Trend Micro

DEFESA CONTRA NOVAS AMEAÇAS DE RANSOMWARE

O ransomware emergiu rapidamente como uma ameaça importante para empresas e organizações de todos os tamanhos. Uma defesa eficaz contra esse tipo de cibercrime começa com uma combinação de uma inteligência global de ameaças avançada, soluções técnicas configuradas adequadamente de acordo com as melhores práticas e uma forte educação e treinamento do usuário que podem ajudar a impedir ataques de ransomware. Além disso, é necessária uma solução segura de backup (de preferência em nuvem).

PANORAMA DA AMEAÇA

O ransomware é um tipo de malware que bloqueia, criptografa ou, de alguma outra forma, impede que os dados e sistemas sejam acessados por seus proprietários, exigindo que a vítima pague um resgate para o cibercriminoso responsável pelo ataque para poder recuperar o acesso.

Ele é distribuído principalmente por spam e emails de phishing enviados para um grande número de endereços de email. Quando um destinatário abre o anexo malicioso ou clica em um link comprometido, o malware é baixado no sistema do usuário. O malware então pesquisa o disco rígido e a rede associada em busca de tipos predefinidos de arquivos e bases de dados. Algumas variantes também pesquisam soluções de backup conectadas para bloquear ou criptografar arquivos em uso e quaisquer arquivos de backup que possa encontrar.

O cibercriminoso por trás do ataque normalmente fornece pouco tempo para o pagamento –perca o prazo e os dados serão apagados. Para pequenas empresas ou outras organizações com recursos ou conhecimento limitado de TI, isso pode trazer uma pressão a mais para pagar o resgate

O número de ataques de ransomware está aumentando, principalmente porque eles costumam ser bem-sucedidos. Embora esses ataques possam resultar em um lucro pequeno –bem menos que o potencial retorno de uma grande violação de dados – são relativamente fáceis de realizar e não requerem que o criminoso monetize os dados roubados no mercado negro ou em qualquer outro lugar.

CryptoLocker é uma família comum de ransomware que trava os sistemas afetados e criptografa arquivos encontrados no disco rígido do sistema. Após o pagamento do resgate, os arquivos criptografados são liberados e decodificados.

Desde sua primeira aparição no final de 2013, o CryptoLocker e suas variantes foram usados em um grande número de ataques de ransomware. O Critroni, ou CTB-Locker, é uma variante mais recente que usa Tor para mascarar suas comunicações de comando-e-controle (C&C).

ESTRATÉGIAS DE DEFESA CONTRA RANSOMWARE

Estas estratégias podem ajudar a garantir que o ransomware (junto com outros tipos de ataques) não possam tomar posse de dados importantes:

1. Políticas cuidadosamente criadas para limitar rigorosamente o número de pessoas e sistemas com privilégios de acesso a armazenamento de dados compartilhados
2. Monitoramento avançado de email de entrada e outros tipos de tráfego que usam inteligência de ameaças em tempo real para identificar emails maliciosos, URLs comprometidas, *hosts* C&C e anexos de arquivos contaminados
3. Monitoramento abrangente do tráfego de rede usando heurística avançada, sandbox e análise de emulação para identificar comportamento suspeito de ataques no perímetro e dentro do perímetro de rede
4. Tecnologias de endpoints da próxima geração como antimalware avançado que pode detectar e bloquear ransomware. Além disso, tecnologia de *whitelisting* de aplicações pode ser configurada para bloquear automaticamente a execução de quaisquer aplicações/malware/ransomware em seus endpoints, permitindo apenas aplicações boas e conhecidas (e suas atualizações associadas)
5. Treinamento do usuário final para minimizar a eficácia de spam malicioso e ataques de phishing que podem infiltrar ransomware na rede

Além dessas estratégias preventivas, também é fundamental usar uma solução segura de backup. Se, apesar de seus melhores esforços, você for vítima de ransomware, a capacidade de restaurar rapidamente seus dados sequestrados de um arquivo recente de backup significa não ter que pagar o resgate. De fato, se todos usassem um sistema de backup automatizado, seguro e independente do armazenamento local e dos sistemas – de preferência uma solução em nuvem – o ransomware deixaria de ser lucrativo e provavelmente desapareceria.

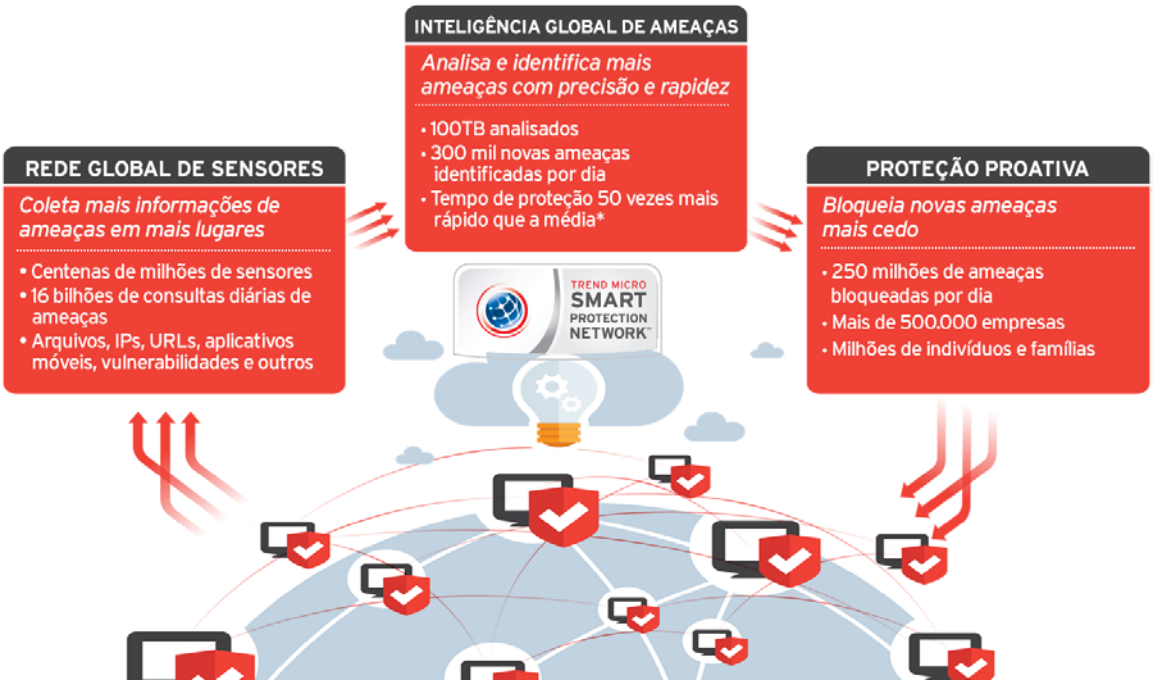
Controle de Acesso

Quando o ransomware infecta um sistema em particular, ele pode acessar quaisquer dados que esse sistema e seus usuários acessam. Portanto, mesmo que alguém na sua empresa clique no link malicioso e abra o arquivo errado, permitindo que o ransomware entre em seus sistemas, se esse indivíduo não tiver acesso aos dados sensíveis críticos da empresa, o ransomware não causará muito dano.

As empresas que impõem políticas fortes que limitam rigorosamente o número de pessoas que têm acesso aos dados críticos da empresa estão menos vulneráveis a ataques de ransomware do que aquelas que permitem um acesso irrestrito.

Trend Micro Smart Protection Network

A Trend Micro™ Smart Protection Network™ é um sistema de inteligência de ameaças em tempo real que reúne informação de milhões de pontos de coleta e usa análises de "big data" para produzir inteligência atualizada sobre as últimas ameaças. Todas as soluções de segurança da Trend Micro são constantemente atualizadas com a informação mais recente para possibilitar a identificação de endereços IP maliciosos, endereços da web, *hosts* C&C, códigos maliciosos escondidos em arquivos e as últimas ameaças de malware e *exploits* de dia-zero.



* CONSUMER EPP COMPARATIVE ANALYSIS: Malware de engenharia social. NSS Labs, 2014.

Solução Network Defense da Trend Micro

O Trend Micro™ Deep Discovery fornece monitoramento em toda a rede, tanto do tráfego interno como entre perímetros, usando análise de *sandbox* personalizada, heurística avançada, e mecanismos analíticos dinâmicos, para identificar comportamento malicioso em todas as fases de um ataque, tanto no perímetro como dentro de sua rede.

Além disso, ele compartilha recursos analíticos e de inteligência com a Trend Micro e outras soluções de email e de *gateways* da web, criando uma defesa personalizada e identificando ransomware e outros ataques, conhecidos ou desconhecidos, antes que eles possam encontrar e comprometer dados e sistemas críticos.

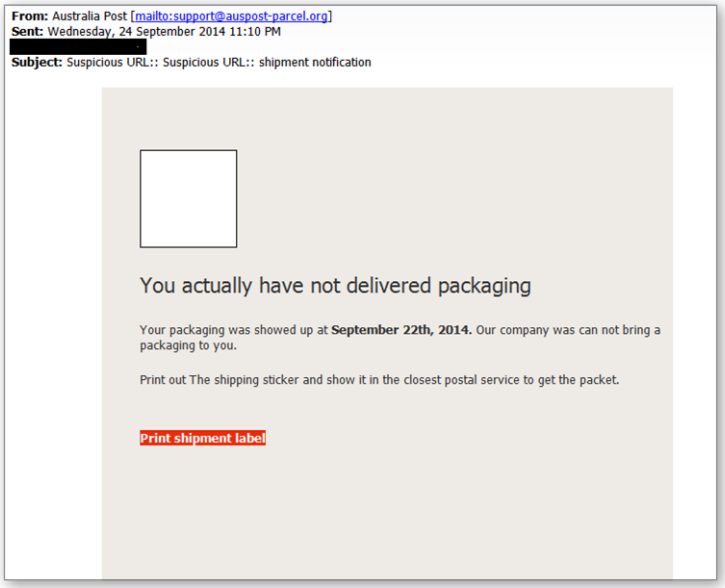
Solução User Protection da Trend Micro

Uma solução para endpoints multicamadas robusta pode ajudar a detectar ransomware se ele conseguir passar por outras camadas de proteção. Com um conjunto de recursos de segurança interconectados, você pode se proteger contra ameaças como ransomware, não importando o que seus usuários façam ou onde eles estejam. As Smart Protection Suites da Trend Micro protegem seus usuários em múltiplas camadas: segurança de endpoint, segurança de email e colaboração, segurança da web e segurança móvel. As suítes também apresentam reputação da web, reputação de arquivos, e monitoramento de comportamento, para ajudar a detectar arquivos de ransomware durante o download ou execução. Além disso, as Smart Protection Suites fornecem a você a mais ampla gama de proteção de ameaças avançadas para antimalware, proteção de variante packer, criptografia, controle de dispositivo, prevenção de perda de dados, blindagem de vulnerabilidades, bloqueio de comando e controle, proteção de exploração no navegador, *whitelisting* de aplicações, proteção de ameaças da web, proteção contra ataques de engenharia social, dados Census e muito mais.

Serviços de Suporte Trend Micro

Depois de implementar soluções técnicas avançadas, ainda é importante garantir que elas sejam configuradas para fornecer a máxima proteção. Além disso, você deve instituir um programa robusto de treinamento para garantir que todos os funcionários dentro de sua empresa estão preparados para reconhecer ataques de phishing e outras tentativas para penetrar em sua rede.

Os serviços de suporte da Trend Micro estão disponíveis para ajudá-lo a adotar as melhores práticas de configurações otimizando suas soluções Trend Micro para identificar e bloquear tentativas de penetrar em sua rede com ransomware e outros tipos de malware.



Exemplo de spam de Crypto Ransomware

Também estamos disponíveis para ajudá-lo a elaborar um programa de treinamento que pode mobilizar seus funcionários no apoio à sua estratégia de segurança com hábitos de email essenciais e saudáveis. Isso é importante devido à frequência com que o ransomware é enviado por meio de email spam de phishing. O hábito mais importante é suspeitar sempre de todos os emails com anexos ou links. Quando você recebe um email suspeito como o exemplo à esquerda:

- NÃO clique no link do email
- NÃO abra o anexo do email
- NÃO digite um CAPTCHA se for solicitado
- Confirme a validade do email entrando em contato com o remetente por diferentes meios – de preferência por telefone ou usando um endereço que você já tem ou que não esteja mencionado no email
- Se o email parece vir de uma empresa ou organização, use um mecanismo de busca para encontrar a URL correta do site dessa organização, depois acesse o site e contate a organização usando a informação que encontrou no site

DÊ O PRIMEIRO PASSO

Quer você já esteja protegido por soluções Trend Micro ou esteja nas primeiras etapas, escolhendo uma maneira para proteger sua empresa contra ransomware e outras ameaças, está na hora de nos contatar para obter uma assistência especializada. Nós podemos ajudá-lo a garantir que suas soluções existentes estão configuradas da melhor maneira para protegê-lo contra as ameaças avançadas atuais. E podemos elaborar recomendações personalizadas para um programa de treinamento de funcionários que torne sua empresa menos vulnerável aos vetores de ataque mais comuns.

TREND MICRO™