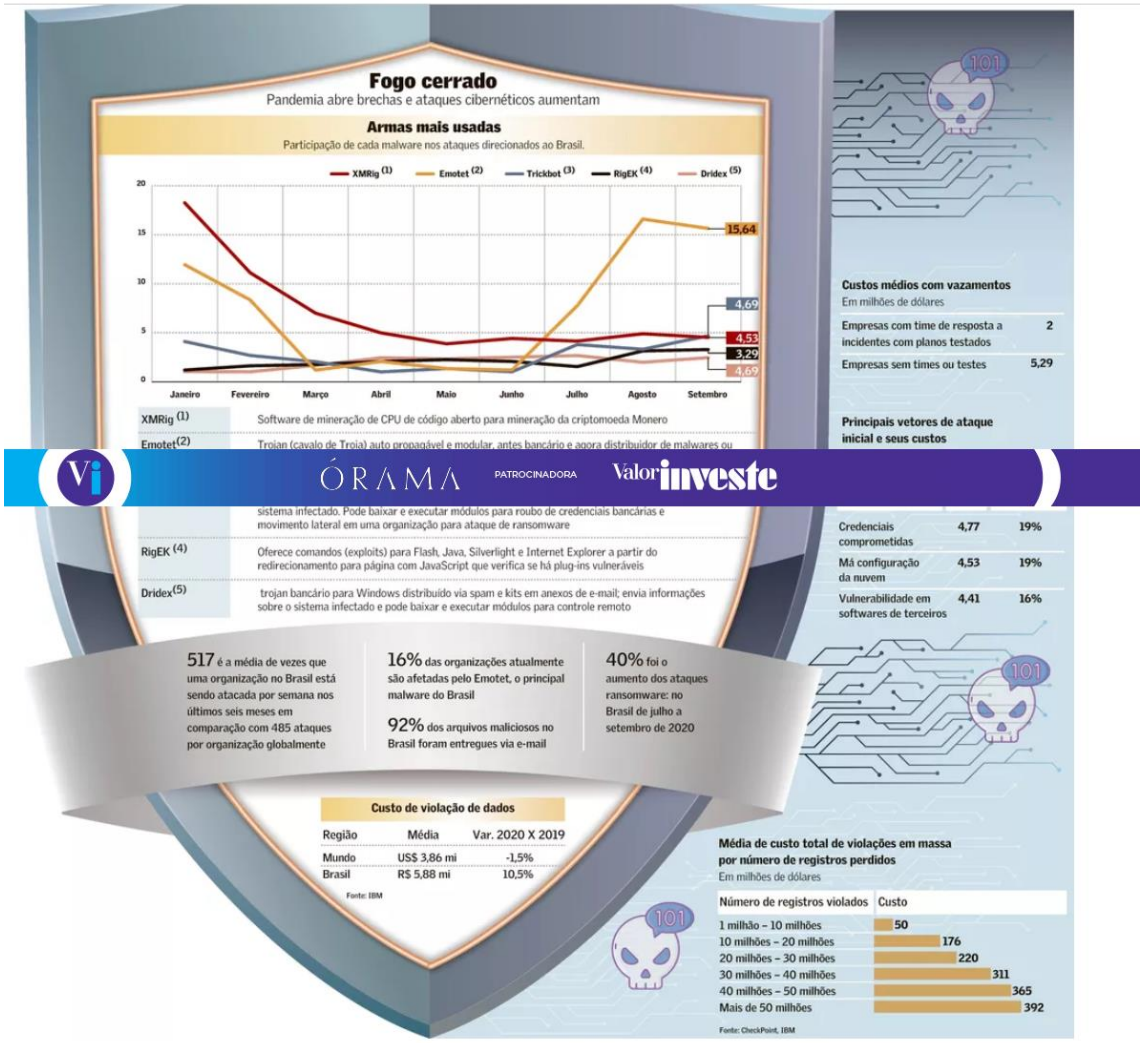
Onde mora o perigo

Crescentes na pandemia, os ataques cibernéticos levam empresas a reforçar seus sistemas

Por Martha Funke — Para o Valor, de São Paulo
19/10/2020 05h01 · Atualizado há 6 horas



ÓRAMA PATROCINADORA Valor investe

Ataques cibernéticos aumentaram em meio à pandemia. Pessoas abaladas e usuários corporativos remotos se tornaram prato cheio para ameaças. Os criminosos empregam automação, recursos de inteligência social e análise de grandes bancos de dados para investidas em massa ou direcionadas a setores ou empresas, e movimentam um mercado trilionário de venda de dados pessoais, códigos e até ataques por encomenda.

Só no segundo trimestre, os ataques de ramsomware, com solicitação de resgate para evitar exposição de dados ou desencriptar arquivos, cresceu 40% no país. E-mails respondem por 91% das ameaças infiltradas nas empresas, principalmente para execução remota de códigos maliciosos, presentes em 72% das organizações atacadas. Temas do momento são iscas, de dicas de saúde a currículos para RHs, aponta Claudio Bannwart, country manager da Check Point, responsável pelos dados.

Os códigos maliciosos buscam credenciais de acesso para atingir desde sistemas com dados sensíveis até os de missão crítica. O movimento chegou a empresas de todos níveis e setores em momento de fluxo de caixa comprometido. Mas o gerente de pesquisa Luciano Ramos, da IDC, estima que o mercado de segurança da informação cresça 11% em 2020 no Brasil, puxado por segurança de rede e de conectividade e serviços gerenciados.

As organizações focaram primeiro redes privadas (VPNs) para acesso seguro às aplicações pelas equipes remotas. Segurança de dispositivos dos usuários e de aplicações consumidas por clientes, de e-commerce a canais de comunicação, gestão de identidade e respostas a incidentes, estão acelerando e ajudarão nos negócios em 2021.

Digitalização veloz, home office, internet das coisas (IoT) e IoT industrial (IIoT) abriram espaço para os criminosos. O consumidor, em mercados como finanças e varejo, foi o principal vetor de ataque, afirma Leandro Augusto, sócio da KPMG.

Pressa na adoção de nuvem também deixou brechas. "Falta de cultura, superfícies com novas oportunidades e facilidade de ganhar dinheiro atraem o crime", diz André Fleury, líder em cibersegurança da Accenture. A consultoria tem ajudado desde clientes sem backups atualizados até proprietários de estruturas gigantescas com equipe própria e necessidade de apoio externo, inclusive para avaliar a segurança de empresas da cadeia de valor.

A Febraban, por exemplo, contabiliza R$ 2 bilhões em recursos anuais dos bancos para cibersegurança e investiu R$ 6 milhões em laboratório com apoio da Accenture para treinamento, simulações, compartilhamento de informações e avaliação de prestadores de serviços. Apesar de seguro, o setor é alvo do crime por potencial de lucro. Estudo da VMware mostra 238% mais ataques ao setor entre fevereiro e abril.

A captura de informações para venda ou encriptação - ou ambos - afetaram varejo, saúde, energia, óleo e gás, manufatura, órgãos de governo e educação. Em março, a Cosan interrompeu sistemas e parte de operações de controladas como Comgás, Raízen, Rumo e Cosan Logística. Energisa, Light, Enel e EDP relataram ataques à TI, inclusive vindos do exterior, com impacto em atividades de back office. Ataque ao Detran-RN expôs a identidade de 70 milhões de condutores. Avon (Natura) e Braskem chegaram a suspender partes de operações. O Hospital Sírio-Libanês, a operadora de saúde Hapvida, Anhembi Morumbi, Uninove e Unicamp estão entre alvos de hackers.

Ramsomware atinge serviços essenciais e segmentos com IoT ou IIot - quanto maior o impacto, maior probabilidade de pagamento, diz o especialista da Trend Micro, Flávio Silva.

"Poucas empresas no Brasil têm visão integrada de riscos para definir investimentos", diz Marco Sêmola, sócio para cibersecurity da EY. Mas, para o especialista Paulo Pagliusi, pouco adianta a tecnologia frente ao "clicador" compulsivo.

Segundo o country manager da Palo Alto, Marcos Oliveira, até setembro foram mais de 40 mil sites registrados ligados à covid-19. Estudo da IBM aponta crescimento de 6.000% em spam com o tema. A curiosidade sai caro. Segundo o head de segurança da IBM Brasil, João Rocha, o custo médio de violação de dados no país está em R$ 5,88 milhões, 10,5% mais que em 2019. O número de dias para identificação subiu de 250 para 265 e, para contenção, de 111 para 115.

Apesar do comportamento inseguro, o Brasil é o país com população mais preocupada quanto à segurança digital no mundo, principalmente fraude bancária (80%) e roubo de identidade (78%), diz Alexis Aguirre, diretor da Unisys.

Os ataques movimentam negócios em todo o mundo. Os investimentos globais em segurança cibernética devem somar US$ 123,8 bilhões este ano, 2,4% mais que em 2019, segundo o Gartner, com crescimento em ofertas baseadas em nuvem e assinaturas em substituição a licenças passando de 50% em segmentos como e-mails seguros.

A percepção de que antivírus e firewall são insuficientes para garantir a segurança corporativa leva empresas a buscar novas formas de proteção. Modernização de sistemas, backups atualizados e testados, planejamento de risco integrado com recuperação de desastres, serviços gerenciados, soluções de software e de hardware entregues como serviço, automação de operações manuais, gestão de identidade de acesso, inteligência de dados, testes de ameaças e centro de serviços de segurança (SOC) apoiado por tecnologias de aprendizado de máquina e inteligência artificial (IA) estão na mesa.

A Accenture comprou da Broadcom a divisão de serviços de segurança digital da Symantec e usa ferramenta de simulação de guerra cibernética (Simoc) empregada pelo Exército brasileiro. Cresceu ainda a oferta de monitoramento das marcas na internet exposta e oculta, diz Wesney Bolzan Silva, diretor da Cipher, que fornece ferramentas de gerenciamento de eventos e segurança de informação (SIEM) e de segurança de dispositivos (endpoints).

A BluePex, considerada empresa estratégica de defesa (EED) pelo Ministério da Defesa, espera crescer 50% este ano com modelo de negócio de software e hardware próprios como serviço (SaaS e HaaS), criado há dois anos depois de aporte de R$ 6 milhões do Criatec 3, do BNDES, explica o CTO Ulisses Penteado. Seu portfólio inclui desde suíte em nuvem com gestão centralizada de soluções como antivírus até backup e recuperação de dados, com mais de 60 mil dispositivos monitorados diariamente.

A Netskope cresceu mais de quatro vezes durante a pandemia no Brasil, diz o diretor de vendas Vinícius Mendes. As áreas mais requisitadas são governança de acesso ao usuário de próxima geração (NGSWG) e acesso a rede zero trust, com visibilidade total de identidade e acesso na rede corporativa.

A Forcepoint prevê expansão de 50% este ano e quer aumentar a equipe em 30% em 2021. A Eset vê maior demanda em apoio ao teletrabalho, como sistemas de proteção para alertar o acesso a links maliciosos em SMS, WhatsApp e e-mails, e soluções capazes de detectar ramsomware, entre outras, diz o especialista em segurança Luis Lubeck.

Para João Rocha, da IBM, investimentos estão mais inteligentes, para suprimir lacunas, manter e integrar o que já existe. Isso desde questões negligenciadas, como backups e criptografia de dados em repouso ou movimento, até correção de abordagem digital equivocada. Lançar serviços digitais ou ir para nuvem sem segurança por design custa caro. "Erros de configuração e desenho de arquitetura estão por trás de 51% dos problemas de segurança."

O volume de negócios levou a Tivit a criar nova divisão de cybersecurity. A área passou de 10 para 70 funcionários em dois anos. Em 2020 sua receita crescerá quase seis vezes e, em 2021, deve alcançar R$ 100 milhões. Serviços de contenção de vazamentos expandem vendas de soluções de monitoramento com IA e capacidade de bloqueio, serviços de gestão de crise, desencriptação, testes de penetração, softwares detecção, resposta a ameaças em dispositivos (EDR), camada de segurança entre dispositivos e aplicações (CASB) e planos com SOCs modernizados. Novas áreas miram conversão segura de softwares para nuvem (devsecops) e análise de ameaças (tech intel), inclusive com iscas, códigos falsos rastreados por robôs na web oculta.

A Microsoft reforçou sua segurança em IoT e IIoT com aquisição da Cyber X. Segundo o diretor de cibersegurança para a América Latina, Nycholas Szucko, os ataques da área cresceram 35% no primeiro semestre em relação ao mesmo período de 2019.