

INFORMÁTICA
OS MAIORES
CIBERATAQUES
DA HISTÓRIA

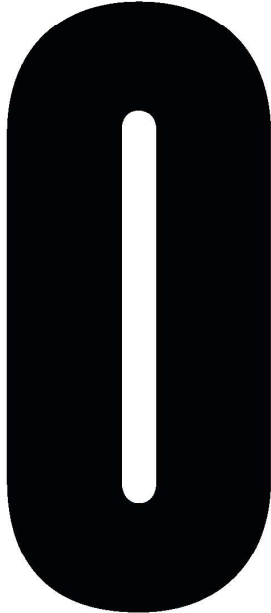
QUANDO O VIRUS É DIGITAL





Entram pela porta dos fundos, bloqueiam o funcionamento das empresas, vendem dados à concorrência, informações pessoais ou chaves de acesso, lucrando milhões na dark web, um dos mais profícuos mercados negros atuais. Como lidar com os cibercriminosos, uma ameaça de que, segundo os especialistas, nenhuma empresa está a salvo?

 MARIANA ALMEIDA NOGUEIRA



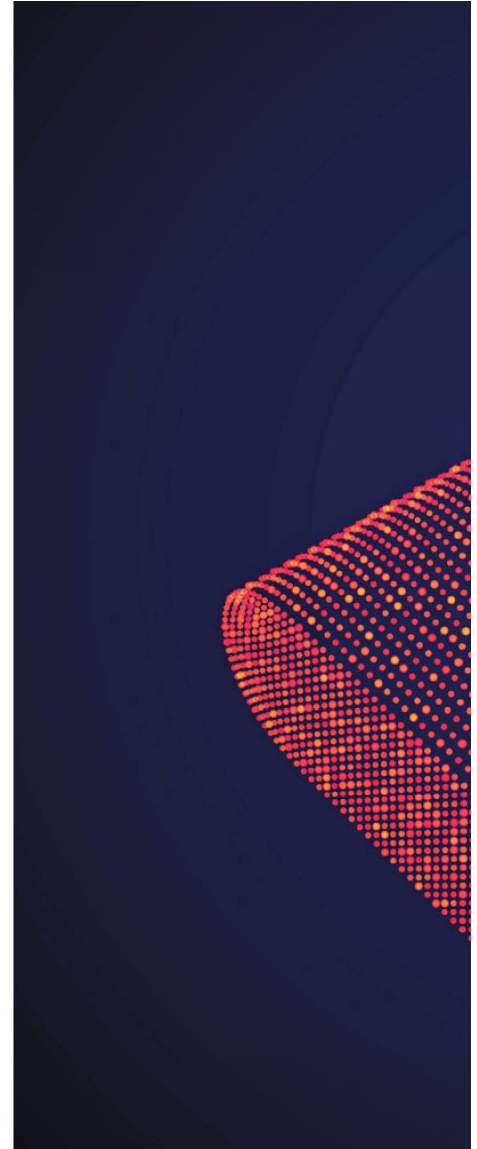
“Os dados serão vazados caso o valor necessário não for pago. Estamos com acesso nos painéis de cloud (AWS) entre outros tipos de dispositivos. O contacto para o resgate está abaixo.” A nota parece saída de uma série policial ou de uma das dezenas de blockbusters protagonizados por Liam Neeson. Só que não. Milhares de pessoas depararam-se com esta

mensagem quando, na manhã de segunda-feira, 3 de janeiro, tentaram aceder aos sites da SIC, da SIC Notícias ou do *Expresso*.

Durante a madrugada de domingo, a Impresa, detentora dos órgãos de comunicação social em causa, havia sido alvo de um ataque informático aos servidores onde se encontram alojadas as páginas oficiais na internet dos canais de televisão, do jornal e da revista *Blitz*, tornando-as inacessíveis à empresa e aos leitores. No dia seguinte, acordava-se assim com a notícia daquilo que o grupo classificou como “um atentado nunca visto à liberdade de imprensa em Portugal na era digital”.

Apesar de a extensão do ataque ser ainda desconhecida à data de fecho desta edição, sabe-se que o responsável foi um grupo de hackers auto-denominado Lapsus\$, que se suspeita ser constituído por colombianos e um espanhol, e que, além da Impresa, já atacou, no Brasil, os sites da Polícia Rodoviária Federal e do Ministério da Saúde e os portais do Ministério da Economia e da Controladoria-Geral da União.

Tudo leva a crer que se trate de um ataque de *ransomware*, o qual, segundo Rui Duro, country manager da Checkpoint Portugal, uma das maiores empresas mundiais de cibersegurança, de origem israelita, “é



OS 10 CIBERATAQUES QUE FIZERAM HISTÓRIA NOS ÚLTIMOS ANOS

▶ **1999 – NASA** Jonathan James, de 15 anos, tornou-se o primeiro adolescente a ser preso por cibercrime, após atacar a Agência Espacial Norte-americana e o Departamento de Defesa dos EUA. O jovem invadiu 13 computadores da NASA, roubando software e dados, obrigando-a a fazer um *shut down* completo de alguns computadores, durante três semanas, com custos de mão de obra e reparação na ordem dos 35 mil euros. No Departamento

de Defesa, James interceptou 3 300 emails internos, 19 dos quais continham usernames e passwords.

▶ **2007 – Estónia** Em abril de 2007, a Estónia viveu o que se pensa ser o primeiro ciberataque a um país inteiro. Cerca de 58 sites ficaram offline, incluindo páginas do governo, bancos e meios de comunicação.

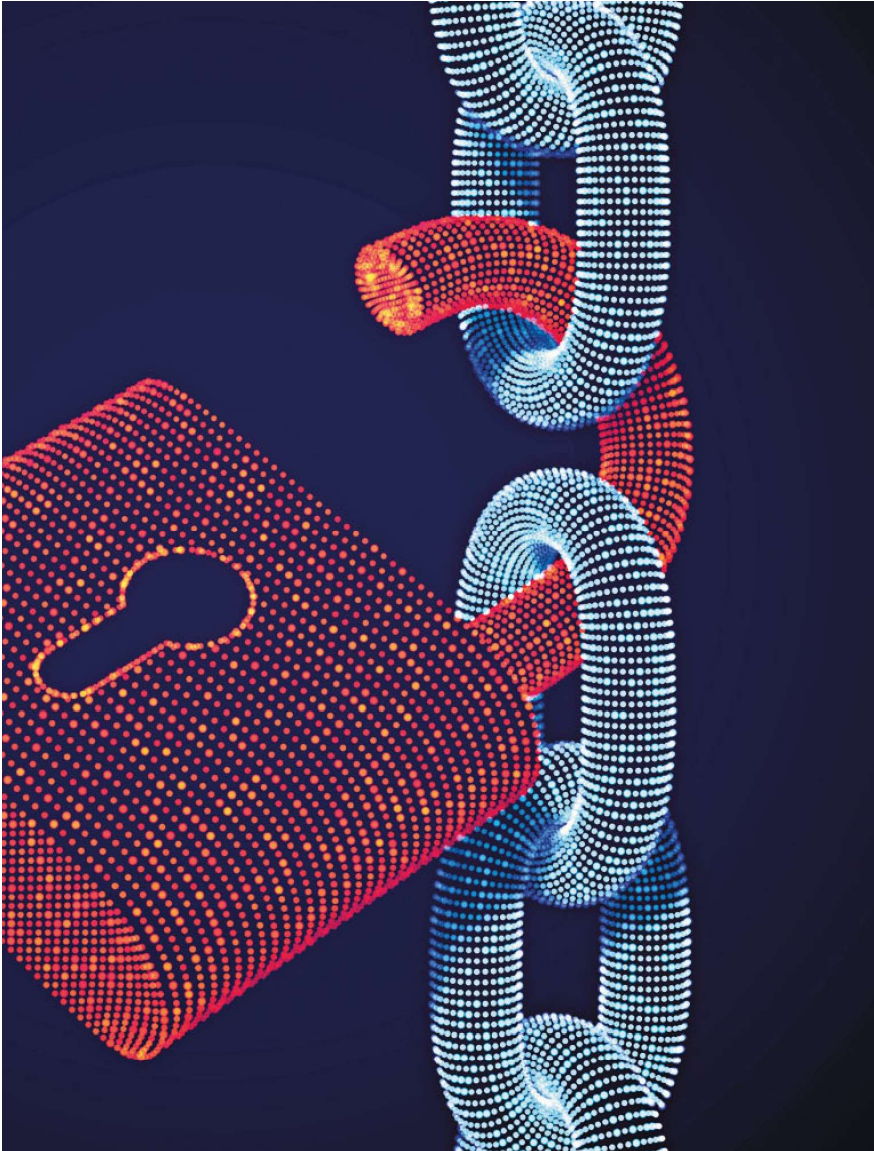
▶ **2011 – SONY** A Sony sofreu um ataque que levou a que cerca de 77 milhões de contas da PlayStation ficassem comprometidas,

durante mais de 20 dias, tendo sido ainda roubados dados de 12 mil cartões de crédito. Além de pagar 13 milhões de euros de indemnização aos utilizadores lesados e de reembolsar as pessoas cujas contas bancárias haviam sido usadas ilegalmente, a Sony teve de responder perante a Câmara dos Representantes dos EUA e foi multada em 1,2 milhões de euros por medidas de segurança impróprias, por parte dos comissários de informação britânicos.

▶ **2012 – LinkedIn** As passwords de quase 6,5 milhões de contas foram roubadas, e os proprietários não conseguiam aceder às mesmas. Em maio de 2016, o LinkedIn descobriu mais 100 milhões de endereços de email e passwords que haviam sido comprometidos no ataque de 2012. No mesmo ano, o hacker russo Yevgeniy Nikulin foi preso e, em 2020, condenado pelo crime e sentenciado a 88 meses de prisão.

▶ **2013 – Adobe** Neste ataque foram roubadas informações pessoais de 150 milhões de contas, 38 milhões das quais ativas (logins, senhas, nomes e números de cartão de crédito). Além das informações dos clientes, os hackers conseguiram obter 40 GB dos códigos-fonte do Acrobat, ColdFusion e do ColdFusion Builder.

▶ **2013 – Target** Dados bancários de 40 milhões de clientes e dados pessoais (nomes, moradas, números de telefone e endereços



GETTY IMAGES

o ataque que tem mais visibilidade e aquele que, atualmente, fornece mais dividendos à maioria das organizações cibercriminosas”.

“Estamos a falar de valores na casa dos sete e oito dígitos”, acrescenta Bruno Castro, CEO da empresa de análise forense a crimes informáticos Visionware, ao referir-se a este tipo de *malware* (programa malicioso) que impede a vítima de aceder a ficheiros e/ou dispositivos, enviando-lhe uma nota de chantagem com um pedido de resgate para recuperar o acesso total ao sistema e a arquivos.

PORQUE TEMEM AS EMPRESAS O RANSOMWARE?

O poder do ataque que faz tremer pequenas e grandes empresas reside naquilo que os especialistas apelidam de “extorsão tripla”. Ou seja, em primeiro lugar, após um encriptamento de dados essenciais da empresa, os criminosos pedem um resgate, alegando que, uma vez pago, fornecerão a chave de acesso à informação encriptada. Em segundo lugar, pedem mais dinheiro para que a informação não seja exposta publicamente e, por fim, vendem a informação roubada no mercado negro (dark web), mesmo que a empresa tenha pago o resgate, asseguram os especialistas. “Podem ser dados corporativos, acessos remotos, vpns, autenticações de emails

de email) de outros 70 milhões de clientes do gigante dos descontos norte-americano foram sequestrados por um grupo de hackers localizado na Europa Oriental. E não foi a Target, mas os serviços de segurança dos EUA que descobriram o ataque. A Target pagou mais de 16 milhões de euros pelas investigações do Estado relativamente ao ataque.

▶ **2015 – Ucrânia**
Naquele que foi considerado o primeiro ciberataque a uma rede elétrica, cerca

de metade das casas da região de Ivano-Frankivsk, na Ucrânia, ficou sem energia, durante algumas horas.

▶ **2017 – Primeiro ataque ransomware**
O WannaCry, primeiro ransomware cryptoworm do mundo, afetou 230 mil computadores com o serviço operativo Windows, em 150 países. Os autores do ataque exigiram 266 euros em criptomoeda bitcoin, em troca do desbloqueio dos arquivos encriptados. Organizações, como a Telefónica e o Serviço

Nacional de Saúde britânico, foram afetadas, bem como outras operadoras de telecomunicações, empresas de transportes, organizações governamentais, bancos e universidades.

▶ **2018 – Marriott**
Devido a uma brecha aberta em 2014, cerca de 500 milhões de hóspedes do grupo de hotéis Starwood, propriedade da Marriott, viram as informações pessoais comprometidas. Os dados iam desde

pagamentos até nomes, moradas, números de telefone, de passaporte, endereços de email e ainda informações sobre a conta Starwood Preferred Guest, um cartão de última geração para viajantes regulares. O governo dos EUA acredita que a responsabilidade foi de um grupo de hackers chinês, ainda que tal tenha sido desmentido pelo ministro chinês dos Negócios Estrangeiros. A Marriott foi condenada a pagar uma multa de 109 milhões de euros pelas autoridades do Reino

Unido, por não ter sido capaz de proteger os dados dos clientes.

▶ **2019 – Alibaba**
Ao longo de oito meses, um programador, que trabalhava para um comerciante afiliado ao site de compras chinês Taobao (propriedade da Alibaba), reuniu dados de clientes, incluindo usernames e números de telemóvel. Apesar de se pensar que ambos desenvolveriam atividade ilegal para uso próprio e não teriam vendido a informação no mercado negro, foram condenados a três anos de prisão.

ou dados de negócio puro e duro”, exemplifica Bruno Castro.

Negociar com criminosos está fora de questão e os especialistas aconselham as empresas a nunca pagar o montante pedido. Além de alimentar uma rede criminosa, não há nenhuma garantia de que, uma vez pago o resgate, se receba realmente a chave para descriptar a informação. “É um cheque em branco. Muitas vezes até acontece haver novos pedidos, depois de um primeiro pagamento”, alerta o mesmo especialista.

Para contornar o problema do encriptamento de dados roubados, sem ceder ao pagamento de resgates, Miguel Romão, diretor do centro de operações da S21Sec, uma das maiores empresas ibéricas de cibersegurança, aconselha a criação de cópias de segurança, que deverão estar em segmentos diferentes da rede, “onde os atacantes não consigam obtê-las”.

Mas esta é apenas uma das medidas para lidar com um ataque. Tal como num assalto físico, vale a máxima: “Casa roubada, trancas à porta.” “Tal como numa casa, para não sermos roubados, não basta trancarmos a porta, ela tem de ser resistente, tem de haver uma campainha, segurança e luz”, lembra Bruno Castro, revelando que, cada vez mais, as novas gerações de gestores alocam um orçamento específico para a segurança digital, “focando-se em auditar os sistemas regularmente, dar formação aos empregados, procurar falhas humanas e tecnológicas, mitigar algumas delas e anular as que podem ser anuladas”.

ANATOMIA DE UM CRIME

Mas afinal o que se passa realmente num ataque de *ransomware*? Porque ultimamente percebemos todos de infeções virais, a analogia perfeita surge mesmo por aí. Tal como em muitas doenças, este tipo de “infeção” começa a espalhar-se semanas antes de dar sintomas. É o que se suspeita que tenha acontecido no caso Impresa e o que, habitualmente, ocorre noutros ataques do mesmo género, confirmaram os especialistas que falaram com a VISÃO.

Ao contrário dos filmes, não há um hacker que, sozinho, bloqueia tudo em segundos. “Os criminosos entram, copiam os dados e podem navegar semanas dentro da infraestrutura para perceberem como funciona e como podem tirar o maior partido dela antes



de encriptar a informação e pedir o resgate”, explica Rui Duro.

Na maioria das vezes, “não estamos a falar de um grupo que faz todo o ataque, mas, muito provavelmente, de vários grupos muito especializados”, afirma Miguel Romão. Outras vezes, nota Rui Duro, as organizações criminosas são “empresas autênticas”, com um investidor, um data center, equipas especializadas em instalar os agentes que comunicam com a consola exterior, “através da qual são encriptados e copiados os dados”, técnicos de informática, um especialista em código, um hacker, “que procura vulnerabilidades nos sistemas das empresas e pensa no ataque” e, até, especialistas em Sociologia e Psicologia que percebem o que leva alguém a ceder a um ataque de *phishing* (técnica através da qual o utilizador é levado a clicar num link que o manipula a fim de obter informações confidenciais).

**OS CRIMINOSOS
ENTRAM, COPIAM
OS DADOS E PODEM
NAVEGAR SEMANAS
DENTRO
DA INFRAESTRUTURA
PARA PERCEBEREM
COMO FUNCIONA
E COMO PODEM TIRAR
O MAIOR PARTIDO DELA
ANTES DE ENCRIPITAR
A INFORMAÇÃO
E PEDIR O RESGATE**



GETTY IMAGES

QUÃO LONGE PODEM CHEGAR OS CRIMINOSOS?

Não nos iludamos – do mais banal email de *phishing* até ao mais complexo esquema de *ransomware*, estamos perante um crime que deve ser investigado pela Polícia Judiciária, tal como a Impresa já avançou que está a fazer.

Habitualmente, os alvos dos ataques a empresas são os sistemas corporativos e de negócio, mas, no pior dos cenários, se o ataque for de grande envergadura, Bruno Castro alerta que, “até os criminosos chegarem aos fornecedores da empresa ou à rede doméstica dos colaboradores, do homebanking às redes sociais, é um saltinho”. É como um vírus assintomático, muito rápido, que, ao contrário dos humanos, trabalha 24 horas sobre sete, “sem ir de fim de semana ou dormir à noite”.

Quanto às empresas, o especialista em análise forense a crimes informáticos garante que um ataque destes

implica sempre uma interrupção nos serviços da vítima, e recorda um caso com o qual lidou, este ano, que desligou mais de 100 sites e dezenas de fábricas de uma rede industrial multinacional, gerando perdas na ordem de um milhão e meio de dólares por dia, ao longo de dez dias. “O ataque veio de um site muito pequenino da empresa, através de uma das cinco pessoas que lá trabalhavam e que foi infetada em casa. A partir desse site, os restantes foram invadidos e daí para todo o mundo.”

O facto de uma empresa ter sido atacada com êxito não quer dizer que seja pouco madura em termos de segurança. De facto, todos os especialistas concordam que o fator humano é sempre o elo mais fraco e sublinham a fragilidade e o risco que, no mundo de hoje, as empresas têm de ser expostas a uma paragem provocada por um ataque informático. “Não é uma questão de se, mas de quando”, acredita Miguel Romão.

Por outro lado, segundo o mais recente Relatório Cibersegurança em Portugal, do Centro Nacional de Cibersegurança, a pandemia provocou “um significativo aumento no número de incidentes de cibersegurança e nos indicadores de cibercrime em 2020”. A explicar a situação está, segundo os especialistas, o teletrabalho.


Por um lado, perante uma migração repentina da maioria dos trabalhadores para a modalidade de trabalho remoto, nem todas as empresas foram capazes de encontrar dispositivos corporativos suficientes para dar a todos, acabando alguns por usar os dispositivos pessoais, menos protegidos. Por outro lado, diz Bruno Castro, “a probabilidade de haver um colaborador interno sentado no sofá de casa a clicar no link errado à hora errada, sem que a empresa consiga protegê-lo remotamente, é elevada”. Este conjunto de fragilidades acrescidas “foi usado e abusado pelos grupos criminosos”, acrescenta Miguel Romão.

Relativamente ao que interessa vender, ainda que, a nível empresarial, o alvo raramente seja a informação pessoal dos empregados, Miguel Romão sublinha que tudo depende do que o mercado negro estiver a pagar e que valor representa essa informação no momento do ataque.

Como revela Rui Duro, “o registo eletrónico de um doente de um hospital vale dez vezes mais do que um cartão de crédito no mercado negro, porque permite, por exemplo, a um narcotraficante da América Latina viajar para a Europa com uma identidade falsa construída através de registos muito válidos e completos”.

Além dos ataques mais diretos, as empresas podem também sofrer ataques indiretos de *phishing*, dando acesso a user names e passwords que permitem aos criminosos utilizarem emails da empresa para se fazerem passar pela mesma e pedirem pagamentos aos fornecedores para contas falsas, por exemplo. “São ataques que não são propriamente diretos às empresas mas que, além de as lesarem, usam os seus sistemas, deixando-os mais lentos”, sublinha o mesmo especialista.

O novo ano apanhou-nos desprevenidos, de olhos postos noutro vírus, e confirmou que o futuro, além de novidade, traz sempre novos desafios.

 mnogueira@visao.pt