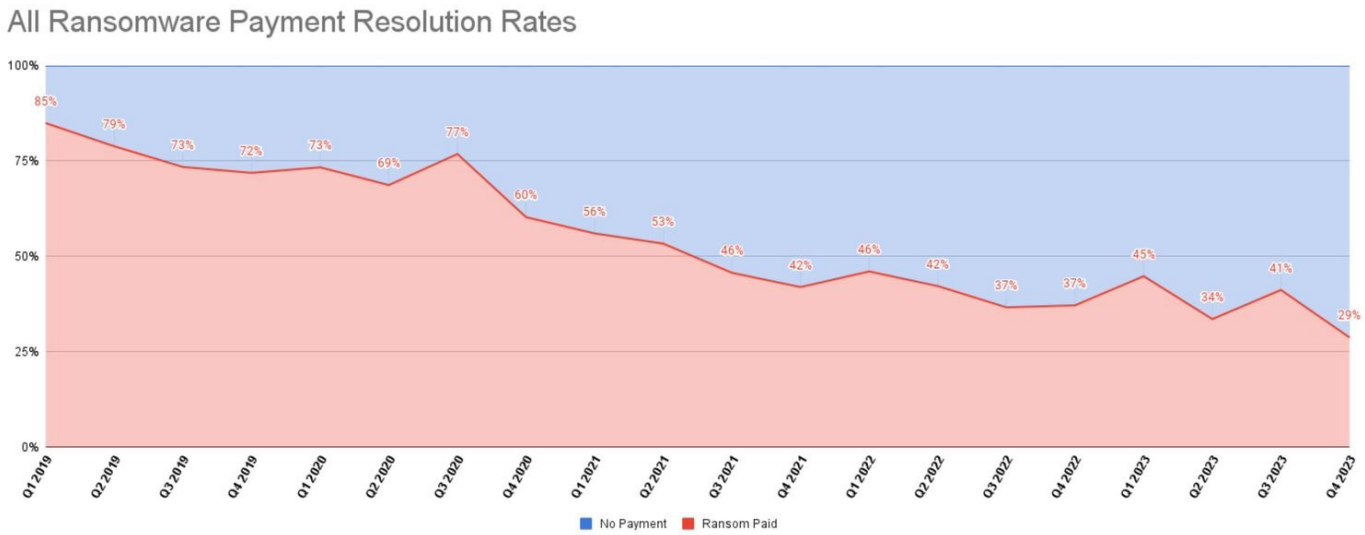
# ptsoc digest

## fevereiro 2024

Diretora | Inês Esteves • Edição | Pedro Fonseca

.pt ptsoc Centro de Operações de Segurança

## Ransomware com novo recorde



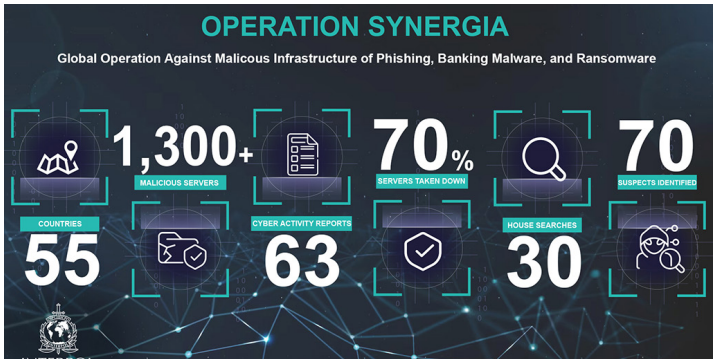

Os cibercriminosos arrecadaram 1.100 milhões de dólares em criptomoedas com os ataques de ransomware em 2023 - estabelecendo um novo recorde, mais do que duplicando os 567 milhões em criptomoedas destes ciberataques obtidos em 2022, segundo a Chainalysis. No entanto, menos vítimas estão a pagar pelos resgates, nota a Coveware.

Esta empresa de negociação de ransomware calcula que apenas 29% das organizações pagou algum resgate no último trimestre de 2024, longe dos 85% transferidos no início de 2019 (ver gráfico acima).

A Coveware atribui este cenário a fatores como melhores redes empresariais ou o maior hábito de ter mais cópias de segurança para ajudar na rápida recuperação de dados das organizações. E mais empresas não confiam que os cibercriminosos cumpram as promessas e devolvam os dados roubados.

A linha de tendência geral de 2019 a 2023 indica que o ransomware continua a ser um problema crescente. Os valores apresentados não captam "o impacto económico da perda de produtividade e dos custos de reparação associados aos ataques".

O número de ameaças tem continuado a aumentar e a atingir novos setores, com 538 novas variantes detetadas em 2023, sintoma da atuação de mais grupos independentes e da disseminação do "ransomware-as-a-service" (RaaS), com ferramentas de mais fácil uso e um melhor conhecimento da predisposição das vítimas (e das seguradoras) para não pagar resgates, desincentivando os cibercriminosos.



Em simultâneo, as autoridades estão mais atentas. Uma recente operação da Interpol contra o phishing, malware bancário e ataques de ransomware, denominada Synergia, levou à identificação de mais de 1.300 endereços IP e URL suspeitos, envolveu 60 agências policiais em 55 países e permitiu identificar mais de 1.300 servidores maliciosos, 70% dos quais já foram eliminados na Europa.

*Fontes: Coveware, Chainalysis, Interpol, The Record, Dark Reading*

## Perceção de risco de ciberataques no seu nível mais elevado


Os ciberataques são a principal ameaça na perceção de riscos num grupo de 12 países, apenas ultrapassados pelos eventos meteorológicos extremos. Segundo o Munich Security Report 2024, publicado em Fevereiro em antecipação à Munich Security Conference, o relatório deste ano posiciona o potencial de risco de ciberataque no seu nível mais elevado de sempre, liderando também como principal preocupação mais recente na China e nos EUA.

Em geral, a percepção destes ataques subiu da quarta posição em Novembro de 2021 para a segunda em Outubro/Novembro de 2023.

*Fonte: Munich Security Report 2024*

## Desinteresse dos partidos políticos na cibersegurança das eleições

O Centro Nacional de Cibersegurança (CNCS) realizou no início de fevereiro um exercício de cibersegurança estratégica para testar a articulação entre algumas das várias entidades envolvidas nas eleições de 10 de março.

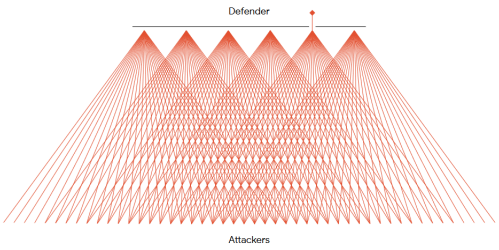
O exercício envolveu o CNCS, a CNE, a ERC, a Lusa, Gabinete Cibercrime do MP, a SGMAI, a PJ e o SIS. Teve como cenário um conjunto de incidentes ligados a campanhas de desinformação, como a disseminação de sondagens fraudulentas, documentos e notícias falsas, entre outros.

O exercício demonstrou "existir um conhecimento amplo das competências de cada uma das entidades em relação às demais e ficou demonstrada a consciência da necessidade de colaboração", segundo o CNCS, sendo no entanto realçadas as dificuldades na sensibilização dos partidos políticos para as questões da cibersegurança.

*Fonte: CNCS*

## Google quer usar IA para alterar "Dilema do Defensor"

A Google lançou a AI Cyber Defense Initiative para usar a inteligência artificial (IA) no aumento da cibersegurança e inverter o "Dilema do Defensor". A empresa explica que, "durante décadas, o principal desafio da cibersegurança tem sido o facto de os atacantes precisarem apenas de uma ameaça nova e bem sucedida para ultrapassar as melhores defesas. Os defensores, por sua vez, precisam de implementar as melhores defesas a todo o momento, num terreno digital cada vez mais complexo - e não há margem para erros. Este é o 'Dilema do Defensor', e nunca houve uma forma fiável de fazer pender essa balança".




A empresa anunciou também a segunda edição da Google for Startups Growth Academy: AI for Cybersecurity, e selecionou a Ethiack (empresa de Coimbra) como única empresa portuguesa.

*Fontes: AI Cyber Defense Initiative, Google for Startups Growth Academy: AI for Cybersecurity*

## BREVES

• Em exclusivo, a CNN Portugal revelou os detalhes do processo de extradição do jovem português que está em risco de passar 57 anos numa prisão nos EUA.

• As Nações Unidas iniciaram uma investigação sobre 58 ciberataques da Coreia do Norte contra empresas de criptomoedas que terão rendido 3.000 milhões de dólares entre 2017 e 2023, tendo como objetivo financiar o programa nuclear ilegal desse país.

• A OpenAI, empresa responsável pelo ChatGPT, com o apoio da Microsoft, encerrou cinco contas de grupos com ações ilegais ligados à China (conhecidos por Charcoal Typhoon e Salmon Typhoon), Rússia (Forest Blizzard), Irão (Crimson Sandstorm) e Emerald Sleet, da Coreia do Norte.


OpenAi

• Cibercriminosos estão a aceder ilegalmente a contas bancárias no sudeste asiático utilizando dados de reconhecimento facial roubados às vítimas, imitando estratégias usadas com Taylor Swift. A "sofisticada campanha" está a ser concretizada pelo grupo denominado GoldFactory, segundo a empresa de cibersegurança Group-IB.

• As autoridades dos EUA neutralizaram uma rede de centenas de routers para pequenos escritórios/escritórios domésticos (SOHO) usados para ciberataques de "spearphishing" e recolha de documentos oficiais por grupos russos. Esta botnet diferenciava-se por usar o malware Moobot, associado a um grupo cibercriminoso.

• A China tornou-se a principal ciberameaça da pirataria informática, com a série recente de ataques dirigidos a infra-estruturas críticas dos EUA. A ameaça "persistente" regista o interesse no acesso a esse tipo de infra-estruturas durante "pelo menos, cinco anos".

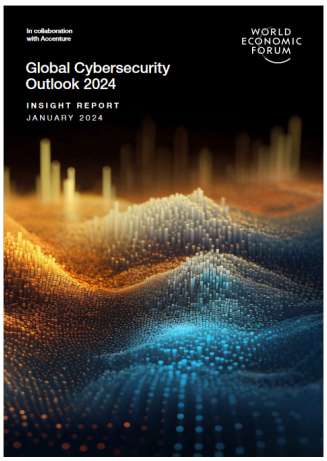

rawpixel.com, Freepik

• As autoridades da Roménia registaram um ataque de ransomware que afetou uma centena de hospitais a partir da aplicação HIS.

• Os governos devem tomar medidas mais agressivas para combater o crescimento da indústria de spyware comercial, que continua a fornecer aos governos malware invasivo.

• Técnicas potenciais que permitem abusar de redes Wi-Fi públicas e comprometer os seus dados.

## A LER




Global Cybersecurity Outlook 2024

Regulamento Ciber-Resiliência: Conselho e Parlamento chegam a acordo sobre os requisitos de segurança dos produtos digitais

Cyber solidarity act: member states agree common position to strengthen cyber security capacities in the EU

Reforço da cooperação entre a CISA e ENISA

Generative AI in EU Law: Liability, Privacy, Intellectual Property, and Cybersecurity

European Commission has published a series of new calls for proposals of the Digital Europe Programme: A dedicated budget of EUR 84 million to enabling technologies for Security Operation Centres and the implementation of cybersecurity EU legislation


First EU-wide cybersecurity certification scheme to make European digital space safer

Generative AI in EU Law: Liability, Privacy, Intellectual Property, and Cybersecurity

ICANN Publishes Paper on Defense Mechanisms Against Harmful Internet Content

Diretora | Inês Esteves

Edição | Pedro Fonseca

fevereiro 2024