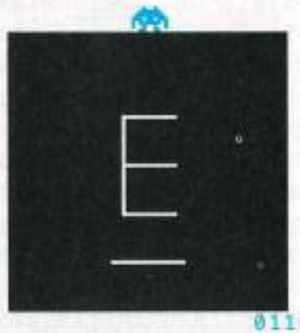
PELA PAZ D1G1TAL

OS ATAQUES CIBERNÉTICOS EXPLODIRAM NA PANDEMIA, EXPONDO UM PROBLEMA QUE, EM 2021, DEVE CUSTAR US$ 6 TRILHÕES À ECONOMIA GLOBAL. A SEGURANÇA DE DADOS GANHA FINALMENTE IMPORTÂNCIA DENTRO DAS EMPRESAS

MARCELO MOURA E DANIEL HAIDAR



"Cybersecurity — Fighting Invisible Threats", do banco suíço Julius Baer. Em 2015, o prejuízo somou a metade desse montante, segundo a consultoria Cybersecurity Ventures. No topo dos países mais prejudicados estão os Estados Unidos, segundo a plataforma de dados Statista, com US$ 27 milhões. O Brasil aparece na décima posição, com US$ 7 milhões desperdiçados. Todos os dias, são perpetrados 8 trilhões de ataques, ao redor do globo. Sim, inacreditáveis 90 mil ações criminosas por segundo — and counting...

Pela primeira vez, em 2020, os ataques cibernéticos apareceram como a principal ameaça aos negócios na pesquisa Risk Barometer, da seguradora Allianz, feito com quase 3 mil especialistas em análise de risco, em cem países. Sete anos antes o assunto figurava na 15ª colocação. A preocupação é natural — quanto mais a vida se digitaliza, mais vulneráveis ficamos à ação dos hackers. Como dizia Willis Ware (1920-2013), cientista da computação e um dos pioneiros nos estudos sobre privacidade: "O único computador completamente seguro é o computador que ninguém consegue usar".

A pandemia só aumentou o risco à segurança digital de empresas e pessoas. "Imagine que você precisa invadir dois edifícios", propõe Stephen McBride, analista-chefe da RiskHedge, consultoria de investimentos. "O primeiro é uma mansão em Bervely Hills. Se a porta da frente não servir, você pode tentar a entrada pelo bar ao lado da piscina, ou por alguma das 20 janelas da casa. O segundo endereço é um bunker subterrâneo: paredes de concreto, nenhuma janela, só uma porta." A mensagem é simples: quanto mais entradas para vigiar, mais vulnerável é a casa. Agora pense em quantos serviços de e-commerce passaram a saber o seu número de cartão de crédito, quantos entregadores souberam o seu endereço — e, antes de entregar a encomenda, pediram seu nome, RG e assinatura.

Ao adotar o home office com o equipamento pessoal de cada funcionário, as empresas fizeram dados corporativos passarem por computadores domésticos antigos (o sistema operacional Windows 7, lançado em 2009, ainda está em cerca de 30% das máquinas), compartilhados por adultos e crianças, com sistemas antivírus desatualizados, conectados a roteadores wi-fi com uma senha boba (um

EM SUAS CONTAS no LinkedIn, funcionários do banco Itaú convidam:

"A fim de trabalhar no red team do maior banco privado brasileiro?".

Enquanto isso, a gigante do varejo eletrônico B2W oferece vagas em seu blue team. Já a EY tem postos disponíveis tanto no blue quanto no red.

Atualmente, tem sido assim... Vermelhos e azuis, analistas de segurança cibernética disputadíssimos no mercado. Com inspiração nos jogos militares, ao blue team de uma companhia cabe defender a empresa e achar vulnerabilidades. Ao red team, a ameaça de invadir e de derrubar as barreiras dos sistemas. Em algumas corporações, as equipes se revezam em turnos de 24 horas por dia, sete dias por semana. Vigilância é tudo. E não é à toa. O cuidado com a segurança da informação se justifica.

Em 2021, os crimes cibernéticos devem custar US$ 6 trilhões à economia global, conforme o relatório

PIONEIRO O cientista da computação Willis Ware (1920-2013) costumava dizer: "O único computador completamente seguro é o computador que ninguém consegue usar"

REPRODUÇÃO: RAND CORP


EM 2021, OS CRIMES
CIBERNÉTICOS DEVEM
CUSTAR US$ 6 TRILHÕES
À ECONOMIA GLOBAL

vazamento dos dados de 117 milhões de usuários do LinkedIn, em 2012, mostrou que as três senhas mais comuns eram "123456", "linkedin" e "password"), compartilhando a rede com equipamentos como smart TVs, videogames ou mesmo aspiradores de pó. "Quanto mais dispositivos ligados à rede, maior a superfície de ataque, facilitando a infiltração de hackers", diz Stephen. Antes da pandemia, residências e empresas não eram exatamente bunkers. Com o isolamento imposto pelo Sars-CoV-2, ganharam novas janelas. "O crime apenas se mudou para o território online. É como se fosse uma temporada de férias, quando as pessoas vão viajar e ladrões aproveitam para invadir as residências. Os vigaristas procuram oportunidades para explorar e, com a covid-19, não é diferente", diz a Época NEGÓCIOS Jaya Baloo, CISO (Chief Information Security Officer) global da Avast Software. "Do ponto de vista corporativo, são grandes desafios, um cenário para o qual ninguém poderia se preparar plenamente."

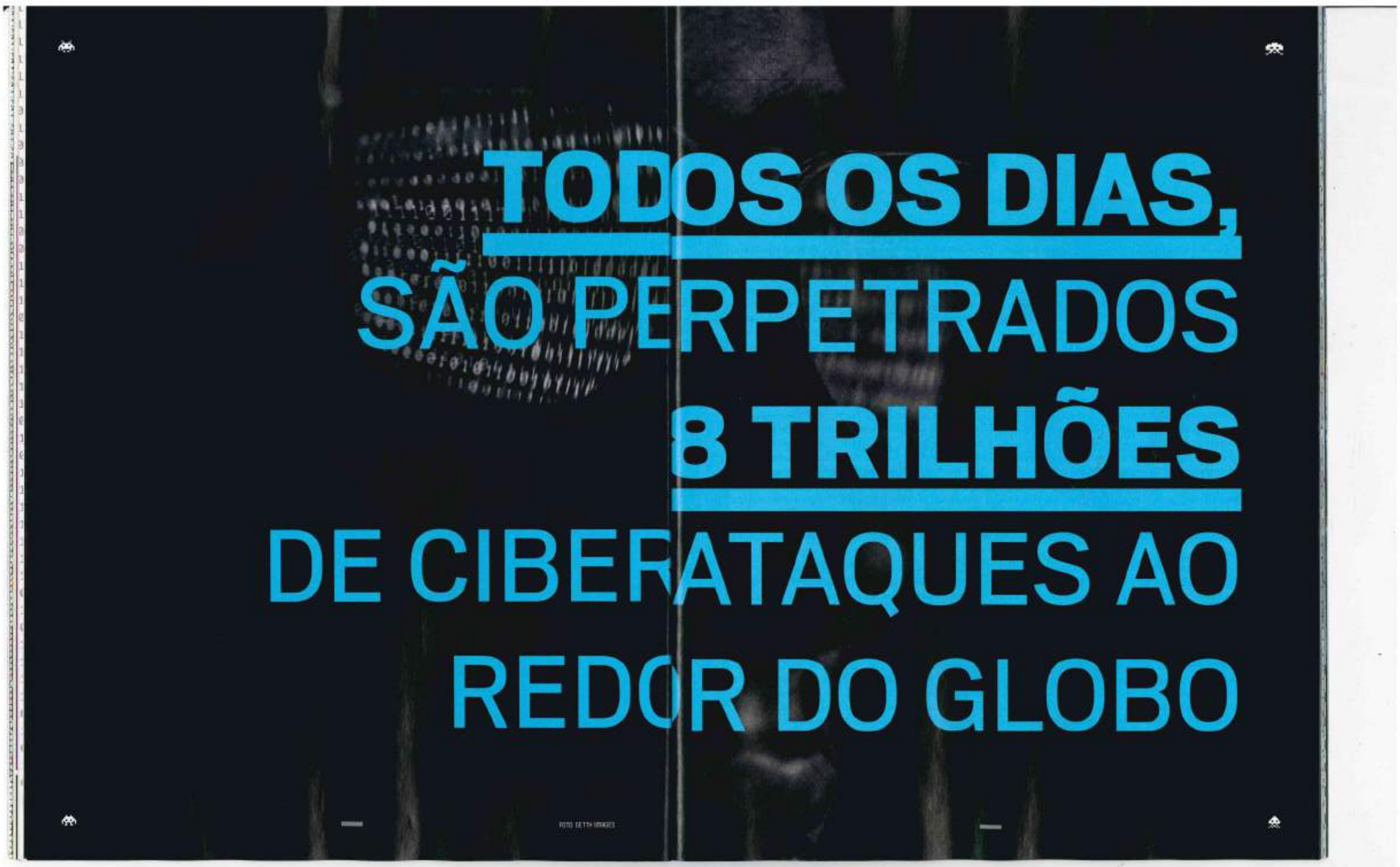
Desde março, ataques hackers causaram prejuízos milionários e paralisações em operações de pelo menos 20 empresas brasileiras. A Cosan, de energia, parou por um dia. Em junho, criminosos cibernéticos invadiram a empresa de energia Light — pediram um resgate de US$ 7 milhões — e a empresa de cosméticos Avon, comprada pela Natura. No mesmo mês, a Honda parou: e-mails internos, quitações de financiamentos, fábricas de carros e motos paralisaram suas atividades em países como Japão, Estados Unidos, Índia, Turquia e Brasil. Segundo a consultoria Malwarebytes, a montadora foi vítima do Snake, programa malicioso identificado pela primeira vez em 2019, que vai contra sistemas de controle industrial. Oportunistas, atacam justamente quando a empresa mais precisa funcionar — porque, assim, está mais disposta a pagar pela normalidade. As investidas mais cruéis atualmente são contra centros médicos e laboratórios de pesquisa e/ou tratamento para o Sars-CoV-2. Repleto de pacientes de covid-19, o segundo maior hospital da República Tcheca foi forçado a desligar os equipamentos e remanejar os doentes. "Esses invasores não têm nenhum tipo de pudor em atacar um lugar que está protegendo vidas", diz Marcos Oliveira, country manager no Brasil da Palo Alto Networks, empresa de software de segurança que atende 85% das companhias da lista Fortune 100. "Quando um ataque acontece, há várias firmas especializadas na recuperação. É um CSI da informação. Mas é um serviço caro, e quem está sofrendo não tem muita margem para reclamar."

As empresas relutam em reconhecer quando são vítimas de algum golpe, por entender isso como uma admissão de fraqueza. Mas guardar segredo, a exemplo do que ocorre em outros tipos de crime, favorece o criminoso. "Eu devo dizer à minha comunidade: 'passei por esse incidente, eles tiraram proveito disso, disso e disso. Por favor, se preparem, porque vocês podem ser os próximos'", diz a Época NEGÓCIOS Nycholas Szucko, diretor de cibersegurança da Microsoft para a América Latina. "Quer dizer que eu sou vulnerável, quer dizer que eu não fiz o meu trabalho bem? Não é isso. O CISO tem de se preocupar com quantas coisas? Um milhão. O invasor precisa de... uma única brecha. A gente já tem um número de alertas muito mais elevado do que é capaz de responder. Precisamos, pelo menos, colaborar." Se o senso de comunidade não for suficiente para dar transparência à comunicação de ataques, a lei haverá de ser.

Adiada para agosto do próximo ano, a Lei Geral de Proteção de Dados (LGPD), a exemplo das legislações similares dos Estados Unidos e da Europa, responsabiliza as empresas pelo extravio de dados sob sua guarda. "O artigo 43 da LGPD diz que você precisa informar a extensão do vazamento e a natureza da informação que vazou, para ser possível apurar se houve dano, ou a extensão do dano", diz Leandro Martinez, vice-presidente no Brasil da seguradora Chubb, uma das líderes

SURPRESA Sobre a explosão de ciberataques provocada pela covid-19, Jaya, CISO global da Avast, define "um cenário para o qual ninguém estava preparado"

FOTO: DIVULGAÇÃO


TODOS OS DIAS,
SÃO PERPETRADOS
8 TRILHÕES
DE CIBERATAQUES AO
REDOR DO GLOBO
FOTO GETTY IMAGES

do mercado global de cobertura a cyber riscos. "Acho que vai mudar bastante quando a Agência Nacional de Proteção de Dados começar a ter dentes e sair mordendo por aí." A lei brasileira prevê multas de até R$ 50 milhões, ou 2% do faturamento bruto anual — o que for maior. Talvez, assim, certas companhias passem a dar o devido valor à proteção. "Tem empresa que investe menos de 0,01% do seu faturamento em segurança. E se parar durante uma hora, já perde várias vezes esse valor", diz Demetrio Carrión, líder de cybersecurity da EY para a América Latina. "As pessoas fazem seguro do carro, mas não fazem seguro contra ataques digitais, meramente porque o concorrente também não faz."

Dados da Susep mostram que a LGPD fez o mercado acordar. De janeiro a maio de 2020, as seguradoras coletaram R$ 14,1 milhões com coberturas contra cyber riscos, 107% mais do que no ano passado. Mais interessante do que o aumento de volume é o aumento no total pago em indenizações: R$ 12,2 milhões até agora, ante apenas R$ 69 mil em 2019. É um sinal de amadurecimento. "Sabe aqueles almoços de família no fim de semana, com uma mesa para os adultos e uma mesinha, à parte, para as crianças? A segurança digital está passando para a mesa dos adultos", diz Cristiano Lincoln Mattos, cofundador e CEO da Tempest, maior empresa de cibersegurança do Brasil (*leia entrevista na página 50*). Em julho, a companhia teve sua participação majoritária vendida para a Embraer. Esta repete a estratégia da Boeing, que nos últimos dois anos comprou cinco firmas de cybersecurity. A rede de varejo americana Target contratou seu primeiro CISO em 2014, meses após perder US$ 252 milhões com o vazamento de dados de 70 milhões de clientes.

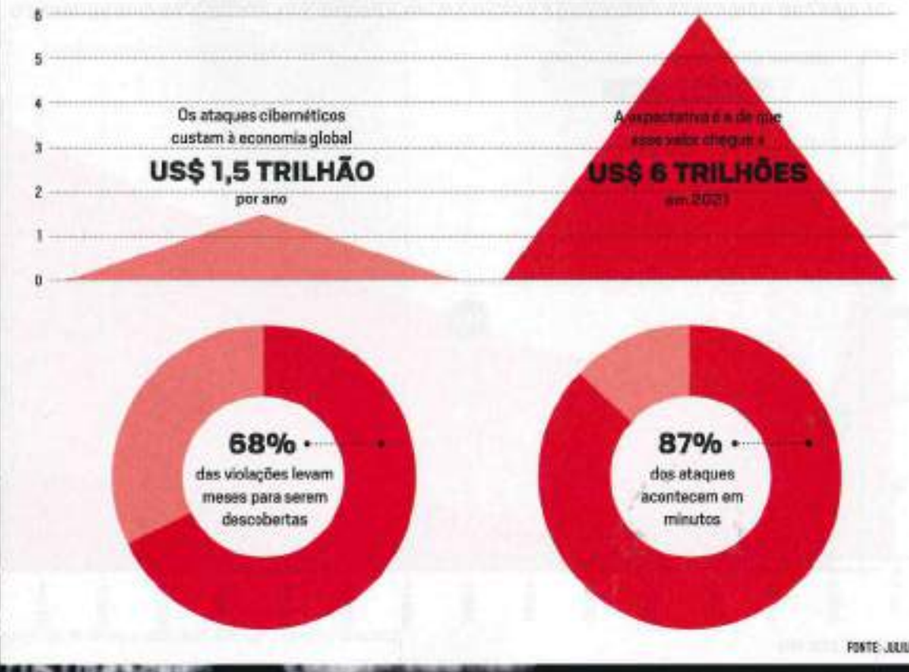
Quem investe em IoT ou transformação digital sem pensar na segurança está colaborando com o hacker. "Você dá eficiência à sua operação e também à invasão. Antes, o ladrão assaltava uma agência. Hoje pode tentar roubar todo o dinheiro, como em Bangladesh", diz Demetrio, em referência à tentativa (parcialmente fracassada) de roubar US$ 1 bilhão do Banco Central do país asiático, em 2016. Digitalizar processos e transferir arquivos e máquinas para a nuvem são formas de dar eficiência à empresa e atualizar a tecnologia. Mas traz desafios novos. "No conceito de cloud, sua infraestrutura é escalável automaticamente. Por exemplo, a Ticketmaster pede mais máquinas quando vai vender ingressos para um show do Paul McCartney", diz Daniel Bortolazo, gerente de Engenharia de Sistemas da Palo Alto. "Mas já vi casos de grandes pedidos de máquinas adicionais sem nenhuma mudança na produção do cliente. O hacker roubou senhas da empresa e começou a pedir máquinas, para minerar criptomoedas. Isso tem um impacto financeiro muito grande, porque a AWS, a Microsoft, o Google, não vão devolver essa grana. A proteção das senhas é sua."

Comprar tecnologia e não treinar periodicamente a equipe é desperdiçar dinheiro. Na Microsoft, as simulações de ataque hacker são mais frequentes do que as de incêndio — uma por semestre na filial brasileira, duas na matriz americana. "Incidentes cibernéticos são eventos emocionais. Você não tem mais controle do seu sistema, não consegue mais acessar nem suas ferramentas de proteção, é muito difícil lembrar o que fazer", diz Nycholas. "Ensaiando várias vezes, na hora em que acontecer alguma coisa — tomara que não aconteça — a gente consegue responder da melhor forma possível."

Para crescer com segurança digital, o CEO precisa decidir o que vale a pena proteger. Não é um conceito absoluto. É uma decisão política, que requer sensibilidade e pragmatismo. "O que você quer guardar? De quem? Por quanto tempo?", pergunta Jaya, da Avast. A proteção em ambiente de nuvem, com trabalhadores remotos, é seletiva. Não é preciso ter todas as peças imobilizadas num canto do tabuleiro de xadrez. Basta proteger o rei. "Você não tem de ser vidrado em ter o melhor do mundo em segurança. Precisa saber, com clareza, quais ameaças a organização pode sofrer", diz Demetrio, da EY. "Acho um erro tratar segurança da informação como uma atribuição do departamento abaixo de TI. Muitas vezes, essas duas áreas têm objetivos distintos."

É fundamental elaborar um mapa de informações — quem tem acesso a que, como e por que —, para discutir restrições e identificar desvios de padrão. Num mapeamento assim, Daniel já encontrou excentricidades como a

AMEAÇA INVISÍVEL



FONTE: JULIUS BAER

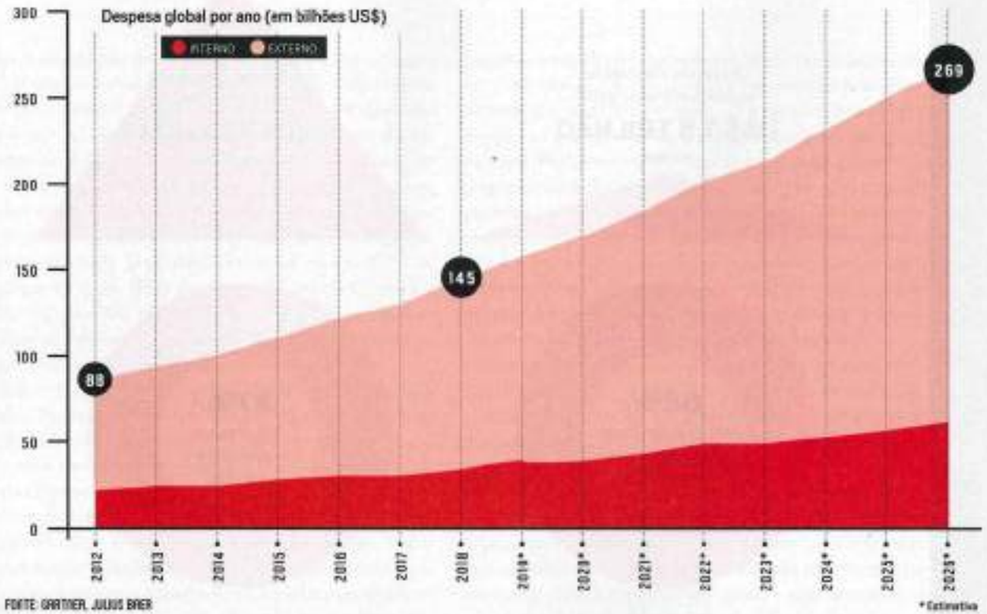
DISPARA O PREJUÍZO COM CIBERATAQUES À INDÚSTRIA DE SEGUROS

A perda de clientes, que tinham contratados seguros cibernéticos, já é bem maior até o fim de maio de 2020 do que em todo o ano de 2019

FONTE: SUSEP

SETOR EM ALTA

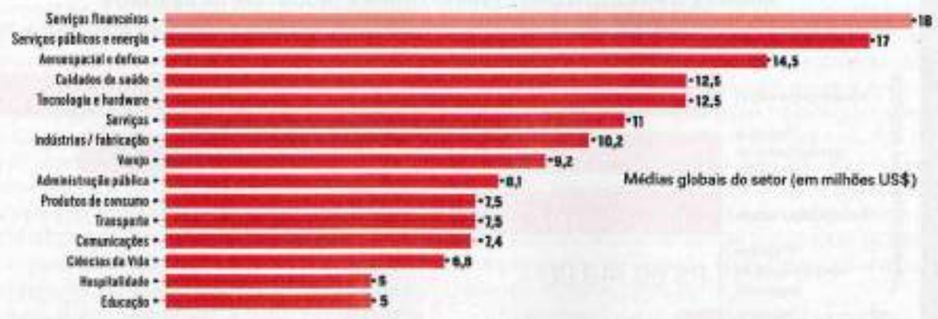
OS GASTOS COM CIBERSEGURANÇA ESTÃO EM UMA FORTE TRAJETÓRIA DE CRESCIMENTO



FONTE: GARTNER, JULIUS BAER

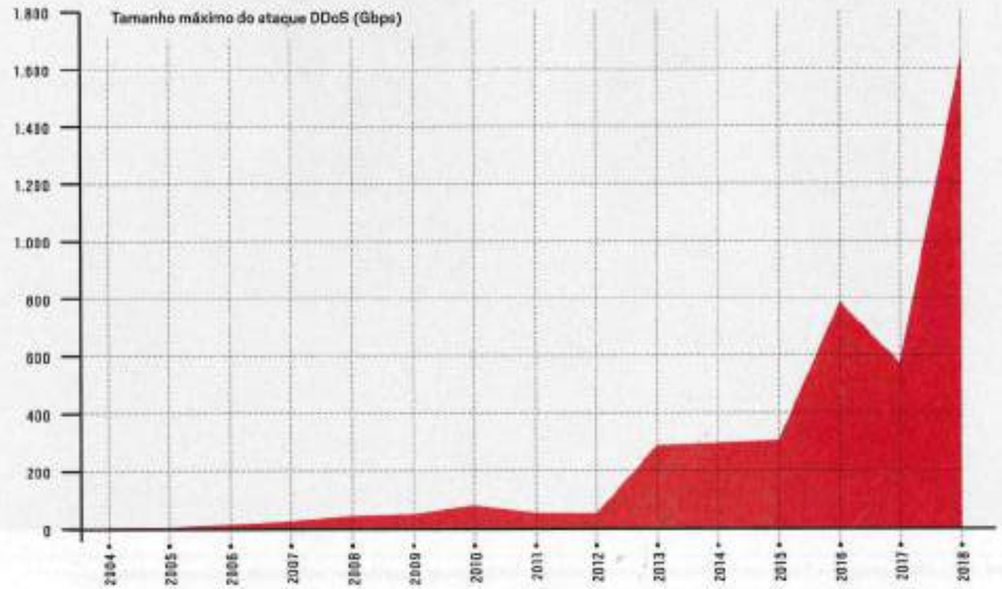
* Estimativa

O CIBERCRIME NÃO É APENAS UMA QUESTÃO DO SETOR FINANCEIRO



FONTE: ACCENTURE, PONEMON INSTITUTE (OS DADOS EXISTEM APENAS PARA EMPRESAS POR IND., AGRUPADOS POR SETOR)

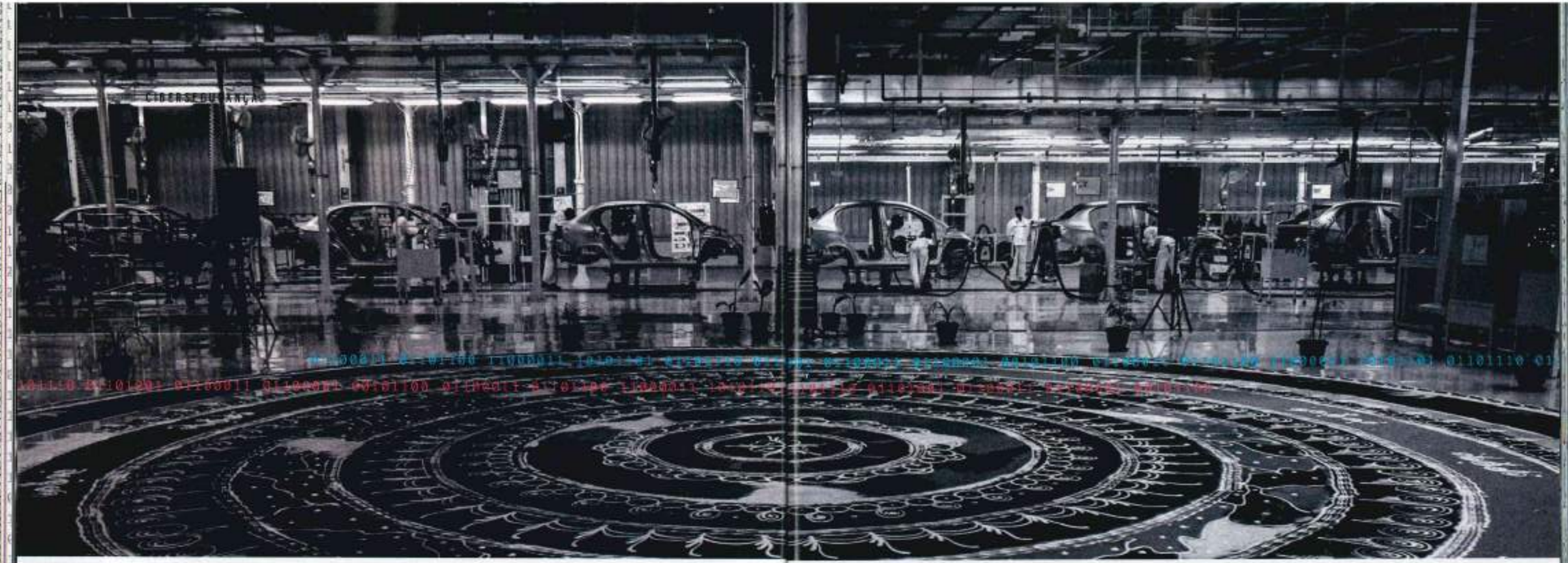
O ATAQUE DDOS SE TORNOU MUITO MAIS AGRESSIVO



FONTE: CATBRIDGE CENTER FOR NOC STUDIES, JULIUS BAER; GBPS = GIGABYTE POR SEGUNDO

O CRESCIMENTO NO NÚMERO DE DISPOSITIVOS CONECTADOS É EXPONENCIAL

FONTE: NEW SIGNATURE, JULIUS BAER



GOLPE Em junho, o programa Snake parou a Honda: e-mails internos, quitações de financiamento, fábricas de carros e motos travaram no Japão, Estados Unidos, Índia, Turquia e Brasil

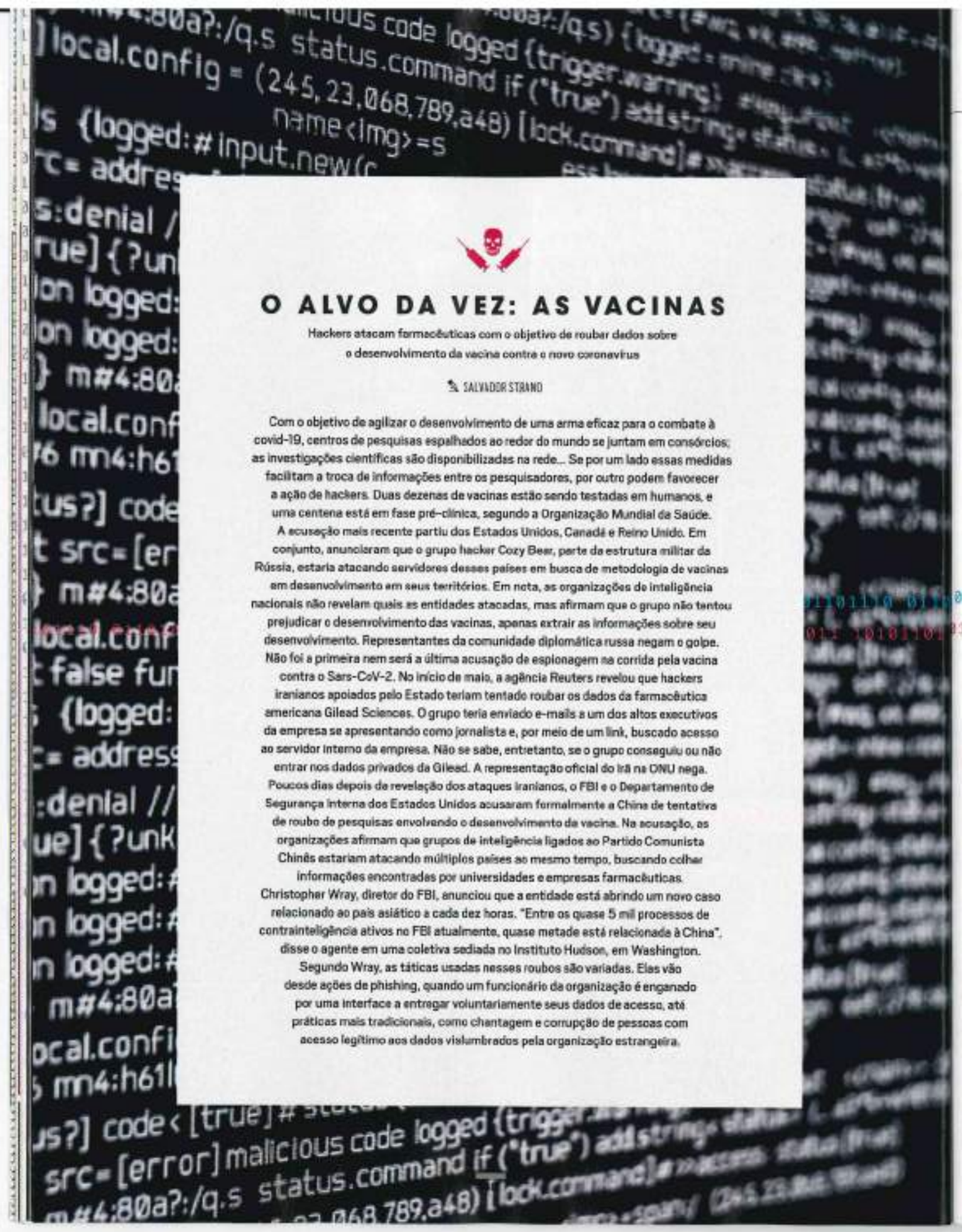
turbina de uma hidrelétrica que, vez ou outra, acessava o Facebook. "Os gestores ficam de cabelo em pé ao descobrir o que acontece com suas máquinas", diz. O conceito mais moderno leva ao limite a ideia de proteger o que realmente interessa. Em vez de apenas identificar e combater programas invasores, identificam-se padrões de comportamento. Se o laptop de um funcionário começa a enviar arquivos fora do horário de expediente, de um país que nunca fez parte de seus contatos, há um potencial problema — não importa se nenhum vírus foi identificado. Para defender uma empresa até do desconhecido, a Palo Alto lançou o primeiro firewall com inteligência artificial e aprendizado de máquina, capaz de identificar e reagir a ataques inéditos numa fração de segundo. "Se as invasões foram automatizadas, a linha de frente da defesa também tem de ser", diz Marcos.

O ambiente de negócios do cyber crime é o mais eficiente possível: uma comunidade sem fronteiras geográficas, preconceitos ou autoridades, onde cada um sente-se livre para fazer o que quiser, regido apenas pela lei da oferta e da procura (*veja reportagem a partir da página 80*). Liberalismo puro. Com usuários escondidos pelo anonimato de navegação (proporcionado por diversos aplicativos, como o Tor) e de pagamento (ao usar uma das muitas criptomoedas), para invadir uma conta de Instagram ou atacar um grande banco basta querer — e pagar. "Antigamente, programadores criavam um vírus e vendiam. Hoje, isso evoluiu para o *hack-as-a-service*. Você escolhe a ferramenta, paga por uso, recebe assistência...", conta Marcos. "Como o custo de desenvolvimento já foi amortizado, o aluguel é irrisório. Está muito fácil e barato empreender um ataque."

Especialistas em várias tarefas necessárias a um golpe, no mundo inteiro, colaboram de maneira eventual ou frequente, com algum propósito ou como mercenários. Diante do anonimato e da natureza transnacional da dark web, é difícil estimar o número de criminosos digitais ou quanto faturam. Mas sabe-se que podem ganhar muito bem. "Um hacker tem várias formas de ganhar dinheiro, idôneas e inidôneas. Quando você começa a avaliar a maneira legal, começa a ter uma noção da outra", diz Daniel. "Empresas como Apple e Microsoft pagam US$ 500 mil a quem descobrir uma vulnerabilidade de um sistema operacional. Por que alguém deixaria de vender legalmente, com risco zero? Porque ilegalmente o lucro será algumas vezes maior."

Vai longe o tempo em que algumas pessoas ou empresas podiam sentir-se fora do radar de criminosos. Como atacar é barato e o fruto do ataque sempre pode interessar a alguém, no mercado de secos e molhados da dark web os alvos são indiscriminados. Máquinas com inteligência artificial pulverizam ataques, em busca de uma fragilidade — é como uma quadrilha que, em vez de tentar arrombar uma casa, resolve testar todas as maçanetas do bairro, até encontrar alguma destrancada. "Se a sua defesa não for automatizada, com aprendizado de máquina e machine learning, você já perdeu o jogo", diz Marcos, da Palo Alto. "Porque o que veio até você foi uma máquina digital, te massacrando." Certos malwares (softwares maliciosos) já carregam, em seu próprio código, a busca pelo uso mais rentável de cada computador infectado. "Encontramos um malware que nos fez discutir como os hackers estão se preparando para se adaptar dinamicamente a uma mudança", diz Daniel. "O programa se comportava de

FOTO: GETTY IMAGES



O ALVO DA VEZ: AS VACINAS

Hackers atacam farmacêuticas com o objetivo de roubar dados sobre o desenvolvimento da vacina contra o novo coronavírus

SALVADOR STRANO

Com o objetivo de agilizar o desenvolvimento de uma arma eficaz para o combate à covid-19, centros de pesquisas espalhados ao redor do mundo se juntam em consórcios; as investigações científicas são disponibilizadas na rede... Se por um lado essas medidas facilitam a troca de informações entre os pesquisadores, por outro podem favorecer a ação de hackers. Duas dezenas de vacinas estão sendo testadas em humanos, e uma centena está em fase pré-clínica, segundo a Organização Mundial da Saúde.

A acusação mais recente partiu dos Estados Unidos, Canadá e Reino Unido. Em conjunto, anunciaram que o grupo hacker Cozy Bear, parte da estrutura militar da Rússia, estaria atacando servidores desses países em busca de metodologia de vacinas em desenvolvimento em seus territórios. Em nota, as organizações de inteligência nacionais não revelam quais as entidades atacadas, mas afirmam que o grupo não tentou prejudicar o desenvolvimento das vacinas, apenas extrair as informações sobre seu desenvolvimento. Representantes da comunidade diplomática russa negam o golpe.

Não foi a primeira nem será a última acusação de espionagem na corrida pela vacina contra o Sars-CoV-2. No início de maio, a agência Reuters revelou que hackers iranianos apoiados pelo Estado teriam tentado roubar os dados da farmacêutica americana Gilead Sciences. O grupo teria enviado e-mails a um dos altos executivos da empresa se apresentando como jornalista e, por meio de um link, buscado acesso ao servidor interno da empresa. Não se sabe, entretanto, se o grupo conseguiu ou não entrar nos dados privados da Gilead. A representação oficial do Irã na ONU nega.

Poucos dias depois da revelação dos ataques iranianos, o FBI e o Departamento de Segurança Interna dos Estados Unidos acusaram formalmente a China de tentativa de roubo de pesquisas envolvendo o desenvolvimento da vacina. Na acusação, as organizações afirmam que grupos de inteligência ligados ao Partido Comunista Chinês estariam atacando múltiplos países ao mesmo tempo, buscando colher informações encontradas por universidades e empresas farmacêuticas.

Christopher Wray, diretor do FBI, anunciou que a entidade está abrindo um novo caso relacionado ao país asiático a cada dez horas. "Entre os quase 5 mil processos de contrainteligência ativos no FBI atualmente, quase metade está relacionada à China", disse o agente em uma coletiva sediada no Instituto Hudson, em Washington.

Segundo Wray, as táticas usadas nesses roubos são variadas. Elas vão desde ações de phishing, quando um funcionário da organização é enganado por uma interface a entregar voluntariamente seus dados de acesso, até práticas mais tradicionais, como chantagem e corrupção de pessoas com acesso legítimo aos dados vislumbrados pela organização estrangeira.

vários jeitos diferentes. No laptop de um executivo da empresa, tentava roubar informação. Se era um desktop qualquer, ficava disponível como bot, para atacar em massa algum ambiente. Estava dedicado a criptografar arquivos, para um posterior pedido de resgate, mas transformou as máquinas infectadas em mineradoras de criptomoeda, quando a cotação subiu bastante. É curioso e muito desconfortável pensar que qualquer um é um potencial alvo para ataque." As leis de mercado funcionam de maneira tão cristalina que certos vírus são programados para, após invadir uma máquina, procurar e exterminar outros possíveis invasores — porque eliminar a concorrência torna a exploração mais lucrativa.

Embora ataques digitais sejam frequentes nas sextas-feiras ou nos fins de semana, profissionais da área de cibersegurança evitam falar em dia ou hora mais vulneráveis. No fim de uma segunda-feira, perto das 11 horas da noite, durante a pandemia, Thiago Bordini, diretor de inteligência cibernética do grupo New Space, foi acionado por uma empresa que sofreu um ataque de ransomware. Todos os dados da companhia foram criptografados, e o grupo criminoso cobrou um resgate de cerca de US$ 60 mil, a serem pagos em monero, uma criptomoeda teoricamente impossível de rastrear pelas autoridades. "Foram alvos mais de cem servidores da empresa, parando toda a operação. O prejuízo estimado era de R$ 1 milhão a R$ 2 milhões por dia. O resgate não foi pago e colocamos o ambiente de volta no ar na madrugada de terça-feira", conta.

Thiago começou montando computadores na adolescência, estudou ciências da computação na faculdade e migrou para a área de segurança de redes empresariais antes de chegar ao mercado de inteligência cibernética, que monitora atividades maliciosas e responde a violações nos sistemas de TI. "Empresas só costumam dar valor à segurança da informação depois que têm algum problema, mas acaba saindo muito mais caro contratar serviços emergenciais de resposta a incidentes", explica.

Para responder a invasões cibernéticas e a sequestros de dados, as companhias também costumam recorrer a escritórios de advocacia com profissionais especializados em direito digital, para avaliar como reduzir os estragos e se devem acionar a polícia. Thiago Sombra, sócio da área de proteção de dados e cybersecurity do Mattos Filho, já atendeu a mais de um caso de ataque digital por mês desde o começo do isolamento social no Brasil. "Dispararam os casos de pretensos hackers do bem. Eles se intitulam pesquisadores éticos e ficam pesquisando uma vulnerabilidade. Quando acham, procuram a empresa e dizem que deixariam de divulgar em troca de uma recompensa. É uma extorsão velada. Na maioria das vezes, é garotada que faz isso", aponta.

No setor financeiro, especialmente sensível aos problemas gerados por ataques digitais e um dos maiores investidores em segurança, normas do Banco Central e da Comissão de Valores Mobiliários também colocam as empresas em maior risco de sanções regulatórias. Desde abril de 2018, uma resolução do BC já obriga empresas financeiras a manter um comitê de crise contra ataques cibernéticos e a comunicar à autoridade monetária em caso de qualquer incidente relevante. Em setembro, começa a valer também uma norma da CVM que torna ainda mais detalhista e rigorosa a comunicação de incidentes. Empresas fiscalizadas pelo xerife do mercado de capitais terão de reportar uma avaliação do número de clientes afetados e as medidas adotadas para solucionar o ataque.

Mesmo obrigadas, nem sempre as empresas comunicam as autoridades ou os clientes. "Algumas preferem absorver o prejuízo e não envolvem a polícia por questão de imagem", diz o delegado Carlos Henrique Ruiz, chefe da Delegacia de Crimes Eletrônicos de São Paulo. Nas polícias e no Judiciário, há quem defenda que as penas a crimes cibernéticos são baixas. O desembargador federal Fausto De Sanctis avulia que as punições previstas não são apropriadas aos danos causados aos consumidores e às empresas. "A lei está desatualizada. A pena de invasão de dispositivos é de 3 meses a 1 ano, o que é muito baixo para um prejuízo potencial de milhões de reais. É uma punição incompatível às consequências. Se não for alterada, estimulará ainda mais a prática desse tipo de crime", diz. Em se tratando de cibersegurança, como tudo na vida, a chave está na prevenção. Boas-vindas aos times azul e vermelho.

FOTO: GETTY IMAGES