ptsoc digest

janeiro 2024

Diretora | Inês Esteves • Edição | Pedro Fonseca

.pt ptsoc Centro de Operações de Segurança

Programa Europa Digital apoia transição digital e cibersegurança

A Comissão Europeia atribuiu mais de 760 milhões de euros de investimento no Programa Europa Digital para a transição digital e a cibersegurança, no âmbito dos programas de trabalho alterados para 2024. O programa de trabalho específico centrado na cibersegurança terá um orçamento de 214 milhões de euros este ano e um destaque especial no apoio às pequenas e médias empresas. Tem como objetivos apoiar "a deteção e a partilha de ciberameaças, a aplicação da legislação da UE em matéria de cibersegurança, a preparação para situações de emergência em caso de ciberataques e a assistência mútua, bem como os centros de coordenação nacionais".

Fontes: Comissão Europeia, ECCC

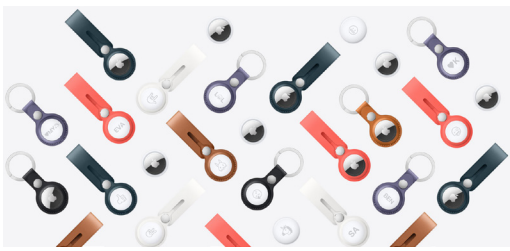
Contas da Google desprotegidas

Uma técnica de acesso não autorizado a contas da Google foi revelada recentemente, explorando uma vulnerabilidade que contorna a autenticação multifator (MFA) ou a alteração da password. Ela já foi incorporada em vários programas de roubo de informações (os denominados "info-stealers").

A técnica passa por aceder aos cookies de autenticação e aumentar a data da sua vida útil. Mesmo que o utilizador altere a password da conta, os cookies asseguram a autenticação durante um período maior do que o esperado nos diversos serviços da Google (Gmail, Calendar ou YouTube, por exemplo).

Fontes: BleepingComputer, Malwarebytes Labs

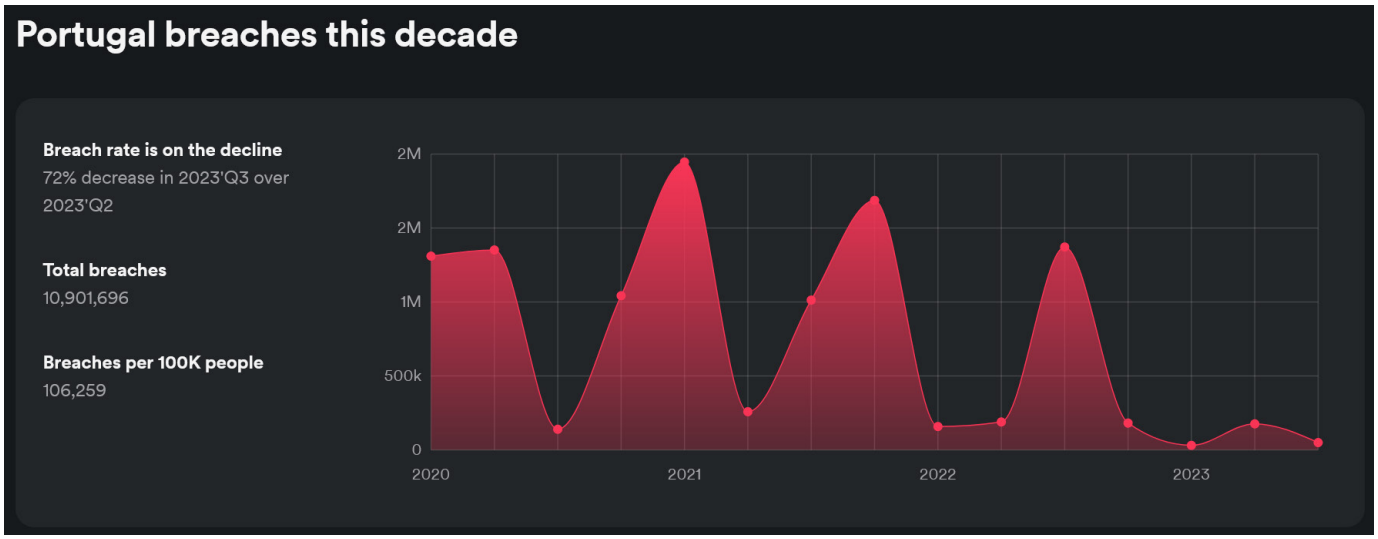
Os perigos da Apple



Um juiz norte-americano considerou que a Apple pode ter sido "negligente" na criação dos AirTags. Algumas vítimas avançaram com um processo em tribunal considerando que o dispositivo de localização facilita perseguições ("stalking"). Além disso, vários investigadores de segurança alertaram a empresa há vários anos para vulnerabilidades na função de partilha AirDrop que têm servido às autoridades chinesas para localizar críticos do governo ou detetar cidadãos que partilham conteúdos proibidos no país. A Apple manteve o silêncio sobre este assunto e não tomou quaisquer medidas, dizem os investigadores.

Fontes: The Record, CNN, PrivateDrop, Ars Technica

A importância dos governos na definição das passwords pessoais



Algumas características dos governos estão entre as variáveis macrossociais que agilizam a previsão e descoberta das passwords dos utilizadores. Por exemplo, conclui a investigadora Andreanne Bergeron, da University of Montreal (Canadá), "os países democráticos e os países em que o governo investe na cibersegurança aumentam o desempenho dos utilizadores em termos de ter passwords mais fortes".

A conclusão está no estudo "Tell Me Where You Live and I Will Tell Your P@Ssw0rd: Understanding the Macrosocial Variables Influencing Password's Strength", em que Bergeron analisa outra vertente de como "o empenho económico dos países na luta contra a cibersegurança provou ser rentável do ponto de vista económico", com os governos a terem "um papel importante a desempenhar na ciberprotecção dos utilizadores, quer seja direto (investindo na cibersegurança) ou indireto (dando prioridade à democracia e à educação)". Neste âmbito, os desafios da protecção e uso das passwords "são provavelmente maiores" para os utilizadores com baixo nível de literacia.

Bergeron aponta ainda que a revelação pública pelas organizações das violações de dados leva os utilizadores a aumentarem a robustez das suas passwords.

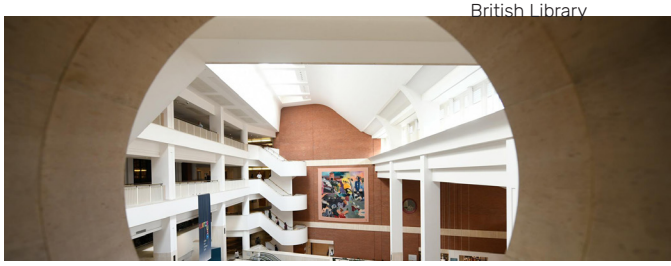
Fonte: Applied Cybersecurity & Internet Governance, gráfico: Surfshark

BREVES

• Dos quase 5.200 casos de ransomware registados em 2023, o número de "famílias" de programas únicos usados pelos criminosos diminuiu, passando de 95 em 2022 para 43 em 2023. Isto demonstra como essas "famílias" e modelos de ransomware estão a funcionar, como sucede com a Medusa, sem necessidade de desenvolver algo novo.

• A perniciosa relação entre jornalistas e grupos de ransomware, que prosseguem com pedidos de resgates à British Library (em recuperação) e ataques a museus, a diversas cidades, a doentes oncológicos ou a hospitais.

British Library



• Casinos: pagar ou não o pedido de ransomware?

• O "Leaksmas", presente de Natal na Dark Web, expôs enormes volumes de dados pessoais.

• Mais de 223 milhões de registos com dados pessoais como o nome, data de nascimento ou número do Cadastro de Pessoas Físicas, "que identifica os contribuintes individuais no Brasil", estiveram acessíveis publicamente.

• A Direção Geral de Tecnologias da Informação e Comunicação (Digetic), ligada às forças armadas do Paraguai, alertou para os perigos do ransomware, após um dos principais fornecedores de Internet (ISP) ter sofrido um forte "incidente de segurança".

• O segundo maior operador espanhol de comunicações móveis, a Orange España, sofreu uma interrupção de serviço após alguém ter acedido a uma palavra-passe "ridiculamente fraca" e a ter usado na conta de "routing" global do tráfego Internet da empresa junto do RIPE.

• A Agência Nacional de Cibersegurança do Qatar quer lançar um programa escolar de educação para a cibersegurança em 270 escolas privadas, após o ter feito para 30 escolas públicas no ano passado.

• Nos Emirados Árabes Unidos, 87% das empresas lidaram com ciberincidentes nos últimos dois anos, sendo os funcionários responsáveis por 25% desses incidentes.

• Jovem autista do Lapsus$ fez ataque por "smart TV" de hotel e foi condenado a internamento hospitalar.

• Uma década depois, o que se aprendeu com os ataques ao Yahoo? "Muito pouco".

• Em 2008, o vírus Stuxnet terá sido libertado pelo holandês Erik van Sabben numa operação dos Estados Unidos e de Israel para sabotar o programa nuclear do Irão.

• Ataques a infra-estruturas críticas já não são exclusivos de nações inimigas.

• Os EUA têm preparado as suas infra-estruturas contra ciberataques da Rússia, Irão ou China. Numa abordagem diferente com a Coreia do Norte, tentam bloquear o uso das criptomoedas obtidas em ciberataques.

• Profissionais de cibersegurança dos EUA e Europa revelam os melhores podcasts sobre o tema.

• Competências dos modernos CISO e dos analistas de ameaças.

• Porque se devem apagar contas antigas sem uso (e alterar passwords originais).

• O que constitui um "ato de guerra" nas apólices de seguros?

• "Tia" dos programas de "bug bounty" preocupada com a regulação internacional.

• Startups e soluções de cibersegurança a ter em atenção.

• Boas notícias na cibersegurança em 2023.

• Com um menor investimento nas fusões e aquisições em cibersegurança, 2024 tenderá a ser um ano perigoso. E o que vai preocupar a Europa ou África?

• Prioridades para líderes de segurança perante as ameaças de 2024: a antecipação de Mikko Hyppönen, tendências nos "services/software as a service" (SaaS), o aumento das fraudes híbridas online, e como o uso de tecnologias enganadoras ("deception technologies") deve crescer este ano e proliferar em 2025.

• Estratégias para as organizações não se enganarem no "teatro da segurança".

• Hacking à mente humana: as vulnerabilidades da engenharia social.

• Sete pecados mortais na sensibilização para a ciber-resiliência.

• Ransomware pela máquina de lavar roupa?

A LER

Breaking (Bad) Bots: Bot Abuse Analysis and Other Fraud Benchmarks

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

Guidelines on Implementing National Coordinated Vulnerability Disclosure Policies

Reforço da cooperação entre a CISA e ENISA

ENISA's new report on the Denial-of-Service (DoS)

ENISA's new report on cybersecurity investment

ICANN Publishes Paper on Defense Mechanisms Against Harmful Internet Content

Diretora | Inês Esteves

Edição | Pedro Fonseca

janeiro 2024