****

|  |  |
| --- | --- |
| [www.coe.int/cybercrime](http://www.coe.int/cybercrime) | Divisão de Proteção de Dados e Cibercrime Direção-Geral de Direitos Humanos e Estado de Direito Estrasburgo, França  Versão de março de 2018 |

**Formação avançada sobre cibercrime e prova eletrónica para juízes e procuradores**

**2018**

*Introdução ao estudo de caso e*

*Guia de formadores*



**Conteúdo**

**1. Introdução ..……………………………………………………..…………………………………………………. 3**

**2. Investigação ………………………………………………………………………………………………….……. 4**

**2.1 Estabelecimento dos factos iniciais**

**2.2 Estabelecimento de dúvida razoável sobre o possível início do crime**

**3. Configuração financeira .…………………………………….………………………………………………… 5**

**4.** **Início do crime efetivo e ponto-chave da investigação ……..…………………….……………….. 6**

**5.** **Fim do crime e início do processo ………………………….………….....................………………… 8**

**6.** **Principais etapas da investigação e principais provas eletrónicas …………………..…..…… 10**

**7. Anexo .………………………………………………….….…….....……………………………………………… 11**

**1. Introdução**

O cenário deste estudo de caso refere-se a esquemas recentes de comprometimento de e-mails empresariais ou "BEC" (do inglês, Business E-Mail Compromise), que derivam de fraudes como "fraude de CEO" ou "ataques indiretos/por intermediários" (*man-in-the-middle*) anteriormente detetadas. O objetivo e a dimensão destas fraudes são surpreendentes.

Os danos substanciais infligidos às vítimas aumentam cada vez mais, embora as autoridades governamentais e o setor privado de um grande número de países em todo o mundo estejam constantemente a tentar aumentar a consciencialização entre as comunidades públicas e privadas. Infelizmente, as informações mais recentes sobre os danos financeiros agregados causados a nível global não permitem concluir que houve qualquer progresso nesta área.

*Nota aos formadores:* **O cenário começa com o estabelecimento do Federal Bank of Atlantis (FBA), banco internacional bem conhecido, bem estabelecido e respeitado. Uma descrição como esta deve levar os formandos a concluir que este tipo de banco não deve estar envolvido em qualquer tipo de problema, muito menos aqueles semelhantes aos que serão descritos mais à frente neste documento.**

Por outro lado, são exatamente estes bancos que são agora alvo regular de esquemas como este, possivelmente devido à sua relutância em ajustar os procedimentos de segurança empresarial para enfrentar os novos desafios que se impõem ou por causa de uma falsa sensação de segurança, importância e presença global.

**No final do curso, os formandos deverão ter noção que até bancos ou instituições financeiras como estas podem ser alvo e vítima de fraudes.** Além disso, neste caso, a investigação em desenvolvimento irá revelar que o caso de BEC é cometido com a influência adicional de uma ameaça persistente avançada (Advanced Persistent Threat - APT) e de engenharia social reversa, combinada com a utilização de criptomoedas.

*Nota aos formadores*: **a ideia por detrás deste exercício é reforçar a abordagem jurídica investigativa que deve levar os formandos a um processo, passo a passo, de utilização das ferramentas legais que têm à sua disposição, para realizar uma investigação quase real e organizar um processo criminal.** Este exercício é uma combinação de artigos da Convenção de Budapeste e de disposições legais nacionais que lhes permitirão resolver com sucesso o caso desde a fase de investigação, passando pelo processo de acusação e terminando no julgamento e na condenação final. Isto inclui também alguns passos importantes que podem e devem ser tomados no processo de MLA em conformidade com a Convenção.

Para este curso foram criados países fictícios. São eles Atlantis, Norland, Ostland, Westland e outros**. Para a preparação do exercício, todos eles ratificaram a Convenção do Conselho Europeu sobre Cibercrime ("Convenção de Budapeste").** Esta abordagem deverá permitir a transferência do curso e do material de formação entre jurisdições, sem a necessidade de alterações significativas aos materiais do curso ao longo do tempo.

*Nota aos formadores:* **No final desta sessão, os formandos deverão ser capazes de:**

* **Identificar as pessoas singulares e coletivas envolvidas no cenário;**
* **Explicar o *layout* do caso e a situação dos factos introdutórios;**
* **Seguir e explicar o fluxo e o desenvolvimento da investigação do caso;**
* **Determinar como e onde é que a investigação criminal deve começar e que vetores processuais devem ser seguidos.**

**2. Investigação**

**2.1 Estabelecimento dos factos iniciais**

"*O Federal Bank of Atlantis (FBA) é um banco conhecido, bem-sucedido e fiável sedeado na Europa. Tem várias filiais e unidades localizadas em diferentes países, não só na Europa, como também no resto do mundo. As suas atividades bancárias e comerciais são conhecidas pela sua reputação conceituada e fiabilidade. Parece que, devido às suas políticas, o banco está a atrair mais clientes do que a concorrência, estando estes a abrir novas contas bancárias e a utilizar outros produtos bancários.*

*O Conselho de Administração do FBA decidiu emitir um bónus especial de aniversário para marcar os seus 100 anos de existência e operações de sucesso. O Conselho de Administração encarregou o Departamento de Logística e Operações (Department for Logistics and Operations, DLO) de preparar tudo o que fosse necessário para a impressão de bónus, incluindo encontrar um parceiro adequado para fornecer todos os elementos de impressão necessários.*

*O DLO identificou um parceiro muito conhecido nesta área, do fornecimento de produtos e serviços de impressão. O parceiro selecionado, a United Bank Printing (UBP) está sediado em Atlantis, tendo uma filial europeia sedeada em Nordland. O DLO também comunicou internamente com o Departamento Financeiro do FBA".*

**Os principais factos são**:

* O Federal Bank of Atlantis (FBA) é um banco conhecido, bem-sucedido e fiável;
* O FBA quer emitir um bónus especial de aniversário;
* O Departamento de Logística e Operações (DLO) está encarregado da logística deste caso;
* A United Bank Printing (UBP) é um fornecedor de material de impressão;
* Inclusão do Departamento Financeiro do FBA por parte do DLO na logística do negócio.

*Nota aos formadores:* **Os formandos devem identificar os principais factos e as principais divisões e decisores, a fim de compreender o âmbito e a configuração do círculo de negócios no qual serão definidos mais detalhes sobre o caso.**

**Material a ser utilizado no estudo de caso**:

* *Pasta "Dia 2/2.2.2 Introdução ao exercício de investigação/Material introdutório"*:
* Sinopse do estudo de caso;
* Introdução à apresentação do estudo de caso e guia dos formadores para investigação do estudo de caso;
* *Pasta "Dia 2/2.2.3 Exercício de investigação/Provas/Perfis":*
* Perfil empresarial do Federal Bank of Atlantis;
* Perfil empresarial da United Bank Printing;
* Perfil empresarial do Docklands Security Bank of Norland.
* *Pasta "Dia 2/2.2.3 Exercício de investigação/Provas/Documentos e relatórios"*:
* Anúncio do bónus de aniversário por parte do FBA;
* Bónus do FBA.
* *Pasta "Dia 2/2.2.3 Exercício de investigação/Provas/E-mails"*:
* 1.º e-mail;
* 2.º e-mail.

**Possíveis perguntas para os formandos**:

*- Que autoridades e que tipo de ferramentas jurídicas serão utilizadas a nível local para averiguar os principais factos mencionados?*

*- Como é que estes factos influenciam o desenvolvimento da investigação?*

**2.2 Estabelecimento de dúvida razoável sobre o possível início do crime**

*"Por causa do* *período de férias de verão, o DLO estava com poucos funcionários e o vice-diretor recorreu a pessoal júnior e recentemente contratado para trabalhar nesta atividade, fazendo chamadas e interagindo com os colegas do Departamento Financeiro".*

*Nota aos formadores*: **a introdução do facto de que, por causa do período de férias de verão, funcionários recentemente contratados foram incluídos numa operação tão importante deve levantar imediatamente suspeitas entre os formandos.** O elemento-chave é que um dos funcionários júnior é, na verdade, membro do grupo de crime organizado que solicitou a posição de nível inferior do DLO, a fim de obter qualquer tipo de acesso direto aos computadores do FBA. O objetivo era introduzir um e-mail específico de spyware capaz de enviar cópias de correspondência por e-mail entre o DLO do FBA, o Departamento Financeiro e empresas terceirizadas para o computador e utilizador designados, neste caso o pessoal júnior/principal suspeito. Com este tipo de acesso, é possível ter acesso próximo e detetar um possível alvo de um esquema de BEC.

**Material a ser utilizado no estudo de caso**:

* *Pasta "Dia 2/2.2.3 Exercício de investigação/Provas/E-mails":*
* 1.º e-mail;
* 2.º e-mail;
* 5.º e-mail;
* 7.º e-mail.

**Possíveis perguntas para os formandos**:

*- Que diligências devem ser feitas e por decisão de que autoridades a fim de estabelecer a identidade do possível criminoso?*

*- Como determinar o tipo de malware que foi utilizado?*

*- Como estabelecer as consequências desse malware, os vestígios da comunicação de malware com pontos de contacto externos e quais são os outros factos importantes que a investigação deve apurar neste momento?*

**3. Configuração financeira**

*"Foi feito um pedido, por parte do FBA, de impressão de 20.000 exemplares em papel pela UBP, pelo preço de 300.000 €. Os departamentos relevantes do FBA e da UBP começaram a tratar da parte logística e financeira.*

*O FBA e a UBP trocaram detalhes sobre faturas e pagamentos, incluindo contas e códigos SWIFT e IBAN. A UBP exigiu um pagamento adiantado de 100.000 €, a ser transferido para a sua conta detida no Docklands Securities Bank of Norland. Este foi efetuado no prazo de 24 horas após a aceitação do pedido".*

Além da introdução de factos financeiros, há outros pontos que foram acrescentados aos factos principais:

*- A inclusão do Docklands Securities Bank of Norland no círculo de negócios como banco designado da UBP para a transferência de dinheiro;*

*- Pagamento efetivo da transferência inicial de 100.000 € entre o FBA e a UBP com contas DSBL;*

*- Introdução do facto de as referências SWIFT e IBAN das contas serem incluídas na transação.*

*Nota aos formadores*: **esta configuração deve indicar que a transferência bancária inicial não teve problemas e que mencionar as contas e referências SWIFT e IBAN significa que a transferência de dinheiro é de natureza internacional e não meramente nacional.** Dito isto, os formandos devem começar a considerar a utilização doas normas de assistência jurídica internacional da Convenção de Budapeste.

**Material a ser utilizado no estudo de caso**:

* *Pasta "Dia 2/2.2.3 Exercício de investigação/Provas/Documentos e relatórios"*:
* Contrato entre o FBA e a UBP.
* *Pasta "Dia 2/2.2.3 Exercício de investigação/Provas/Extratos bancários"*:
* Fatura pró-forma da UBP;
* Extrato bancário do FBA;
* Extrato bancário da UBP.
* *Pasta "Dia 2/2.2.3 Exercício de investigação/Provas/E-mails":*
* 3.º e-mail;
* 4.º e-mail;
* 6.º e-mail;
* 7.º e-mail;
* 8.º e-mail

**Possíveis perguntas para os formandos**:

* *Quais são os principais artigos substantivos do contrato?*
* *Como e quando é que o pagamento antecipado foi transferido?*
* *A transferência foi efetuada sem problemas e porquê?*
* *Há a possibilidade de a transferência ter sido monitorizada por uma parte indesejada?*
* *Se sim, como?*

**4.** **Início do crime efetivo e ponto-chave da investigação**

"*O contrato exigia que a impressão dos 20.000 exemplares em papel fosse concluída em sete dias. A UBP cumpriu esta obrigação um dia antes do prazo. A Divisão Comercial informou o Departamento Financeiro da UBP de que o material estaria pronto para envio após o pagamento final ser recebido.*

*O Departamento Financeiro da UBP enviou um e-mail aos seus homólogos do FBA informando-os que a encomenda estava pronta para entrega e que o pagamento final no valor de 200.000 € deveria ser efetuado no prazo de 48 horas. Nessa noite, o FBA recebeu um e-mail da UBP a informar que a conta bancária da empresa em Norland não estaria acessível durante os 3 dias seguintes, devido a um feriado nacional do país. O e-mail solicitava que o valor fosse transferido para a conta da UBP na filial de Ostland do Docklands Securities Bank of Norland"*

*Nota aos formadores*: **este deve ser reconhecido como um momento determinante da perpetração de todo o esquema.** O membro anteriormente mencionado do grupo de crime organizado, através de spyware, conseguiu detetar e acompanhar o desenvolvimento da transação entre o FBA e a UBP. A única ação que restava era identificar e reagir prontamente no momento do pagamento final, o que deveria ocorrer assim que a UBP informasse o FBA que a impressão dos exemplares em de papel solicitada estava concluída.

Depois de o Departamento Financeiro da UBP notificar os seus homólogos do FBA de que o pagamento deveria ser efetuado, a "toupeira" conseguiu intercetar o e-mail e notificar o resto do grupo criminoso. Juntamente com outros criminosos, conseguiu assim enviar faturas falsas previamente elaboradas com cabeçalhos de e-mail quase iguais aos do Departamento Financeiro da UBP, utilizando os serviços de servidor aberto SMTP que foram alugados antes da perpetração do crime.

**Variante do cenário,** incluindo o facto de o e-mail ter sido alterado com algumas pequenas alterações ao nome real da conta de e-mail do funcionário do Departamento Financeiro da UBP, em vez de utilizar o servidor SMTP gratuito; deve ser utilizada em situações em que os formadores observam menos conhecimentos técnicos por parte dos formandos, o que pode gerar problemas na conclusão do exercício de investigação.

Uma conta bancária sob controlo do grupo criminoso foi aberta propositadamente com intenção criminosa no outro país (Ostland, neste exercício), em nome de uma empresa "fictícia" com um nome semelhante ao original (UBP, neste caso), que foi anteriormente registada junto da filial do banco principal, o que significa que a conta bancária fraudulenta foi aberta na filial de Ostland do Docklands Securities Bank of Norland. A conta bancária não foi nunca utilizada anteriormente com o FBA e foi aberta pelo autor principal deste projeto criminoso e pelos seus cúmplices. Os dados utilizados durante o processo de registo foram forjados e eram quase idênticos aos originais, neles se incluindo detalhes de funcionários do Departamento Financeiro do FBA.

Todo o esquema assumiu um caráter mais urgente devido ao feriado nacional de Norland. Os criminosos aproveitaram este facto para justificar a mudança da conta bancária. Deste ponto em diante, estava tudo montado.

**Factos principais:**

* *A impressão efetiva do material em papel foi feita e a UBP notificou deste facto o FBA, a quem solicitou o pagamento devido;*
* *O membro infiltrado do grupo de crime organizado, através de spyware, detetou os momentos finais da execução do negócio;*
* *O grupo registou-se como empresa "fictícia" em Ostland e abriu uma conta bancária comercial nesse país junto da filial do banco utilizada em operações regulares da UBP em Norland;*
* *Falsa documentação, incluindo as principais partes da mesma – foi elaborada uma fatura falsa, além do servidor de e-mails e os e-mails;*
* *O servidor SMTP aberto foi alugado e testado para envio de e-mails falsos (ou pode ser utilizado um exemplo de uma conta de webmail com uma pequena alteração ao nome da conta de e-mail, consoante as habilidades do formador);*
* *Os serviços do servidor de correio SMTP abertos foram pagos em Bitcoins (ou num exemplo de caso de webmail, sem ele);*
* *Foram elaborados e-mails falsos, incluindo os nomes das pessoas do Departamento Financeiro, detalhes sobre o contrato e o idioma que foram utilizados anteriormente;*

**Material a ser utilizado no estudo de caso**:

* *Pasta “Dia 2/2.2.3 Exercício de investigação/Provas/E-mails"*:
* 9.º e-mail;
* 10.º e-mail.
* *Pasta "Dia 2/2.2.3 Exercício de investigação/Provas/Extratos bancários"*:
* Fatura falsa da UBP
* *Pasta "Dia 2/2.2.3 Exercício de investigação/Provas/Documentos e relatórios":*
* Registo da empresa fictícia UBP em Ostland;
* Registo de uma conta bancária da empresa fictícia UBP no DSBN em Ostland;
* Relatório de resultados da verificação de software anti-spyware;
* Relatório de rastreamento da rede do servidor SMTP;
* Relatório de pagamento por Bitcoins da empresa de servidores SMTP
* *Pasta "Dia 2/2.2.3 Exercício de investigação/Provas/Depoimentos de testemunhas*":
* Depoimento do Departamento de TI do FBA.

**Possíveis perguntas para os formandos**:

* *Como é que as informações sobre a finalização do negócio foram adquiridas e como se pode recuperá-las, se possível?*
* *Como se podem obter informações sobre a empresa "fictícia" e detalhes da conta bancária em Ostland?*
* *Que tipo de informação deve ser solicitada à filial de Ostland e de que forma?*
* *Algumas das informações são urgentemente necessárias e justificar-se-á, por esse motivo, a ativação do ponto de contacto permanente da rede 24/7 do Conselho da Europa?*
* *Como se podem obter provas sobre documentação falsa/forjada e como analisá-las?*
* *Como se podem obter informações sobre o servidor SMTP aberto (ou informações da empresa de e-mails baseada na web) e o que pode ser revelado a partir disso?*
* *O que são Bitcoins, como é que foram utilizadas e de que forma podem ser utilizadas como provas eletrónicas?*
* *Qual é o resumo que se pode concluir relativamente às provas eletrónicas?*

**5.** **Fim do crime e início do processo**

"*No dia útil seguinte, o Departamento Financeiro do FBA estava pronto para transferir o dinheiro. O Diretor Financeiro autorizou a transferência dos restantes 200.000 €, que foram transferidos para a suposta conta bancária da UBP em Ostland.*

*Na manhã do vencimento do prazo de 48 horas, o Departamento Financeiro da UBP contactou os seus homólogos do FBA e solicitou o pagamento imediato do valor devido. O FBA informou a UBP de que o pagamento já tinha sido efetuado e que aguardava a entrega dos materiais. Como um aparte, o FBA felicitou a UBP pelo feriado nacional.*

*O Departamento Financeiro da UBP conferiu a sua conta bancária e respondeu à FBA dizendo que não foi recebido qualquer pagamento. Também perguntaram porque é que a UBP estava a felicitá-los por um feriado nacional, quando faltavam dois meses para o próximo feriado".*

*Nota aos formadores*: **a finalização do esquema ocorreu no dia seguinte, quando o Diretor Financeiro do FBA autorizou a transferência bancária com base em documentos apresentados anteriormente: correio falso da UBP com uma fatura falsa que continha a conta bancária falsa, noutro no país, desconhecida tanto pelo FBA como pela UBP.**

Naquele exato momento, a fraude foi cometida. 200.000 EUR foram transferidos para a conta fraudulenta. Dependendo do desenvolvimento do cenário, os formadores podem criar transações adicionais entre a conta bancária em Ostland e as contas bancárias que se encontram noutros países pertencentes às partes estatutárias da Convenção de Budapeste ou não, como exercício de acompanhamento de transações online através de uma investigação financeira efetiva e de testes de conhecimento sobre o procedimento de assistência jurídica mútua.

Ao critério dos formadores fica ainda determinar que o fim último das transferências bancárias possa ser em país que seja Estado Parte da Convenção de Budapeste ou não. No segundo caso, provavelmente os vestígios e provas finais serão perdidos ou não poderão ser recuperados. No entanto, ambos os exemplos podem ser úteis para os formandos.

**Factos principais:**

* *O Diretor Financeiro do FBA autoriza a transferência com base em documentos apresentados anteriormente;*
* *O documento constitui correio falso da UBP com uma fatura falsa que indicava a conta bancária falsa;*
* *200.000 EUR foram transferidos. Consoante as necessidades locais de formação, as transferências bancárias podem ser continuadas para outros países ou interrompidas. Além disso, a transferência final pode ser destinada a país que seja Parte da Convenção de Budapeste ou a outro país, terceiro;*

**Material a ser utilizado no estudo de caso**:

* *Pasta "Dia 2/2.2.3 Exercício de investigação/Provas/E-mails":*
* 9.º e-mail;
* 10.º e-mail;
* 11.º e-mail.
* *Pasta “Dia 2/2.2.3 Exercício de investigação/Provas/Depoimentos de testemunhas*":
* Depoimento do DLO do FBA;
* Depoimento do FD do FBA;
* Depoimento do Departamento de TI do FBA.
* Declaração AD da DSBN em Ostland.
* *Pasta "Dia 2/2.2.3 Exercício de investigação/Provas/Extratos bancários*":
* Extrato bancário da DSBN em Ostland;

**Possíveis perguntas para os formandos**:

* *Porque é que o Diretor Financeiro autorizou a transação?*
* *Para que conta foi efetuada a transação?*
* *Visto que a Ostland ratificou a Convenção de Budapeste, que medidas poderão ser adotadas pelas entidades competentes para investigar?*
* *Que documentos e de que forma devem estes ser obtidos do FBA?*
* *Que documentos e de que forma devem estes ser obtidos da UBP?*
* *Que banco deve ser contactado e de que forma (com que tipo de solicitação) durante a investigação?*
* *Como é que o dinheiro pode ser levantado, se possível?*
* *Que tipo de pedidos e/ou despachos podem ser emitidos para todas as entidades comerciais e bancos?*
* *Quais são os motivos para este tipo de ação?*
* *Que artigos da Convenção de Budapeste serão utilizados?*

**6.** **Principais etapas da investigação e principais provas eletrónicas**

Os formandos irão presumir que o primeiro momento de contacto entre o FBA e as autoridades de justiça criminal ocorreu no dia da transferência, quando o e-mail da UBP chegou com dúvidas sobre a falta da transferência de dinheiro e o feriado. A partir desse momento, consoante o sistema jurídico local, a investigação ira começar. O modelo é versátil e pode incluir a polícia, o Ministério Público, juízes de instrução e outras entidades, se necessário. Todas as instituições podem desempenhar um determinado papel e as suas ações têm um objetivo comum com diferentes abordagens.

No entanto, as **principais etapas da investigação devem ser**:

* *Registo dos depoimentos dos possíveis suspeitos;*
* *Registo dos depoimentos dos representantes do FBA;*
* *Obtenção de provas eletrónicas e outras provas do FBA;*
* *Registo dos depoimentos dos representantes da UBP;*
* *Obtenção de provas eletrónicas e outras provas da UBP;*
* *Registo dos depoimentos dos representantes da DSBN em Norland e Ostland;*
* *Obtenção de provas eletrónicas e outras provas de ambos os bancos;*
* *Obtenção de provas da autoridade de registo comercial competente em Ostland;*
* *Cooperação entre a polícia, o Ministério Público e, se for caso disso, juízes de instrução;*
* *Inclusão de procedimentos de auxílio judiciário internacional contidos nas disposições da Convenção de Budapeste;*
* *Outras ações investigativas importantes reconhecidas e definidas pelos formandos com o apoio dos formadores.*

**Principais provas eletrónicas:**

* *Registos informáticos do FBA;*
* *Spyware utilizado no FBA;*
* *Servidor SMTP e registo do envio de e-mails falsos;*
* *Criptomoeda (Bitcoin), blockchain, registo (ledger) de blockchain;*
* *E-mails verdadeiros;*
* *E-mail falso com cabeçalho completo;*
* *Fatura falsa;*
* *Registos informáticos da UBP;*
* *Registos bancários e de contas da DSBN;*
* *Registos comerciais da empresa;*
* *Registos de vigilância;*
* Outra provas eletrónicas.

As listas não são exaustivas e podem ser alteradas ou atualizadas com outras etapas de investigação e provas eletrónicas, conforme necessário.

**Material adicional a ser utilizado no estudo de caso**:

* *Pasta "Dia 2/2.2.3 Exercício de investigação/Glossário*":
* Ameaça persistente avançada;
* Criptomoedas;
* Engenharia social;
* Spyware;
* Servidor SMTP aberto e spoofing de e-mail.

**7. Anexo**