Sequestro digital do WannaCry não rouba dados; entenda o ransomware

O vírus de resgate *WannaCry* não é programado para roubar as informações das vítimas. O código não prevê o envio dos arquivos criptografados para os chamados "servidores de controle" - as máquinas que enviam comandos a cada computador infectado pelo vírus. O que a praga envia aos criminosos é uma chave criptográfica gerada durante a infecção.

Mesmo que a vítima do vírus decida pagar para ter os seus arquivos de volta, os dados não são enviados para os criminosos. Apenas a chave criptográfica gerada pelo próprio vírus precisa ser transferida para os golpistas. Os criminosos usam uma chave em posse deles para decifrar essa chave criada pelo vírus e a devolvem para a vítima, permitindo que o vírus recupere ele mesmo os arquivos da vítima.

Em outras palavras, o vírus gera uma chave para criptografar os arquivos da vítima ("chave do vírus") e depois criptografava esta chave com outra chave controlada pelos criminosos ("chave-mestra"). O vírus faz uso da chamada "criptografia assimétrica", o que significa que ele pode criptografar algo de modo que só a chave-mestra pode abrir sem de fato possuir a chave-mestra. Isto é o que dificulta a recuperação dos dados.

Esse método de operação dispensa o armazenamento de dados detalhados sobre cada vítima. Tudo que é necessário para recuperar os arquivos está no próprio computador infectado.

Embora o vírus não tenha sido criado com a intenção de roubar informações das vítimas, a praga consulta "centrais de controle", que dá aos criminosos a possibilidade de enviar comandos às máquinas contaminadas. Na prática, o vírus parece funcionar mesmo sem instruções específicas.

Segundo as análises de especialistas, o vírus é capaz de usar dois códigos desenvolvidos pela Agência de Segurança Nacional dos Estados Unidos (NSA). Na agência, os códigos eram conhecidos como "*DoublePulsar*" e "*EternalBlue*". O *EternalBlue* permite ao vírus se espalhar automaticamente de um computador para outro, caso a vítima utilize o Windows 7 ou Windows Server 2008 e não tenha aplicações as correções da Microsoft de março.

Já o "*DoublePulsar*" permite o acesso remoto da máquina e tem a particularidade de não usar arquivos -- ele reside exclusivamente na memória. Assim, mesmo que os arquivos da contaminação do *WannaCry* sejam removidos, o computador ainda precisa ser reiniciado para garantir uma limpeza da memória onde o *DoublePulsar* reside.

O *DoublePulsar* está ativo na internet desde abril e já teria atacado cerca de 500 mil computadores, segundo a empresa de segurança *BinaryEdge*.

Segundo a "BBC", uma análise das carteiras de *bitcoin* usadas para a receptação do dinheiro revela que apenas US$ 60 mil (R$ 187 mil) foram arrecadados com resgates. Como o vírus solicita um mínimo de US$ 300 por vítima, isso indicaria que cerca de 200 pessoas teriam pago

pelo resgate, cerca de 0,1% das 217 mil vítimas contabilizadas pelo especialista em segurança "*Malwaretech*".

Fonte: g1.com.br

.