Global Threat Landscape Report da Fortinet revela aumento do cibercrime baseado em IA e crescimento de 389% nas vítimas de ransomware

A Fortinet utiliza inteligência de ameaças para combater o cibercrime global, transformando conhecimento em ações concretas

Lisboa, Portugal, 02 de junho de 2026 - A Fortinet, líder global em cibersegurança que promove a convergência entre redes e segurança, divulga o Global Threat Landscape Report para 2026, elaborado pelos FortiGuard Labs. Baseado exclusivamente na telemetria dos FortiGuard Labs, o mais recente relatório anual apresenta uma visão geral do panorama atual de ameaças e tendências, desde 2025, incluindo uma análise abrangente de todas as táticas utilizadas em ciberataques, mapeadas para a *framework* MITRE ATT&CK. Os dados revelam que o cibercrime já não funciona como uma série de ações isoladas – opera como um sistema, com atores maliciosos a interagirem ao longo do ciclo de vida completo do ataque, encurtando a sua duração suportados por agentes de IA.

"O cibercrime é uma das ameaças mais generalizadas e dispendiosas do mundo, e o nosso mais recente Global Threat Landscape Report revela como os agentes maliciosos estão a começar a utilizar IA para executar ataques mais sofisticados. À medida que os cibercriminosos recorrem cada vez mais à IA para reforçar as suas estratégias, os profissionais de cibersegurança precisam de evoluir as operações de segurança para um modelo de defesa industrializado e adotar ferramentas potenciadas por IA que respondam à mesma velocidade das ameaças modernas", **refere Derek Manky, Chief Security Strategist and Global VP of Threat Intelligence, Fortinet FortiGuard Labs.**

Técnicas de ataque e setores visados no Global Threat Landscape Report

O cibercrime moderno ultrapassa fronteiras e setores, e até mesmo as definições tradicionais do próprio crime. À medida que os ataques se tornam mais sofisticados e interligados, as principais conclusões do mais recente Global Threat Landscape Report do FortiGuard Labs revelam:

- **A velocidade determina o risco à medida que o tempo de exploração (TTE) diminui:** à medida que a IA acelera o reconhecimento, a preparação e a execução, os dados da Fortiguard revelam que o TTE é de 24 a 48 horas para incidências críticas, um aumento acentuado em relação a relatórios anteriores que indicavam um TTE de 4,76 dias. Os incidentes reais mostram como alguns minutos podem determinar os resultados: foram realizadas tentativas de exploração ativas poucas horas após a divulgação pública da vulnerabilidade React2Shell.

- **O número de vítimas de *ransomware* disparou:** a inteligência de ameaças FortiRecon identificou 7.831 vítimas confirmadas de *ransomware* em todo o mundo, um aumento acentuado face às cerca de 1.600 vítimas identificadas no *Global Threat Landscape Report 2025*, da Fortinet. A disponibilidade de kits de cibercrime como serviço, como WormGPT, FraudGPT e Brute Force IA, contribuiu para este crescimento homólogo de 389%. Os três setores mais visados foram a indústria transformadora (1.284), os serviços às empresas (824) e o retalho (682). Geograficamente, os países mais afetados foram os Estados Unidos (3.381), o Canadá (374) e a Alemanha (291).
- **A gestão e complexidade das identidades são hoje um dos principais fatores de exposição na cloud:** a inteligência do FortiCNAPP confirma que, ao longo de 2025, a maioria dos incidentes confirmados em ambientes *cloud* teve origem em credenciais roubadas, expostas ou utilizadas indevidamente, e não na exploração da infraestrutura. A análise por setores mostra que hospitais, clínicas médicas e estabelecimentos de retalho são os principais alvos. O elevado número de identidades, os modelos de acesso federado e as integrações complexas na *cloud* tomam estas organizações especialmente vulneráveis e ataques de agentes maliciosos.

Por dentro dos hábitos dos cibercriminosos modernos, equipados com IA

Tal como previsto nas ***Cyberthreat Predictions for 2026 da FortiGuard Labs***, os grupos de ameaça mais sofisticados operam como empresas semi-autónomas, apoiados por agentes de IA, intermediários de acesso e operadores de botnets que disponibilizam serviços sob pedido. As prinicipais conclusões do *Global Threat Landscape Report 2026* revelam que:

- **Os agentes de IA reduzem a necessidade de competências técnicas por parte dos operadores, ao mesmo tempo que aumentam a rapidez dos processos.** Os sinais recolhidos pela FortiRecon na dark web identificaram ferramentas ofensivas potenciadas por inteligência artificial, comercializadas como serviços e produtos, incluindo versões melhoradas do WormGPT e do FraudGPT, bem como novas soluções como o HexStrike AI, uma ferramenta de IA ofensiva capaz de automatizar o reconhecimento e a definição de vetores de ataque; e o BruteForceAI, uma ferramenta de testes de intrusão que integra modelos de linguagem de grande escala (LLMs) para análise inteligente de formulários e consegue executar ataques sofisticados em simultâneo, em múltiplos processos concorrentes.
- **Com a IA, os cibercriminosos trabalham de forma mais inteligente, e não mais intensa.** A telemetria do FortiGate IPS registou uma diminuição de 22% nas tentativas de força bruta em termos anuais (YoY), o que indica ganhos de eficiência: com técnicas de força bruta otimizadas e mais inteligentes, os agentes de ameaça realizam menos tentativas, mas contra alvos melhor selecionados, aumentando a probabilidade de sucesso por credencial testada. Esta atividade traduz-se em cerca de 67,65 mil milhões de eventos de força

bruta a nível global, com aproximadamente 185 milhões de tentativas por dia, 1,3 mil milhões por semana e 5,6 mil milhões por mês. Ao mesmo tempo, a inteligência revelou um aumento de 25,49% nas tentativas globais de exploração de vulnerabilidades em termos anuais (YoY).

- **Os dados roubados têm vindo a ganhar maior relevância do que as credenciais expostas.** No *Global Threat Landscape Report 2025*, a FortiGuard Labs observou um aumento de 500% nos registos provenientes de sistemas comprometidos por malware do tipo *infostealer*. Em 2026, a inteligência da FortiRecon identificou um aumento adicional de 79% e revelou uma mudança para o roubo de conjuntos de dados mais completos, impulsionada pela IA autónoma. Na atividade de "bases de dados" na dark web, os *stealer logs* dominaram os conjuntos de dados anunciados e partilhados (67,12%), ultrapassando as *combolists* (16,47%) e as credenciais expostas (5,96%). Estes *stealer logs* reduzem o esforço dos atacantes ao agregarem informação de identidade com artefactos contextuais, incluindo dados armazenados no navegador, permitindo a sua reutilização imediata e uma conversão mais rápida do que ataques de força bruta ou *password spraying*.
- **O malware de roubo de credenciais continua a persistir.** Este tipo de malware continua a ser uma indústria altamente lucrativa e o principal fator na criação de exposições de segurança. A telemetria da FortiRecon mostra que a atividade de *stealers* é dominada pelo RedLine (911.968 infeções; 50,80%), seguido do Lumma (499.784; 27,84%) e do Vidar (236.778; 13,19%).

Recursos Adicionais

- Descarregue uma cópia do *Global Threat Landscape Report 2026* do FortiGuard Labs.
- Saiba mais sobre a inteligência de ameaças, a investigação e os alertas do FortiGuard Labs, que fornecem medidas oportunas para mitigar ataques de cibersegurança de última hora.
- Saiba mais sobre o papel da Fortinet como membro fundador do Cybercrime Atlas.
- Leia mais sobre a Fortinet Security Fabric.
- Visite fortinet.com/trust para saber mais sobre a inovação da Fortinet, os seus parceiros de colaboração, os processos de segurança dos produtos e os produtos de nível Empresarial.
- Leia sobre como os clientes da Fortinet estão a proteger as suas organizações.
- Saiba mais sobre o compromisso da Fortinet com a segurança e a integridade dos produtos, incluindo a sua abordagem e políticas responsáveis de desenvolvimento de produtos e divulgação de vulnerabilidade.
- Siga a Fortinet no X (anteriormente Twitter), LinkedIn, Facebook e Instagram. Subscreva a Fortinet no nosso blogue ou no YouTube.

Sobre a Fortinet

A Fortinet é uma força motriz na evolução da cibersegurança e na convergência da rede com a segurança. A sua missão é proteger pessoas, dispositivos e dados em qualquer lugar, sendo que hoje oferece cibersegurança onde for necessário, com um portfólio com mais de 50 produtos de nível empresarial. Mais de meio milhão de clientes confiam nas soluções Fortinet, que se encontram entre as mais adotadas, mais patenteadas e mais validadas na indústria. O Fortinet Training Institute, um dos maiores e mais amplos programas de formação da indústria, dedica-se a tornar a formação em cibersegurança e novas oportunidades de carreira disponíveis a todos. A colaboração com organizações de alto nível e respeitadas dos sectores público e privado, incluindo CERTs, entidades governamentais e académicas, é um aspeto fundamental do compromisso da Fortinet para melhorar a ciber resiliência a nível global. A FortiGuard Labs, a organização de elite de investigação e inteligência sobre ameaças da Fortinet, desenvolve e utiliza tecnologias inovadoras como *Machine Learning* e *AI* para fornecer atempadamente aos clientes a melhor proteção de forma consistente e medidas de ação inteligentes na contenção de ameaças. Saiba mais em https://www.fortinet.com, no Blog da Fortinet, e na FortiGuard Labs.

Para mais informação contacte:

Lift Consulting
Beatriz Santanita | beatriz.santanita@lift.com.pt | 918 186 584
Bruna Rocha | mailto:bruna.rocha@lift.com.pt | 910 751 944