E-mail: (netjen@netjen.com.br)

Site: (www.netjen.com.br). CNPJ: 05.687.343/0001-90

JUCESP, Nire 35218211731 (6/6/2003)

Matriculado no 3º Registro Civil de Pessoa Jurídica sob nº 103.