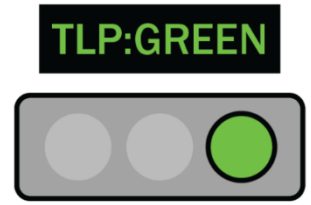


RNEP-GW

MÓDULO RANSOMWARE

fct csirt

RNEP-GW

O QUE É RANSOMWARE?

- Malware que criptografa ficheiros, bloqueando-os
- Exige pagamento para que ficheiros sejam desencriptados e o acesso seja restabelecido
- Ransom = resgate; Ware = abreviação de malware

CASOS FAMOSOS

WannaCry

- “Epidemia global” em 2017
- ~230 mil computadores infetados
- ~US$ 4MM de prejuízo

GRUPOS FAMOSOS

REvil

- Desmantelado em 2022
- Supostamente atacou e tentou extorquir pessoas famosas e grandes empresas. Ex.: Donald Trump, Lady Gaga, Acer, empresa ligada à Apple.

Akira

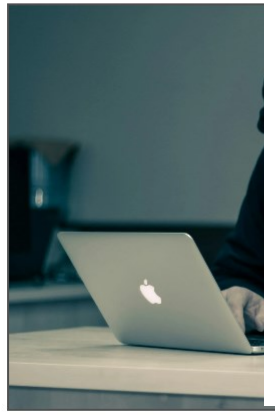
- Formado em 2023, ainda activo
- Ataque a empresas de diversos setores. Ex.: BHI Energy, Nissan Austrália, Universidade de Stanford.

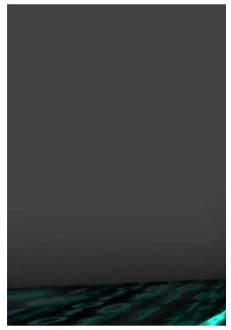
RANSOMWARE NÃO SAI DE MODA

Home › Tecnologia ›

Pesquisa aler número de at ransomware

Pesquisa de cibersegurança da Acror brasileiras; saiba mais detalhes





Ransomware:

A Sophos apresentou, em encontr de organizações que optaram pc impact

por Vinicius Marques 07 de julho de 2025 às 08:17 6 minutos de leitura

O Brasil foi o sétimo país do mundo que mais sofreu ataques de ransomware ao longo de 2024. A informação está registrada na edição mais recente do "Cyberthreats Report". Este é um relatório semestral produzido pela equipe global de inteligência de ameaças da Acronis, especializada em soluções de cibersegurança.

Ransomware attack contributed to patient's death

25 June 2025

Jess Warren
BBC News

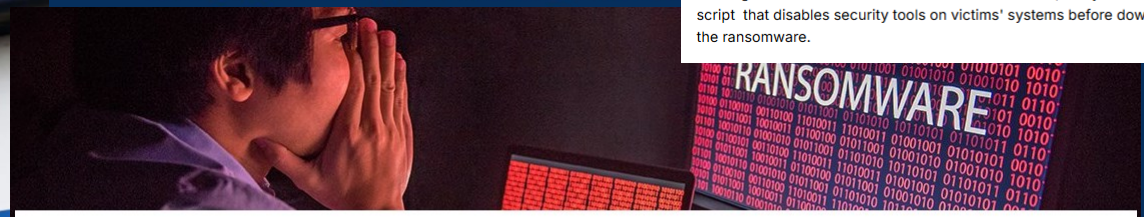
King's College Hospital

The death of on services at Lond

Share Save

Society

Poland is top target for glob



Only 59% of Polish companies report using security software. Photo by Jakub Porzycki/NurPhoto via Getty Images

SHARE

FACEBOOK

Poland recorded the highest number of ransomware attacks worldwide in the first half of 2025, accounting for 6% of all global incidents, according to the ESET cybersecurity company.

Beware of Bert: New ransomware group targets healthcare, tech firms

A new ransomware group has been breaching organizations across Asia, Europe, and the U.S., with victims reported in the healthcare, technology and event services sectors, researchers have found.

The group, calling itself Bert, was first identified in April by researchers at cybersecurity firm Trend Micro, who detailed their findings in a report published Monday.

The ransomware has infected both Windows and Linux systems, the researchers said. Although the initial access method remains unknown, analysts discovered a PowerShell script that disables security tools on victims' systems before downloading and executing the ransomware.

NEWS

Ingram Micro hit by ransomware attack

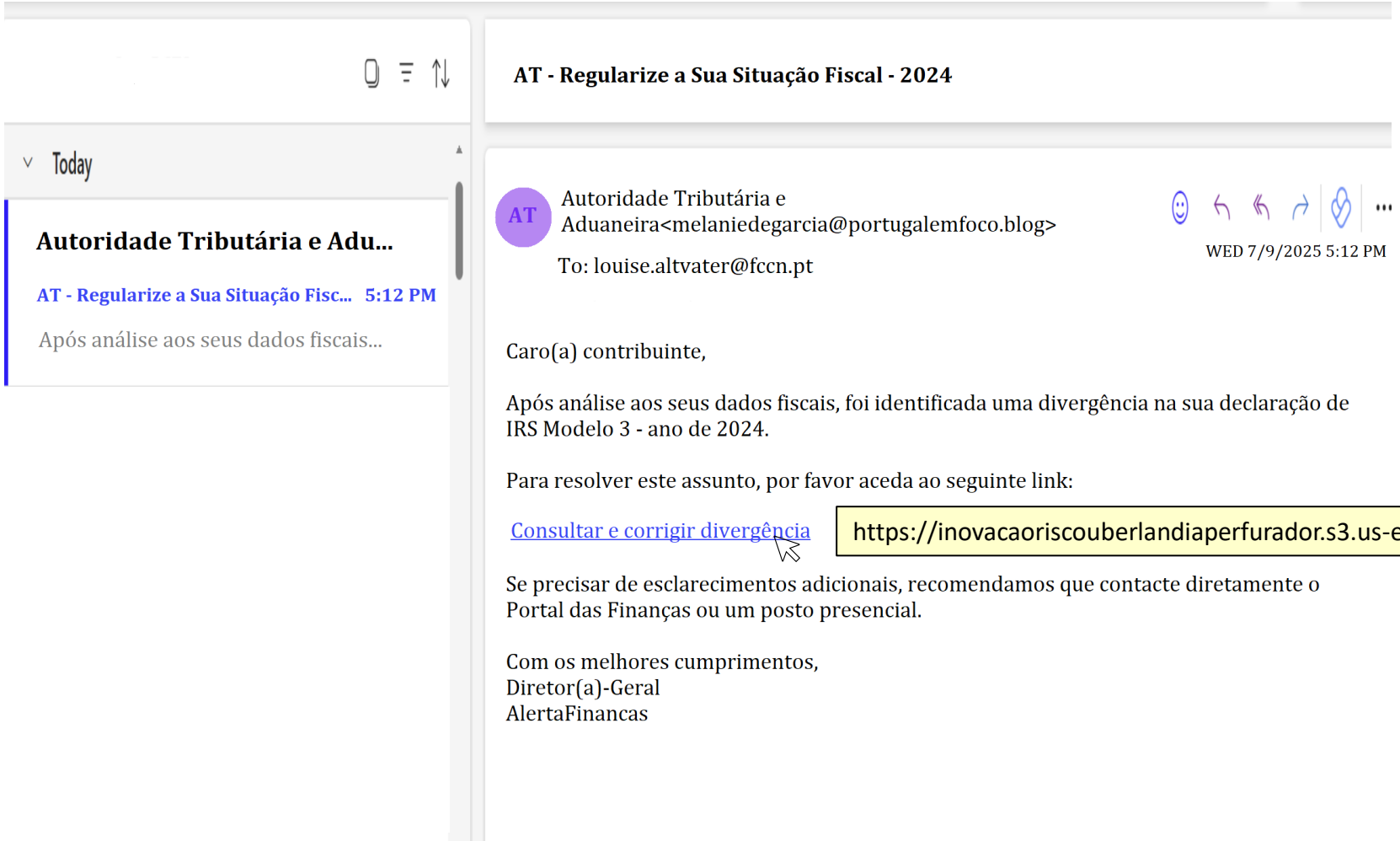
Distributor Ingram Micro suffers outages after ransomware group targets the channel player

By **Simon Quicke**, Microscope Editor Published: **07 Jul 2025 12:48**

Ingram Micro has revealed it has become the victim of a ransomware attack. The distributor shared an update over...

MEIOS DE PROPAGAÇÃO

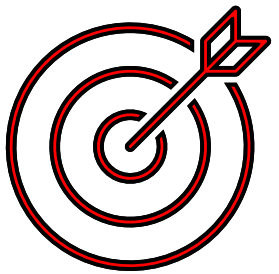
Engenharia Social e Phishing



MEIOS DE PROPAGAÇÃO

Ataques direcionados (Spear Phishing)

- Vítima específica: empresa ou pessoa com acesso privilegiado
- Tempo dedicado a coleta de informações
- Criam armadilhas personalizadas

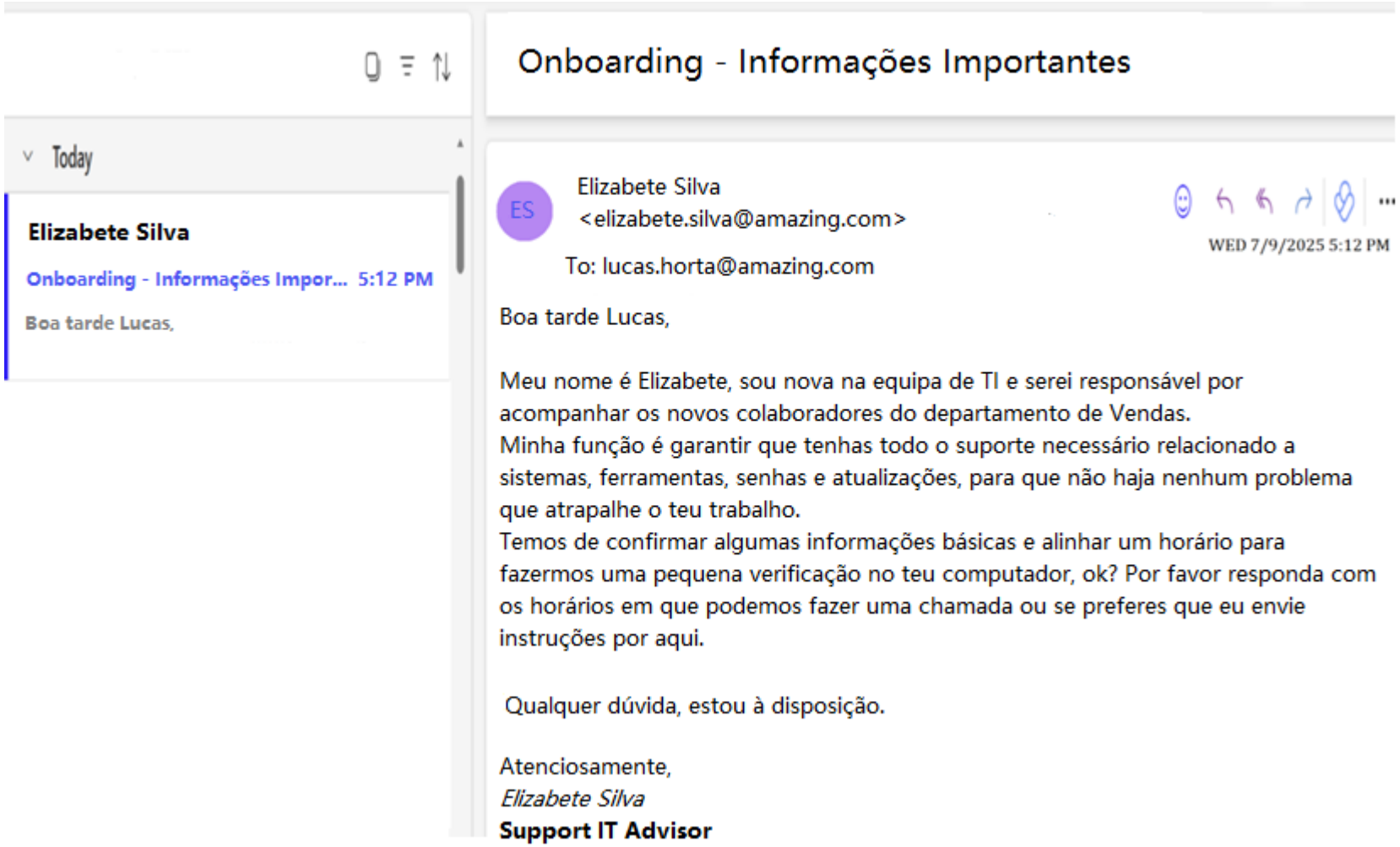


MEIOS DE PROPAGAÇÃO

Ataques direcionados (Spear Phishing)

Plataforma de Vendas Amazing	
Campo	**Dados**
Customer ID	102547
Name	Maria Silva
Data de nascimento	15/09/1985
Morada	Rua das Flores, 123, Lisboa
Telefone	+351 982 822 988
Email	maria.silva@example.com
Cartão de crédito	4111 1111 1111 1111 (VISA)
Tipo de assinatura	Basic+
Data da última Compra	10/07/2025
Valor Gasto Total	€ 2.350,00

MEIOS DE PROPAGAÇÃO



Today

Elizabete Silva

Onboarding - Informações Impor... 5:12 PM

Boa tarde Lucas,

Onboarding - Informações Importantes

ES

Elizabete Silva
<elizabete.silva@amazing.com>

WED 7/9/2025 5:12 PM

To: lucas.horta@amazing.com

Boa tarde Lucas,

Meu nome é Elizabete, sou nova na equipa de TI e serei responsável por acompanhar os novos colaboradores do departamento de Vendas.
Minha função é garantir que tenhas todo o suporte necessário relacionado a sistemas, ferramentas, senhas e atualizações, para que não haja nenhum problema que atrapalhe o teu trabalho.
Temos de confirmar algumas informações básicas e alinhar um horário para fazermos uma pequena verificação no teu computador, ok? Por favor responda com os horários em que podemos fazer uma chamada ou se preferes que eu envie instruções por aqui.

Qualquer dúvida, estou à disposição.

Atenciosamente,
Elizabete Silva
Support IT Advisor

MEIOS DE PROPAGAÇÃO

Dispositivos USB “perdidos”

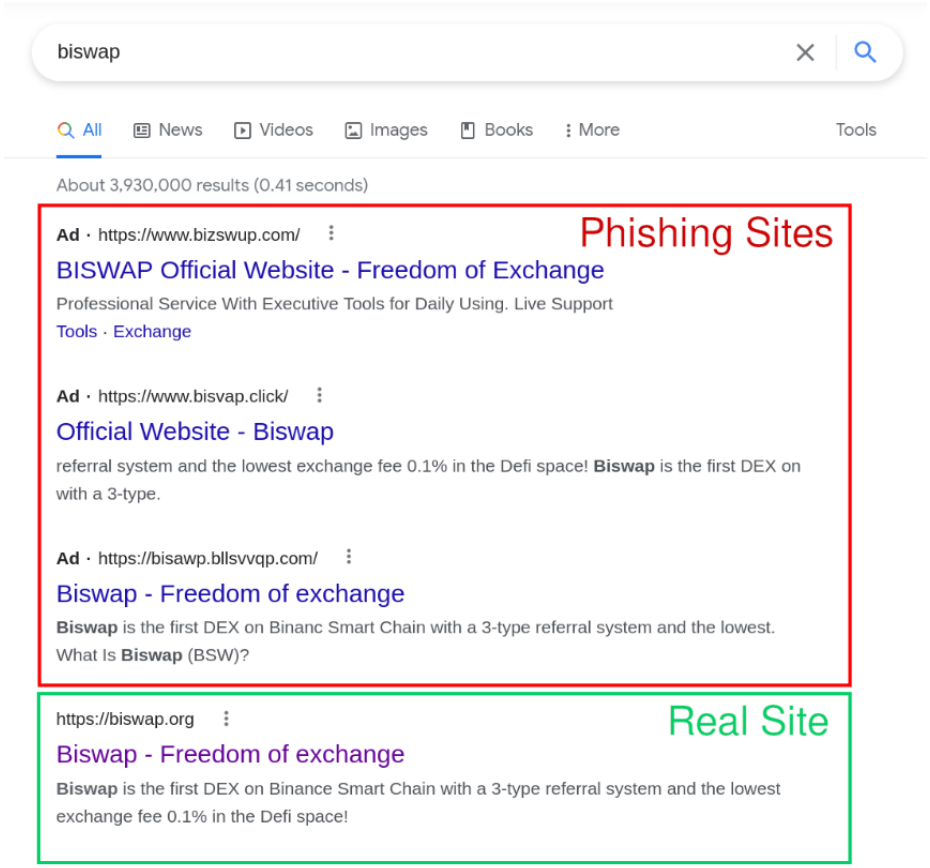
- “Perdidos” em estacionamentos, salas de reunião, casa de banho…

- Ransomware instalado assim que o dispositivo USB é conectado ao computador

MEIOS DE PROPAGAÇÃO

Downloads de sites infetados

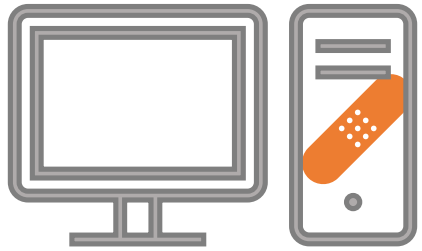
- Phishing
- Programas gratuitos ou piratas
- Atualizações falsas
- Anúncios patrocinados



MEIOS DE PROPAGAÇÃO

Vulnerabilidades em sistemas desatualizados

- Falhas de segurança conhecidas
- Softwares e plugins obsoletos
- Dispositivo vulnerável com acesso à rede



COMO SE PROTEGER

- Manter sistemas atualizados
- Fazer backups frequentes de dados relevantes
- Desconfiar de e-mails e links suspeitos
- Treinar equipas e ter políticas de segurança
- Apenas manter serviços estritamente necessários em máquinas críticas

E SE ACONTECER?

- NUNCA pagar o resgate!
- Isolar os dispositivos infetados
- Notificar as autoridades
- Restaurar backups seguros
- Aprender com o incidente

IDEIAS CHAVE

- Ransomware é um tipo de malware que criptografa ficheiros e exige pagamento para que estes sejam desencriptados
- A maior porta de entrada ainda é o fator humano: phishing, engenharia social e descuidos
- Manter backups confiáveis em lugares seguros e sistemas atualizados

Questões?

Obrigado.

csirt.fct.pt/podcast

csirt.fct.pt/mooc

csirt.fct.pt/etc