Ransomware Decryptors

Universal Encryption

Universal Encryption

Ransomware variants like Ryuk, WastedLocker, and Dopplepaymer are also file level encryption. These groups will gain access to the network and perform reconnaissance to identify the victim, understand their business, identify critical systems, and delete backups to force their victims into making a payment. The groups can have access to the network for a few hours or upwards of over a month. Ryuk is commonly associated with precursor trojans such as Trickbot and Emotet. Arete has observed Ryuk deployed as quickly as 6 hours after a Trickbot infection. Ryuk infections result with *.ryk appended to the file name. Comparatively, the deployment of WastedLocker is much more calculated with the TA staying on the network for an average of 2 weeks from initial infection to ransomware deployment. Wasted infections result with *.abcwasted appended to the file name where “abc” is a 3 letter abbreviation relating directly to the victims name.

Figure 3 - WastedLocker Decryptor

Communication preference: Email usually protonmail.com domains or TOR Website

Average ransom payment: Ryuk $598,000; WastedLocker $2,400,000; Dopplepaymer $304,000

Preferred currency: Bitcoin (BTC)

Decryptor received: 100% of the time. The decryptor received is universal. It is typically a 32-bit executable that will work on any windows OS version. While these groups are known for a high ransom price, their decryptor is probably the simplest to run.

Watch out: WastedLocker is extremely difficult to negotiate. In fact, if negotiation is attempted, they may threaten to increase the ransom by approximately 5% of the ransom per day until it is paid. They are also very slow to respond to email and even post their business hours of UTC 5am-8am and 5pm-8pm.

Notes: Dopplepaymer has been linked to gaining access to large environments and deploying cryptomining malware before launching their ransomware attack.