BLACK CASE

Hospital do Câncer de Barretos

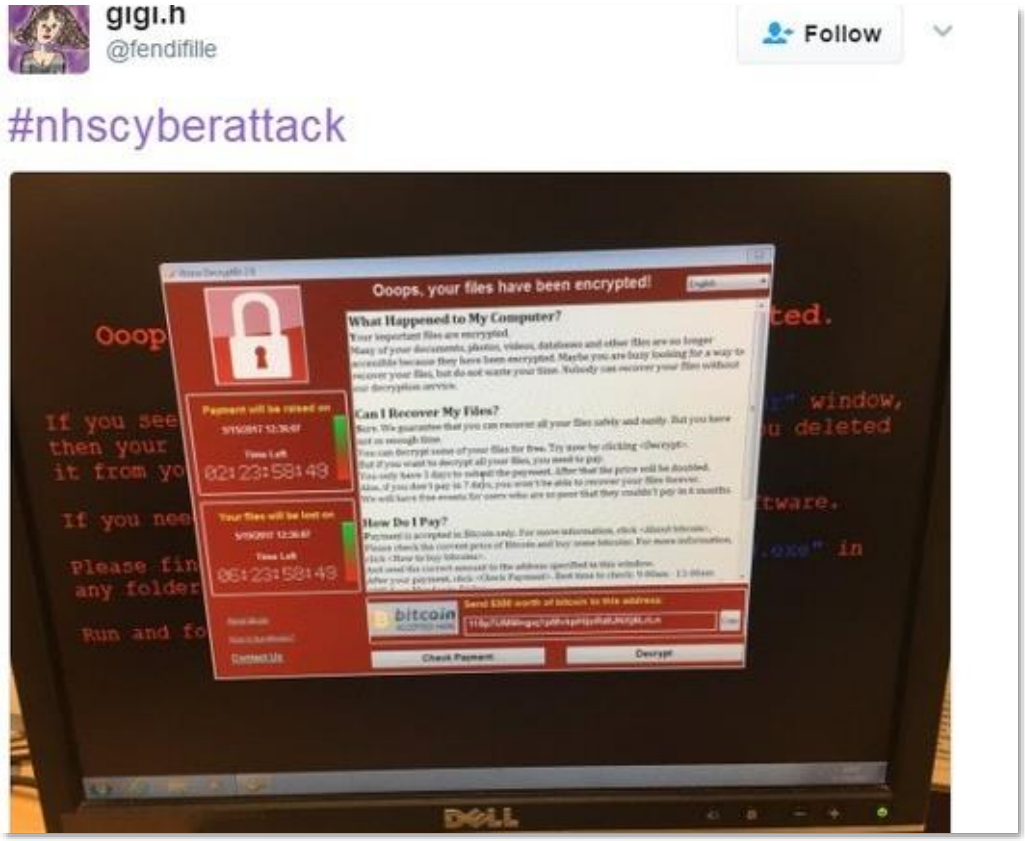
A tecnologia por trás de mais um mega-ataque cibernético global

UOL DIVEO

27/06/2017

A tecnologia por trás de mais um mega-ataque cibernético global

Em nova onda de sequestros digitais, hackers afetam computadores de empresas em diversos países, incluindo o Brasil



Tela de um ataque de ransomware. É o segundo em escala global em 2017 (Foto: Reprodução/ Twitter)

Uma variante de ransomware, chamada de NotPetya, um tipo de vírus que sequestra dados digitais, está afetando grandes empresas em dezenas de países neste momento. As primeiras estimativas colocam o ciberataque como potencialmente maior do que o WannaCry, que ocorreu no mês de maio.

O vírus se instala nas máquinas de empresa, reinicia o sistema e bloqueia o acesso. Para liberar, os hackers pedem o pagamento de US$ 300 em moeda virtual Bitcoin.

O ataque partiu de hackers russos, segundo empresas de segurança que divulgaram as informações preliminares. Até agora, a Ucrânia foi o país mais atingido pelo ransomware, que afetou departamentos do governo, o sistema bancário, a rede de metrô, além do aeroporto de Kiev. Mas há relatos de empresas que pararam no Brasil, na Rússia, no Reino Unido, na Espanha, na Holanda e na Dinamarca.

No Brasil, o Hospital do Câncer e a Santa Casa de Barretos, no interior de São Paulo, foram afetados. Na página no Facebook do Hospital do Câncer, a instituição diz que as unidades de Jales, em São Paulo, e de Porto Velho, em Rondônia, além dos Institutos de Prevenção da unidade foram vítimas do ataque cibernético. Devido ao incidente envolvendo um vírus de computador alguns atendimentos foram suspensos nas unidades afetadas.

Ao redor do mundo, a empresa de logística portuária Maersk, o gigante de publicidade WPP e a companhia francesa Saint-Gobain confirmaram que foram hackeados.
Esta nota será atualizada à medida que novas informações surgirem sobre os ataques.

No último mês de março, publicamos aqui no Experiências Digitais a reportagem "O crime quase perfeito", mostrando o avanço do ransomware, nome dado a esse tipo de ataque envolvendo sequestro de dados digitais. O ransomware ocorre quando um hacker invade o computador, o smartphone ou algum dispositivo conectado à internet, bloqueia informações por meio de criptografia. Se o dono das informações quiser vê-las novamente, precisa pagar um resgate, ransom, em inglês.

Fonte: http://epoca.globo.com/tecnologia/experiencias-digitais/noticia/2017/06/tecnologia-por-tras-de-mais-um-mega-ataque-cibernetico-global.html

O PLANO DETALHADO DO SEQUESTRO DIGITAL

Como funcionam os ataques de ransomware e por que é tão difícil rastrear os criminosos

1 ATAQUE

Como funciona o ransomware

O hacker invade o computador da vítima, normalmente após ela clicar num link malicioso

O criminoso copia os dados para um servidor externo protegido por um código e torna os arquivos do computador da vítima inacessíveis

A vítima vê os arquivos, mas o computador não reconhece a extensão. Para reaver os dados, é preciso usar um código enviado pelos criminosos

Os criminosos enviam links com tutoriais de como fazer o pagamento usando a moeda virtual bitcoin. Há até SACs dedicados a facilitar o pagamento

2 INFECÇÃO

Como hackers encontram suas vítimas

PHISHING
Os criminosos enviam e-mails ou mensagens com links maliciosos. Ao clicar neles, a máquina é infectada

POR PÁGINAS INFECTADAS
Muitos anúncios espalhados pela internet escondem links maliciosos

DOWNLOAD DE SOFTWARE
Sites para baixar programas, apps e filmes piratas estão repletos de vírus

PEN DRIVE
Criminosos deixam pen drives perto de escritórios. Quem acha e usa o dispositivo acaba infectando a rede

3 OPÇÕES DA VÍTIMA

Como proceder depois que o ataque ocorre

IGNORAR O ATAQUE
Quem tem cópias dos dados (ou não precisa deles) pode ignorar o ataque e remover o vírus

ENCONTRAR UMA CHAVE
Há um consórcio de empresas de segurança digital que liberam senhas para recuperar arquivos criptografados por criminosos. É necessário, porém, que o servidor usado pelo hacker já tenha sido alguma vez descoberto e "derrubado" por empresas de segurança ou autoridades

PAGAR
Uma parte das vítimas paga, porque o valor do resgate é baixo ou por temer ameaças, como divulgação de fotos íntimas


4 IMPUNIDADE
Por que os criminosos não são descobertos
000.000.0.00
IP MASCARADO
Os hackers mudam seu endereço de IP, ou seja, sua localização, a fim de confundir autoridades
PAGAMENTO EM BITCOIN
Os hackers pedem que a vítima pague em moeda virtual, mais difícil de ser rastreada