Um pouco sobre Ransomwares

Gustavo Lopes Rodrigues

Novembro de 2020

Ransomware é um tipo de ataque criptográfico que: ao ganhar acesso do computador da vítima, o software criptografa os dados da máquina. Para restaurar os dados comprometidos, a usuário receberá instruções em como pagar um valor X (geralmente em **criptomoedas**, pois elas deixam menos vestígios, logo, são mais difíceis de serem re-encontradas) para receber a chave de decriptografia e ganhar acesso novamente. Infelizmente, existe casos onde os sofredores não recebem seus dados, ou pior ainda, aqueles que fizeram o pagamento tem chance de serem alvos novamente de futuros ataques.

Existe diferentes formas na qual um Ransomware pode ganhar acesso a um computador:

- ***Pishing*** - Ciberataques que envolve o uso de e-mails, mensagem de celulares(SMS), onde o recipiente é enganado a baixar um arquivo ou acessar um link. O nome "Pishing"é derivado da palavra "Fishing"que é a palavra em inglês para "pescar". Ao ser "pescado", o hacker acaba de ganhar um ponto de acesso ao seu computador, assim instalado o Ransomware.
- ***Exploit Kit*** - ao contrário do Pishing, em vez de "pescar"a vítima, o Exploit Kit aproveita-se de falhas de programas ou até de sistemas, para acessar os computadores de pessoas distraídas. Um exemplo disso está no famoso ataque ***WannaCry*** que infectou computadores ao redor do mundo, por causa de uma falha nos sistemas operacionais Windows.

Referências

[1] https://www.csoonline.com/article/3236183/what-is-ransomware-how-it-works-and-how-to-remove-it.html

[2] https://br.malwarebytes.com/phishing/

[3] https://www.trendmicro.com/vinfo/us/security/definition/ransomware