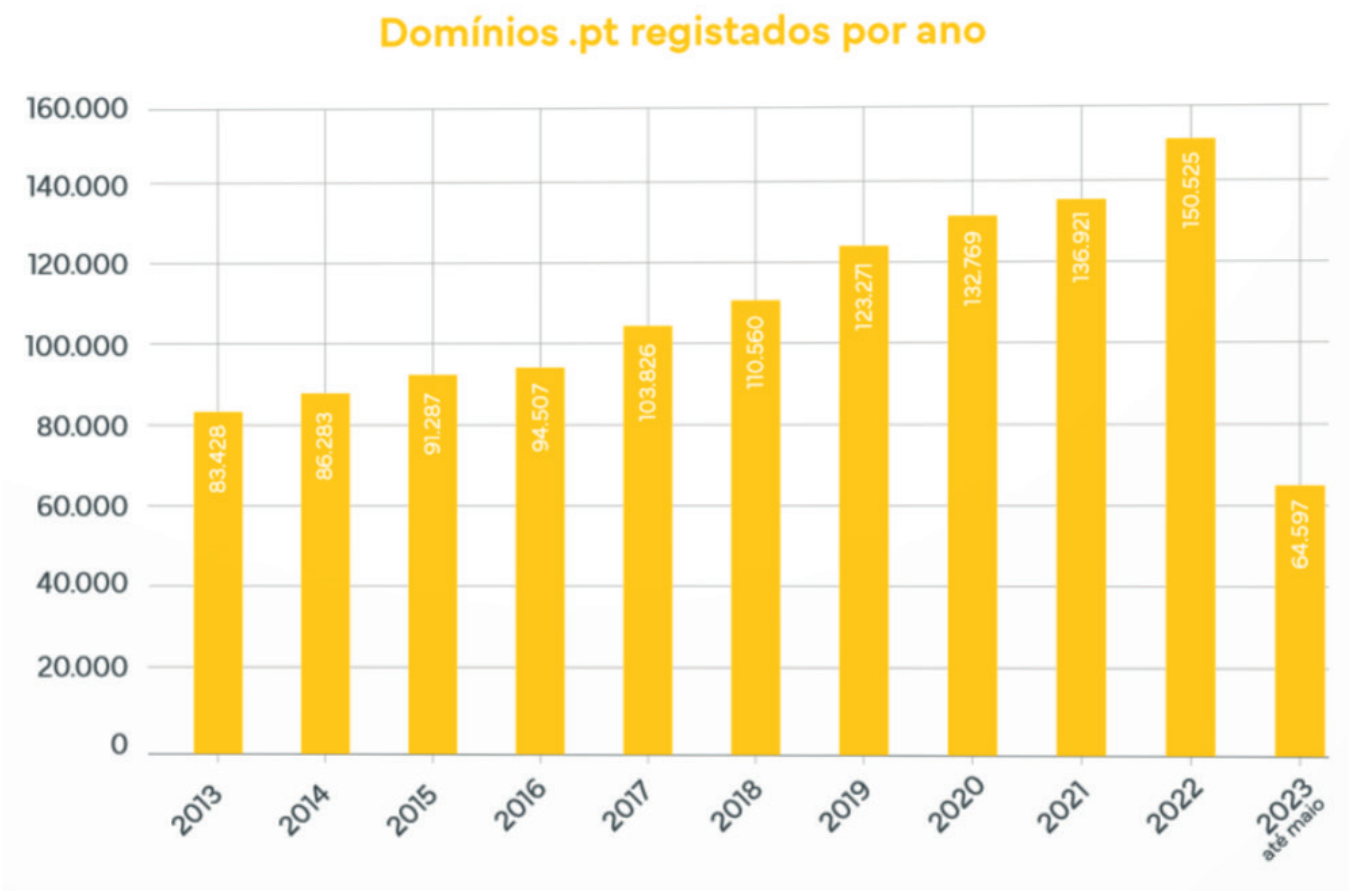
ptsoc digest

junho 2023

Diretora | Inês Esteves • Edição | Pedro Fonseca

.pt ptsoc Centro de Operações de Segurança

Associação DNS.PT comemora uma década como “casa da Internet portuguesa”



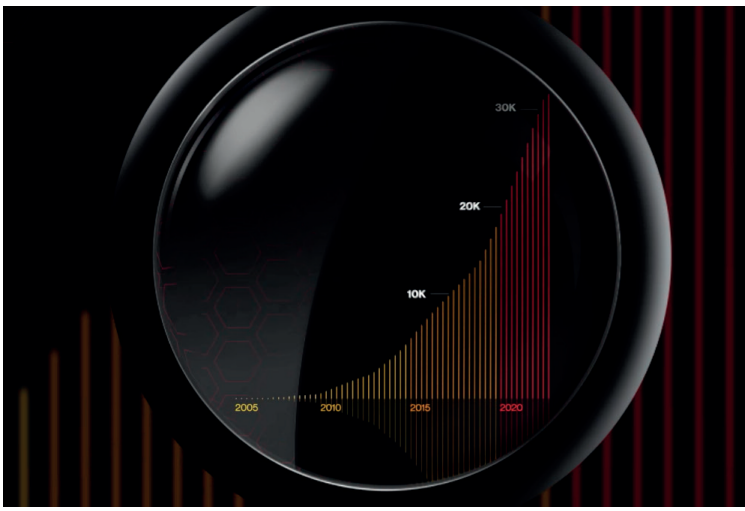
A Associação DNS.PT, onde se integra o PTSOC, comemorou a 1 de junho a sua primeira década de atividade. Numa rápida retrospetiva, ela permitiu criar “pontes entre os atores da Internet portuguesa e fora de Portugal, tivemos um olhar atento para as empresas, as organizações e as necessidades da economia, tivemos também um olhar humanista e de responsabilidade social, sem esquecer ações fundamentais ao nível da sustentabilidade e solidariedade, estivemos presentes em grandes momentos e eventos do país, e distinguimo-nos, em Portugal e na Europa, como uma verdadeira casa da Internet portuguesa”. As memórias marcantes destes 10 anos foram registadas num novo site na Web e em livro.

Fontes: .PT, 10anos.pt, livro

Cisco lança Cybersecurity Academy em setembro

Tendo como objetivo diminuir a escassez de recursos humanos em cibersegurança, a Cisco anunciou o lançamento a 12 de setembro próximo da Cybersecurity Academy em Lisboa, pretendendo captar os primeiros 18 formandos em universidades técnicas nacionais. O recrutamento, formação e posterior trabalho em regime híbrido é assegurado pela Warpcom.

Esquemas de engenharia social mais sofisticados



A engenharia social pode acompanhar o setor da segurança desde o início dos ciberataques, mas a sua sofisticação tem evoluído. O número de incidentes com recurso a esta estratégia mais do que duplicou no ano passado, revelou a Verizon. Metade dos casos registados utilizaram falsos pretextos num "cenário inventado que leva alguém a ceder informações ou a cometer um acto que pode resultar numa violação de dados".

A identificação destes esquemas nem sempre é fácil, mas alguns sinais podem agilizar a sua detecção, nomeadamente quando existe uma pressão para a urgência do assunto, erros ortográficos ou endereços errados, ligações para endereços falsos na Web, envio de ficheiros não solicitados por estranhos, ou compensações "demasiado boas para serem verdade".

Fontes: DBIR (Verizon), 20 Minutos

Ataques aos dados clínicos

O interesse nos dados pessoais de saúde tem vindo a gerar diversos problemas. Nos EUA, o hospital St. Margaret's Health anunciou o seu encerramento devido à falta de pessoal mas também por ter sofrido um ciberataque. A empresa de biotecnologia Enzo Biochem revelou que um ataque de ransomware expôs publicamente informação clínica de 2,5 milhões de pacientes, enquanto na Índia milhões de dados pessoais relacionados com vacinas foram divulgados ilegalmente. Entretanto, decorre até 19 de maio a Cybersecurity Healthcare Week.

Fontes: Security Affairs, TechCrunch, Wired, ENISA

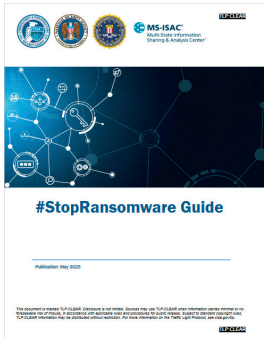
Novas publicações da ENISA

A ENISA publicou a "5G Security Controls Matrix" para apoio às autoridades europeias na segurança das redes 5G. O atual formato disponibilizado de folha de cálculo deverá ser substituído em breve por uma ferramenta Web.

A agência europeia para a cibersegurança lançou ainda o relatório "DNS Identity", relacionado com a autenticação, verificação e controlos de segurança da propriedade dos detentores de registos de domínio, assim como um " Good Practices for Supply Chain Cybersecurity".

Fonte: ENISA

Breves



• Um conjunto de agências governamentais dos EUA atualizou o "#StopRansomware Guide", adicionando mais recomendações, recursos e ferramentas ao guia editado originalmente em 2020.

• O artigo "Banks' cyber security - a second generation of regulatory approaches" defende que muitos países "introduziram ou melhoraram a regulamentação sobre cibersegurança bancária nos últimos anos", demonstrando na prática que "a cibersegurança é uma das principais prioridades das autoridades de supervisão bancária em todo o mundo".

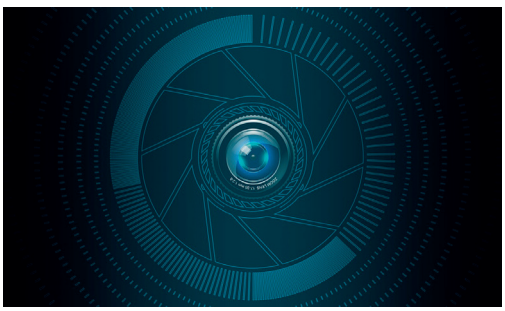
• Asylum Ambuscade: um grupo dividido entre o "crimeware" financeiro na Europa e EUA e a espionagem governamental também na Europa e Ásia Central.

• O mercado dos ciberseguros "está a estabilizar após anos de turbulência, em que subiram os preços e a oferta restringiu o mercado, tornando difícil para muitas empresas obter uma cobertura".

• A Comissão Europeia quer financiar propostas da administração pública, de empresas e de outras entidades para reforçar a cibersegurança e a resiliência contra ciberameaças na Europa.

• A ENISA revelou a constituição do Team Europe para competir no segundo International Cybersecurity Challenge, que integra o português Bruno Mendes como suplente.

• "Passkeys", o princípio do fim das passwords?



• A Microsoft apontou como origem das recentes falhas de conetividade na plataforma Azure um "aumento anormal de pedidos HTTP" na sequência de um ataque de "distributed denial of service" (DDoS).

• O governo do Reino Unido vai remover as videocâmaras de vigilância chinesas e divulgar uma lista de vendedores considerados como ameaça à segurança nacional.

• O regulador britânico das telecomunicações Ofcom revelou que informação confidencial sobre empresas que tutela e dados pessoais dos seus funcionários foram acedidos por hackers.

• O negócio do hacking por aluguer na Índia.

• Seis mitos sobre ciberataques.

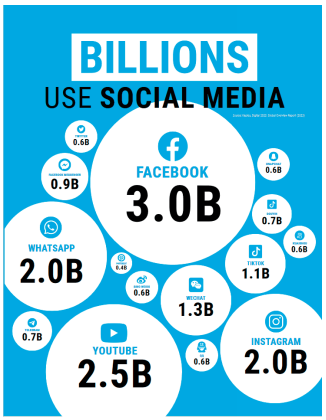
• O PowerDrop é um malware com foco na indústria aeroespacial dos EUA, enquanto falhas na cibersegurança dos fatos dos astronautas podem colocá-los em perigo.

• Algumas caixas de Android TV vendidas em plataformas como a Amazon podem conter malware.

• São necessários apenas três segundos da voz de uma pessoa para a clonar e a aproveitar, por exemplo, em esquemas para se fazer passar por um fornecedor de cuidados de saúde ou um mediador de seguros automóveis.

• A "crescente ameaça" dos "infostealers" agiliza o uso deste malware para "roubar informações sensíveis, como credenciais de login, detalhes financeiros e dados pessoais de computadores e redes comprometidas".

• Mais de 100 conceituadas marcas de vestuário, roupa e calçado foram envolvidas num esquema de phishing com mais de 6.000 sites maliciosos, que dura desde junho de 2022.



• As Nações Unidas publicaram um Código de Conduta para a Integridade da Informação nas Plataformas Digitais, onde se analisam princípios como a integridade da informação, transparência, capacitação dos utilizadores, reforço da investigação e do acesso aos dados ou uma maior confiança e segurança.

• Em "Defining the reporting threshold for a cybersecurity incident under the NIS Directive and the NIS 2 Directive", argumenta-se que os ciberincidentes com ou sem danos devem ser tratados de forma idêntica para se conseguir obter uma imagem completa dos cenários de ameaças e assim criar mais valor para a sociedade.

• Os CISOs precisam de estar mais bem preparados com métricas estratégicas para melhor alinharem a sua organização na defesa contra os cenários em constante mudança das ciberameaças.

• Como é que os criminosos executam os esquemas de "business email compromise" (BEC), também conhecido como "email account compromise (EAC), que têm vindo a aumentar no cibercrime relacionado com o correio eletrónico empresarial.

• Dois anos após o ataque à Colonial Pipeline, "os fornecedores de infraestruturas críticas não estão a fazer o suficiente para mitigar os ataques de forma proactiva".

• Um retrato da proteção do ciberespaço em Espanha.

Diretora | Inês Esteves

Edição | Pedro Fonseca

junho 2023