Há diversas maneiras do computador ser infectado por um ransoware por exemplo um pendrive infectado, e-mail com link, ou ate mesmo um site.

Como exemplo prático eu estava no trabalho e ao utilizar um pendrive em uma conputador qualquer o conteúdo havia sumido aparecendo somente um atalho que não servia para nada.

**1. Ryuk, 2019 e 2020**

Como a maioria das infecções causadas por ransomware, o Ryuk é propagado principalmente via [**e-mails maliciosos**](https://gatefy.com/pt-br/blog/emails-falsos-e-perigosos/) ou **[phishing](https://gatefy.com/pt-br/blog/iscas-usadas-em-golpes-de-phishing-para-enganar/" \t "_blank)**, contendo links e anexos perigosos. O valor do resgate a ser pago para liberar um sistema inteiro pode exceder USD 300.000, tornando o **[Ryuk um dos ransomwares mais caros da história](https://gatefy.com/pt-br/blog/ataque-de-malware-afeta-jornais-dos-eua/" \t "_blank)**, bem acima da média.

De acordo com o FBI, os ataques de Ryuk já causaram mais de USD 60 milhões em prejuízos no mundo todo desde que este tipo de ransomware ganhou destaque em 2018, após interromper as operações de grandes jornais nos EUA. Mais de 100 empresas sofreram ataques

Em 2020, por exemplo, o EMCOR Group (empresa de engenharia e construção industrial) e a Epiq Global (empresa de serviços jurídicos) sofreram ataques envolvendo o Ryuk.

Um fato interessante é que as mensagens de resgate do Ryuk contêm e-mails de contato com o final @protonmail.com ou @tutanota.com. A vítima precisa enviar um e-mail para saber quanto devem pagar pela chave de descriptografia.

**2. SamSam, 2018**

O ransomware SamSam já foi identificado há alguns anos, mais precisamente no final de 2015. Mas foi em 2018 que ganhou muito mais destaque depois de infectar a cidade de Atlanta, o departamento de transporte do Colorado e o Porto de San Diego, nos EUA, paralisando serviços abruptamente.

Em 2018 ainda, dois hackers iranianos foram acusados de usar o SamSam contra mais de 200 organizações e empresas nos EUA e no Canadá, incluindo hospitais, municípios e instituições públicas. É estimado um prejuízo de USD 30 milhões como resultado dos ataques.

Apenas a cidade de Atlanta gastou mais de USD 2 milhões para reparar os danos. O Hancock Health, um hospital de Indiana, pagou um resgate de USD 55.000. Para se propagar, este tipo de ransomware costuma explorar vulnerabilidades em Remote Desktop Protocols (RDP) e File Transfer Protocol (FTP).

Um fato curioso em relação ao SamSam é que a vítima é convidada a fazer um primeiro pagamento por uma primeira chave, que desbloquearia apenas algumas máquinas. Seria como um sinal de honestidade.

“Ao comprar a primeira chave, você descobrirá que somos honestos”, diz a mensagem de ransomware. Você acreditaria nisso?

fonte : https://gatefy.com/pt-br/blog/casos-reais-famosos-ataques-ransomware/