Comunicado de Imprensa

**No Mês Europeu da Cibersegurança**

**Relatório de Defesa Digital da Microsoft: Ataques cibernéticos aumentam em volume, sofisticação e impacto**

* ***58% dos ciberataques de estados-nação tiveram origem na Rússia***
* ***Retalho (13%), serviços financeiros (12%), manufatura (12%), administração pública (11%) e saúde (9%) são os setores mais afetados***
* ***Ransomware é o cibercrime mais grave e continua a crescer***

**Lisboa, 11 de outubro 2021** – As conclusões do segundo [**Relatório de Defesa Digital da Microsoft**](https://www.microsoft.com/en-us/security/business/microsoft-digital-defense-report?rtc=1)não deixam margem para dúvidas: a segurança cibernética é um desafio complexo, em constante evolução e sem data de finalização. Com base em **mais de 24 mil milhões de sinais diários**, além de **observações feitas em 77 países, incluindo Portugal**, o estudo cobre o período **entre julho de 2020 e junho de 2021**.

*“A posição única da Microsoft, potenciada pela utilização da Inteligência Artificial, permite-nos obter uma imagem precisa do estado da cibersegurança, incluindo indicadores que nos dão a oportunidade de prever os próximos passos dos cibercriminosos. Este relatório mostra-nos que os ataques estão a tornar-se mais criativos, inovadores e sofisticados e esperamos que ajude as organizações a continuar a compreender melhor e a protegerem-se no cenário de constante mudança da segurança cibernética”,* refere **Manuel Dias, NTO da Microsoft Portugal**.

**Ataques de Estados-nação**

Durante o ano passado, **58%** de todos os ciberataques de estados-nação observados pela Microsoft tiveram origem na Rússia e dirigiram-se sobretudo aos Estados Unidos, Ucrânia e Reino Unido. Destaca-se o aumento da eficácia dos ataques da Rússia, passando de uma taxa de sucesso de **21%** para **32%** em apenas um ano. Da mesma forma, focaram de forma mais intensa os órgãos de política externa, segurança nacional ou defesa para a recolha de informações, meta que passou de **3%** dos seus alvos para **53%** num ano.

Mas embora os ataques russos sejam os mais comuns, não são os únicos, nem a espionagem é a única motivação. Estes também vêm de países como Coreia do Norte, Irão e China, bem como Coreia do Sul, Turquia (novo participante no relatório) e Vietname em menor grau. Independentemente dos diferentes objetivos estratégicos de cada ataque, os objetivos operacionais comuns, além da captura de informação, centram-se na interrupção de processos e serviços ou destruição de dados e ativos físicos, juntamente com a obtenção de receitas.

No geral, as vítimas preferidas dos ataques de estado-nação que a Microsoft detetou são **empresas (79%)**, tendo como setores mais específicos os **Governos (48%)**, **ONG e grupos de reflexão (31%)**, **Educação (3%)**, **organizações intergovernamentais (3%)**, **TI (2%)**, **energia (1%)** e **meios de comunicação (1%)**. Por outro lado, **21%** destes ataques cibernéticos são direcionados aos **consumidores**. No total, a Microsoft notificou os seus clientes de **20.500** tentativas de violação dos seus sistemas nos últimos três anos.

**O cibercrime como serviço**

O cibercrime – especialmente o *ransomware* – continua a ser considerado o mais grave e crescente. Enquanto os atores do estado-nação visam sobretudo a obtenção de informações, o objetivo dos cibercriminosos é económico. Como resultado, as vítimas têm um perfil diferente e os cibercriminosos procuram atacar a infraestrutura crítica.

O *ransomware* é um tipo de *malware*, ou software malicioso, projetado para impedir o acesso a dados, arquivos ou sistemas até que o pagamento do resgate seja realizado. Nesse contexto, o *ransomware* operado por humanos foi uma mudança de paradigma: evoluiu e tornou-se mais prejudicial, tornando os ataques cibernéticos um perigo generalizado para todos.

Conforme concluído a partir de intervenções de *ransomware* pela Equipa de Deteção e Resposta Rápida da Microsoft (DART), os cinco principais setores visados ​​no ano passado são o **retalho (13%), serviços financeiros (12%), indústria de manufatura (12%), administração pública (11%) e saúde (9%)**. Os Estados Unidos são de longe o país mais atacado, recebendo mais do triplo de ataques de *ransomware* do que o seguinte da lista, a China. De seguida, vêm o Japão, a Alemanha e os Emirados Árabes Unidos.

Além disso, o [**Relatório de Defesa Digital da Microsoft**](https://www.microsoft.com/en-us/security/business/microsoft-digital-defense-report?rtc=1)mostra que, no ano passado, a economia do “crime cibernético como serviço” evoluiu para uma indústria criminosa madura. Hoje, qualquer pessoa, independentemente do seu conhecimento técnico, pode aceder um robusto mercado online para adquiri um leque de serviços necessários e executar ataques para qualquer finalidade: de kits de infeção prontos a utilizar, que custam pouco mais de 56 euros, a credenciais que são vendidas por valores entre 1 e 43 euros.

Entre julho de 2020 e junho de 2021, a Microsoft bloqueou **9 mil milhões de ameaças a dispositivos**, **32 mil milhões de ataques por e-mail** e **31 mil milhões de ameaças**. Para isso, conta com uma equipa composta por mais de **8.500 especialistas** na área de segurança, apoiados em ferramentas de Inteligência Artificial para análise de sinais. A Microsoft irá continuar a investir de forma significativa nesta área, que inclui o reforço de **20 mil milhões de dólares nos próximos 5 anos.**

**Os desafios de um ambiente de trabalho híbrido**

Quase da noite para o dia, a força de trabalho de milhares de organizações em todo o mundo tornou-se totalmente remota e milhões de alunos tiveram que aprender em casa. Embora nos últimos anos existiram cada vez mais oportunidades de trabalho à distância, a pandemia acelerou estes esforços.

Em plena transição para modelos híbridos e à medida que as ameaças à *cloud* aumentam, devem ser tomadas medidas para fortalecer a primeira linha de defesa. Embora a Microsoft ofereça autenticação *multifator* (MFA) gratuita para os seus clientes e eles possam disponibilizá-la remotamente para os seus utilizadores, **menos de 20%** estão a tirar partido destes recursos de autenticação fortes. Na verdade, se as organizações aplicassem apenas MFA, utilizassem *anti-malware*, e mantivessem os seus sistemas atualizados, estariam protegidas **contra** **mais de 99% dos ataques** a que assistimos.

Nos últimos 18 meses, assistimos a um **aumento de 220%** na utilização de autenticação forte, mas ainda existe um longo caminho a percorrer. Os novos desafios de segurança concentram-se na infraestrutura, dados e pessoas. A arquitetura VPN, a virtualização e os princípios Zero Trust permitem que as empresas apoiem os colaboradores remotos com segurança e façam a gestão dos direitos de acesso às informações para cumprir as políticas de proteção de informações confidenciais e propriedade intelectual.

Aceda [aqui](https://www.microsoft.com/en-us/security/business/microsoft-digital-defense-report?rtc=1) ao **Relatório de Defesa Digital da Microsoft**.

**CONTACTOS:**

|  |  |  |
| --- | --- | --- |
| **Marta Pereira** | **Sofia Lareiro** |  |
| marta.pereira@lift.com.pt | sofia.lareiro@lift.com.pt |  |
| 934 847 486 | 934 847 492 |  |

**Sobre a Microsoft**

A Microsoft possibilita a transformação digital na era da Intelligent Cloud e Intelligent Edge. A sua missão é capacitar cada pessoa e cada organização no planeta para alcançarem mais.