Cibersegurança. Como a pandemia deixou vários executivos com a cabeça a prémio

visao.sapo.pt/exameinformatica/noticias-ei/mercados/2021-03-19-ciberseguranca-como-a-pandemia-deixou-varios-executivos-com-a-cabeca-a-premio

19 de março de 2021

De um momento para o outro, milhares de empresas e centenas de milhares de pessoas passaram a trabalhar a partir de casa e a dependerem da ligação à internet – 'cortesia' do SARS-CoV-2 e da Covid-19. E já lá diz o ditado que o azar de uns é a sorte de outros. "A superfície de ataque, para quem vive do cibercrime, explodiu. Qualquer disparo que se faça, acerta em alguém".

É assim que Bruno Castro, diretor executivo da Visionware, resume o que se tem passado nos últimos doze meses como resultado da pandemia. Por a transição para o teletrabalho ter sido feita de forma quase instantânea, sem preparação ou formação, os piratas informáticos ficaram em mãos com uma oportunidade rara para fazerem aquilo que sabem melhor – explorar vulnerabilidades de software... e também humanas.

"Cresceu o número de ataques e a taxa de sucesso. Os ataques com sucesso são agora mais do que tínhamos há um ano", acrescenta o porta-voz da tecnológica. Lidar com ataques informáticos é o que a equipa de 60 pessoas da Visionware faz no seu dia-a-dia. Mas o que se passou nos últimos meses ultrapassa muito do que tinha sido visto até então. "Grande parte das pessoas não estava preparada para o mundo perigoso que se chama internet", sublinha o CEO em entrevista à *Exame Informática*.

O responsável da Visionware não adianta números concretos dos ataques detetados pela empresa, mas revela aquela que tem sido a grande tendência nos últimos meses – roubo de dinheiro através de campanhas maliciosas que envolvem diretamente os principais executivos das empresas. "São ataques direcionados para a camada executiva", começa por explicar o CEO da empresa de análise forense.

"São ataques elaborados. Estudam as pessoas, planeiam, pesquisam, preparam-se. Quem é o CEO, quem é o CFO [diretor financeiro], a secretária, quem é o tipo que faz as encomendas. Depois fazem ataques de spear phising", acrescenta, sobre a forma de atuação em alguns dos cibercrimes nos quais a empresa foi chamada a analisar.

Spear phishing é um termo que designa tentativas direcionadas de enganar pessoas específicas, levando-as a partilharem dados confidenciais. "Tipicamente é um phishing que estuda a pessoa: se gosta de futebol, se gosta de carros, se é louca por saldos... É phishing apontado para pessoas específicas e com conteúdos feitos para essas pessoas".

Esta técnica contrasta com aquele que é o modus operandi mais comum no mundo do cibercrime – fazer uma campanha de phishing massificada, na lógica de quantas mais pessoas a receberem, maior será a probabilidade de alguém cair na armadilha. Mas o

trabalho minucioso executado pelos cibercriminosos nas campanhas de spear phishing tem uma recompensa mais choruda do outro lado: “O objetivo é roubar grandes volumes de dinheiro em pouco tempo”.

Por estarem a trabalhar a partir de casa, considera Bruno Castro, existe uma maior tendência para as pessoas “clicarem no sítio errado à hora errada”. “E o facto de o gestor de conta estar em casa, quer facilitar a transferência bancária rapidamente”.

Bruno Castro é diretor executivo da Visionware

Um ano recorde

Com o número de ataques bem sucedidos a crescer, cresceu também o número de solicitações à Visionware. Bruno Castro revela que a empresa teve “o melhor ano de sempre por causa da pandemia cibernética”, que, diz, fez explodir a procura por serviços e ferramentas de segurança informática. Mas ao contrário de outras empresas do setor, a Visionware não vende produtos de hardware ou de software. “Nós trabalhamos na vertente pós-crime, na área forense”. A empresa tem mais de 100 clientes, metade portugueses, metade internacionais.

À medida que as solicitações aumentaram, a Visionware recrutou mais pessoas. Em menos de um ano, a equipa cresceu em 15 novos membros. Mas a lógica de ‘mais potenciais clientes, mais funcionários’ deixou de ser uma opção. “O nosso processo de recrutamento é altamente rigoroso porque trabalhamos num setor no qual a exigência e a confidencialidade são ultra apertados. Chegamos a um momento em que tivemos de dizer que não a potenciais novos clientes.”

Mas os efeitos do cibercrime em tempo de pandemia não vão ficar por aqui. Bruno Castro lembra que há grupos de cibercriminosos que, ao contrário do que aqui foi descrito, não atuam para roubar dinheiro – roubam dados. “Chama-se espionagem. Roubam informação a instituições públicas para vender no mercdo negro e fazem isso de forma silenciosa. Aí a ideia é ficarem encobertos o máximo de tempo possível”. Ou seja, muitos ataques já terão sido concretizados, mas só daqui a meses, quem sabe anos, os efeitos dos mesmos é que poderão vir a ser conhecidos.

Bruno Castro aponta como potenciais vítimas na mira desta ‘tropa de elite’ do cibercrime as organizações do Estado e também as grandes empresas. “São alvo de ataques mais demorados e personalizados. Envolvem muito esforço, [os cibercriminosos] têm que ter um mote muito valioso. Vai ser mais numa ótica de roubar dados. Seja sensível ou valiosa”.