esquerda.net

Published on *Esquerda* (http://www.esquerda.net)

Os ataques informáticos podem (e devem) ser travados

Author(s):
Pedro Filipe Soares [1]
Show Author Info?:
0

Parece uma história saída de um filme de ficção científica: um grupo de piratas informáticos consegue criar um vírus superpoderoso, capaz de se infiltrar em qualquer computador, ameaçando lançar o caos no mundo caso não seja pago um resgate milionário. Ora, mais uma vez a realidade passou a perna ao grande ecrã.

Em meados do mês de maio fez-se história pelos piores motivos: aconteceu o primeiro grande ataque informático à escala mundial. E, claro, seguiu a narrativa cinematográfica. O vírus foi batizado de *Wanna Cry* e fez muita gente chorar no dia em que se apresentou à sociedade. Espalhou-se pelas redes rapidamente e "raptou" ficheiros indiscriminadamente. Para que as pessoas ou empresas pudessem recuperar os seus ficheiros era exigido o pagamento de centenas de euros através de uma moeda virtual, a *bitcoin*. Por isso se chama a este tipo de software maligno um *ransomware*: exige o pagamento de um resgate para reatar o acesso à informação que tenha sido infetada.

O resultado do ataque com o vírus *Wanna Cry* foi assustador. Espalhou-se pelas redes de 150 países e atingiu os sistemas de mais de 200 000 empresas. Um exemplo do risco que se correu com este ataque foi o do Serviço Nacional de Saúde inglês. Na sequência do acontecimento, houve blocos operatórios em risco, impossibilidade de acesso a dados clínicos dos pacientes ou a resultados de análises. Demorou vários dias para o sistema regressar à normalidade e, mesmo assim, há dados que foram considerados irrecuperáveis.

O nosso país não passou à margem desta ameaça: A PT confirmou que tinha sido atacada e deu ordens aos seus trabalhadores para se desligarem da rede interna, enquanto a EDP, a NOS, o BCP, a Caixa Geral de Depósitos e a SIBS também avançaram com medidas de prevenção especiais.

A característica fundamental deste *ransomware* foi a forma veloz e escala, nunca vistas, como se propagou. O dado arrepiante deste processo é que a vulnerabilidade do sistema operativo, que permitiu a propagação do vírus, já era há muito conhecida pela Agência de Segurança Nacional norte-americana (NSA, no seu acrónimo em inglês). Era conhecida e explorada por esta agência para poder espiar computadores pelo mundo fora. Só que o código informático foi roubado à NSA e acabou por cair nas mãos dos *hackers* que realizaram o ataque. Só na altura em que o código foi roubado é que a NSA alertou o fabricante de *software* para a vulnerabilidade no seu sistema. A ação da NSA colocou-nos a todos em risco.

Um dos responsáveis da Microsoft compara a situação resultante da falha de segurança da NSA com o roubo de mísseis do exército norte-americano. E a coisa não é para menos. A agência de espionagem não denunciou a vulnerabilidade do sistema operativo porque a usava para seu próprio proveito. "O mais recente ataque representa uma ligação não intencional, mas preocupante, entre as duas formas mais graves de ameaça à cibersegurança - a ação do Estado-nação e a ação do crime organizado", dizia esse responsável. Tem toda a razão. Há mesmo motivo para não estarmos descansados e exigirmos uma mudança radical nesta atitude.

Vários governos, com os Estados Unidos da América à cabeça, estão a investir milhões na procura por vulnerabilidades em programas e sistemas operativos. O mesmo objetivo está a ser perseguido por corporações privadas e até organizações criminosas. É a corrida ao armamento no mundo virtual que, como se vê, poderá ter efeitos devastadores numa sociedade cada vez mais dependente de sistemas informáticos ou redes de telecomunicações. E estas armas são muito valiosas no mercado negro, onde também são transacionadas.

Ainda esta semana um sósia do *Wanna Cry* assustou o mundo. O foco principal do ataque sentiu-se na Ucrânia, onde foi derrubado o sistema informático do governo, bancos, e até do aeroporto. Mas, mais uma vez a situação alastrou-se por todo o mundo. Em Portugal, os Serviços Partilhados do Ministério da Saúde desativaram o serviço de *e-mail* e o acesso à internet.

A guerra virtual está a bater-nos à porta com cada vez mais violência e armas mais potentes. Exige-se uma mudança de atitude em prol da cibersegurança. A criação de uma convenção internacional que obrigue à denúncia de vulnerabilidades de sistemas informáticos é uma urgência. Mas é apenas um primeiro passo. No mundo dos serviços partilhados, da *cloud*, da desmaterialização de processos, temos de garantir uma proteção dos dados pessoais, dos processos e dos sistemas muito mais exigente. Estamos à altura? Parece-me que ainda há muito a fazer.

Artigo publicado no ?Diário de Notícias? a 29 de junho de 2017

Sumário da Home:

A guerra virtual está a bater-nos à porta com cada vez mais violência e armas mais potentes. Exige-se uma mudança de atitude em prol da cibersegurança.

Lead:
A guerra virtual está a bater-nos à porta com cada vez mais violência e armas mais potentes. Exige-se uma mudança de atitude em prol da cibersegurança.

Sobre o/a autor(a):

- Biblioteca
- Agenda
- Jornal Esquerda
- Blogosfera
- Comunidade
- Revista Vírus
- Wikifugas
- Ficha Técnica

Source URL: http://www.esquerda.net/en/node/49482

Links:
[1] http://www.esquerda.net/en/node/91