JULHO 2020

B O L E T I M

OBSERVATÓRIO DE CIBERSEGURANÇA

Nº3/2020

NÚMEROS

34%

é a tendência de crescimento no número de incidentes registados pelo CERT.PT no 2º trimestre, relativamente ao 1º trimestre deste ano, de 295 para 394. Face ao período homólogo do ano anterior, com um registo de 176 incidentes, verifica-se um crescimento de 124%.

160

é o nº de incidentes de *phishing* registados pelo CERT.PT durante o 2º trimestre. É o tipo de incidente mais frequente, seguido do sistema infetado por *malware* (68 incidentes) e do acesso não autorizado (41 incidentes).

37%

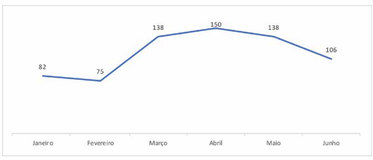
dos incidentes de *phishing* registados pelo CERT.PT no 2º trimestre de 2020 afetaram o setor bancário.

(CERT.PT)

Nota: a taxonomia de incidentes do CERT.PT sofreu alterações entre 2019 e 2020, nomeadamente passando a considerar as vulnerabilidades como incidentes. Essa mudança não afeta significativamente os resultados.

GRÁFICO

Número de incidentes registados pelo CERT.PT no 1º semestre de 2020



(CERT.PT)

Ao longo do 1º semestre de 2020, registou-se um aumento significativo no nº de incidentes entre os meses de fevereiro e abril, ocorrendo depois uma diminuição constante entre os meses de abril e junho. O aumento coincide com o momento de confinamento devido à pandemia de Covid-19. Comparando com o período homólogo de 2019, o 1º semestre de 2020 regista um aumento de 101% no nº de incidentes.

PERFIL DOS ATAQUES

Uma análise de conteúdo aos incidentes de *phishing* registados pelo CERT.PT durante o 2º trimestre de 2020 identificou as técnicas de persuasão mais utilizadas, os tipos de pedidos realizados, entre outros aspetos. Com base nessa análise, é possível chegar às seguintes conclusões:

- Embora o *phishing* tenha aumentado, 99% dos casos não referem a temática da pandemia diretamente;
- Considerando os 6 princípios de persuasão de Robert Cialdini (autoridade, escassez, reciprocidade, consistência, afinidade e prova social - ver aqui), aplicáveis na engenharia social, o mais utilizado é o que se sustenta na autoridade, isto é, na apresentação de uma imagem credível (90% dos casos), muito comum no *phishing* bancário. São ainda identificados conteúdos em que a escassez de uma oferta é apresentada como uma oportunidade (8%), frequente na venda de produtos e serviços. Por fim, verificam-se alguns casos em que se apela a uma reciprocidade, ou seja, à retribuição por um favor/benefício prestado (1%), situações em que se promove a interação social. Não se verifica a presença dos outros 3 princípios em qualquer dos incidentes de *phishing*;
- Os casos de *phishing* analisados solicitam ações específicas: 79% incentivam o *login* numa conta, 12% pedem dados relacionados a um produto/serviço, 7% prometem um ganho financeiro e 3% referem-se ao preenchimento de um documento;
- Outros aspetos: 3% são *spear phishing*, 94% pedem para clicar num URL e 90% são dirigidos a clientes, 7% a trabalhadores e 3% ao cidadão em geral.

NOTÍCIAS

Publicações sobre Cibersegurança e Covid-19:

A **ECHO**, a 8 abril, publicou o White Paper "The COVID-19 Hackers Mind-set", onde mostra que os agentes de ciberameaças, durante a pandemia, aproveitaram sobretudo o trabalho à distância e as fragilidades do fator humano como oportunidades para atacar as suas vítimas.

O **MINISTÉRIO PÚBLICO** divulgou, a 1 de junho, mais uma nota informativa "Covid-19: Cibercrime em Tempo de Pandemia", evidenciando como o 2º trimestre de 2020 registou um aumento elevado no nº de denúncias de cibercrime, principalmente em abril.

Outras publicações:

A **DGEEC** já divulgou os resultados relativos às câmaras municipais do seu inquérito IUTIC 2019, no qual se indica, por exemplo, que 19% das câmaras municipais têm formação e/ou consulta de informação obrigatórias em cibersegurança para os seus colaboradores.

A **Comissão Europeia**, no dia 11 de junho, publicou o "Digital Economy and Society Index 2020", no qual a componente de cibersegurança é considerada, através de uma panorâmica sobre os principais dados do Eurostat.

O **Relatório Anual de Segurança Interna** 2019 foi publicado no dia 30 de junho, mostrando um aumento de 42,7%, entre 2018 e 2019, nos casos de crimes informáticos participados às autoridades.