Proteção de Dados Pessoais, Cibersegurança e Privacidade

“Perspetivas do combate ao crime informático”

Encontros com a Justiça na Comarca de Leiria – 26 de junho 2021

Cibercrime – competências PJ (LOIC)

Artigo 7.º

Competência da Polícia Judiciária em matéria de investigação criminal

1 - É da competência da Polícia Judiciária a investigação dos crimes previstos nos números seguintes e dos crimes cuja investigação lhe seja cometida pela autoridade judiciária competente para a direção do processo, nos termos do artigo 8.º

...

3 - É ainda da competência reservada da Polícia Judiciária a investigação dos seguintes crimes, sem prejuízo do disposto no artigo seguinte:

...

l) Informáticos e praticados com recurso a tecnologia informática;

Cibercrime – definição e categorias

Qualquer crime cometido por meio de redes de comunicações eletrónicas e sistemas de informações ou contra tais redes e sistemas.

- Como meio para o cometimento de formas tradicionais de criminalidade (fraude, falsificação)
- Como meio de divulgação de conteúdos ilícitos (pornografia infantil)
- Crimes informáticos propriamente ditos da (Lei 109/2009, de 15.09)
- Relativos à proteção de dados pessoais ou privacidade (Lei 67/98, de 26.10)

A Unidade Nacional de Combate ao Cibercrime e à Criminalidade Tecnológica - UNC3T

Unidade operacional especializada que dá resposta preventiva e repressiva ao fenómeno do cibercrime.

Organizada em secções:

- da Cibercriminalidade Contra as Pessoas
- De Investigação dos Meios de Pagamento Eletrónicos
- De Investigação Digital

Extensões (secções e brigadas) nas Unidades Territoriais

Competências de investigação da PJ

Hacking, ciberatacks

- Intrusão em sistemas
- Botnets, Malware, Ransomware
- Banca online (phishing)
- Furto de identidade (Identity thief)
- Extorsão
- Exfiltração de dados (privada, concorrência desleal, segredo comercial)
- “CEO fraud”

Competências de investigação da PJ

Meios de pagamento eletrónicos

- Contrafação e clonagem de cartões
- Cartão não presente – *e-commerce*
- Cartões pré-pagos
- Mercados virtuais
- Cripto moedas (bitcoin)

Competências de investigação da PJ

Abuso sexual de crianças online

- Pedofilia/pornografia de menores
- “Sextortion”
- Repositórios de imagens
- Deslocalização do crime (anonimização, Tor, P2P)
- Cooperação internacional

Cooperação internacional

"Cyber attacks"

Recolha e análise de informação que permita estabelecer prioridades em termos de ameaças e alvos principais

"Child sexual exploitation online"

Reduzir a vulnerabilidade de menores à vitimização pela exploração sexual online

"Payment card fraud"

Aumento da segurança de pagamentos que não são efetuados em numerário.

Cooperação internacional

- “EMAS – EUROPOL MALWARE ANALYSIS SYSTEM” Plataforma de análise que faz exames forenses
  - Deteção e análise automática de malware enviado pelos EM
  - Submissão a exame forense em ambiente e sistema protegido
  - Eliminação de efeitos adversos noutros sistemas
  - Facilidade de cruzamento de informação
- “No More Ransom” - European Cybercrime Centre (Europol) - Ajuda as vítimas de ransomware a recuperar os dados encriptados
- Plataforma do EC3 – European Cybercrime Centre (Europol) - coordena operações policiais contra o cibercrime e é um centro de assistência técnica e de excelência
- ECTEG- European Cybercrime Training and Education Group
- ICSE - International Child Sexual Exploitation – Interpol – Base de dados de imagens e vídeos

Cibercrime - características

- Deslocalização de práticas criminosas para a internet (crimes contra a honra)
- Deslocalização de conteúdos de um servidor para outro (ocultação de provas, questões relativas à aplicação da lei)
- Não tem restrições geográficas ou de tempo
- Possibilidade de dano sobre número elevado de pessoas e num curto espaço de tempo

Cibercrime - características

- Rastreabilidade dificultada
- Encriptação, fácil destruição
- Anonimização / Falsa identidade
- Utilização de recursos alheios (botnets)
- Prova essencialmente técnica / Não existe prova testemunhal
- Maior lucro e menor risco
- Menores penas e menor probabilidade de condenação

Cibercrime – perfil do autor

- Um génio na área da informática
- Perito em computadores e programação
- Estudante com um Q.I. acima da média
- introvertido, associal
- Age pelo desafio de superação da máquina

(Sendo, por vezes, aceite e não censurado pela sociedade)

Cibercrime – perfil do autor

Verifica-se contudo que…

- Podem não ser tão jovens
- Nem tão inteligentes
- Desprovidas de qualquer sentido ético
- Com o objetivo de extrair informação e usá-la ou vende-la.

Cibercrime – motivações do autor

Mais do que a personalidade do autor é o móbil que o carateriza

- Criminalidade associada ao lucro
- Crime organizado
- Grupos extremistas com motivações políticas, religiosas e ideológicas
- Espionagem industrial e sabotagem
- Espionagem internacional, Guerra de informação
- Terrorismo

Cibercrime – vítimas

- Vítima – alvo (direcionada a determinada pessoa)
- Particulares – cartões bancários; *phishing*; *smishing*; burla em relacionamentos amorosos; MBWAY; *money mules;* empréstimos pessoais…
- Empresas – *man in the middle*; *ransomware*
- Burla online (Comércio eletrónico e bancário)
- Outros (cifras negras – motivadas pelo desconhecimento ou ignorância de que foi vítima, crença da ineficácia da investigação e na impunidade destes crimes, questões de reputação e confiança junto do mercado e clientes, responsabilidade legal, devido ao dever de proteção de dados confidenciais)

Cibercrime – prova digital

Prova de natureza instável e fungível quando comparada á prova tradicional

Admissível - Observância da lei

Autêntica - Foi gerada e registada na cena ou lugar de um crime e não sofreu qualquer alteração

Precisa – De fonte credível com a possibilidade de a mesma ser verificada

Completa - Correlacionada entre os diversos registos e dados informáticos armazenados, sem que se perca a integridade, sincronização e significado

Cibercrime - prova digital

- Acesso aos dados em tempo útil
- Remoção de conteúdos e Bloqueio de acesso ((Inexistência de regime legal; Impossibilidade de atuação em tempo)
- Encriptação (Ocultação e Impossibilidade de leitura, Uso de algoritmos próprios)
- Anonimização (Redes (“Tor” , “deepweb”); Mercados virtuais (Silk Road); Moedas virtuais (bitcoin)

Cibercrime - investigação

- Cooperação (lentidão da cooperação e falta de partilha de informações tanto entre entidades nacionais diferentes como ao nível internacional)
- Procedimentos de investigação - coordenação (metodologia no tratamento da especificidade deste crime)
- Ferramentas tecnológicas de analise de informação
- Rede de especialistas
- Sistemas legais compatíveis (ratificação da Convenção sobre o Cibercrime pelo maior número de países)
- Métodos avançados de recolha de prova (A prova digital – recolhida em tempo útil, atendendo à sua temporalidade volatilidade, de modo a evitar a sua destruição)

Cibercrime - investigação

- Elevado número de processos e de dados a rastrear (morosidade; encargos económicos e de gestão insustentáveis)
- Ações encobertas
- Interceções “online”
- “Remote Forensics”
- Especialização e resposta técnica
- Análise de motivações

Cibercrime - investigação

- “Conflitos” entre a LC e a Lei 32/2008, de 17.07
- Dar resposta a todos os crimes informáticos independentemente da quantia do prejuízo verificado
- Critérios de atualidade e oportunidade da investigação.
- Combater o sentimento de impunidade em relação a estes crimes que contribui para o aumento das cifras negras

Cibercrime - tendências

- Aumento de anonimização na navegação e cifragem de dados;
- Insuficiência dos Estados na resposta pronta;
- Crescente sofisticação
  - Diferentes “divices” (notebook, pc,smartphone, tablet)
  - Diferentes sistemas operativos (Win, android, Ios, linux, blackberry,)
  - Tecnologias de acesso (2/3/4G/5G)
- Data *storage* e sua localização
- Engenharia social
- Aumento acentuado de ameaças a dispositivos móveis
- Kits de ataque

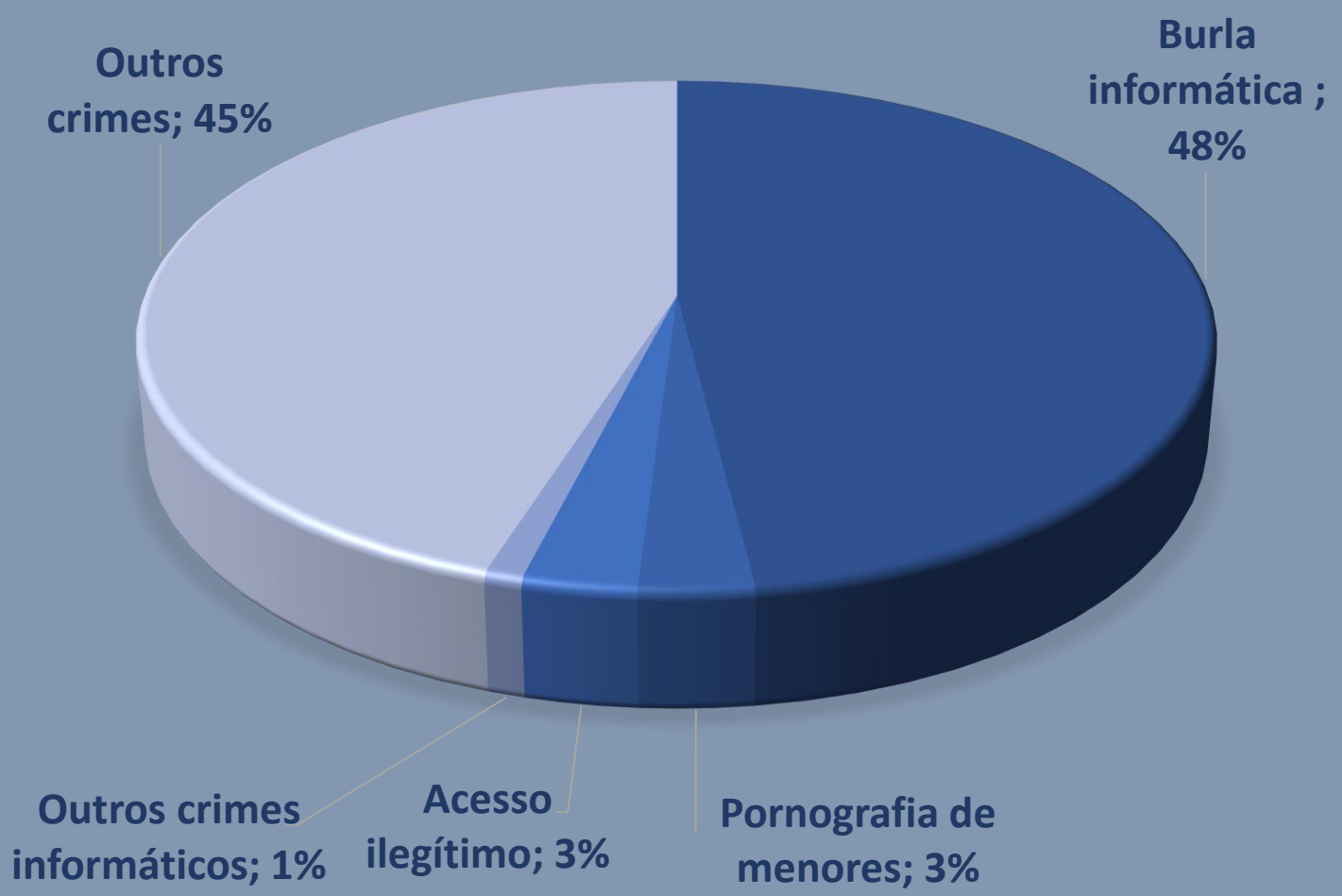
Cibercrime - tendências

- Aumento de APT (Advanced Persistent Threat – ameaças de natureza política e/ou económica)
- Interligação de *botnets* e *malware* bancário
- Branqueamento com recurso a moedas, contas bancárias e cartões virtuais
- Ataques dirigidos com exfiltração de informação sensível/dados pessoais
- Exposição a campanhas de extorsão com base em programas maliciosos - “ransomware”, “sextortion”
- Hacktivismo (uso de ferramentas ou meios digitais para reivindicação política ou social)

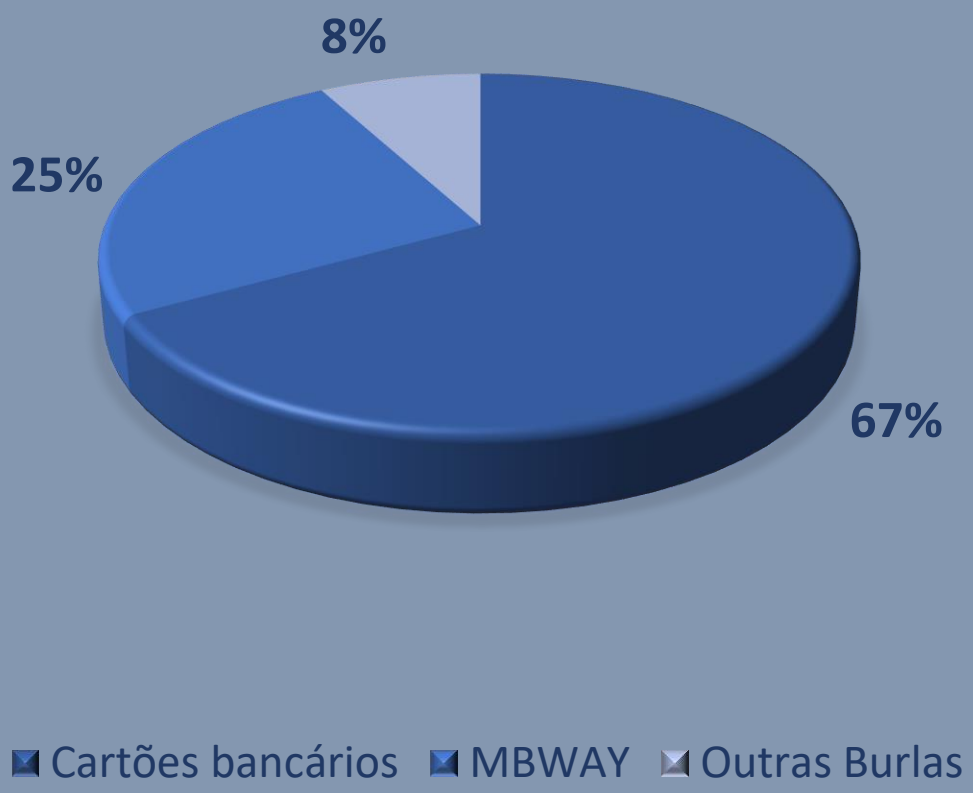
Cibercrime - prevenção

- Aumentar a literacia informática
- Educação no meio escolar
- Junto da sociedade em geral
- Junto das empresas (aposta no desenvolvimento na área da segurança e em medidas de proteção)

Cibercrime – dados 2020 - DIC

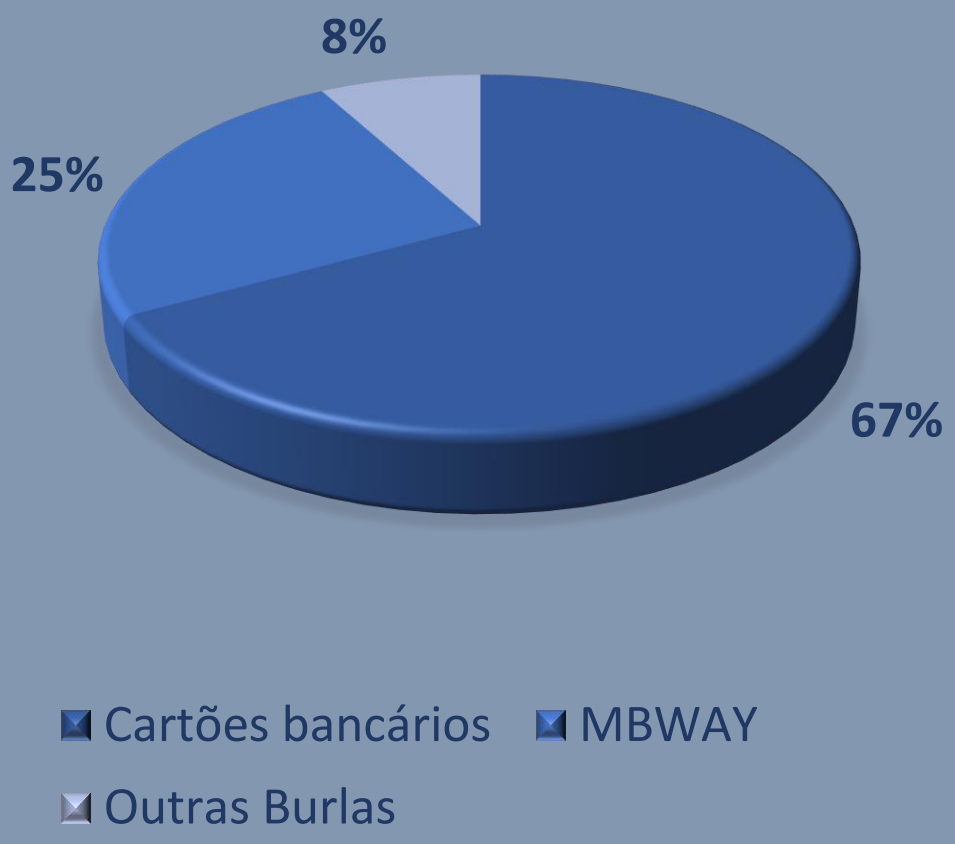


Cibercrime – burla informática 2020 - DIC



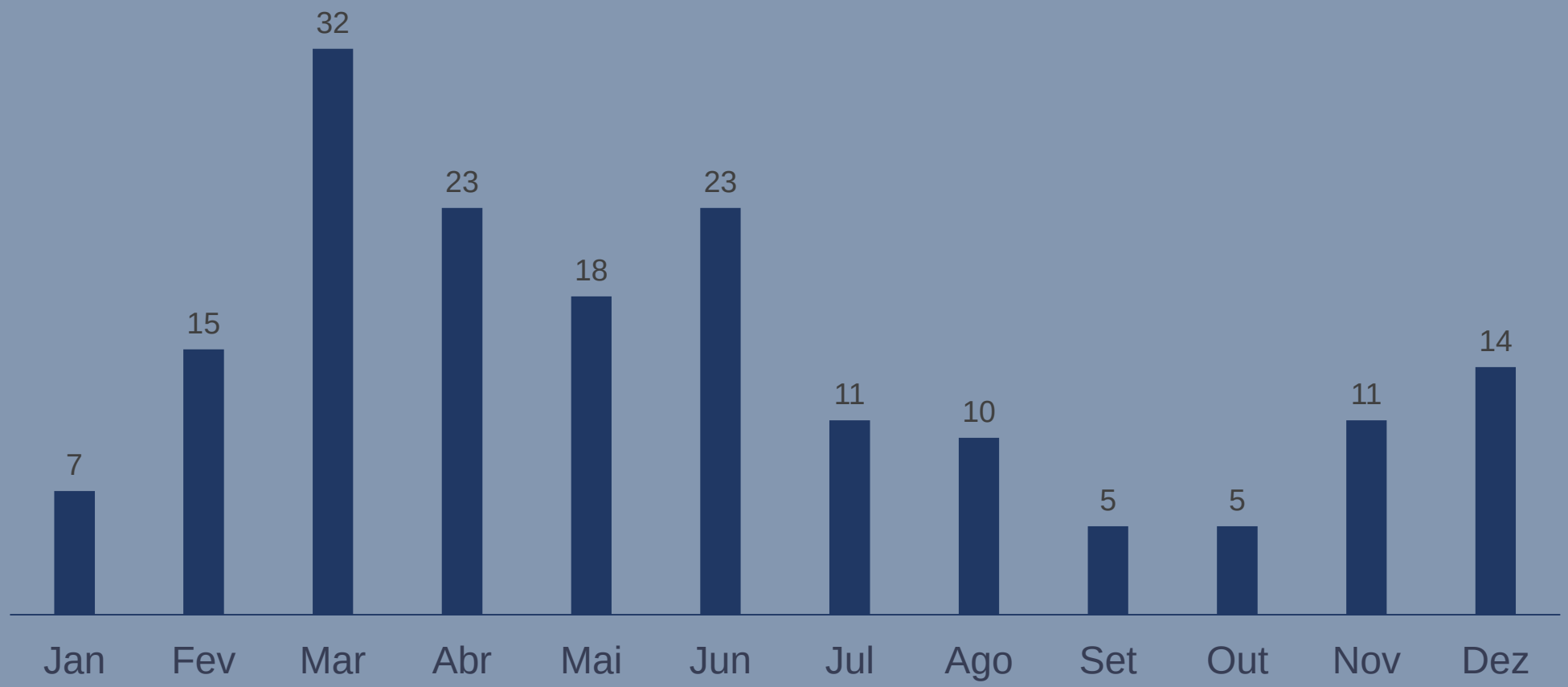
- 67% do crime de burla informática são relativos a fraudes com cartões de crédito / débito
- A recolha dos códigos são efetuados com recurso ao “phishing” e, por vezes, à “engenharia social”
- A maioria dos casos reportam a compras efetuadas na Internet e no estrangeiro.

Cibercrime – MBWAY 2020 - DIC



- 25% do crime de burla informática são cometidos através da aplicação MBWAY
- A recolha dos códigos são efetuados com recurso ao “phishing” e à “engenharia social”
- “Money Mules”
- Leiria é uma zona de vítimas não de autores

Cibercrime – dados 2020 - DIC



Cibercrime – 2020 - DIC

Pornografia de menores – são sobretudo investigações iniciadas no âmbito das comunicações do NCMEC (National Center for Missing and Exploited Children)

Acesso ilegítimo – acessos a contas de correio eletrónico ficando em poder de informação que servirá para o cometimento de outros crimes.

Outros crimes informáticos – Falsidade informática, Difamação, Sabotagem informática, Extorsão (sextortion), Devassa da vida privada, Interceção ilegítima…

Contatos

Fernando Jordão
Coordenador de Investigação Criminal

Departamento de Investigação Criminal de Leiria-Polícia Judiciária
Quinta dos Maristas – Pousos
2401-916 Leiria
Telefone: 244 845 200
E-mail: dic.leiria@pj.pt