Paulo Vasconcelos

>> Ataque virtual, defesa real

O que estará a acontecer no mundo do cibercrime? Haverá números que nos ajudem a percecionar o impacto e a grandeza deste fenómeno? O sucesso de um ataque cibernético a uma organização dependerá mais da especialização em encontrar vulnerabilidades técnicas parcas em sistemas complexos ou do mero desleixo dos utilizadores?

A Microsoft divulgou os resultados do Relatório de Defesa Digital 2022, onde revela que os ciberataques de estado aumentaram o nível de eficácia, passando de uma taxa de sucesso de 20% para 40%, em apenas um ano. O estudo tem por base mais de 43 mil bilhões (triliões) de sinais diários, entre julho de 2021 e junho de 2022, e no qual foram reportados o bloqueio de 37 mil milhões (biliões) de ameaças por email e 34,7 mil milhões de ameaças de roubo de identidade. Os principais setores afetados pelos ataques detetados pela Microsoft e reportados foram as tecnologias de informação (TI) (22%), ONG e grupos de reflexão (17%), educação (14%), governos (10%), finanças (5%), meios de comunicação (4%), serviços de saúde (2%), transportes (2%), organizações intergovernamentais (2%) e comunicações (2%).

Estes dados são de uma empresa relevante no mundo digital, mas não abrange obviamente o todo, longe disso.

Desde fevereiro deste ano, com a guerra iniciada pela Rússia à Ucrânia, há ataques quer físicos quer digitais. O relatório da Microsoft indica que 90% dos ataques detetados no ano passado provenientes da Rússia visaram os estados-membros da OTAN, sendo que 48% desses ataques comprometeram empresas de TI sediadas em países da OTAN. Países como o **Irão, Coreia do Norte e China são** também atores de ataques cibernéticos retratados no relatório. Além da **recolha de informação**, estes estados procuram a **interrupção de serviços, roubo de criptomoedas** ou **destruição de dados e ativos físicos**. O relatório não menciona, nem poderia, as ações inversas.

A superfície de ataque no mundo digital tem vindo a alargar-se, tendo a recente pandemia contribuído para a acelerada transformação digital. Os atacantes são cada vez em maior número, tentando a oportunidade oferecida pela explosão de dispositivos digitais e aproveitando vulnerabilidades no *firmware* para infiltração em redes corporativas. À medida que as defesas cibernéticas melhoram e mais governos e empresas adotam uma postura proativa na prevenção, a intrusão usa basicamente duas estratégias: campanhas com alvos amplos que dependem do volume e direcionamento seletivo para aumentar a taxa de retorno. O cibercrime continua a apoiar-se nas redes sociais e na exploração de questões atuais para maximizar o sucesso das campanhas. A falsa informação também é uma ameaça digital. Assiste-se à proliferação de ferramentas que facilitam, criam e disseminam imagens artificiais altamente realistas, vídeos e áudio. A internet é um meio através do qual se reverberam ideias e comportamentos tóxicos assim como notícias falsas.

Os ataques digitais ou virtuais são em geral fruto de atividades de *ransomware* **e** *phishing***.** No último ano, foram registados mais de 900 ataques a palavras-chave por segundo, representando um aumento de **74%** face ao ano homólogo anterior. A Microsoft terá bloqueado cerca de 710 milhões de emails de *phishing* **por semana.**

O *ransomware* (software malicioso que bloqueia o acesso a dados, arquivos ou sistemas contra o pagamento de um resgate) é a ameaça mais prevalente e a que mais tem crescido, evidenciando que o maior objetivo do cibercrime é, mesmo em tempo de guerra explícita, económico. Cerca de 30% dos alvos são comprometidos com sucesso e 5% destes são resgatados, evidencia o relatório. Também o chamado *phishing* tem aumentado, atingindo de forma indiscriminada caixas de correio eletrónico. Esta é a forma mais simples e talvez eficaz de ciberataque pois não procura vulnerabilidades nos sistemas, mas antes no ser humano. Em vez de procurar falhas técnicas, em geral raras, num código informático, é muito mais simples obter de um utilizador, através de um email ou mensagem de texto que copia uma organização ou pessoa conhecida, informação confidencial. Reporta o relatório uma estimativa de roubo de 66 mil biliões de dólares em ataques cibernéticos para este ano.

Continuamos a encarar de forma lasciva o acesso à internet na procura rápida e cega de informação e a precipitar a leitura e resposta a emails. Proteja-se a si e à instituição em que está inserido: use autenticação multifator (prática já comum e imposta na maior parte dos serviços), aplicação do princípio de confiança zero, usar *anti-malware* moderno, ter software atualizado, e dados protegidos. Segundo dados do relatório, a segurança básica ainda protege contra cerca de 98% dos ataques. A resiliência cibernética requer uma abordagem holística e adaptativa para suportar as ameaças em permanente evolução, sendo a grande maioria dos ataques cibernéticos evitados usando estes princípios básicos de segurança.

O ano de 2022 foi profícuo em ciberataques em Portugal: TAP, Estado-Maior-General das Forças Armadas, Impresa, Vodafone Portugal, Segurança Social. Uso abusivo da sua imagem tem sido relatado pela banca (CTT em particular), AT, EDP, Hospital Garcia da Horta, Sonae MC, agência Lusa, o jornal I e o Nascer do Sol. O ano que se avizinha poderá/deverá ser ainda pior.

O Centro Nacional de Cibersegurança (CNCS) mantém no endereço https://dyn.cncs.gov.pt/pt/alertas/?persona=organizations uma lista atualizada de alertas de vulnerabilidade em sistemas. Só neste mês de dezembro, que ainda não terminou, existem 4 avisos de sistemas afetados. A notificação de incidentes ao CNCS é recebida e processada pelo CERT.PT, quer proveniente de particulares quer de empresas. E a partilha é fundamental para proteção mútua.