Expresso Online

País: PT
Âmbito: Informação Geral
OCS: Expresso Online

ID: 102361296 23/11/2022

Ciberataque à Segurança Social "visava a destruição" de bases de dados que são das mais valiosas para Portugal

URL: https://expresso.pt/life_style/ciencia/2022-11-23-Ciberataque-a-Seguranca-Social-visava-a-destruicao-de-bases-de-dados-que-sao-das-mais-valiosas-para-Portugal-0217bbfa

Ministério garante que não há indícios do comprometimento de dados de cidadãos, mas incidente revelado na segunda-feira deixa na memória um susto e um aviso: as bases de dados da Segurança Social são especialmente valiosas e, se alguma vez forem eliminadas, podem gerar disrupções à escala nacional

Os ciberataques costumam ser lançados para chegar ao lucro, mas a investida desta segunda-feira contra os sistemas que suportam a Segurança Social teve um objetivo diferente: "O ciberataque visava a destruição [de dados]", explicou ao Expresso fonte bem colocada, sob a condição de anonimato, e recusando fornecer mais detalhes. A confirmar-se a tese, a deteção atempada do ataque terá evitado um "apagão" de dados com potenciais efeitos nefastos para o dia-a-dia da população.

O Expresso apurou que, por via oficial e contactos oficiosos, que estão ser tomadas diferentes diligências para localizar e extrair potenciais códigos maliciosos que possam ter sido inseridos nas redes tuteladas pela Segurança Social. Estes procedimentos são comuns, mas especialmente importantes para se perceber quais as vulnerabilidades exploradas, os suspeitos da autoria do ataque ou a tomada de medidas que garantem que não existem mais códigos maliciosos comparáveis a cavalos de Tróia que poderão ser acionados, mais tarde, para levar a cabo novas vagas de ataque.

À semelhança daquilo que sucedeu no início da semana, o Ministério do Trabalho e da Segurança Social informa que tem vindo a trabalhar com a Polícia Judiciária (PJ) e o Centro Nacional de Cibersegurança (CNCS) na análise do ciberataque. Tanto o Ministério como as autoridades têm optado por não fornecer pormenores.

Não são revelados os serviços que foram alvo de ataque, nem há qualquer menção à reivindicação da respetiva autoria. Não é referida a data em que o ataque foi detetado, ou as estimativas quanto à data em que os cibercriminosos conseguiram levar a cabo a intrusão (que pode não ter sido detetada de imediato). Também tem havido especial cuidado para não revelar dados sobre a forma como se conseguiu detetar o ataque.

Apesar do teor genérico das respostas, o Instituto de Informática da Segurança Social (IISS) informa que foram tomadas as medidas necessárias para "garantir a segurança dos sistemas e respetivos dados, bem como cumpridas todas as obrigações legais em matéria de dados pessoais".

"Não há ainda indicações de que os cibercriminosos tenham alcançado os dados dos cidadãos", refere ainda uma das fontes consultadas pelo Expresso. Uma outra fonte nega que os cibercriminosos tenham conseguido aceder aos repositórios com informação do cidadãos. "Até à presente data, não existe qualquer evidência de ter existido acesso indevido a dados de cidadãos ou de empresas", refere também o IISS.

A base da soberania

As respostas sucintas de Governo e autoridades poderão estar relacionadas com uma estratégia de gestão de danos e com o facto de as bases de dados da Segurança Social serem um dos mais valiosos repositórios do País, uma vez que envolvem informação sobre baixas médicas e, eventualmente,

dados bancários, atividades profissionais, remunerações, subsídios e pensões, e ainda dados de identificação, contactos ou moradas - que vão do nascimento até ao óbito dos cidadãos, ou da constituição até ao fecho de empresas. Muito poucas bases de dados terão uma informação tão completa e valiosa sobre cada cidadão e empresa do País.

"A Segurança Social é uma organização que trata dados sensíveis ou categorias especiais de dados, como é o caso de dados de saúde ou sobre incapacidades, que merecem uma proteção reforçada", explica Luís Neto Galvão, especialista em privacidade e tecnologias que trabalha na SRS Advogados.

Histórico de prestações sociais, atribuição de habitação social com relatórios que descrevem situações económicas de famílias, gestão de dívidas ou acolhimento de refugiados são alguns dos exemplos de informação que poderá ser exfiltrada a partir das bases de dados da Segurança Social. "Nessa medida, devem existir medidas reforçadas de segurança. Um ataque que comprometa a integridade ou a disponibilidade destes dados pode pôr em causa o pagamento de prestações que são muito necessárias ou ainda o acolhimento de refugiados, por definição em situação de grande fragilidade", acrescenta.

Pedro Fortuna, especialista em cibersegurança e diretor de tecnologias da empresa Jscrambler, admite que, se for bem sucedido, um ataque à Segurança Social permite extrair dados ainda mais pormenorizados que aqueles que, eventualmente, seria possível obter nos serviços da Autoridade Tributária. "No caso da Segurança Social é, se calhar, pior, pois tem também informação relativa à saúde do utente, como doenças associadas a baixas, ou informação relativa a invalidez", lembra.

Fortuna lembra ainda que a informação que consta nas bases de dados da Segurança Social, "por ser muito detalhada, é muito útil para fazer ataques de phishing e comprometer os dispositivos das vítimas".

Os ataques de phishing podem ser desencadeados de várias formas - mas as mais conhecidas recorrem a códigos maliciosos que pretendem intercetar senhas ('passwords') e nomes de utilizador usados nos vários serviços usados na Internet - em especial contas bancárias. Caso alguma vez consigam aceder às bases de dados da Segurança Social, os denominados hackers ficam em posição de lançar estratagemas de phishing com maior probabilidade de sucesso, pois passam a ter conhecimento de contactos e assuntos que mais interessam às potenciais vítimas.

No segmento empresarial, além de estratagemas que visam o lucro, há o risco de fuga de informação que possa ser usada para chegar às empresas que suportam infraestruturas críticas.

E, se alguma vez forem extraídos ou forem vendidos na Darkweb, os riscos são multiplicados pelo número de intervenientes mal intencionados que tiverem acesso à informação. Um verdadeiro pesadelo para qualquer especialista em cibersegurança. "Estes dados não são apenas valiosos para cibercriminosos. Podem também ser muito úteis para outros estados que queiram ter informação sensível sobre os nossos cidadãos. Portanto, perder dados desta natureza é uma ameaça à nossa cibersoberania", avisa Pedro Fortuna, quando questionado sobre a importância dos repositórios da Segurança Social.

Até à data, não há notícia de extração de dados dos cidadãos. E as notícias avançadas por CNN Portugal e Observador na segunda-feira referem que o alerta começou a circular através de um e-mail interno que solicitava aos profissionais da Segurança Social que procedessem a alteração de senhas. O pedido de mudança de passwords confirma que, possivelmente, a autenticação usada pelos profissionais da Segurança Social poderá ter sido posta em causa. Os próximos tempos tratarão de revelar mais dados sobre a extensão dos danos.

Hugo Séneca

Hugo Séneca