manchete

i

09-01-2019

Periodicidade: Diária
Classe: Informacão Geral
Âmbito: Nacional
Tiragem: 14000

Temática: Tecnologia
Dimensão: 4118 cm²
Imagem: S/Cor
Página (s): 1/2 a 5

Mercado de Benfica.
Hackers assustam escritórios de advogados

Piratas informáticos acederam a informação da Operação Marquês, Vistos Gold e Parvalorem

Fonte da investigação diz que várias entidades públicas não estão preparadas para ataques informáticos // PÁGS. 2-5

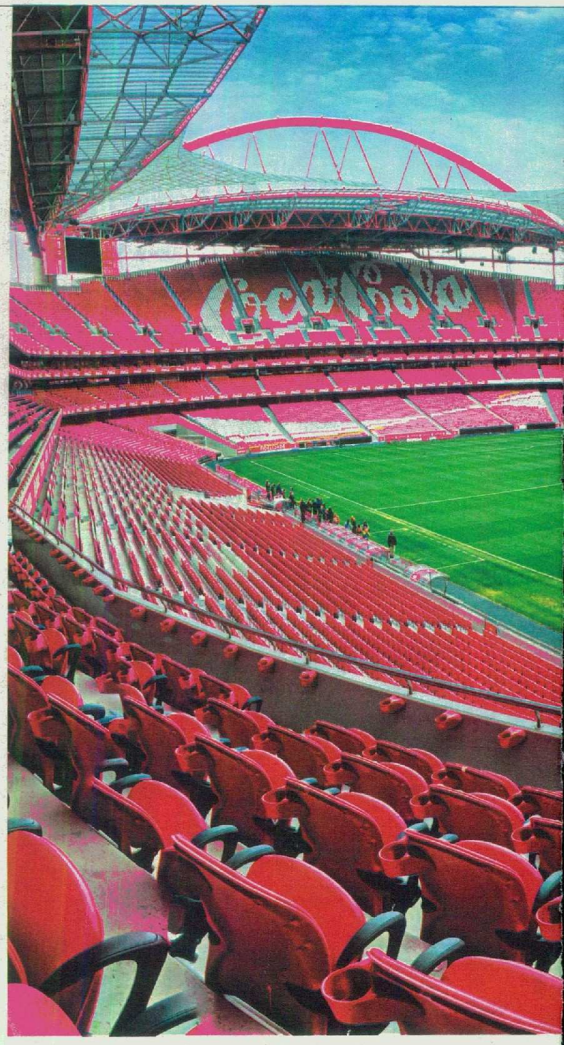
manchete

i

09-01-2019

Periodicidade: Diária
Classe: Informacão Geral
Âmbito: Nacional
Tiragem: 14000
Temática: Tecnologia
Dimensão: 4118 cm²
Imagem: S/Cor
Página (s): 1/2 a 5

Radar



Hackers atacam advogados e blogue vai continuar a divulgar dados do Benfica

Autoridades estão a investigar o blogue Mercado de Benfica, mas na internet é fácil aos hackers trocar as voltas aos investigadores. Blogue foi fechado e reabriu de seguida, aparentemente sediado no Irão

CARLOS DIOGO SANTOS
carlos.santos@ionline.pt
JOANA MARQUES ALVES
joana.alves@ionline.pt

O blogue Mercado de Benfica voltou – depois de ter sido encerrado por divulgar dados internos do Clube da Luz – e começou a mostrar que vinha para continuar o que estava a fazer até então. Logo nas primeiras horas divulgou um conjunto de informações sobre processos como a Operação Marquês, os Vistos Gold e o caso BPN. As informações terão sido conseguidas no âmbito de um ataque ao escritório de advogados PLMJ, que, entretanto, já confirmou ter sido vítima de acesso ilegítimo. Mas depois destas fugas, estão já a ser preparadas outras, que têm o Benfica como parte. É que este escritório da PLMJ é um dos que defende os encarnados nos grandes processos em que o clube está envolvido – através da equipa do advogado João Medeiros.

manchete

i

09-01-2019

Periodicidade: Diária
Classe: Informacão Geral
Âmbito: Nacional
Tiragem: 14000

Temática: Tecnologia
Dimensão: 4118 cm²
Imagem: S/Cor
Página (s): 1/2 a 5

O blogue já prometeu a divulgação de novos dados sobre o Benfica

DREAMSTIME

Ao que o *i* apurou os escritórios Morais Leitão Galvão Teles, Soares da Silva & Associados e Saragoça da Matta & Silveiro de Barros - Sociedade de Advogados – que também estão a defender a Benfica SAD através dos advogados Rui Patrício e Paulo Saragoça da Matta – não registaram até ao momento qualquer ataque. Fonte oficial da Morais Leitão explicou mesmo que, "em relação à alegada informação ilegalmente tornada pública, não tem qualquer evidência de entrada no sistema".

Para os próximos dias, o blogue, que agora estará sediado no Irão, promete a divulgação do "primeiro arquivo de Miguel Moreira, CFO do SL Benfica". Em jeito de provocação os autores do blogue garantem que o ficheiro terá cerca de 12 gigas.

O *i* tentou ontem esclarecer junto da Wordpress se o encerramento do primeiro blogue foi a pedido das autoridades nacionais, não tendo sido dada qualquer resposta até à hora de fecho desta edição. Também a Procuradoria-Geral da República, contactada, não nos fez chegar qualquer esclarecimento sobre este caso.

INVESTIGAÇÃO ATENTA AO BLOGUE O Mercado de Benfica divulgou durante vários meses a informação sigilosa do Benfica. Apesar de, aparentemente, nada ter sido feito para travar, a verdade é que nos bastidores o Ministério Público e a Polícia Judiciária estiveram sempre atentos. Uma fonte próxima da investigação explicou ontem ao *i* que nestes casos "é preciso considerar que a internet é um espaço de liberdade, que não tem fronteiras".

Blogue anunciou a divulgação de arquivo de Miguel Moreira, CFO do SL Benfica

Dos escritórios que defendem o Benfica apenas a PLMJ foi atacada pelos hackers

A mesma fonte lembrou ainda que "o facto de hoje se aceder a determinada informação que está alocada num determinado local nada impede de que, bloqueado esse acesso, amanhã não esteja num outro sítio". E foi isso que terá agora acontecido.

"Tudo o que tem que ver com as investigações nesses casos tem esses entraves que são específicos e que são relacionados com a própria tecnologia", acrescenta.

A GUERRA DO BENFICA PARA CHEGAR AOS HACKERS A batalha para encontrar os autores dos blogues e fazê-los chegar às barras dos tribunais tem sido intensa para o Benfica. O caso tomou dimensões internacionais quando, em outubro do ano passado, jornal norte-americano "New York Times" revelou que o Benfica tinha recorrido à Google para tentar resolver este problema, pedindo os dados pessoais dos bloggers que tinham divulgado ilegalmente correspondência de vários dirigentes da Luz.

"O Benfica foi vítima de um roubo e posterior divulgação da sua correspondência privada, primeiro por um canal televisivo ligado a um dos seus rivais, o FC Porto, e, depois, no seguimento de uma decisão do tribunal que proibiu essa divulgação, esses emails, muitos deles distorcidos, começaram a ser publicados por blogues ligados aos clubes rivais", lê-se no pedido feito pelos encarnados na altura.

Na mesma altura, o "New York Times" revelou que a Google tinha concordado em ceder informações sobre os autores dos blogues, após os encarnados terem avançado com um processo no tribunal da Califórnia, no início do ano. O jornal explicou que o gigante tecnológico "notificou os utilizadores em questão, dando-lhes uma oportunidade para responder ao processo legal a decorrer na justiça dos Estados Unidos".

O semanário "Sol" noticiou em novembro do ano passado que o Benfica estaria muito perto de avançar com uma queixa contra "certos" com base nas informações dadas pela Google, o jornal revelou que em causa estariam "pessoas ligadas ao Sporting e ao FC Porto e que alguns deles foram colegas de escola e amigos de Rui Pinto", o hacker português de 29 anos suspeito de estar ligado ao Footbal Leaks e ao roubo da correspondência do Benfica, o que deu origem ao caso dos e-mails.

DOCUMENTOS DA OPERAÇÃO MARQUÊS REVELADOS O novo blogue Mercado de Benfica disponibilizou diversos volumes do processo que tem José Sócrates como peça principal. Nos documentos retirados da PLMJ constam informações relativas a Manuel Pinho, António Mexia, Ricardo Salgado, Henrique Granadeiro e ainda à Pravalorem.

Ao "Jornal Económico", a PLMJ confirmou na segunda feira o ataque: "Na sequência de sucessivas tentativas de intrusão ilícitas, a segurança de rede de PLMJ foi recentemente comprometida. A PLMJ está a avaliar o impacto potencial desse acesso ilegítimo a informação, tendo definido de imediato, em conjunto com uma equipa de especialistas, medidas preliminares de proteção e contenção".

manchete

i

09-01-2019

Periodicidade: Diária
Classe: Informacão Geral
Âmbito: Nacional
Tiragem: 14000

Temática: Tecnologia
Dimensão: 4118 cm²
Imagem: S/Cor
Página (s): 1/2 a 5

Cibersegurança. Ataques informáticos quase duplicaram desde o início da década

Não são novas as ameaças à cibersegurança em Portugal. Entre os casos mais graves está o dos hackers que invadiram o sistema da Procuradoria-Geral da República, de vários ministérios e de outras instituições públicas. Especialista em segurança informática assinala uma "carência significativa de recursos humanos especializados" na área. As forças de segurança responsáveis por investigar os ataques informáticos não conseguem competir com os salários dos privados

BEATRIZ DIAS COELHO
beatriz.coelho@ionline.pt

O ataque informático do blogue "Mercado de Benfica" ao Clube da Luz pode ter recebido mais atenção mediática do que outros, mas a verdade é que Portugal não tem passado ao lado do fenómeno dos ciberataques e das suas consequências. O *i* contactou a Procuradoria-Geral da República para saber quantas investigações relacionadas com crimes informáticos estão em curso, mas não obteve resposta até ao fecho da edição. Contudo, os dados mais recentes disponibilizados nas estatísticas da justiça, acessíveis online, revelam que em 2017 as autoridades policiais registaram 719 crimes vulgarmente conhecidos como ataques informáticos. Para a contagem entram dois tipos distintos de crime: o de acesso e interceção ilegítimos e o de sabotagem informática, que somaram, respetivamente, 470 e 249 ocorrências.

Os números têm vindo a crescer nos últimos anos – entre 2010 (366 crimes) e 2017 aumentaram 96 % –, o que não surpreende se se considerar que também o acesso à internet tem exponenciado, sustentado numa rápida evolução da tecnologia e na multiplicação dos dispositivos que permitem aceder à rede. Se nos primeiros anos desta década o crime de acesso e interceção ilegítimos registava ocorrências na casa das três centenas e diminuiu para as duas centenas em 2012, em 2014 os números inverteram e passaram a casa das três centenas. Desde aí, têm vindo a aumentar de ano para ano. O mesmo pode dizer-se quanto ao crime de sabotagem informática, que no início da década registava pouco mais de uma dezena de ocorrências.

O crescimento dos ciberataques, de resto, é visível nas notícias. Antes do ataque informático, na segunda-feira, à PLMJ, e do ataque ao Benfica, outras instituições portuguesas já figuravam na lista das entidades alvo de ataques informáticos. Foi o caso da Portugal Telecom (hoje Altice), uma das empresas afetadas pelo ciberataque a empresas a nível mundial e que, em Portugal, levou a EDP a cortar os acessos à internet da sua rede por prevenção.

Mas aquele que é provavelmente o incidente mais grave na história dos ciberataques em território nacional aconteceu em 2014, quando um conjunto de piratas informáticos invadiu os sistemas informáticos da PGR, do Parlamento, de vários ministérios e de diversas câmaras municipais e ainda de várias forças da autoridade – a PJ, a PSP e a GNR. O processo envolve 23 arguidos, que vão ser julgados por crimes de sabotagem informática, associação criminosa e acesso ilegítimo. Nas palavras de um pirata informático que participou no ataque, os envolvidos eram "apenas uma cambada de miúdos com picardias" e não "ativistas".

As implicações do ataque suscitam dúvidas quanto à preparação do país para este tipo de ataques e a verdade é que existem, realmente, motivos para preocupação. Quem o reconhece é o coordenador do Centro Nacional de Cibersegurança (CNCS) – autoridade nacional especialista em matéria de cibersegurança, cuja missão é contribuir para o uso livre e seguro do ciberespaço, em articulação com as autoridades competentes –, que admitiu em novembro do ano passado, na conferência "Cibersegurança: reduzir o risco, combater as ameaças", que o país está um "pouco atrasado" na definição de uma estratégia nacional de cibersegurança.

Na mesma ocasião, Lino Santos recusou, contudo, que os responsáveis políticos não estejam despertos para o tema. "Não tenho nenhum problema em dizer que o Estado está um pouco atrasado no tempo relativamente a este assunto. Portugal criou o CNCS em 2014 e devia ter criado esse centro em 2005 ou 2006", considerou o responsável.

Os números do CNCS, de resto, mostram que o trabalho desenvolvido tem dado resultados. O mais recente Relatório Anual de Segurança Interna (RASI), relativo a 2017, revela que a equipa de reação a incidentes da entidade recebeu 1895 notificações de ataques no ciberespaço. Dessas, 535 "resultaram na abertura de incidentes analisados e resolvidos com sucesso", lê-se no documento. Entre os casos, mostra o relatório, "17% afetaram direta ou indiretamente entidades do Estado, o que representa um acréscimo de 8% em relação ao ano transato". A maioria dos crimes teve como objetivo a recolha de informação e as instituições do setor bancário foram as mais afetadas.

FALTA DE PREPARAÇÃO? Se os hackers conseguem entrar nos sistemas governamentais – que

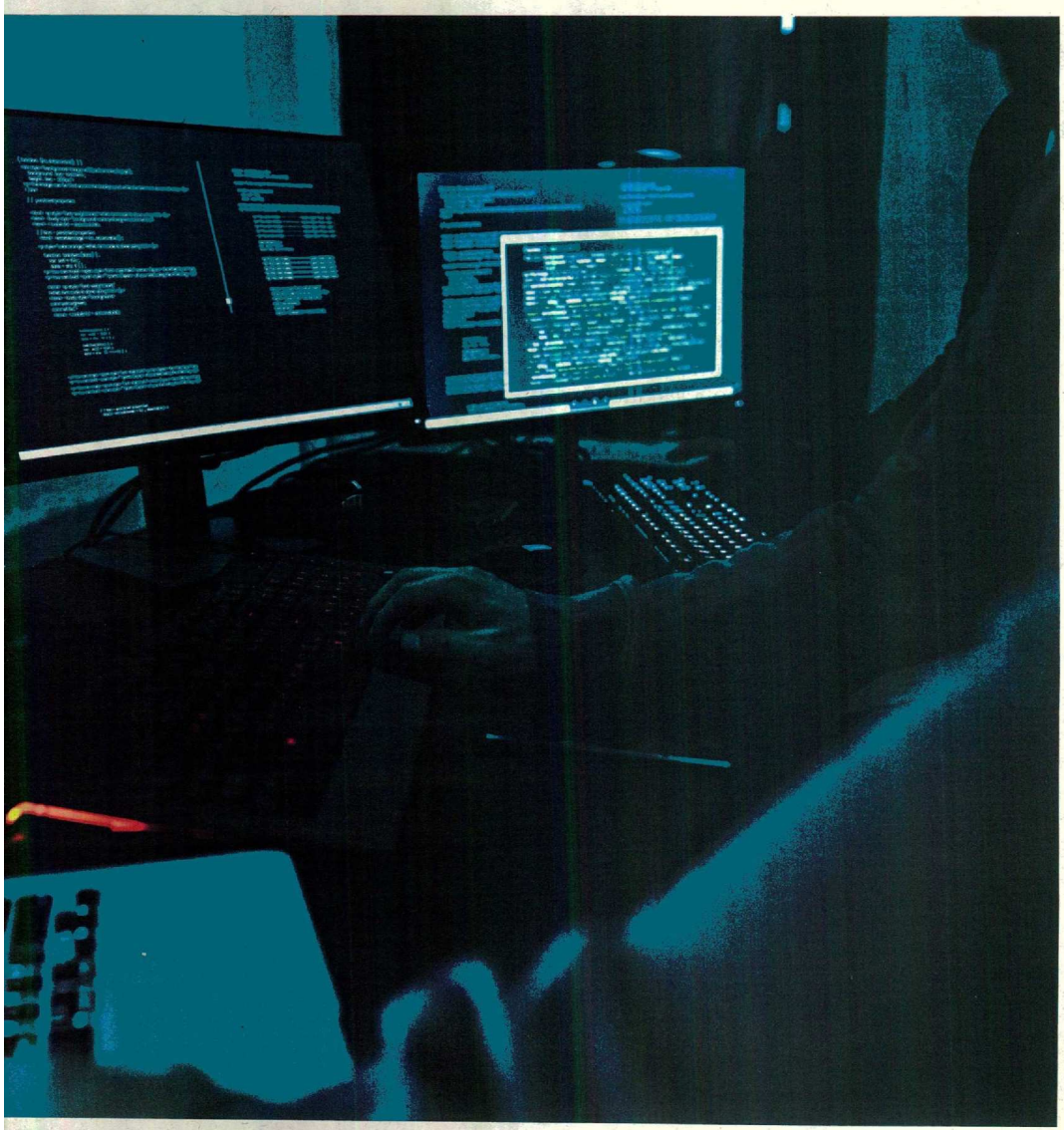
manchete

i

09-01-2019

Periodicidade: Diária
Classe: Informacão Geral
Âmbito: Nacional
Tiragem: 14000

Temática: Tecnologia
Dimensão: 4118 cm²
Imagem: S/Cor
Página (s): 1/2 a 5



De acordo com o RASI, em 2017 o Centro Nacional de Cibersegurança recebeu 1895 notificações de ataques no ciberespaço

DREAMSTIME

Em 2017, 719 ataques foram considerados crime. Mais 353 do que em 2010

Entidades públicas têm investido em prevenção e resposta, mas nem todas

deveriam, por princípio, ser os mais bem preparados e os mais seguros –, não haverá algo de errado com a estratégia de cibersegurança do país? Ao *i*, Nuno Ferreira Neves, Professor Catedrático do departamento de Informática na Faculdade de Ciências da Universidade de Lisboa – que oferece desde 2007 o Mestrado em Segurança Informática –, defende que "o país deu alguns passos importantes que visam melhorar a sua postura no campo da cibersegurança, que envolveram por exemplo a criação do Centro Nacional de Cibersegurança", ainda que "existam vários aspetos a melhorar, nomeadamente relacionados com a concretização no terreno de algumas das melhores práticas recomendadas internacionalmente".

A área, assinala o professor, debate-se com uma dificuldade premente: é que "existe atualmente uma carência significativa de recursos humanos especializados em segurança informática, o que torna muito difícil a contratação de peritos", em particular pelas forças de segurança, que não conseguem competir "em termos de salários com os valores praticados no setor privado". No entanto, reconhece, "tanto as forças na área da investigação criminal como as forças na área da defesa têm procurado melhorar as suas competências para lidar com atividades ofensivas no ciberespaço".

A investigação destes casos cabe à Unidade Nacional de Combate ao Cibercrime e a Criminalidade Tecnológica (UNC3T) e vão sendo alocados os investigadores necessários em cada momento, revela fonte ligada à investigação de cibercrimes que preferiu não ser identificada.

E as instituições públicas estão preparadas para lidar com ciberataques? O especialista da Faculdade de Ciências traça um retrato "heterogéneo", referindo que algumas organizações já investiram na "prevenção e resposta a ataques", enquanto outras ainda não deram esse passo.

A fonte que optou por não ser identificada tem igual percepção: "Há as que revelam alguma falta de segurança informática", diz.

Tendo em conta essa realidade, as autoridades agem em muitos casos de forma proativa e preventiva. "A PJ tem a atividade preventiva e proativa, esta última sobre casos em concreto. A preventiva tem que ver com alertas que a PJ desenvolve", explica a mesma fonte, lembrando que neste tipo de crimes é fundamental a cooperação internacional, salientando a da Europol e a da Interpol. Ainda assim, a mesma fonte nota que este tipo de ataques nem sempre são denunciados pelas entidades atingidas, que muitas vezes nem sequer se apercebem. "Há as duas situações: umas vezes as pessoas apercebem-se e denunciam e outras vezes é a PJ que nota e procede à investigação", esclarece.

Por sua vez, Nuno Ferreira Neves nota que a prevenção não é fácil. "Há um consenso entre os especialistas de segurança informática segundo o qual é extremamente difícil (ou impossível) defender totalmente um sistema complexo", diz. Ainda assim, há mecanismos que podem ser postos em prática: a autenticação, o controlo de acesso e a monitorização de sistemas são alguns exemplos.

** com Carlos Diogo Santos*