manchete

Público

06-02-2015

Periodicidade: Diário
Classe: Informacão Geral
Âmbito: Nacional
Tiragem: 51453

Temática: Justica
Dimensão: 513
Imagem: N/Cor
Página (s): 11

PJ investiga máfias de Leste que atacaram sistemas informáticos de escolas e ministérios

Criminalidade

Pedro Sales Dias

Suspeitos tomam controlo dos dados que encriptam e exigem dinheiro para devolver o acesso à informação

A vaga de ataques aos sistemas informáticos de empresas portuguesas, com a exigência às vítimas de resgates em Bitcoins (moeda virtual) para repor o acesso aos dados encriptados, já afectou escolas e todos os ministérios do Governo, adiantou ao PÚBLICO fonte da PJ. À Judiciária, que investiga a situação através da unidade especialista no combate ao cibercrime, chegaram 20 queixas referentes à zona de Lisboa.

Ao contrário do que foi noticiado, esta situação não está a ser levada a cabo por piratas informáticos (que habitualmente apenas roubam os dados), mas por grupos organizados do Leste europeu que pretendem extorquir dinheiro. Fonte da PJ sublinhou, por isso, estarem em causa crimes de extorsão através de meios informáticos levados a cabo por máfias.

O Ministério da Educação e Ciência (MEC) garantiu, porém, não terem sido reportados este ano ataques aos sistemas das escolas. "No ano passado registou-se uma ocorrência [que afectou o sistema de uma escola] com pedido de resgate (não em Bitcoins, mas similares)", acrescentou o MEC adiantando que a situação foi reportada às autoridades. Fonte do gabinete do primeiro-ministro garantiu que os sistemas dos ministérios estão neste momento a funcionar correctamente sem registo de ataques.

Em Setembro de 2014, foram detidos dois ucranianos numa grande operação policial em Madrid, Espanha. Também então estava em causa um esquema que incluía o recurso a Bitcoins e que terá afectado 21 mil empresas de 80 países, 1500 delas em Espanha.

Em Portugal também foram afectados técnicos de contas, advogados e contabilistas. Algumas das vítimas terão pago resgates na ordem dos mil euros. Nuns casos, recuperam os dados, noutros não, apesar de cederem à exigência. A nova vaga de ataques terá começado no início deste ano, mas a maioria das queixas é referente já ao ano passado. Nos restantes países europeus, esta tentativa de extorsão por meios informáticos já foi detectada pelas autoridades há cerca de três anos.

Tudo começa com o envio de um *email* suspeito, normalmente intitulado "mensagem de fax". Se o ficheiro em anexo (com a extensão .zip) for aberto pelo receptor, o computador fica remotamente acessível ao grupo. Os dados são todos encriptados e o dono do computador deixa de ter acesso a estes. Se o computador estiver ligado a uma rede, os restantes computadores e servidores podem ficar expostos. Após os dados serem encriptados, é enviada uma mensagem em inglês exigindo o pagamento de um resgate. Segue-se outra mensagem que explica onde se podem adquirir Bitcoins. A moeda virtual é utilizada como pagamento em alguns *sites* e não deixa rasto. O grupo desbloqueia parte da informação encriptada para provar à vítima que tem a possibilidade de resolver a situação mediante o pagamento.

Segundo a PJ, o grupo explora duas fragilidades nos computadores: o facto de o acesso remoto estar ligado e de os *backups* automáticos estiverem activados, embora neste caso os investigadores ainda não tenham conseguido apurar com exactidão essa fragilidade.