There are several ways to spread ransomware, the method been used to deliver ransomware are same as delivering other malware, the only difference is the payload is changed to an automated encryption executable and methods are as follow:

Email phishing

One common way of delivering ransomware is the attacker sending fake email mimic as legitimate email to victim, victim with less awareness of email security will likely to download the malicious executable.

Drive-by-download

A high-value website or high-volume website is likely to be the perfect target of the extortioner, by exploiting the vulnerabilities attacker may take control of the entire website host upload malicious executable file or is able to inject malicious script targeting vulnerable browser, when victim visit this website the malicious script will attempt to access to attacker’s domain and download ransomware or been lured to download malicious file which is uploaded by the attacker but appears to be legit.

Exploit vulnerability

Like other self-spreading warms, nowadays ransomware is capable of propagate through networks, more valid affection will appear because the devices with selected vulnerability will be affected inevitably in a network. Wannacry exploits EternalBlue infected over 300000 computers. EternalBlue is an exploit developed by NSA but leaked by Shadow Broker, the exploit is targeting Microsoft’s operating system,

Ransomware installation and initialization.

The evolution of Ransomware.

The evolution of ransomware has been greatly influenced by a range of technological and economical development since the first extortion application was born.

Ransomware has became a worldwide threat and the author of these applications quickly adapt to latest technology making ransomware more sophisticate and harder to break, adapting and evolving to fit in and jeopardize system became a mandatory lesson for the attackers, those that can not adapt will eventually disappear from the ransomware world.

The very first ransomware known as AIDS Trojan was implemented by Joseph Popp in 1989,after the victims computer been affected AIDS hides directories and encrypts the name of all files on drive C: making system unusable then pop up a dialog and like many current ransomware it asks user to pay to a company called PC Cybrog Corporation to renew users license. At that time being, bad implementation of cryptography mechanism, number of users of personal computer is not much and internet infrastructure was still in development, these circumstances limited the damage of the AIDS Trojan but the idea of extortion application has opened the Pandora’s box, Young and Yung brought the idea of Cryptovirology few years after AIDS attack.

(briefly introduce the essay).

Ransomware went off the radar since the first documented ransomware attack until the mid-2000s. Ransomware attack re-surfaced in 2005, attacker has not only demonstrated the capability of such application denying ordinary user from using their device but also their adaptability to technologies. The analysis of samples of ransomware(e.g. Gpcode, TROJ.RANSOM.A, Archiveus, Krotten, Cryzip, and MayArchive) reviewed that more sophisticated encryption scheme(namely RSA)has been utilised by the attacker in the application with increasing key-size. As the chart has shown, the key-size has increased from 56-bits in version ac to 660-bits long in version ag only in the short period of 6 months. In June 2008 the variant ak group has adopt a RSA scheme with 1024-bits long RSA key and it is believed that it is large enough to be not feasible to break. And since early 2006 the concept of crypto ransomware began to draw attention from researchers and public as the idea of cryptography been used in a hostile mean.

Locker ransomware has engaged to the ransomware market in 2008 and rapidly grown to a major threat in 2011 and 2012. This type of ransomware require user interaction to download the malicious application to fix issues which does not exist in the first place. But nowadays ransomware is fully automated without the need of tricking victim to install the application.

Fast forward to 2013 and present days, the defect in other extortion application and the technology development made attacker move their attention to crypto ransomware. Instead of well-scripted dialogue to trick user to pay for the decryption, the attacker now simply pop up a window asking for a larger ransom payment and returning data in exchange.

Cryptography in Randomware

In the research and experiment of AIDS Trojan, Young and Yung has introduced public key encryption scheme for data hijacking. The failure of AIDS Trojan is caused by fatal design defect: Hard coded decryption key. The symmetric key is used for both encrypting and decrypting therefore the key is embedded in the malware giving security practitioner window to crack the ransomware. The author implemented RSA and TEA(Tiny encryption algorithm) in the experiment. In the simulated attack, TEA encryption scheme uses a symmetric key as encryption/decryption key to pollute victim data and RSA scheme to protect the encryption key of attacker. The encryption key is encrypted by the public key and based on the RSA scheme it can only be decrypted by the attacker’s private key, thus, in order to get files recovered, the victim needs to pay for the ransom and send the ciphertext of encryption key back to attacker to get the ciphertext decrypted. Many extortion virus then developed years later using similar scheme but with more sophisticated delivery method and encryption algorithm.

[process flow

Graph + bullet point]

Breaking the