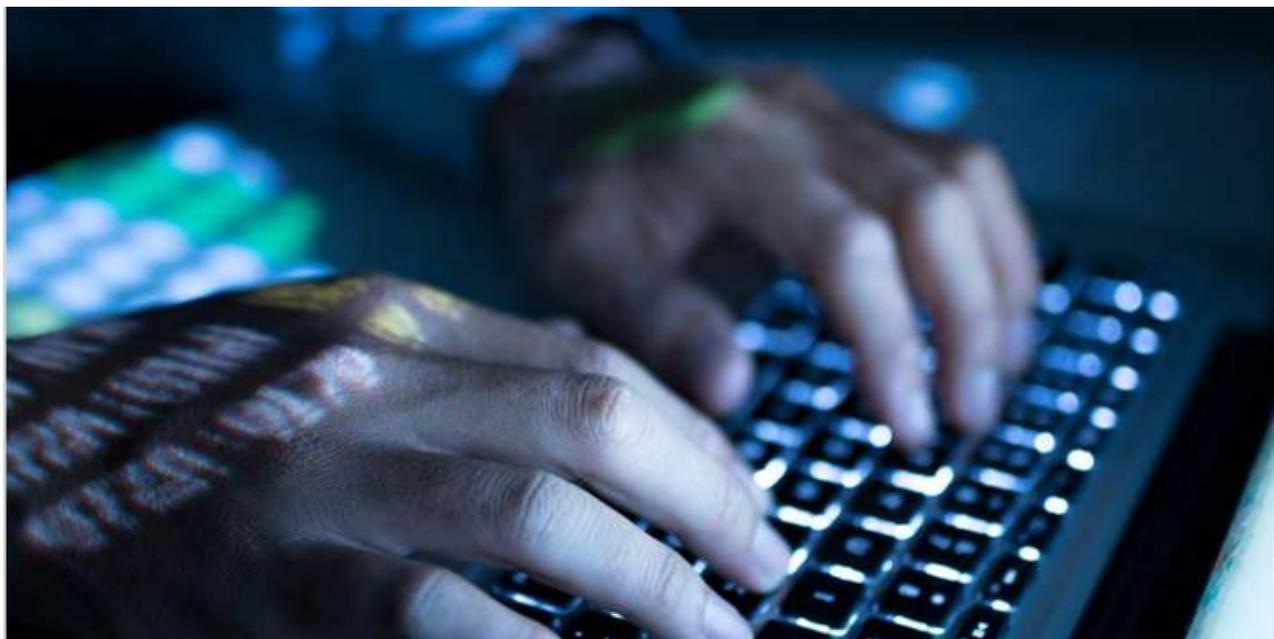


Visionware posiciona-se na linha da frente contra ciberataques a nível mundial

apdc.pt/noticias/atualidade-nacional/visionware-posiciona-se-na-linha-da-frente-contra-ciberataques-a-nivel-mundial

2023-02-08



Portugal está no top 10 dos países que mais sofreram ataques ransomware no primeiro mês de 2023, facto que não marca positivamente o início do ano na perspetiva da segurança de informação. O alerta é da VisionWare, de acordo com dados divulgados através do DarkFeed/DeepWeb Intelligence Feed, 2023 Top Targeted Countries, January 2023. Estes mostram que o país ficou em 7º lugar, numa altura em que se assinala um ano após o grave ciberataque infligido à Vodafone.

Para precaver os perigos desta tendência mundial em crescimento, e pelo facto de Portugal estar na mira dos cibercriminosos, a tecnológica portuguesa lançou no final do ano passado um centro pioneiro de operações e análise a ameaças cibernéticas à escala mundial, denominado VisionWare Threat Intelligence Center.

O objetivo deste centro é estudar, reportar e alertar as instituições públicas e privadas sobre os perigos da cibercriminalidade, desinformação, informação falsa e deepfake. O projeto, que surge em linha com a recentemente anunciada promulgação da Estratégia Nacional de Ciberdefesa, conta com especialistas das áreas de intelligence e cibersegurança, que procedem à monitorização, análise e report urgente, e em tempo real, para responder aos novos desafios e ciberameaças.

"O novo Centro de Inteligência da VisionWare desenvolve-se em consonância com o apelo do Governo para uma maior atenção da sociedade civil face ao perigo iminente das novas ameaças e riscos globais", refere Bruno Castro. Para o CEO da VisionWare os ataques

cibernéticos são "as novas armas usadas contra a segurança como um todo, para atacar infraestruturas críticas nas sociedades. A criação deste Centro permite agora agregar especialistas que, através de um modelo sólido de análise em tempo real, respondem às necessidades dos nossos clientes e parceiros, em Portugal, mas também pelo mundo".

De acordo com a empresa, os ciberataques de ransomware continuam em ascensão, transformando-se numa força disruptiva no setor de segurança cibernética, afetando todas as áreas de atividade. Devido ao incremento (e manutenção) do trabalho remoto, motivado e acelerado pela pandemia, estima-se que estes ataques tenham aumentado 148% em todo o Mundo. O ransomware constitui por isso, uma ameaça visível para milhares de organizações e empresas. Os protagonistas deste tipo de ciberataques sabem que o seu modelo de negócio, altamente destrutivo, terá garantia de sucesso contínuo, desde que consigam inovar as suas técnicas de exploração e formatos de dispersão dentro da organização.

Apesar dos esforços do governo português e da maior atenção e sensibilização da sociedade civil atual, os ciberataques continuam a ser uma grande preocupação no País. Os peritos em cibersegurança advertem que a ameaça representada pelos cibercriminosos está a crescer e que é necessário fazer mais para prevenir acontecimentos futuros. Como tal, Portugal precisa de continuar a reforçar as suas infraestruturas de cibersegurança e a desenvolver estratégias eficazes para proteger os seus cidadãos, empresas e infraestruturas contra o número crescente de ciberataques, oriundos de redes criminosas diversas, cada vez melhor organizadas e com uma maior capacidade disruptiva.

O VisionWare Threat Intelligence Center produz relatórios geopolíticos relacionados com as ameaças em estudo, aos quais acrescenta a monitorização de atores de risco e a partilha de notificações em tempo real quando os dados das instituições ficarem comprometidos. Mas, além destas soluções práticas, torna-se fundamental capacitar as autoridades de ferramentas (e conhecimento) para o constante controlo e monitorização da deepweb/darkweb (identificação de leaks), análise de riscos de cibersegurança das infraestruturas críticas, profiling de determinados indivíduos através de técnicas de humint, deteção e defesa de ciberataques e a supervisão contínua de determinados grupos cibercriminosos.