SETEMBRO 2020

B O L E T I M

# OBSERVATÓRIO DE CIBERSEGURANÇA

Nº4/2020

## NÚMEROS


é a tendência no nº de incidentes registados pelo CERT.PT se compararmos os primeiros 2 meses do 2º trimestre (abril e maio - 288, pico de incidentes no período de Covid-19), com os primeiros 2 meses do 3º trimestre (julho e agosto - 218, período habitual de férias).

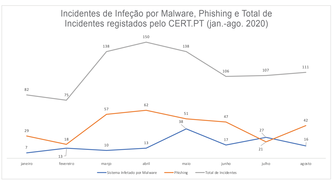

de incidentes referentes a sistema infetado por *malware* registados pelo CERT.PT se compararmos junho e julho - um aumento na importância relativa deste tipo de incidente. Em agosto os valores voltaram aos níveis de junho (ver gráfico).


dos tipos de observáveis registados pelo CERT.PT, em 2020, até ao final de agosto, são *malware* (cerca de dois milhões e meio de registos), em 2ª posição no *ranking*, depois das vulnerabilidades, com 90%. O *phishing*, neste âmbito, representa apenas 0,01% do total de observáveis, em 9ª posição.

(CERT.PT)

Observável (instância): "representa uma efetiva observação específica que ocorreu no domínio ciber. As propriedades detalhadas desta observação são específicas e não ambíguas." (fonte: STIX). Um observável é um evento que representa uma ameaça no ciberespaço de interesse nacional. Contudo, nem sempre é convertido em incidente registado devido à falta de relevância ou é agrupado com vários observáveis num único incidente.

## GRÁFICO




Durante o 2º trimestre, o *phishing* foi o tipo de incidente mais registado pelo CERT.PT. O 2º tipo de incidente mais registado durante esse período foi o sistema infetado por *malware*. Contudo, à medida que se aproximou o período de férias, o *phishing* diminuiu. Com a entrada no mês de julho, verificaram-se mais incidentes referentes a sistema infetado por *malware* do que a *phishing*. Em agosto, a tendência inverteu-se para uma situação semelhante a junho.

## PERFIL DA AMEAÇA


Em 2020, até agosto, o sistema infetado por *malware* representou 16% do total de incidentes, por tipo, registados pelo CERT.PT, o 2º mais frequente, depois do *phishing*, com 36%. Estes nºs são superiores aos do período homólogo de 2019, no qual 14% dos incidentes foram infeção por *malware* e 31% foram *phishing*. As posições no *ranking* de incidentes são as mesmas. Por vezes, o *phishing* é um veículo de disseminação do *malware*. Este último, porque é menos visível, pode atingir as vítimas de forma mais discreta e silenciosa, colocando os respetivos dispositivos infetados ao serviço de todo o tipo de atividades criminosas, tais como a mineração de criptomoedas, o furto de identidade, ou a participação em ataques distribuídos de negação de serviço.

O Eurobarómetro especial 499, de 2020, *Europeans' attitudes towards cyber security*, com dados relativos a 2019, mostra que, entre os portugueses utilizadores de Internet, 76% estão preocupados com a possibilidade de serem vítimas de *malware* (a média da UE é de 66%); mas apenas 11% identificam ter sido vítimas desta ameaça pelo menos uma vez nos últimos 3 anos (a média da UE é de 28%); e 65% destas vítimas conscientes reagiram com alguma ação em relação à ameaça (a média da UE é de 52%).

Verifica-se, portanto, que se trata de uma ameaça relevante e que existe preocupação, mas que isso não se reflete em níveis semelhantes na percentagem de pessoas que se identificam como vítimas, em Portugal, comparando com a média da UE, embora os portugueses tendam a reagir mais do que a média da UE quando se reconhecem como vítimas.

(CERT.PT e Eurobarómetro 499)

## NOTÍCIAS

A **ENISA**, no dia 10 de julho, publicou o *Trust Services Security Incidents 2019 Annual Analysis Report*, um relatório com os nºs dos incidentes reportados no âmbito dos serviços de confiança eletrónicos, em 2019, como assinaturas digitais, certificados digitais, selos temporais, etc., usados nas transações eletrónicas. O documento mostra que o nº de incidentes reportados em 2019 aumentou 78% - o que, segundo o relatório, se deve a um maior reporte pelas entidades e não tanto a um aumento efetivo no nº de incidentes.

A **Comissão Europeia**, a 22 de julho, publicou o texto *Cybersecurity: Our digital anchor, a European perspective 2020*, em que a cibersegurança é colocada no centro da estratégia digital europeia.

A **Comissão Europeia**, a 24 de julho, publicou o documento *Report on Member States' Progress in Implementing the EU Toolbox on 5G Cybersecurity*, providenciando uma visão sobre o estado da implementação da *toolbox* sobre o 5G e a cibersegurança na União Europeia.

A **Resolução do Conselho de Ministros nº 55/2020**, de 31 de julho de 2020, aprovou a *Estratégia para a Inovação e Modernização do Estado e da Administração Pública 2020-2023*, contemplando, entre outras medidas, o reforço dos níveis de cibersegurança dos organismos da Administração Pública, através do Quadro Nacional de Referência para a Cibersegurança.

A **APDSI**, a 31 de julho, apresentou o documento *Mapeamento das necessidades de competências na área das TICE visando o ajuste da oferta formativa*, no qual se identifica a cibersegurança como uma das áreas com mais procura e a exigir maior investimento em formação.

A **INTERPOL**, a 4 de agosto, divulgou o documento *Cibercrime: Covid-19 Impact*, no qual apresenta o impacto mundial da Covid-19 no cibercrime. O documento destaca algumas ameaças que usam este tema: *phishing* e esquemas fraudulentos; *malware* disruptivo (*ransomware* e DDoS) contra infraestruturas críticas; *malware* de recolha de dados; domínios maliciosos; e desinformação.

A **Comissão Europeia** abriu uma *call*, no âmbito do *CEF Telecom 2020, na componente de Cibersegurança*, com o prazo limite de 5 de novembro de 2020, para a apresentação de projetos que estimulem a cooperação europeia no aumento da resiliência em cibersegurança e reforcem a confiança nas redes e nos serviços do mercado único digital.