FOLHA INFORMATIVA

# CRIMES CIBERDEPENDENTES

## O QUE É?

O crime ciberdependente pode ser definido como qualquer crime que só pode ser cometido por meio de computadores, redes de computadores ou outras tecnologias de informação e comunicação (TIC). Estes crimes são normalmente direcionados a computadores, redes ou outros recursos de TIC e sem a Internet não poderiam ser cometidos.

Desta forma, os crimes ciberdependentes referem-se, essencialmente, aos crimes previstos na Lei do Cibercrime[1] (Lei n.º 109/2009).

De entre os tipos de ataques associados a esta criminalidade, destacamos:

- O *ransomware* - tipo de *software* malicioso (*malware*) desenhado para negar o acesso a um sistema ou dados de computador, sendo geralmente disseminado por *e-mails* de *phishing* ou ao visitar um *website* infetado;
- O *hacking* – acesso não autorizado a sistemas informáticos com intenção criminosa;
- O furto de informação pessoal online - prende-se sobretudo com a obtenção ilegal de informação financeira, como credenciais de cartão de crédito, dados bancários ou carteiras de cripto-moedas, o que permitirá a sua posterior venda ou utilização para furto do património das vítimas;
- Os ataques distribuídos de negação de serviço (DDoS) - visam degradar e inviabilizar serviços *online*, como *websites*, *e-mail* e serviços DNS (*Domain Name System*).

## QUEM É A VÍTIMA?

Qualquer pessoa (singular ou coletiva) pode ser alvo deste tipo de crimes.

Neste tipo de criminalidade, a origem dos ataques pode ser diversa, desde a abertura de um ficheiro executável que descarrega um vírus para um computador ou outro dispositivo, até à utilização de um suporte de armazenamento de ficheiros (e.g., pen USB) infetado que, de forma oculta, se auto executa num determinado dispositivo da vítima.

Existem, porém, estratégias e comportamentos que aumentam a proteção contra este tipo de ataques, tais como:

- Ativação de filtros de *spam*, para impedir a entrada de *e-mails* de *phishing* nas caixas de correio eletrónico;
- Utilização de mecanismos de autenticação de *e-mail* com *Sender Policy Framework* (SPF), relatórios e conformidade de autenticação de mensagens de domínio (DMARC) e *Domain Keys Identified Mail* (DKIM), para impedir a falsificação de *e-mails*;
- Utilização de mecanismos de análise de ficheiros executáveis de *e-mails* enviados ou recebidos, prevenindo que os/as utilizadores/as os recebam;
- Configuração da *firewall* de forma a bloquear o acesso a IPs (*Internet Protocol address*) que são reconhecidos como uma ameaça;
- Configuração de antivírus e programas de *anti-malware* nos computadores, incluindo configuração para a realização de análises regulares;
- Realização de cópias de segurança de informação e/ou documentação em dispositivos móveis (e.g., disco rígido externo) ou na *cloud*;
- No que diz respeito a empresas, deverá ser aplicado o "Princípio dos Privilégios Mínimos": a nenhum utilizador/a deve ser atribuído acesso administrativo superior, apenas ao estritamente necessário para o exercício da sua atividade;
- Ainda em contexto organizacional, é importante a sensibilização e (in)formação de funcionários/as relativamente aos tipos de ataques a que podem ser sujeitos e aos riscos associados.

## QUAL O IMPACTO?

Como referido, o crime ciberdependente pode afetar pessoas singulares e pessoas coletivas.

Quando as vítimas deste tipo de crime são pessoas singulares, embora os efeitos ao **nível psicológico** possam ser diversificados, de acordo com diferentes fatores, entre os quais as características da vítima, alguns sintomas mais comuns são: medo, ansiedade, raiva ou mesmo desconfiança constante e prolongada, que muitas vítimas descrevem como "paranoia".

O **impacto emocional** dos crimes ciberdependentes é descrito como sendo semelhante às reações das vítimas de crimes violentos. Muitas vítimas sentem a sua privacidade violada, sentem-se desamparadas, impotentes e receosas de uma nova vitimação. As vítimas podem ainda desenvolver sentimentos de culpa e/ou vergonha por terem sido ludibriadas. Estas vítimas têm ainda de lidar com a desilusão de, na generalidade dos casos, não ser possível identificar o/a autor/a do crime.

[1] A Lei do Cibercrime pode ser consultada em https://apav.pt/apav_v3/images/pdf/L_Cibercrime.pdf.

A **perda patrimonial** pode também ser consequência de crimes ciberdependentes em pessoas singulares. Veja-se, a título de exemplo, os casos em que uma pessoa, no âmbito de um ataque de *phishing*, é redirecionada para uma página falsa idêntica à da sua entidade bancária, na qual introduz os seus dados bancários, o que permite a sua obtenção ilícita por terceiros. Para além da perda patrimonial, o impacto do crime na estabilidade financeira da vítima contribui negativamente para a sua insegurança e mal-estar emocional.

Este tipo de criminalidade implica ainda, para a vítima, um sério aborrecimento e muito tempo perdido para procurar reparar as suas consequências.

No caso das **empresas/organizações**, o **impacto económico** desta criminalidade pode ser o mais significativo, pois este tipo de ataques pode resultar em disrupções graves no funcionamento habitual, bem como em danos reputacionais junto da opinião pública e consequentes perdas económicas.

## QUE APOIO ESTÁ DISPONÍVEL?

Ser vítima deste tipo de ataques pode desencadear uma série de reações físicas e comportamentais, como as acima descritas. Pode despoletar uma combinação de emoções e pensamentos com os quais é, por vezes, difícil lidar. Mesmo que estas emoções sejam reações completamente normais, a vítima pode sentir que está a perder o controlo. É importante lembrar que, na maioria das situações, com o tempo, irá gradualmente voltar a adquirir um sentimento de controlo sobre a sua vida.

O acesso a serviços de apoio à vítima pode revelar-se essencial para ultrapassar ou, pelo menos, minimizar o impacto do crime. Muitas vezes, é difícil e perturbador falar sobre o crime, mas pode ser positivo para a vítima partilhar com um/a profissional a experiência de vitimação, incluindo os pensamentos e sentimentos precipitados pela situação vivida e seus efeitos. Para além disso, os/as profissionais (Técnicos/as de Apoio à Vítima) podem auxiliar a vítima a lidar com as diferentes **necessidades – jurídicas, psicológicas, sociais, práticas, etc**. - resultantes do crime sofrido.

A criminalidade informática é, em regra, muito complexa, pelo que as vítimas necessitam de apoio individualizado e qualificado para as auxiliar a recuperar dos efeitos do crime. Será, designadamente, necessária ajuda para operar meios informáticos, tarefa que as vítimas poderão não dominar. Adicionalmente, as vítimas de crime ciberdependente encontram-se numa posição de particular fragilidade e desproteção, tendo em conta que este tipo de ataques, pelo seu carácter recente, ainda é pouco valorizado e compreendido pela população em geral e que escasseiam os recursos e serviços preparados para lidar com os seus efeitos.

Por tudo isto, é importante que a vítima de crime informático receba o **apoio adequado para mitigar os danos causados pelo ataque**, incluindo nos casos em que os alvos do crime são entidades coletivas, como empresas ou organizações.

Através da APAV, é possível ser prestado apoio prático e reencaminhamento destas situações para entidades que saberão implementar o apoio técnico necessário à resolução do ataque, como também encaminhar a situação para a autoridade competente para a investigação.

Para além disso, a vítima tem direito a beneficiar de serviços de apoio, antes, durante e após o processo-crime, podendo também recorrer a estes serviços ainda que não tenha denunciado o crime. A APAV disponibiliza, de forma gratuita, confidencial, qualificada e humanizada, apoio emocional, acompanhamento psicológico, informação jurídica, encaminhamento social e auxílio em questões práticas a todas as pessoas que foram ou são vítimas de crime.

Poderá contactar a APAV:

- Pela Linha Internet Segura - 800 21 90 90 | chamada gratuita | dias úteis das 09h às 21h | linhainternetsegura@apav.pt;
- Pela Linha de Apoio à Vítima - 116 006 | chamada gratuita | dias úteis das 09h às 21h;
- Através de qualquer Gabinete de Apoio à Vítima da APAV (contactos em https://apav.pt/apav_v3/index.php/pt/contactos).

**RECURSOS APAV**

https://apav.pt/cibercrime/
https://www.internetsegura.pt/
http://infovitimas.pt