manchete

Diário Notícias	Periodicidade: **Semanal**
	Classe: **Informação Geral**
08-09-2022	Âmbito: **Nacional**
	Pagina(s): **1,4,5**

DOCUMENTOS PORTUGUESES DA NATO APANHADOS À VENDA NA *DARKWEB*

VIOLAÇÃO António Costa foi informado pelos Serviços de Informações norte-americanos de "ciberataque prolongado e sem precedentes". Dimensão dos estragos ainda está a ser averiguada. Suspeitas de quebra de segurança recaem em computadores do EMGFA, das secretas militares e do Ministério da Defesa. PÁGS. 4-5

manchete

Diário Notícias

08-09-2022

Periodicidade: Semanal
Classe: Informação Geral
Âmbito: Nacional
Pagina(s): 1,4,5

CIBERATAQUE

Documentos portugueses da NATO apanhados à venda na *darkweb*

DEFESA A dimensão dos estragos ainda está a ser averiguada pelo Gabinete Nacional de Segurança, mas as suspeitas da quebra de segurança que facilitou a exfiltração de documentos secretos da NATO recaem em computadores do EMGFA, das secretas militares e do MDN.

TEXTO **VALENTINA MARCELINO**

O Estado-Maior-General das Forças Armadas, comandado pelo chefe de Estado-Maior, almirante Silva Ribeiro, foi alvo de um "ciberataque prolongado e sem precedentes" que teve como resultado a exfiltração de documentos classificados da NATO. O governo português só soube porque foi informado pelos Serviços de Informações norte-americanos, através da embaixada em Lisboa, com uma comunicação que terá sido feita diretamente ao primeiro-ministro António Costa, no passado mês de agosto.

De acordo com fontes que estão a acompanhar o caso, considerado de "extrema gravidade", terão sido os ciberespiões da Inteligência norte-americana a detetar "à venda na *darkweb* centenas de documentos enviados pela NATO a Portugal classificados como Secretos e Confidenciais". Confrontada com esta informação, a porta-voz oficial da embaixada dos EUA em Lisboa, não desmente, limitando-se a afirmar: "Não comentamos assuntos da Inteligência".

Esta ciber-crise tem estado a ser gerida pelo gabinete de Costa, mas várias estruturas ligadas à segurança estão também ativamente empenhadas, como o Gabinete Nacional de Segurança (GNS) e as Secretas Externas (SIED) e Internas (SIS). No entanto, apesar de ter competências reservadas na investigação da cibercriminalidade, a Polícia Judiciária (PJ), pelo menos até à tarde de ontem, não tinha sido envolvida – questionada pelo *DN*, declinou comentar.

A NATO terá exigido explicações e garantias ao governo português e, na próxima semana, em representação de António Costa, deverão deslocar-se ao quartel-general da NATO, em Bruxelas, para uma reunião de alto nível no NATO *Office of Security*, o secretário de Estado da Digitalização e da Modernização Administrativa, Mário Campolargo, que tutela o GNS, e o próprio diretor-geral deste Gabinete, vice-almirante Gameiro Marques, que é responsável pela segurança das informações classificadas enviadas para o nosso país.

De acordo com várias fontes da Defesa ouvidas pelo *DN*, depois de terem sido alertados, os peritos do GNS e do Centro Nacional de Cibersegurança juntaram-se aos militares do Centro Nacional de Ciberdefesa, situado no EMGFA, e fizeram um rastreio completo a todo o sistema de comunicações interno da Defesa. Dessa primeira averiguação terão identificado computadores no EMGFA, nas secretas militares (CISMIL) e da Direção Geral de Recursos de Defesa Nacional, de onde foram exfiltrados os documentos, e constataram que tinham sido quebradas regras de segurança para a transmissão de documentos classificados. Isto porque, sublinham as mesmas fontes, estas entidades têm ligações seguras – o Sistema Integrado de Comunicações Militares (SICOM) – para receber e reencaminhar os documentos classificados, mas terão utilizado as linhas não-seguras.

"Foi um ciberataque prolongado no tempo e indetetável, através de *bots* programados para detetar este tipo de documentos, que depois ia sendo retirado em várias fases", explicou uma dessas fontes.

Questionado sobre esta crise e que medidas estavam a ser tomadas para garantir a confiança da NATO, fonte oficial de S. Bento assegura que "o governo pode garantir que o MDN e as Forças Armadas trabalham diariamente para que a credibilidade de Portugal, como membro fundador da Aliança Atlântica, permaneça intacta".

A mesma porta-voz de António Costa sublinha que "a troca de informação entre aliados em matéria de Segurança da Informação é permanente nos planos bilateral e multilateral. Sempre que existe uma suspeita de comprometimento de cibersegurança de redes de Sistema

ATAQUES INFORMÁTICOS

ANONYMOUS DIVULGAM DOCUMENTOS DO BANCO CENTRAL DA RÚSSIA

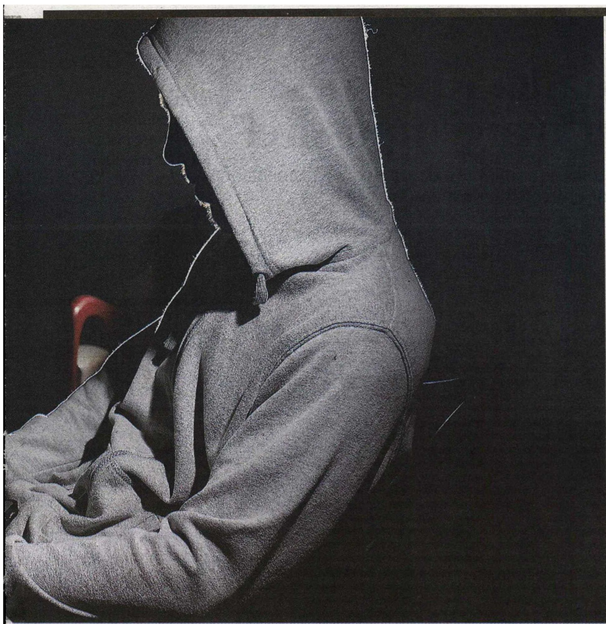
O grupo *Anonymous* publicou 28 *gigabytes* de documentos que obteve depois de invadir o sistema de segurança informático do Banco Central da Rússia. Os *hackers*, caracterizados pelo uso de máscaras, criaram vários *links* na internet que continham "segredos", advertindo Vladimir Putin de que estavam "em todo o lado: no seu palácio, onde come, na sua mesa, no seu quarto".

AMNISTIA INTERNACIONAL PORTUGAL SOFRE CIBERATAQUE

O *website* da Amnistia Internacional Portugal foi *hackeado* por um grupo de *hackers* defensores da Ucrânia, após um relatório da organização sobre a guerra que criticou Kiev por colocar a vida dos cidadãos em risco durante os combates contra a Rússia. O grupo de piratas informáticos acusou a ONG de colocar "em pé de igualdade a vítima e o criminoso".

HACKERS PRÓ-UCRÂNIA ATACAM CÂMARA MUNICIPAL DE SETÚBAL

A página da Câmara Municipal de Setúbal foi alvo de um ciberataque classificado por um grupo de *hackers* como "uma operação especial de ciberataques cirúrgicos à Rússia e seus aliados", depois da alegada receção de refugiados ucranianos em Setúbal por vários funcionários ligados ao Kremlin. O ataque deixou o *website* da autarquia desativado durante cerca de quatro horas.



GARQUIVO / DN - LOBAL IMAGENS

de Informação, a situação é extensamente analisada e são implementados todos os procedimentos que visem o reforço da sensibilização em cibersegurança e do correto manuseamento de informação para fazer face a novas tipologias de ameaça. Se, e quando, se confirma um comprometimento de segurança, a subsequente averiguação sobre se existiu responsabilidade disciplinar e/ou criminal automaticamente determina a adoção dos procedimentos adequados".

O Ministério da Defesa Nacional, por seu lado, salienta que "todos os ciberataques a qualquer entidade pública são objeto de coordenação estreita entre as entidades que, em Portugal, são responsáveis pela cibersegurança. Todos os indícios de tentativa de intrusão ou de potenciais quebras de segurança são averiguados e, se se verificar um incidente, as autoridades competentes são notificadas e os procedimentos adequados são desencadeados".

Por seu lado, o GNS remeteu a resposta sobre a sua ação para o gabinete do primeiro-ministro. Uma vez que a PJ não terá sido chamada, fica também por saber se foi instaurado algum inquérito interno para apurar responsabilidades nas entidades onde se presume que houve a quebra de segurança.

O Estado-Maior-General das Forças Armadas tem ligações seguras – o Sistema Integrado de Comunicações Militares (SICOM) – para receber e reencaminhar os documentos classificados, mas terão sido utilizadas linhas não-seguras.

Esse é, aliás, um dos poderes do GNS, que deve assegurar "a proteção e a salvaguarda da informação classificada emanada das organizações internacionais de que Portugal faça parte". Segundo a sua lei orgânica , compete-lhe, sempre que haja suspeita ou efetivo comprometimento, quebra ou violação de segurança, determinar a abertura de inquéritos de segurança e proceder à respetiva instrução, indiciar os seus responsáveis e participar, nos termos da lei, às entidades competentes.

Não é a primeira vez que Portugal se vê envolvido numa quebra de segurança de documentos da NATO. Aconteceu também no âmbito do processo do ex-espião do SIS, Carvalhão Gil – condenado por espionagem a favor da Rússia, em 2018 – quando foram detetadas falhas de segurança nas secretas na tramitação destes documentos. Portugal foi alvo de uma inspeção do já referido *NATO Office for Security*.

Victor Madeira, especialista em Segurança Nacional e investigador associado do *Centre for Information Resilience*, no Reino Unido, destaca que "este caso, mais uma vez, demonstra três pilares essenciais na luta contra atividades hostis no domínio ciber. O primeiro é haver uma vigilância e perceção situacional constantes, ambas atualizadas regularmente através de treino e equipamento de ponta para especialistas de talento neste ramo. Segundo, a importância fundamental de qualquer Estado, verdadeiramente soberano, possuir funções eficazes de contrainformações – tanto no domínio mais tradicional da espionagem humana, como também no domínio ciber. Sem este alicerce crítico, todas as outras funções de Estado e, eventualmente, a própria soberania, desmoronam-se. Finalmente, um terceiro pilar é a importância contínua de alianças e parcerias de Segurança e Defesa Nacional. Sem a colaboração constante entre serviços aliados de segurança e informações, o cenário de ameaças por atores hostis seria muito pior. Especialmente no domínio ciber, onde cada segundo é precioso."

Um despacho assinado pela ministra da Defesa , Helena Carreiras, no passado dia 5 de agosto, vem reforçar o cumprimento da Lei de Programação Militar, em matéria de Ciberdefesa. Determina que, de 2022 a 2030, sejam investidos 11,5 milhões de euros em "serviços de formação e consultoria especializados em ciberdefesa e na condução de operações militares no, e através do, ciberespaço".

valentina.marcelino@dn.pt

CASO EQUIFAX: "UMA DAS MAIORES VIOLAÇÕES DE DADOS DA HISTÓRIA"

A Equifax, uma empresa de gestão de crédito norte-americana, sofreu um ciberataque que comprometeu cerca de 143 milhões de dados de pessoas e quase destruiu a empresa, entre maio e junho de 2017. De acordo com o procurador-geral dos EUA, William Barr, esta foi "uma das maiores violações de dados da história". Quatro oficiais militares da China foram acusados como os culpados pelo ciberataque.

LAPSUS GROUP ATACA PÁGINAS DO GRUPO IMPRESA

O Grupo Impresa foi vítima de um ataque informático às suas páginas na internet, bem como o jornal *Expresso* e a estação televisiva SIC, por um grupo de *hackers* conhecido por Lapsus Group. "Os dados serão vazados caso o valor necessário não for pago. Estamos com acesso nos painéis de *cloud*. Entre outros tipos de dispositivos, o contacto para o resgate está abaixo", foi a mensagem divulgada pelo grupo de piratas informáticos. A Impresa classificou o sucedido como um "atentado nunca visto à Liberdade de Imprensa em Portugal na era digital" e apresentou queixa-crime.

ATAQUE INFORMÁTICO AFETA HOSPITAL GARCIA DE ORTA

O Hospital Garcia de Orta, em Almada, foi alvo de um ataque informático na noite de 26 de abril deste ano, tendo sido afetados os servidores da unidade hospitalar. Apesar de ter sido mantida "praticamente toda a atividade clínica", com exceção das consultas externas, o hospital admitiu algumas dificuldades nos serviços, tendo sido canceladas consultas, cirurgias e exames de imagem, como TAC e radiografias. Os registos clínicos foram assegurados em formato papel.

CIBERATAQUE "CRIMINOSO" PREJUDICA VODAFONE PORTUGAL

A operadora de telecomunicações Vodafone Portugal assumiu que foi alvo de um ciberataque de "ato criminoso" que levou à interrupção abrupta dos seus serviços, com o objetivo de tornar a rede indisponível, "com gravidade, para dificultar ao máximo o nível dos serviços", tendo afetado a rede Multibanco. De acordo com a empresa, os dados dos clientes não foram comprometidos.

PIRATAS INFORMÁTICOS PARAM SERVIÇOS DO MINISTÉRIO DA DEFESA

Alguns setores do Ministério da Defesa tiveram os seus serviços parados devido a um ciberataque que os atingiu no dia 27 de agosto de 2020. Este ataque teve como objetivo entrar nas contas de *e-mail* de vários funcionários intermédios, que estão instalados no edifício do ministério. No entanto, o ataque – DOS (*Denial of Service*) – acabou por não atingir os seus objetivos.