Como se proteger do sequestro de dados

Ramsomware

TECNOLOGIA E INOVAÇÃO

Supreme

O que é ransomware?

O Ransomware é uma espécie de malware (software mal-intencionado) que os criminosos instalam em seu computador sem seu consentimento. O ransomware dá aos criminosos a possibilidade de bloquear seu computador de um local remoto. Depois, ele apresenta uma janela pop-up com um aviso de que seu computador está bloqueado e você não poderá acessá-lo, a menos que pague.

Como os criminosos instalam o ransomware?

O ransomware geralmente é instalado quando você abre um anexo mal-intencionado em uma mensagem de e-mail ou quando clica em um link mal-intencionado em uma mensagem de e-mail, mensagem instantânea, site de rede social ou qualquer outro website. O ransomware pode ser instalado quando você visita um site malicioso.

Também é comum os criminosos explorarem falhas em sistemas que não foram atualizados com as correções liberadas pelo fabricante, como ocorreu na **mega infecção mundial** de maio de 2017, onde milhares de computadores ao redor do mundo foram infectados ao ser explorada uma falha no sistema operacional Windows, que já havia sido corrigida meses antes.

G1 TECNOLOGIA E GAMES

Ciberataques em larga escala atingem empresas no mundo e afetam Brasil

Ataques ocorreram em ao menos 74 países, com 'vírus de resgate' que exige dinheiro, diz empresa de segurança. No Brasil, sites de empresas e órgãos públicos saíram do ar. Hospitais na Inglaterra foram atingidos no início do ataque.

Por G1
12/05/2017 11h45 · Atualizado 15/05/2017 13h23

O ransomware está crescendo e evoluindo rapidamente – neste momento existem mais de 50 famílias deste tipo de malware em circulação. Com cada

nova variante surge melhor encriptação e novas funcionalidades. Isto é algo que não se pode ignorar!

Uma das razões porque é tão difícil encontrar uma única solução para o ransomware é que a cifragem por si só não é algo malicioso. Muito pelo contrário, é algo que muitos softwares utilizam de forma legítima.

O primeiro crypto-malware utilizava algoritmos de chave simétrica, a mesma chave era usada tanto para cifrar como para decifrar. Isto permitia que a informação cifrada fosse recuperada com sucesso com a assistência de empresas de segurança informática. Ao longo do tempo, os criminosos começaram a utilizar algoritmos de criptografia assimétrica, que usam duas chaves diferentes - uma chave pública para cifrar ficheiros, e uma chave privada que é necessária para decifrar os mesmos ficheiros.

O CryptoLocker é um dos mais famosos ransomwares. Utiliza um algoritmo assimétrico de chave pública. Assim que cada computador é infetado, liga-se ao servidor de comando e controle para fazer download da chave pública. A chave privada associada é acessível somente aos criminosos que operam o ransomware. Normalmente, a vítima não tem mais de 72 horas para pagar o resgate antes que a chave privada seja apagada para sempre e se torne impossível desencriptar qualquer arquivo com essa chave.

Por isso, tem que se pensar em prevenção. A maior parte dos programas antivírus corporativos possuem uma funcionalidade que permite identificar uma ameaça de ransomware nas primeiras fases da infeção, sem que ocorra perda de dados. É importante que os usuários confirmem que esta funcionalidade está ativa nas suas soluções antivírus.

Abaixo listamos algumas ações a serem tomadas a fim de prevenir as infecções, e também as ações a tomar caso você seja uma vítima de um desses malwares:

Prevenção

- Garantir que todo o software de seu computador esteja atualizado. Habilitar as atualizações automáticas para obter as últimas atualizações de segurança.

- Utilizar um antivírus atualizado e eficiente, que contenha as ferramentas de segurança adequadas.

- Não abrir links suspeitos em mensagens de e-mail, links enviados por desconhecidos em redes sociais, nem anexos de e-mail suspeitos.

- Fazer backups regularmente, e a conferência dos mesmos.

Ações a tomar se for infectado

- NÃO PAGUE o resgate, em nenhuma hipótese. O pagamento não dá nenhuma garantia de que seus dados serão liberados ou recuperados.

- Desligue todos os seus equipamentos da internet

- Contate seu suporte de TI para que analise o mais rápido possível, e descubra a fonte da infecção.

- Após certificar-se de que a infecção foi eliminada, efetue a restauração dos backups e serviços.

Caso você tenha dúvidas, e queira saber como pode implementar políticas e ferramentas de segurança em sua empresa, converse com nossa equipe!

Temos soluções de ponta, usadas por grandes empresas, e com condições que se ajustam a qualquer tamanho de infraestrutura.

TECNOLOGIA E INOVAÇÃO

Supreme

E-mail: contato@supreme.inf.br

Fanpage: facebook.com/supremeinfo

Instagram: @supreme_informatica

Telefone: (54) 8139-9299

Referências e links úteis:

https://www.nomoreransom.org/

https://www.microsoft.com/pt-br/security/resources/ransomware-whatis.aspx

TECNOLOGIA E INOVAÇÃO

Supreme