ALERTA CIBERCRIME

24 de maio de 2018

Ransomware – Stalin Locker

1. Chegou, ao Gabinete Cibercrime, nota de que está em curso mais uma campanha de *ransomware* – embora atípico, porque ao invés de solicitar um resgate, exige a introdução de um código específico de desbloqueio. Trata-se, pois, de um tipo de ataque informático híbrido, que usa o método do *ransomware*, mas se aproxima dos vírus da década de 1990.

2. Em geral, este tipo de ataques é perpetrado por via da difusão de *emails*, aos quais vai anexo *malware*. Caracteriza-se pelo bloqueio do computador da vítima, cujos dados ficam inacessíveis e, normalmente, são irremediavelmente perdidos.
Neste caso, quando ativado, o *Stalin Locker* bloqueia o computador da vítima e apresenta uma mensagem de erro. Em simultâneo, é mostrada uma imagem do antigo presidente soviético Joseph Stalin, ao mesmo tempo que se ouve o hino nacional da antiga União Soviética. No écran é ainda exibido um cronómetro, em contagem regressiva, de 10 minutos. Findo esse lapso de tempo, os dados do computador são encriptados, sem que seja fornecida forma de os desencriptar.

3. A originalidade deste *ransomware* híbrido estará precisamente na exigência da introdução desse código: em vez de ser pedido ao dono do computador um pagamento, é-lhe pedido que introduza um "código correto".
Tal "código correto" é variável. Para o encontrar, é necessário considerar a data concreta (ou seja, a data em que o vírus foi executado) e subtrair 1922.12.30 (número que esconde a data em que foi formalmente assinado o tratado que instituiu a antiga URSS). Após esta operação é ainda necessário converter o resultado em dias.
Caso o código não seja inserido nos 10 minutos disponíveis, os dados do computador são automaticamente encriptados, não sendo conhecida forma de os reaver. Claro está que a vítima não sabe que esta é a forma de travar o processo.

4. Sugere-se, pois, aos colegas, que atentem particularmente a mensagens de correio eletrónico de origem desconhecida e que não abram anexos dos mesmos ou não acedam a links desconhecidos.
Mais informação pode ser encontrada aqui: e https://www.bleepingcomputer.com/news/security/stalinlocker-deletes-your-files-unless-you-enter-the-right-code/ e aqui: https://sputniknews.com/viral/201805161064520141-stalin-locker-virus-nature/.