A INDÚSTRIA DO Ransomware

Apenas **34%** das empresas brasileiras reconhecem a séria ameaça que os ransomwares representam[2]

O Locky é um tipo de crypto-ransomware que em apenas **1 DIA** de fevereiro registrou **90.000** infecções[1]

50 novas famílias de ransomware foram identificadas no 1º trimestre de 2016[1]

FBI estima que até o final de 2016 a indústria do ransomware terá gerado **1 BILHÃO** de dólares para os cibercriminosos

BRASIL é o país mais afetado na América Latina, seguido por Costa Rica, Chile, Argentina e Colômbia[2]

Infraestrutura operacional do ransomware Locky

SITES DE DISTRIBUIÇÃO

Sites legítimos são invadidos (usando Bots ou Worms) para hospedar softwares maliciosos que são utilizados em campanhas de phishing ou técnicas de *watering hole*. Ficam, em média, 7 dias distribuindo o ransomware. Depois disso, os componentes são retirados do servidor e remanejados para outros. Esse processo acontece a cada 5 horas.

CENTROS DE COMANDO

Também em sites legítimos estão ocultos os controladores da rede de ransomware, que ativam na deep web os componentes de geração de chaves criptográficas. Estes controlam o tempo necessário para que todos os arquivos sejam criptografados de forma silenciosa nos computadores infectados. Só após este processo ser realizado, o usuário é avisado.

SERVIDORES DE PAGAMENTO

Os servidores de pagamento funcionam na deep web. A maioria dos nodes de entrada da rede Tor vão para os EUA e Europa, principalmente, Alemanha e Suíça. Não por acaso, estes países possuem leis rigorosas com relação a privacidade e leis que impedem análises financeiras de agentes externos. Verdadeiros paraísos fiscais para a indústria do ransomware!

Direto do Arcon Labs

Números detectados pela nossa plataforma de Threat Intelligence

Cerca de **260** novos servidores de pagamento são criados por semana para receber os resgates da rede Locky.

A rede Locky cresce em média **5%** por semana.

Cerca de **520** novos servidores são comprometidos semanalmente.

Atualmente existem 1008 sites comprometidos (**30** no Brasil) que fazem parte da rede Locky, sendo que 94 deles estão online (**10** no Brasil) e distribuindo o ransomware.

A randomização dos servidores de distribuição é feita a cada **5** horas. Já os servidores de centros de comando, entre **2 a 3** horas.

arcon
serviços gerenciados de segurança

Fontes:
[1] Blog Trend Micro | 2016
[2] Blog Kaspersky | 2016