O QUE É O CRYPTOLOCKER RANSOMWARE?

Cryptlocker Ransomware é uma aplicação maliciosa que encripta os ficheiros do computador tornando-os ilegíveis sendo necessário efetuar um pagamento monetário a fim de os recuperar.

VAMOS AOS NÚMEROS?

Existem mais de 190 estirpes de Ransomware e 4000 computadores infetados por hora (Alien Vault, 2016).
Em 2015, a PandaLabs reportou que são criados 225.000 programas maliciosos por dia e em 2016 a AV-TEST aumentou esse número para 390.000.
No relatório da Verizon Data Breach Investigation Report, de 2016, "30% das mensagens de phishing foram abertas, 12% abriram anexos infetados".
No SANS Incident Response Survey de 2016 "54% das empresas infetadas demoram 2 ou mais dias a detetarem que foram infectados". De acordo com a nbcnews.com, em 2015 as empresas pagaram 24.000,000€ e 209.000,000€ em 2016 por ataques de CryptoLocker.
A infosecurity-magazine.com em 2016 divulgou um estudo no qual 42% das falhas de segurança são responsabilidade do Ransomware.

COMO FUNCIONA O CRYPTOLOCKER RANSOMWARE?

Propaga-se normalmente via email através de um anexo no formato zip.
Ao extrair o conteúdo do anexo encontra-se um ficheiro tipo .pdf que aparenta ser inocente. Infelizmente, esse pdf esconde uma extensão .exe que executa um programa de malware, infetando o computador.

O programa malicioso contata um servidor Command and Control (C&C) remoto e começa a encriptar ficheiros de vídeos, documentos, folhas de cálculo, entre muitos outros

tipo de dados nos discos locais, e em drivers mapeadas. Para ter uma noção, todas estas extensões são alvo do Cryptolocker:
*.odt, *.ods, *.odp, *.odm, *.odc, *.odb, *.doc, *.docx, *.docm, *.wps, *.xls, *.xlsx, *.xlsm, *.xlsb, *.xlk, *.ppt, *.pptx, *.pptm, *.mdb, *.accdb, *.pst, *.dwg, *.dxf, *.dxg, *.wpd, *.rtf, *.wb2, *.mdf, *.dbf, *.psd, *.pdd, *.pdf, *.eps, *.ai, *.indd, *.cdr, *.jpg, *.jpe, img_*.jpg, *.dng, *.3fr, *.arw, *.srf, *.sr2, *.bay, *.crw, *.cr2, *.dcr, *.kdc, *.erf, *.mef, *.mrw, *.nef, *.nrw, *.orf, *.raf, *.raw, *.rwl, *.rw2, *.r3d, *.ptx, *.pef, *.srw, *.x3f, *.der, *.cer, *.crt, *.pem, *.pfx, *.p12, *.p7b, *.p7c
De seguida uma janela pop-up aparece exigindo o pagamento de uma quantia monetária na forma de bitcoin (moeda virtual) normalmente até 72 horas.
Caso não pague dentro do prazo estipulado, a chave privada desaparece do servidor remoto tornando-se virtualmente impossível recuperar os dados nem recorrendo à ajuda da National Security Agency (NSA), a famosa agência americana de segurança.

QUERO SABER MAIS

Outra forma de propagação é através do redireccionamento do utilizador para um site malicioso originando-se a transferência não intencional de software a partir da Internet, sendo conhecido por Drive-by download.
O Ransomware utiliza técnicas algorítmicas de geração de domínios. Estes algoritmos permitem ao administrador de Ransomware criar milhares de domínios aleatórios por dia usados para comunicar com o servidor Command and Control (C&C). Esta técnica impossibilita o uso de blacklists para bloquear ligações a endereços IP fixos ou domínios.
O Ransomware está a evoluir para plataformas de serviço as a service nas quais os malfeitores vendem ferramentas e infraestrutura de malware a terceiros.
Outro fenómeno é o Pay It Forward onde os utilizadores infetados são convidados a infetar outros para remover o Ransomware.

inCentea

COMO POSSO PROTEGER-ME DO CRYPTOLOCKER RANSOMWARE?

As empresas de tecnologias de informação costumam usar o mesmo discurso no que toca ao CryptoLocker.

- Não abrir anexos de email desconhecidos.
- Ter o computador e o antivírus sempre atualizados.
- Realizar salvaguardas automáticas dos seus dados.

É aqui que entra a inCentea. Sendo a primeira consultora Nacional certificada em 4 normativos, um dos quais focado na segurança de informação, possui o know-how necessário para ajudar a capacitar a sua empresa a dar resposta adequada à ameaça real do Cryptolocker Ransomware. Como? Através do Modelo inCentea Cryptolocker Ransomware Prevenção são usadas um conjunto de técnicas de segurança por camadas, que em simultâneo previnem a infeção e a propagação do Cryptolocker Ransomware na sua organização. A prova da eficácia do modelo é o caso da inCentea em si, que nunca teve um caso de Ransomware.

MODELO INCENTEA CRYPTOLOCKER RANSOMWARE PREVENÇÃO

O nosso modelo assenta em múltiplas camadas de proteção usadas em simultâneo, as quais permitem obter uma proteção eficaz, credível e total contra a proliferação do Ransomware.

• Group Policy Object
Ativação de mecanismos de segurança disponíveis no sistema operativo Windows.

• Applocker
Controlo de ficheiros executáveis (.exe and .com), scripts (.js, .ps1, .vbs, .cmd, .bat), ficheiros de instalação do Windows (.msi and .msp), e DLL (.dll and .ocx).

• SRP
Restrição à execução de aplicações através da utilização de Hash, Certificate, Path e Zone.

• FSRM
Despoletar alertas e paragem dos serviços de partilha em caso de infeção.

• NTFS
O CryptoLocker não possui privilégios especiais para ultrapassar a permissão de negação. Se o utilizador infetado tiver as permissões mínimas a fim de executar as suas tarefas, o impacto do Ransomware será mínimo. Se, por outro lado, permitir o grupo Everyone com acesso de escrita nas partilhas e drivers mapeadas, a propagação de uma infeção será mais rápida e difícil de parar.

• Ações de formação
O elo mais fraco de todas as organizações são as pessoas. Têm de ser treinadas e sensibilizadas para a temática da segurança.

• URL Filtering
Bloquear acesso a sites de phishing e malware baseado em categorias.

• Body Content Types
Bloqueia o download de ficheiros executáveis baseado em assinaturas.

• APT Blocker
Através de heurísticas, determina se um ficheiro é malicioso, enviando-o para uma cloud-based sandbox onde o código é executado a fim de detectar a ameaça potencial.

• Email
Descartar executáveis e anexos zip não encriptados.

• *Sandstorm*
Bloqueia ameaças evasivas enviando-as para uma cloud-sandbox a fim de serem analisadas e destruídas.

• InterceptX
Faz uso da tecnologia CryptoGuard que bloqueia processos que tentam fazer alterações não autorizadas aos dados.