Observatório de Cibersegurança

CNCS Centro Nacional de Cibersegurança PORTUGAL

MAIO 2020

B O L E T I M

OBSERVATÓRIO DE CIBERSEGURANÇA

Nº2/2020

NÚMEROS

84%

tendência entre fevereiro e março de 2020 no número de incidentes registados pelo CERT.PT, de 75 para 138.

176%

tendência se compararmos março de 2019 com março de 2020 no número de incidentes registados pelo CERT.PT, de 50 para 138.

217%

tendência entre fevereiro e março de 2020 no número de incidentes de *phishing* registados pelo CERT.PT, de 18 para 57. Estas campanhas de *phishing* aproveitaram o confinamento para simular serviços digitais que têm um maior consumo e fidelização, como, por exemplo, serviços de *homebanking*, conteúdos digitais em *streaming* e lojas *online*.

(CERT.PT)

GRÁFICO

(Gráfico de Ministério Público, 2020)

As denúncias recebidas pelo Gabinete de Cibercrime do Ministério Público aumentaram de 20 em fevereiro para 46 em março de 2020. Em abril, até dia 16, a tendência de crescimento tornou-se exponencial, com 76 queixas até essa data (um incidente para o CERT.PT configura uma companha, independentemente do número de vítimas; cada denúncia no Ministério Público configura uma possível vítima).

AMEAÇAS

Desde que surgiram os primeiros casos de Covid-19 em Portugal e as medidas de confinamento, entre fevereiro e março, assistiu-se a um aumento de ciberataques que utilizam a engenharia social para tirar partido das fragilidades das vítimas. Os tipos de ataques mais relatados foram os seguintes:

- *Phishing* que utiliza o nome de organizações ligadas à saúde para capturar dados pessoais;
- *Malware* distribuído através de *emails* ou de redireccionamento de DNS;
- Aplicações com funcionalidades no âmbito da Covid-19, mas que distribuem *malware*, em alguns casos *ransomware*;
- Fraudes digitais que recolhem donativos através de *crowdfunding* para a falsa compra de materiais médicos;
- *Websites* falsos, ou ofertas fraudulentas, para venda de materiais médicos;
- Venda na *darkweb* de Kits Covid-19;
- Campanhas de desinformação que culpabilizam pela pandemia grupos minoritários e Estados;
- *Ransomware* a serviços essenciais.

NOTÍCIAS

Publicações sobre Cibersegurança e Covid-19:

A **EUROPOL**, a 3 abril, publicou o relatório "Catching the Virus Cybercrime: Disinformation and the COVID-19 Pandemic".

A **OCDE**, a 3 de abril, publicou o documento "Dealing with Digital Security Risk During the Coronavirus (COVID-19) Crisis".

O **MINISTÉRIO PÚBLICO** divulgou, a 17 de abril, o documento "Covid-19: Cibercrime em Tempo de Pandemia", com dados sobre as denúncias feitas ao Gabinete de Cibercrime durante o início da pandemia.

A plataforma **MEDIA LAB**, do ISCTE-IUL, partilha dados sob o título "Covid na Rede: Pesquisas, Redes Sociais e 'Fakes'", onde é possível identificar casos de desinformação relativos à Covid-19 em Portugal.

Outras publicações:

A **ENISA**, a 26 de março, publicou o relatório "Cybersecurity Skills Development in the EU", sobre o sistema de educação em cibersegurança e a dificuldade que este tem em atrair mais estudantes.

A **APAV** divulgou, a 23 de abril, as conclusões do Barómetro APAV/Intercampus sobre a "Perceção da População sobre Cibersegurança".