Hackers alegam ter exposto dados roubados ao Porto de Lisboa

eco.sapo.pt/2023/01/18/hackers-alegam-ter-exposto-dados-roubados-ao-porto-de-lisboa

Flávio Nunes 18 de janeiro de 2023

Um grupo de *hackers* diz ter **publicado a informação alegadamente roubada ao Porto de Lisboa no ciberataque que ocorreu em dezembro**, apurou o ECO. Os burlões dizem que entre essa informação estão relatórios financeiros, orçamentos e auditorias, bem como dados pessoais de clientes e trabalhadores, correspondência eletrónica e outra documentação.

Contactada pelo ECO, fonte oficial do Porto de Lisboa não quis fazer comentários adicionais e remeteu esclarecimentos para os comunicados divulgados a 26 de dezembro e 6 de janeiro.

No primeiro comunicado, a administração **confirma ter sido "alvo de um ataque informático,** tendo sido rapidamente ativados todos os protocolos de segurança e medidas de resposta previstas para este tipo de ocorrências, estando garantida a atividade operacional" da infraestrutura.

Dias depois, já em janeiro, o Porto de Lisboa deu conta de que **o ataque foi do tipo *ransomware*.** Ou seja, os *hackers* terão roubado informação à empresa e exigido um resgate para não a divulgar.

"Tratou-se de um ataque de *ransomware*, um *software* malicioso usado para bloquear dados através de sistemas de criptografia. **Este ataque provocou a encriptação de diversa informação,** o que criou constrangimentos nos sistemas informáticos e aplicações internas da APL – Administração do Porto de Lisboa, estando os serviços administrativos a retomar a total normalidade e tendo já sido reestabelecido o portal do Porto de Lisboa", lia-se na nota.

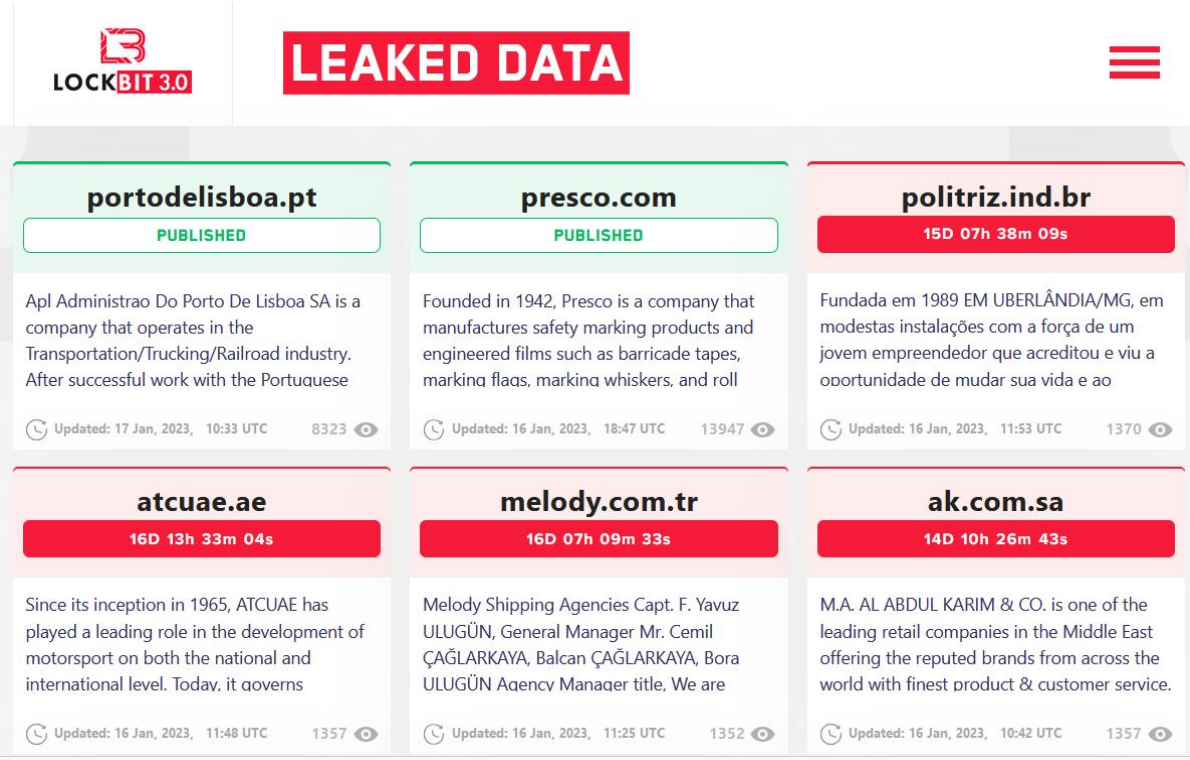
A empresa admitiu também **ter "conhecimento da existência de dados na *dark web* e de um pedido de resgate**, mantendo ativos todos os protocolos de segurança previstos nestas situações". A *dark web* é uma parte da internet que não está imediatamente acessível à generalidade da população e onde tende a ocorrer este tipo de atividade ilícita.

O ECO não pôde verificar a autenticidade da informação que os *hackers* alegam ter exposto, **pelo que não é possível afirmar com certeza que dados do Porto de Lisboa foram mesmo divulgados.** No entanto, as alegações dos atacantes são claras e o método a que recorrem – o sequestro de dados e pedido de resgate – tem sido amplamente reportado a nível mundial.

Na *deep web*, num portal onde são publicados estes pedidos de resgate, o ECO constatou que o grupo de atacantes alega ter roubado a informação à empresa **e deu até 18 de janeiro para não a tornar pública**. A página permite uma de três coisas: pagar 1.000 dólares para estender o prazo por mais 24 horas; pagar 1,5 milhões para destruir toda a informação; ou pagar 1,5 milhões para descarregar a informação "a qualquer momento". Os pagamentos são feitos em criptomoedas.

- 

Captura de ecrã do pedido de resgate e indicação de que os dados foram publicados

- 

A plataforma também mostra outras entidades que foram atacadas

Na terça-feira, um dia antes do prazo, o relógio desapareceu e passou a exibir a indicação "publicado", **incluindo um suposto *link* para descarregar os alegados dados**. Os *hackers* divulgaram também algumas imagens do que dizem ser informação privada roubada no ataque, incluindo um recibo de vencimento, contratos e outros documentos (cuja autenticidade também não pôde ser validada pelo ECO).

De acordo com Bruno Castro, CEO da VisionWare, uma empresa de cibersegurança, a indicação LockBit 3.0 que surge associada ao pedido de resgate é "um dos *malwares* utilizados" neste tipo de ataques de *ransomware*. "Há várias variantes. **Através desse *malware*, podemos associar a um grupo de cibercriminosos específico.** É *malware* recente e não será possível de recuperar [os dados] através de mecanismos de desencriptação", explica ao ECO.

Em dezembro, o Porto de Lisboa referia que **"o caso está a ser acompanhado pelo Centro Nacional de Cibersegurança e pela Polícia Judiciária**, estando a APL a trabalhar em permanência e estreita articulação com todas as entidades competentes, no sentido de garantir a segurança dos sistemas e respetivos dados". "Temos uma equipa experiente de profissionais de cibersegurança que estão já a acompanhar o caso, em conjunto com as autoridades competentes, e a realizar uma investigação aprofundada para perceber e ultrapassar a situação", referia ainda a empresa.