**NTT DATA revela como a IA se está**

**a tornar aliada dos cibercriminosos**

**Lisboa, 14 de outubro de 2025 –** O "[Relatório de Tendências e Ciberameaças – 1º semestre de 2025](https://pt.nttdata.com/pt.nttdata.com/insights/reports/cyber-threat-intelligence-trends)*",* da NTT DATA, revela a convergência entre conflitos geopolíticos, eventos climáticos extremos e ciberataques a infraestruturas críticas, o que demonstra um cenário composto por riscos altamente relacionados. Neste contexto, o ritmo de evolução das ameaças cibernéticas intensificou-se de forma expressiva. A crescente sofisticação operacional dos grupos de ransomware, o uso estratégico de IA ofensiva, a padronização dos acessos iniciais e a exploração recorrente de vulnerabilidades estão a dar origem a um ecossistema de ameaças mais dinâmico, opaco e imprevisível.

A NTT DATA acaba de divulgar o seu *"Relatório de Tendências e Ciberameaças – 1º semestre de 2025"*, elaborado pelo departamento de Cyber Threat Intelligence (CTI), que compreende uma análise detalhada da evolução do cenário global de ameaças cibernéticas, com projeções estratégicas para os próximos meses. As interrupções operacionais lideram os impactos negativos, seguidas por investimentos crescentes em deteção e resposta, além do pagamento de resgates por ataques de ransomware. Este ambiente complexo contribui diretamente para a escalada do custo global do cibercrime. De acordo com estimativas da Cybersecurity Ventures, o custo global atingiu 10,5 biliões de dólares por ano em 2025 e poderá chegar aos 12 a 15 biliões de dólares até ao final do ano, caso se mantenha o ritmo atual das ameaças.

O estudo destaca que 2025 está a ser marcado por um ambiente de risco profundamente interligado, em que ameaças cibernéticas, instabilidade geopolítica e eventos climáticos extremos convergem para pressionar infraestruturas críticas. Neste contexto, a cooperação internacional e a resiliência organizacional tornam-se elementos-chave para mitigar ameaças dinâmicas e imprevisíveis, que exigem respostas coordenadas, que possam ser adaptadas e orientadas por dados de inteligência.

Esta tecnologia tem vindo a ser utilizada para desenvolver campanhas de engenharia social altamente convincentes, na criação de identidades falsas, deepfakes e disseminação massiva de desinformação com fins eleitorais. A IA também possibilita a automação de ataques, a aceleração da criação de scripts maliciosos, diminuindo igualmente as barreiras à entrada de agentes com pouca experiência técnica.

A redução de 8% na variabilidade de impacto entre setores evidencia que todos os segmentos estão vulneráveis. A liderança em volume de ataques permanece com a administração pública, seguida pelas áreas de educação, setor público e entidades governamentais, finanças e serviços de TI.

Entre as tendências emergentes de ataques, observa-se um nível de profissionalização sem precedentes. Os Initial Access Brokers (intermediários que vendem acessos a redes corporativas) ampliaram a sua oferta em 15%, facilitando operações de ransomware (que cresceram 32%) e de roubo de dados. Já o modelo ransomware-as-a-service consolida-se como uma prática dominante, na medida em que os cibercriminosos agora terceirizam etapas de ataques, partilham infraestruturas e reaproveitam ferramentas de grupos desarticulados. Tecnologias como o FraudGPT e WormGPT permitem a automação de e-mails de spear phishing, enquanto sistemas de clonagem de voz e vídeo permitem burlar mecanismos de verificação de identidade. O modelo malware-as-a-service também está a fortalecer-se, com milhões de credenciais comprometidas diariamente.

Os principais destaques do relatório são:

* Em momentos críticos, as organizações podem aumentar em até 40% o orçamento destinado à contenção de incidentes.
* A dark web passa por uma profunda reconfiguração após a queda do BreachForums (abril de 2025), com a descentralização do mercado de dados roubados e ferramentas de hacking.
* O modelo crime-as-a-service está em pleno crescimento, com plataformas clandestinas a oferecer hacking a pedido, ataques DDoS, spam e SMS flooding via interfaces SaaS, com suporte técnico e segmentação geográfica. A acessibilidade destes serviços permite que até agentes inexperientes lancem ataques sofisticados, sem interação direta com fornecedores, democratizando o cibercrime e ampliando o risco para empresas e governos.

*“Já não se trata de saber quem vai atacar, mas sim quando, como e com que propósito”*, destaca **María Pilar Torres Bruna, Head of Cybersecurity at NTT DATA for Iberia, International Organizations, LATAM, and Consulting in Benelux and France.**

*“A proteção já não pode ser reativa. É preciso adotar uma postura de recolha proativa de informação sobre ameaças, deteção precoce, colaboração internacional e fomentar uma cultura de cibersegurança institucionalizada, que vá além dos discursos e se converta em práticas sólidas e contínuas”,*acrescenta **María Pilar**.

O *"Relatório de Tendências e Ciberameaças – 1º semestre de 2025"* tem por objetivo orientar os decisores empresariais e governamentais no sentido de anteciparem ameaças emergentes e de fortalecer a capacidade de resposta e resiliência digital das suas organizações.

**Sobre a NTT DATA**

A NTT DATA é uma empresa líder em serviços de negócio e tecnologia, com um volume de faturação superior a 30 mil milhões de dólares, que presta serviços a 75% das empresas do Fortune Global 100. Estamos empenhados em acelerar o sucesso dos clientes e em ter um impacto positivo na sociedade através da inovação responsável.

Somos um dos principais fornecedores mundiais de infraestruturas digitais e inteligência artificial, com capacidades incomparáveis em IA à escala empresarial, *cloud,* segurança, conectividade, centros de dados e serviços de aplicações. As nossas soluções de consultoria e de especialização setorial ajudam organizações e comunidades a avançar com confiança e sustentabilidade rumo ao futuro digital.

Como *Global Top Employer*, contamos com especialistas em mais de 50 países. Oferecemos também aos nossos clientes acesso a um ecossistema robusto de centros de inovação, bem como a parceiros consolidados e *startups*. A NTT DATA faz parte do Grupo NTT, que investe mais de 3 mil milhões de dólares por ano em investigação e desenvolvimento.

Visite-nos em pt.nttdata.com

**Para mais informações contactar:**

**Lift Consulting**

Ana Santos | ana.santos@lift.com.pt | +351 914 409 595

Erica Macieira – erica.macieira@lift.com.pt | +351 910 549 515