Cryptolocker

Technology, Information Technology

CryptoLocker, in technical terms, can be described as a form of malware which uses the conceptions of encryption and decryption for harassing the victims. The common methods for this malware transmission include emails, botnets and concealed transmission within network data. In terms of severity, cryptolocker malware can be ranked within one of the most deadly malwares and tacking the same might turn out to be highly tedious.

One of the prime threats, which might arise from CryptoLocker, is disrupting the operational systems, resulting in losing valuable or confidential data (Oregon, “ Computer Help Documents”). The designing pattern of CryptoLocker malware generally projects it to be a

type of ransomware code, which gets activated through remote triggering and eventually encrypts all crucial files within the infected systems incorporated with ‘ RSA encryption algorithm’. This kind of encryption algorithm requires the involvement of public as well as private key so as to carry out file encryption along with decryption procedures effectively (Oregon, “ Computer Help Documents”). The infection procedure is conducted in such a manner so that once all he crucial files within a system gets encrypted, the intruder or the designer of that malware starts demanding a lump-sum amount of payment to the owners of the infected systems. On failure or rejection in terms of making such payment, the intruder starts threatening the owners regarding deletion of private key without which the encrypted files cannot be decrypted (Oregon, “ Computer Help Documents”). Another specific advantage for the intruders can be ascertained as that, since the encryption procedure gets initiated by the malicious codes, which is itself regarded as ‘ 2048-bit RSA encryption’ type,

it becomes completely impossible for the system analysts to decrypt the encrypted files using ‘ brute force’ programs. This changes the entire game in favor of the intruders. One countermeasure, which can be deployed in staying clear from this malware and the above stated unfavorable condition, is the creation of periodic system restore points through which certain portion of the previously backed up file versions can be retrieved, once the systems get infected (ESET, “ 11 things you can do to protect against ransom ware, including Crypto locker”). Apart from these, the system analysts might also perform periodic malware scans within updated malware signature databases. Under such circumstances, continuous up gradation of the malware detection tools is also necessary. The analysts might also refer to the utilization of online malware sandbox tools so as to understand the malware behavioral patterns and thus eradicate those accordingly (ESET, “ 11 things you can do to protect against ransom ware, including Crypto locker”).

From the above analysis and discussion, a clear understanding can be made regarding the fact that malware attacks might result in causing huge figure of financial losses to an enterprise or a nation as well. Multiple initiatives need to be taken into concern for preventing these sorts of negatively intended practices. However, technology has its own bindings and thus requires considerable amount of time for developing itself. Thus, it might be perceived that effective safeguard against malwares such as CryptoLocker will get developed in future depending upon the rate of development in the area of information technology security.

Works Cited

“ 11 Things You Can Do To Protect Against Ransom Ware, Including Crypto Locker.” ESET. 2013. Web. 28 Sep. 2014.

“ Computer Help Documents.” Oregon. 2014. Web. 28 Sep. 2014.