



Jornal Notícias

22-10-2019

Periodicidade: Diário

Classe: Informação Geral

Âmbito: Nacional

Tiragem: 60963

Temática: Justiça

Dimensão: 1441 cm²

Imagem: S/Cor

Página (s): 1/14

Hackers sequestraram mais de 30 organismos públicos só neste ano

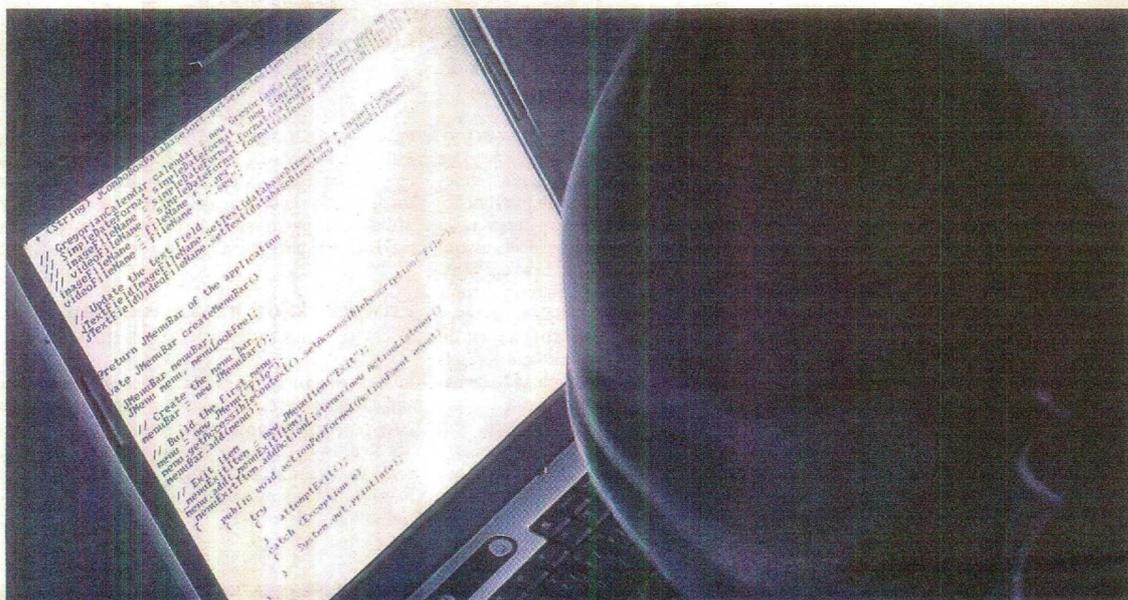
Piratas informáticos exigem resgates após ataques a câmaras, juntas e escolas

Autarquia de Vinhais tenta recuperar dados desde a semana passada

Página 14

JUSTIÇA

Dezenas de câmaras e juntas atacadas por piratas desde janeiro



Autores dos ataques operam normalmente a partir do estrangeiro e são muito dificilmente detetáveis.

PORMENORES

“WannaCry” lançou caos em todo o Mundo. O vírus “WannaCry” foi usado no maior ataque de “ransomware”, lançado em todo o Mundo, em 2017. Obrigou todos os serviços do Estado, em Portugal e em muitos outros países a blindar ou desligar os sistemas informáticos e a condicionar as comunicações para evitar infeções e sequestro que resultavam em pedidos de resgate. Empresas e serviços vitais como hospitais, transportes ou fornecimento de energia foram também atacadas.

“Nomoreransome” O site “nomoreransome.org” presta ajuda aos internautas para prevenir casos de extorsão e recuperar o acesso. Permite, em alguns casos, decifrar dados.

Entre os organismos públicos vítimas de pedidos de resgate há ainda agrupamentos de escolas. “Hackers” pedem dinheiro para devolver dados

Alexandre Panda, António Soares e Glória Lopes
 justica@jn.pt

CIBERCRIME Desde o início do ano, mais de três dezenas de organismos públicos foram alvo de “hackers” que conseguiram sequestrar os sistemas informáticos de câmaras municipais, juntas de freguesia ou agrupamentos de escolas, entre outros, para exigir um resgate. O último caso conhecido é o da Câmara Municipal de Vinhais, que se debate há exatamente uma semana para tentar recuperar os dados, capturados pelos piratas.

O fenómeno, chamado “ransomware” afeta sobretudo empresas, mas não está agora a poupar os organismos públicos. Os atacantes usam software nocivo para se apoderarem de sistemas e ficheiros,

exigindo aos utilizadores um resgate, muitas vezes em bitcoins (moeda virtual), para acabar com o “sequestro”.

Normalmente, os piratas lançam ataques massivos a várias entidades públicas e privadas. Sob a forma de e-mails, o “vírus” chega ao computador de um ou mais funcionários que, sem dar conta da ameaça, os abrem. O pirata de nada mais precisa para ter acesso a toda a rede informática da organização e começar a copiar todos os dados que ela contém, e blindá-los. Quando acaba a operação, manda uma mensagem à vítima, exigindo dinheiro para enviar a “chave” que permite descifrar (libertar) os dados.

Questionado pelo JN, o Centro Nacional de Cibersegurança (CNCS) adiantou que, desde o início do ano, registou 21 casos de “ransomware”, incluindo o de Vinhais, sem distinguir entre Estado e empresas, ressalvando “que os números indicados espelham os incidentes reportados ao CNCS ou de que o CNCS teve conhecimento, e não o panorama geral ao nível nacional”.

De acordo com informações recolhidas pelo JN, a Unidade Nacio-

nal de Combate ao Cibercrime e à Criminalidade Tecnológica (UNC3T) tem investigado mais de 30 casos, entre eles Vinhais, para o qual não existe ainda uma data de resolução total.

Na autarquia transmontana já foram recuperados ficheiros danificados pelo ataque pirata, mas o controlo do sistema informático não foi ainda recuperado e o mesmo ainda não se encontra a funcionar. Uma fonte do município adiantou que a empresa que tem procurado resolver o problema estava a tentar detetar qual o computador que terá sido infetado com o vírus e contaminou os restantes. Há pelo menos 11 tipos de ataques “ransomware” catalogados. O ataque pirata com software nocivo que encriptou dados do município, detetado na manhã de terça-feira, obrigou a autarquia a gastar cerca de seis mil euros para o solucionar. Os “piratas” pediam um resgate de valores bem mais elevados, entre 20 e 30 mil euros.

Os serviços municipais nunca pararam, apesar de terem sido obrigados a reajustar alguns procedimentos, voltando os funcionários, sempre que possível, a trabalhar normalmente e com papel. ●

RASI

Mais ataques a afetar organismos do Estado em 2018

Em 2018, o Centro Nacional de Cibersegurança reportou para o Relatório Anual de Segurança Interna (RASI) um aumento na casa dos 0,8% dos ataques a sistemas informáticos com consequências para o Estado. Nesse período, foram recebidas 2456 notificações de todo o tipo de ataques, das quais 629 resultaram na abertura de incidentes analisados e resolvidos. Destes, mais de uma centena afetaram direta ou indiretamente organismos do Estado. A recolha de informação sensível, a introdução de vírus e as tentativas de intrusão foram os principais tipos de ameaças detetadas, segundo o RASI.