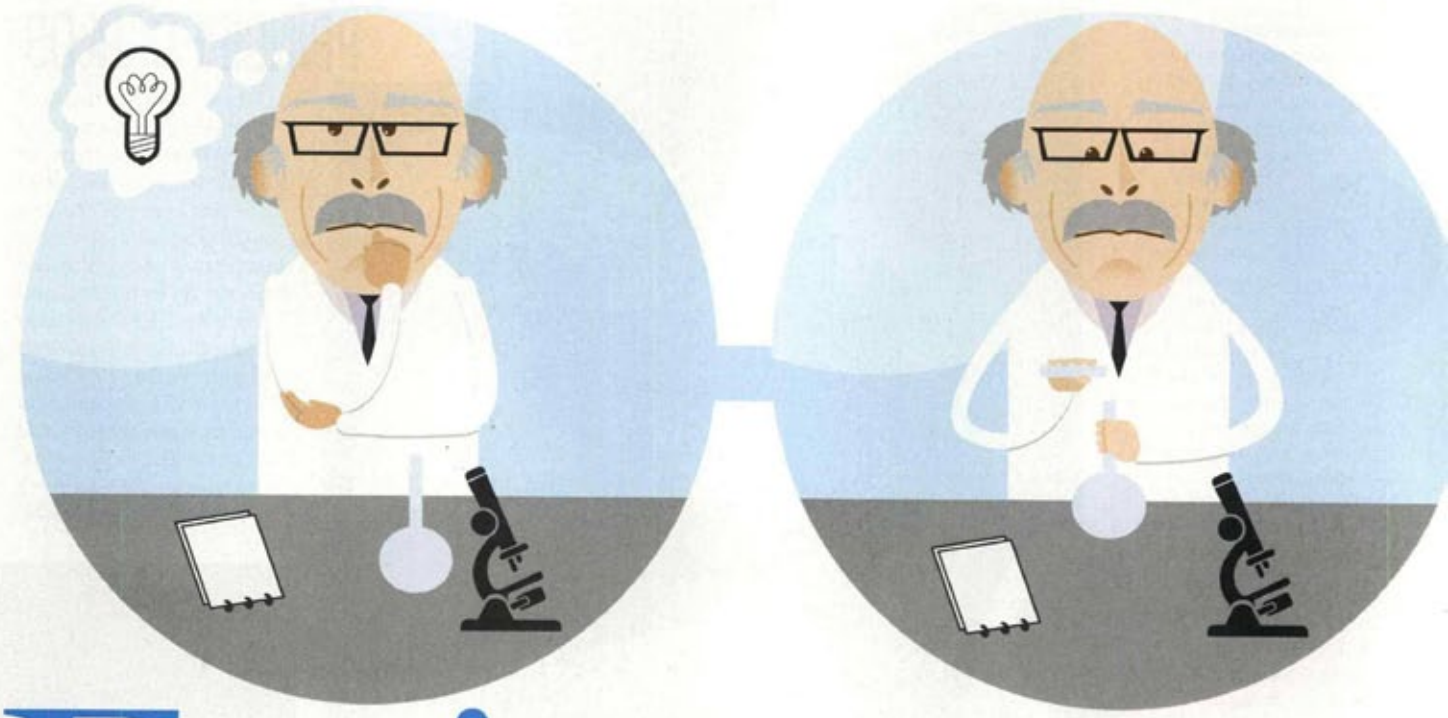


Espionagem branco

Talvez seja melhor começar a estimar mais ou, então, a desconfiar dos seus colaboradores mais directos, pois qualquer um poderá tornar-se num espião industrial, passando segredos da sua empresa a um rival comercial. Qualquer fotocópia, *email* com informação sigilosa ou mesmo conversa pode ser negociado por muito dinheiro

Por Bruno Horta

Não só os espiões e agentes duplos ao estilo de 007 não terminaram com o fim da Guerra Fria, como evoluíram com a globalização e a actual crise financeira e económica. O cenário deste jogo de infiltração deslocou-se dos quartos de hotel e dos corredores do poder para os circuitos de computador. E os segredos mais valiosos já não se encontram apenas nos Governos e embaixadas. Hoje, os principais alvos são, muitas vezes, as sedes de empresas, as multinacionais, assim como os laboratórios. Falamos de espionagem virtual e, sobretudo, económica e industrial. Pormenor: os países emergentes estão metidos na maioria deste tipo de acções (China, Índia, Brasil, Rússia) e Portugal também está debaixo de fogo.

Duas notícias recentes comprovam a tendência. No início de Junho, soube-se que tinham sido roubadas palavras-passe de várias contas de *email* da Google, incluindo de membros da administração norte-americana. O FBI disse que o ataque tinha tido origem na China, mas o governo chinês negou responsabilidades. Pouco depois, o jornal *New York Times* revelava que o Fundo Monetário Internacional (FMI) tinha sofrido ao longo de várias semanas um "ataque informático grave e complexo", cujos pormenores não foram divulgados. Claro que ainda é cedo para tirar conclusões, mas tudo indica que estamos perante dois casos de espionagem económica e industrial.

"Qualquer empresa ou entidade que esteja conectada à rede e que assente o seu negócio em sistemas de informação está exposta a um risco extremamente abrangente e, cada vez mais, de teor invisível", comenta à *Penthouse* Bruno Castro, engenheiro informático e director da empresa portuguesa de segurança informática Visionware. "A rede proporciona muitas mais-valias para o negócio", afirma, "mas, simultaneamente, acrescenta ameaças concretas e bastante perigosas para qualquer

de colarinho

indivíduo ou empresa. Não existe forma de estar na rede sem se saber conviver com isto".

"Parece um paradoxo, mas a verdade é que os documentos e dados estão hoje mais seguros dentro de um armário, sob o olhar atento de um funcionário de escritório, do que dentro de um computador", lê-se no relatório *Shadows in The Cloud* (2010), produzido pela Fundação Shadow Server e pela Universidade de Toronto.

780 páginas da Ferrari

Três indústrias surgem como alvos preferenciais: aeroespacial, biotecnológica e automóvel. O governo chinês, por exemplo, recorre a piratas informáticos privados para aceder às redes informáticas dos EUA e da Europa e já terá roubado de tudo um pouco: fórmulas farmacêuticas, projectos de bioengenharia, segredos de nanotecnologia, dados sobre armas e produtos industriais do dia-a-dia, diz o livro *Cyber War* (2010), de Richard Clarke, o todo-poderoso especialista em contra-terrorismo e assessor da presidência dos EUA entre 1992 e 2003. Com todas as letras, assegura o relatório *Innovation, Espionage, and Chinese Technology Policy*, publicado há poucas semanas pelo "*think tank*" americano Council on Foreign Relations (Conselho de Relações Internacionais): "Por volta de 2020, a China será a sociedade da inovação. Em 2050,

será líder na área da ciência e tecnologia. Para conseguir estes objectivos, o país tem seguido três caminhos: política de industrialização, estratégia de inovação e espionagem industrial".

Não admira, por isso, que as empresas andem obcecadas com a China e a ciberespionagem. Às vezes, até parecem esquecer-se de que os segredos das empresas não são feitos apenas de *bits* e *bytes*. O episódio que envolve as equipas de Fórmula 1 Ferrari e McLaren é um bom exemplo de como um método nada sofisticado – fotocópias – pode ter o mesmo resultado que a mais sofisticada pirataria informática. Passou-se em 2007 e só teve um desfecho no ano passado. Ficou conhecido como *Stepneygate*, em referência ao nome do principal culpado, o engenheiro mecânico Nigel Stepney.

Nigel trabalhava na Ferrari e, em vésperas do Grande Prémio da Austrália, em Março de 2007, terá enviado ao desenhador-chefe da McLaren, Mike Coughlan, 780 páginas de documentos da Ferrari relativos a carros de competição. Ambos terão também trocado 320 *emails* e mensagens de telemóvel. Stepney foi despedido em Julho daquele ano, já com um processo judicial às costas e sob a acusação de espionagem industrial a favor da McLaren. A FIA, organismo que supervisiona a Fórmula 1, lançou também um inquérito.

A marca britânica acabou por ter de pagar 60 milhões de euros de compensação aos italianos e, no ano seguinte, ambas as equipas emitiriam um comunicado conjunto dizendo ter enterrado o machado de guerra. Mike Coughlan foi despedido (trabalha agora na Williams) e Stepney conheceu a sentença em Setembro do ano passado: 20 meses de prisão e 600 euros de multa.

Outro caso, que também envolve construtores de automóveis, passou-se na Alemanha, em 1993, e durou até há muito pouco tempo. O antigo chanceler alemão Helmut Khol chegou a vir a público pedir contenção às partes. A saber: General Motors (GM) e Volkswagen (VW).

Também aqui, foi um empregado, o espanhol Jose Ignacio Lopez de Arriortua, quem deu origem ao problema. Tinha trabalhado para a GM, nos EUA, como chefe de vendas e, em 1993, saiu abruptamente a caminho da empresa alemã, na qual assumiu o posto de director de produção. A GM acusou-o de roubar e entregar à concorrência documentos relativos a novos modelos de automóveis que iriam ser produzidos. Em Novembro de 1996, Lopez demitiu-se da VW e foi viver para Espanha. No ano seguinte, os alemães concordaram pagar à GM uma indemnização de 100 milhões de dólares, bem como comprar material aos americanos no valor de um bilião de dólares. Nunca admitiram, no entanto, ter havido espionagem. Lopez, por sua vez, teve a justiça americana à perna até 2001. Nesse ano, os tribunais espanhóis recusaram-se a extraditar o antigo chefe de vendas pelo que, até hoje, nunca foi julgado.

Pepsi não quis atacar Coca-Cola

Em concreto, de que é que se fala quando se fala em espionagem económica e industrial? "O dono de um segredo comercial acaba por ficar destituído da vantagem que teria conseguido se o seu segredo se tivesse mantido fora do alcance da concorrência e do público em geral", diz o livro *Economic Espionage and Industrial Spying* (2005), da professora americana de Direito Hedieh Nasher. Bruno Castro aponta as situações mais comuns: "Pode ser um trabalhador da própria empresa que, a troco de um incentivo financeiro ou por vingança e insatisfação, rouba e transfere informação confidencial para uma empresa concorrente. Recentemente, temos tido alguns

O facto de Portugal se encontrar na vanguarda das energias renováveis torna-o um alvo apetecível

Por volta de 2020, a China será a sociedade da inovação. Em 2050, será líder na ciência

Mike Coughlan, desenhador-chefe da McLaren, recebeu 780 páginas de documentos confidenciais da Ferrari

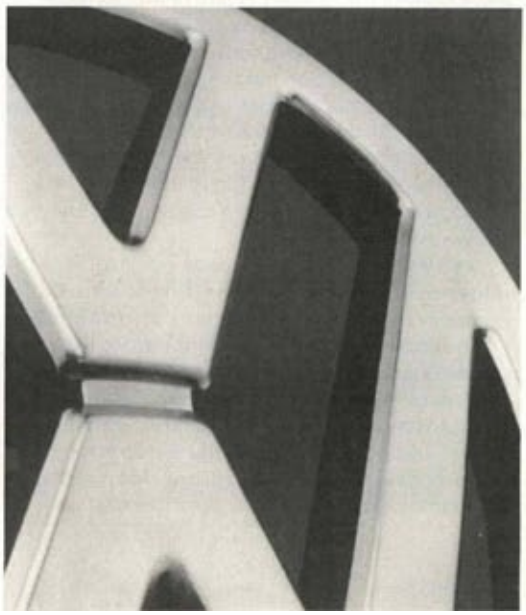
casos de ataques anónimos, cujos autores não têm qualquer relação com a empresa, e que roubam ou manipulam informação para benefício próprio, incluindo venda posterior no mercado negro".

Os métodos utilizados são complexos (intercepção de chamadas, aparelhos espiões, pirataria informática) ou simples (memorização, roubo de papéis, fotocópias), esclarece o livro de Hedieh Nasher.

O relatório *Targeting U.S. Technologies*, publicado este ano pelo Departamento de Defesa americano (equivalente ao nosso Ministério da Defesa), acrescenta um método tão simples que não passa pela cabeça de ninguém, excepto pela dos próprios espiões, claro: "Pedir informações directamente, através de *email*, é a primeira forma de fazer espionagem. Por detrás desses pedidos pode estar uma recolha metódica de dados que, além do mais, é eficiente e barata".

O problema está de tal forma na ordem do dia que foi escolhido pelo gigante da indústria Warner Bros. como tema central de um *blockbuster* de Verão, *A Origem*, de Christopher Nolan, estreado em Portugal em Julho de 2010. O filme conta a história de Dom Cobb (Leonardo DiCaprio), especialista na arte de roubar segredos industriais da mente das pessoas, enquanto estas estão a dormir. Ficção científica, obviamente. Mas espionagem industrial pura e dura. As maiores

Bruno Castro, director da empresa de segurança informática Visionware



empresas do mundo mostram tanta preocupação quanto excesso de zelo. Este ano, a Renault acusou o governo chinês de lhe roubar planos para a construção de carros eléctricos, para depois descobrir que se tinha enganado. A 3 de Janeiro, a empresa suspendeu três administradores: Michel Balthazard, Bertrand Rochette e Matthieu Tenenbaums, porque uma carta anónima dizia que empregados da Renault andavam a passar ao governo chinês informações sobre os novos carros eléctricos e a receber pagamentos através de contas na Suíça e no Liechtenstein. A marca, cujo maior accionista é o Estado francês, com 15 por cento do capital, recorreu à justiça e apresentou queixa contra desconhecidos por "espionagem industrial organizada, corrupção, quebra de confiança, roubo e encobrimento".

Chegados a Março, uma reviravolta. A Renault deixou cair as acusações de espionagem, pediu desculpas públicas aos três administradores suspensos e admitiu estar perante um "possível embuste", relatou o *New York Times*. Resultado: os três demitidos moveram acções judiciais contra a Renault para serem indemnizados e o presidente da marca, Carlos Ghosn, viu diminuídos os poderes dentro da empresa e o bónus anual, escreveu o *Financial Times*.

A responsabilidade pelo episódio recai agora sobre Dominique Gevrey, membro dos serviços internos de segurança da Renault, e a pessoa que terá dado crédito à carta anónima.

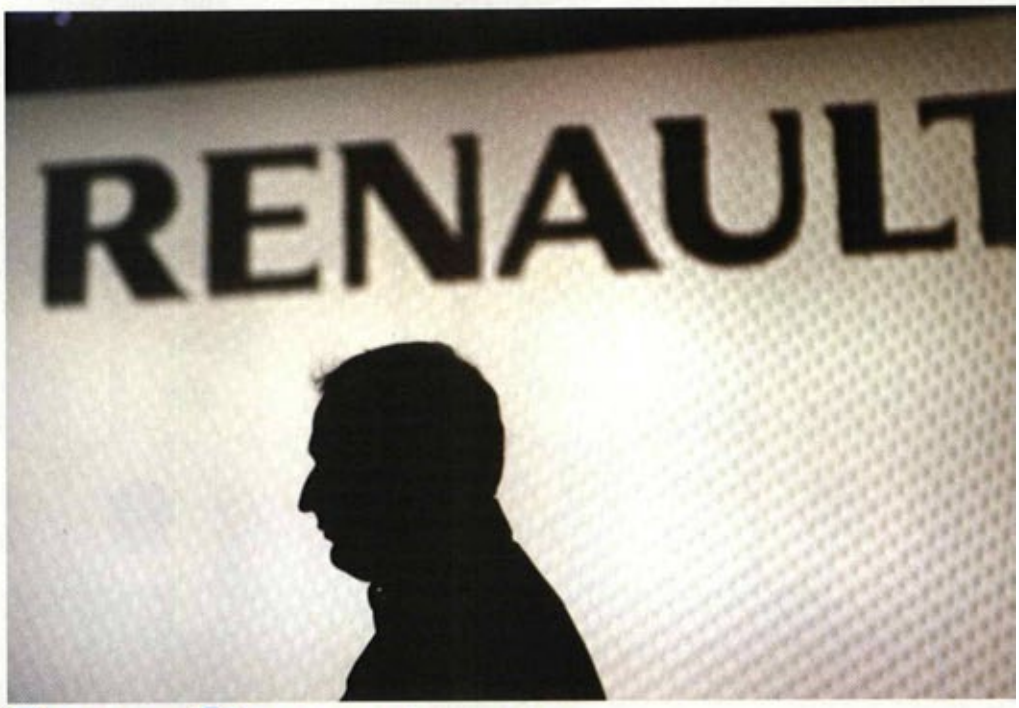
Gevrey alega ter agido de boa-fé, mas está preso preventivamente e é acusado de fraude. Há uns anos, nos EUA, o FBI prendeu três pessoas em Atlanta acusadas de roubarem segredos comerciais da Coca-Cola e de os quererem vender à Pepsi por mais de um milhão e meio de dólares. Mas aqui não só o crime não se concretizou como as duas empresas concorrentes decidiram colaborar com as autoridades.

A coisa, escrevia em 2006 o *Washington Post*, passou-se assim: uma funcionária administrativa da Coca-Cola, Joya Williams, de 41 anos, contactou a Pepsi com o objectivo de lhe vender documentos da marca concorrente, mas a Pepsi avisou a Coca-Cola e esta avisou o FBI. As câmaras de videovigilância da Coca-Cola terão até apanhado Joya Williams a guardar vários papéis que pertenciam à sua empresa. Com ela colaboravam mais dois empregados, um no estado da Geórgia, outro em Nova Iorque. Um agente do FBI, devidamente disfarçado, foi ao encontro da funcionária e deu-lhe 30 mil dólares em dinheiro em troca dos documentos e de uma amostra de um novo produto que a Coca-Cola estava a desenvolver.

Joya Williams seria condenada, em 2007, a oito anos de prisão e multa de 40 mil dólares. Os cúmplices apanharam cinco e dois anos de prisão.

No início da década de 90, também nos EUA, outras duas empresas aliaram-se contra a espionagem. Harold C. Worden foi acusado de roubar à empresa em que trabalhara durante 28 anos, a Kodak, páginas e páginas de fórmulas secretas para produção de películas fotográficas. Estávamos em 1994. Depois de roubar os papéis,

Em *A Origem*, Leonardo DiCaprio é um especialista na extracção de segredos do inconsciente



O SIED e o SIS confirmam que Portugal é um alvo importante da espionagem económica e industrial

quis vendê-los às empresas concorrentes Konica e Agfa. Foi denunciado por ambas. Em Maio de 1996, o FBI encontrou os documentos em casa dele. Worden confessou o crime e, em 1997, foi condenado por um tribunal americano a 15 meses de prisão efectiva e multa de 30 mil dólares.

Espiões em Portugal?

O Serviço de Informações Estratégicas de Defesa (SIED) e o Serviço de Informações de Segurança (SIS) confirmam que Portugal é um alvo importante da espionagem económica e industrial. O Relatório Anual de Segurança Interna de 2010 vai um pouco mais longe nos pormenores. Explica que as empresas tecnológicas são as mais vulneráveis e que as novas potências mundiais são as mais interessadas na espionagem. "Têm vindo a ser detectadas actividades de espionagem económica e industrial junto de sectores e de áreas relacionadas com o conhecimento, nomeadamente aquelas que se encontram associadas à inovação", lê-se no documento. "As potências emergentes procuram aproveitar o presente momento de crise económica para melhorar a sua posição relativamente às potências consolidadas." Estão, portanto, em causa o Brasil, a Rússia, a Índia e a China, mas também a Turquia e a Indonésia.

Bruno Castro, da Visionware, diz que os serviços da sua empresa são solicitados, na maior parte dos casos, "para estabelecer estratégias e acções de carácter preventivo", mas "tem vindo a ser cada vez mais regular a sua participação em cenários de crime informático, depois de o mal já estar feito". O engenheiro já foi chamado a intervir em casos de "roubo de informações confidenciais, bases de dados de clientes, acesso ilícito ao *email* de trabalhadores e até ataques directos aos sistemas informáticos, com vista à destruição ou manipulação da informação da empresa". À comunicação social raramente chegam estes relatos. O único episódio conhecido passou-se este ano, mas foi desmentido pela alegada vítima.

A empresa de metalurgia e energias renováveis Martifer teria despedido um engenheiro de topo alegadamente envolvido na transmissão de segredos sobre contratos e concursos à rival Enercon, noticiava o *Diário de Notícias* em Maio. Dias depois, uma fonte anónima da Martifer disse ao *Jornal de Negócios* que a notícia se referia a "um fantasioso caso de espionagem industrial". Por seu lado, a Enercon, produtora de aerogeradores, considerou "ridícula" a notícia.