12 de maio de 2017, algum computador na Europa...

Em 12 de maio de 2017 começaram relatos de ataques de ransomware em computadores do NHS (UK)

Em poucas horas sistemas Windows foram atacados em vários países da Europa.

Em pouco tempo a praga cruza o oceano fazendo vítimas nas Américas, inclusive no Brasil.

Observa−se um número incomum de "probes" na porta 445/tcp tanto em IPv4 quanto em IPv6.

Nesse mesmo dia, Marcus Hutchins, aka MalwareTech, do UK, descobriu que o wannacry tenta resolver o curioso nome *iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com*

Hutchins registrou o domínio e notou que ele funciona como uma chave de desligamento do wannacry.

Por que um malware teria uma chave de desligamento?

1. para ser parado por controle remoto?

2. (mais provável) para evitar que fosse analisado em ambiente controlado.

Pouco tempo depois, Adrien Guinet, francês, descobriu que o wannacry deixava intactos na memória dados suficientes para quebrar−lhe a criptografia e publicou um destravador para o velho Windows−XP.

O susto maior passou, mas fica a pergunta:

O QUE FIZEMOS DE TÃO ERRADO?

O QUE FIZEMOS DE TÃO ERRADO?

1. não manter software atualizado. A Microsoft havia lançado remendos contra as vulnerabilidades exploradas pelo wannacry, mas poucos sistemas foram atualizados;

2. não configurar firewalls adequadamente. CIFS/SMB são serviços que só fazem sentido em redes internas, não há porque disponibilizá−los para a Internet!

3. backup, backup, backup!
   prevenção e canja de galinha só fazem mal à galinha!

No final, tivemos muita sorte, se a chave de desligamento não tivesse sido encontrada e não se descobrisse como decifrá−lo, o mundo ainda estaria em pânico como na manhã do dia 12.