

Governos debatem segurança da inteligência artificial (IA)

Uma ordem executiva do presidente norte-americano Joe Biden relativa à IA acentua a importância dos testes por “red teams” e insta o National Institute of Standards and Technology a definir regras antes do lançamento de novas ferramentas de IA.



No Reino Unido, a Declaração de Bletchley, assinada por países presentes no AI Safety Summit, revela preocupação com os riscos da IA “em domínios como a cibersegurança e a biotecnologia, bem como nos casos em que os sistemas de IA de ponta podem amplificar riscos como a desinformação. As capacidades mais significativas destes modelos de IA podem causar danos graves, ou mesmo catastróficos, deliberados ou não intencionais”. Isto quando já estão a ocorrer ataques DDoS ao ChatGPT.



Fontes: [Executive Order](#), [Fact Sheet](#), [AI Safety Summit 2023](#), [Declaração de Bletchley](#), [Security Affairs](#), [The Conversation](#), [Wired](#)

Grupos de ransomware visam entretenimento e estão mais agressivos

O ciberataque contra os MGM Resorts em Las Vegas (EUA) revelou o interesse dos criminosos nos gigantes do setor do entretenimento. Os ataques focaram-se nas redes internas, dados pessoais, “slot machines”, caixas ATM ou nos cartões de acesso aos quartos dos hotéis. Entre outras, os atacantes usaram estratégias de engenharia social.



Após o MGM, foram atacados o Caesars Entertainment (EUA) e o Marina Bay Sands (Singapura). O primeiro não pagou o resgate, enquanto o Caesars o fez para, segundo afirmou, evitar a revelação de dados dos clientes.

O FBI alertou que os grupos de ransomware “estão a explorar vulnerabilidades nos sistemas de acesso remoto controlados pelos fornecedores” para atacar casinos, cadeias hoteleiras e estâncias de luxo. Soube-se também que grupos de

ransomware como o Octo Tempest se tornaram mais agressivos, “recorrendo mesmo a ameaças físicas”.

Fontes: [Dark Reading \(1,2\)](#), [Cybersecurity Dive](#), [Microsoft](#), [The Verge](#), [Security Affairs](#), [Forbes](#), [Engadget](#), [Axios](#)

Portugal adere ao CARF

A deficiente regulamentação na Estónia das criptomoedas transformou o país num centro de criminalidade financeira. O país endureceu as leis e os criminosos internacionais estão a deslocar-se para outros países. “Isto mostra que corrigir o sistema num país não muda

grande coisa". No entanto, 47 países – incluindo Portugal – comprometeram-se a adotar até 2027 o Crypto-Asset Reporting Framework (CARF), um novo quadro internacional para o intercâmbio automático de informações entre autoridades fiscais.

Fontes: [VSquare](#), [Autoridade Tributária](#), [Australian Government](#), [Cointelegraph](#)

CRA protege ou diminui cibersegurança europeia?



O artigo 11 do Cyber Resilience Act europeu desagrada aos profissionais e empresas de cibersegurança e também aos defensores dos direitos civis. "O artigo diz que os fornecedores de software devem comunicar as vulnerabilidades de 'zero day' aos organismos governamentais no prazo de 24 horas após a sua descoberta", mas esta obrigação "pode ser utilizada indevidamente para fins de vigilância e até comprometer os esforços de cibersegurança".

Fontes: [Stack Diary](#), [Cyber Resilience Act](#), [Open letter](#), [CyberScoop](#)

BREVES

- A Alemanha triunfou na edição de 2023 do [European Cybersecurity Challenge](#), seguida da Suíça e Dinamarca. Pela primeira vez, [Portugal](#) teve uma representação feminina.

- A ENISA formalizou um [Working Arrangement](#) com os homólogos ucranianos centrado no reforço das capacidades da cibersegurança e na partilha de boas práticas.

- [Porque se deve estabelecer uma NATO da cibersegurança](#), apesar da "[falsa promessa das ciberconvenções](#)"? "Os cibercriminosos já operam além-fronteiras. As nações devem fazer o mesmo para proteger as suas infraestruturas críticas, pessoas e tecnologia contra ameaças estrangeiras e nacionais". Na primeira Cyber Defence Conference, os aliados da NATO aceitaram a necessidade de novos métodos para enfrentar [potenciais ameaças](#) e apoiaram a [criação de um NATO Cyber Centre](#).

- [Mercenários dos DDoS](#) atacam ambos os lados em conflito.

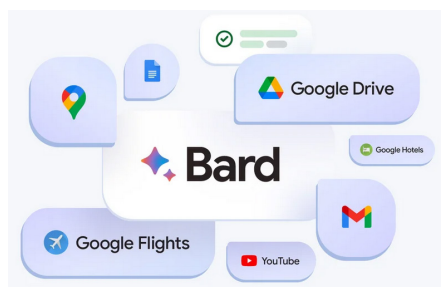
- A [ciberguerra entre Oriente e Ocidente](#) passa por África.



- O Comité Internacional da Cruz Vermelha (ICRC) publicou [regras de atuação para hackers civis](#) envolvidos em conflitos, onde inclui a proibição de ataques a hospitais ou o uso de malware de propagação automática que tanto pode danificar objetivos militares como civis. [As regras não obtiveram grande aceitação](#).

- A escassez de profissionais está a facilitar o aparecimento de [sites maliciosos](#) para a alegada avaliação de competências profissionais.

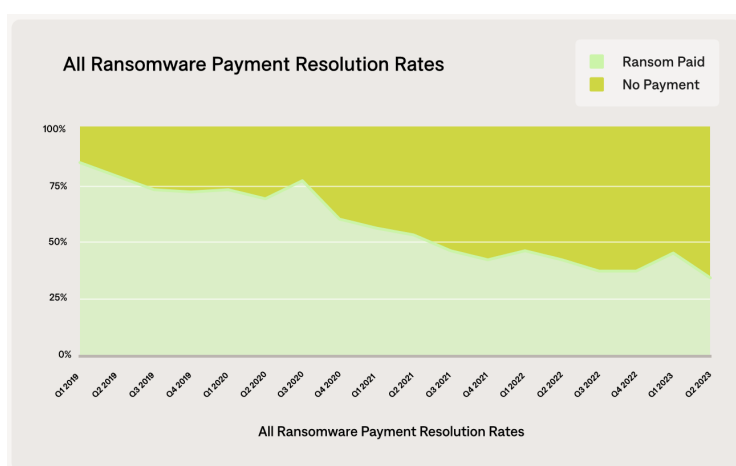
- O [novo Outlook envia passwords, mensagens e outros dados para a Microsoft](#), mesmo sendo de um fornecedor de email diferente. E o [Word é usado para ataques de phishing](#).



- A [Google processou burlões](#) que se estão a aproveitar do interesse pelas ferramentas de IA generativa para induzirem os utilizadores a fazer download de malware. O Bard, ferramenta de IA da Google, não necessita de ser descarregado.

- A rede de publicidade [Google Ads está a ser usada para distribuir o malware RedLine](#).

- A filial norte-americana do banco ICBC teve de entregar as suas [transações numa pen USB](#) após um ciberataque.
- Depois de uma vaga de ataques que lhe proporcionou o acesso a milhões de dólares, o [Lazarus Group alterou as suas táticas e acelerou as suas atividades criminosas](#).
- Pode ser impossível impedir as violações de dados no [universo educativo](#) pela crescente sofisticação dos ataques, mas há [passos importantes que podem dificultar o acesso ilegal](#).
- Só a aquisição de um ciberseguro não é suficiente para as PMEs, porque elas [“precisam de uma cibersegurança proativa”](#). Por seu lado, as seguradoras estão a usar as empresas de cibersegurança para [avaliar](#) o mercado [“antes de aprovarem os pedidos de apólices de novos clientes”](#).
- A escolha das passwords pelos administradores de TI [“é totalmente deprimente”](#) e eles [não se diferenciam](#) do resto dos [utilizadores infelizes no trabalho](#).
- Desmontar falsas alegações num hipotético ciberataque ou [“o que há de verdadeiro na oferta do recente conjunto de dados do LinkedIn”](#).



- Diversas nações, incluindo da União Europeia, comprometeram-se na [Counter Ransomware Initiative \(CRI\)](#) a [não pagar resgates em caso de ciberataque](#).

Algumas [dúvidas](#) e sinais apontam que essa [tendência pode estar a diminuir](#), embora 2023 também possa ser o [segundo ano mais lucrativo nos EUA](#) do ecossistema do ransomware. Este está a profissionalizar-se [“numa tentativa de ganhar eficiência e maximizar os lucros”](#).

- [Críticas](#) ao Cloud Certification Scheme ([EUCS](#)), sistema europeu de certificação de cibersegurança para serviços em cloud, e o que se pode [aprender com os ataques à cloud](#).
- O valor global da cibercriminalidade deve atingir os 9,5 biliões de dólares em 2024. Se fosse um país, [“o cibercrime seria a terceira maior economia do mundo, depois dos EUA e da China”](#). Mas porque se deve quantificar o [valor do cibercrime](#)? E porque pode a [cooperação público/privada](#) proteger contra o cibercrime?

- Será que um [Estado desativou a botnet](#) Mozi?
- [Há algum software seguro?](#)
- Malware foi disseminado em dispositivos Android usando [falsos alertas sobre uma erupção vulcânica](#) em Itália.
- [Cortes orçamentais](#) na Cybersecurity and Infrastructure Security Agency (CISA) podem afetar a defesa das redes federais nos EUA e a ajuda aos operadores de infraestruturas críticas contra ataques informáticos.
- Na “[semana infernal](#)” em que as infra-estruturas críticas da Dinamarca foram atacadas, as vagas registaram [22 organizações afetadas em poucos dias](#).
- A Austrália revelou ter sofrido um “[ciberincidente significativo a nível nacional](#)” após um [ataque ao principal operador portuário](#) o ter levado a encerrar atividades.
- A cibersegurança ferroviária pode ser um “[ambiente complexo](#)”.
- Num novo esquema detetado no Aeroporto Internacional John F. Kennedy, em Nova Iorque, o [sistema de despacho dos táxis foi pirateado](#) para vender os melhores lugares aos condutores.
- Se um familiar lhe telefonar, aos gritos de que foi raptado, qual é a probabilidade de [encarar a situação com calma](#)? No entanto, tudo pode não passar de um “[rapto virtual](#)”.

ALER

- [Orientações da Comissão sobre a aplicação do artigo 4.º, n.os 1 e 2, e sobre a aplicação do artigo 3.º, n.º 4, da Diretiva NIS 2](#)
- [Europol publica o relatório anual Internet Organised Crime Threat Assessment](#)
- [ENISA Threat Landscape 2023](#)
- [Designados os membros da Comissão de Planeamento de Emergência da Cibersegurança](#)
- Consulta sobre [Sistema Europeu Comum de Certificação da Cibersegurança \(EUCC\)](#)
- [Comissão congratula-se com acordo](#) alcançado pelo [Parlamento Europeu e pelo Conselho da UE](#) na [carteira europeia de identidade digital](#)

