Ransomware

Ransomware is a malicious software that covertly installs on a victim's computer to block access to information or system and demand payment for returning access. The use of ransomware has grown exponentially over the last few years. The first ransomware was developed in 1989; therefore, the method is not new but has become much more effective in recent times due to universal use of computers and the advent of Bitcoin to anonymize payments.

Ransomware in general targets individual users; however, organizations are increasing targeted due to value of the data and reliance on data for daily operations. The rationale for targeting individual users is the lack of backups performed by individuals, however cyber criminals have found ransomware is as effective against organization and have had substantial success.

Paying ransom has long been a debatable issue not only from ethical standpoint but also legal. In some countries, paying ransom is a criminal offense. However, law enforcement authorities have turned a blind-eye considering the position of victims. Nonetheless, ransomware is becoming a major issue and the most effective approach is to prevent it in the first place by putting preemptive controls in place. In order to implement effective controls, a comprehensive understanding of the ransomware lifecycle is essential. The following figure depicts the working of a typical ransomware.

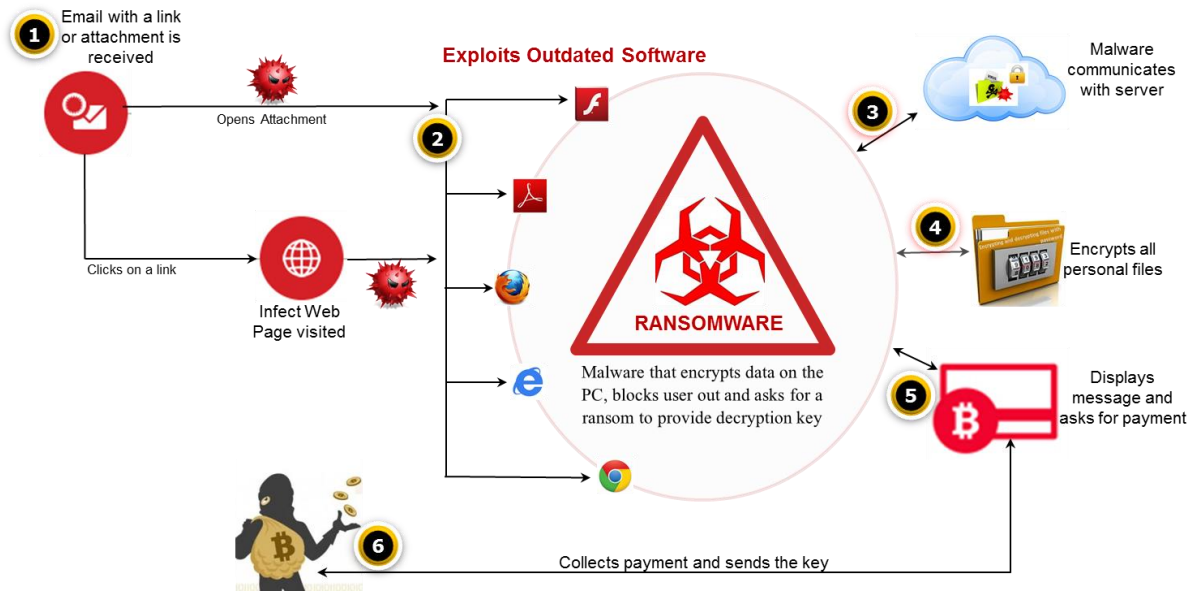

FIGURE 1. – TYPICAL RANSOMWARE EXECUTION/ LIFECYCLE

It is important to note that not all ransomware works the same way and some ransomware have weakness that can be leveraged to decrypt data without making payment. Most modern ransomware are much more robust and leverage asymmetric keys (separate keys for encryption and decryption) where the private key is never on the machine during the

encryption process, therefore making it impossible to decrypt the data without making the payment. The steps details the lifecycle of typical ransomware.

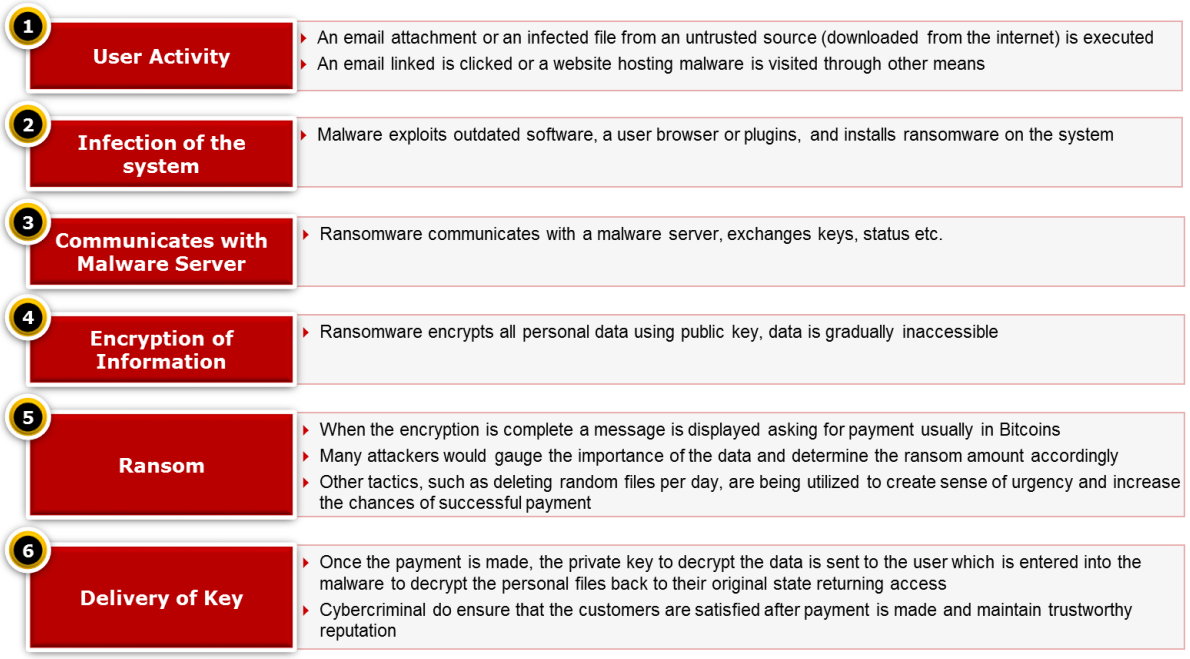

FIGURE 2. – TYPICAL RANSOMWARE EXECUTION/ LIFECYCLE STEPS

Entities should consider putting in place appropriate measure at the various phases of the ransomware lifecycle to protect themselves and prevent falling prey to ransomware. Naturally, we have more control during the first two steps, once the message pops up demanding payment; we have no control except to may be restrict the spread of the malware on to other systems. Abu Dhabi Government Entities should consider the following:

- Conduct security awareness sessions regularly, educate users to be aware of malware and downloading files from untrusted sources
- Make sure that systems are patched with the latest patches available for the software
- Ensure Endpoint Protection products are current have the latest signatures installed
- Block communication to know bad URLs (servers hosting malware)
- Ensure that backups are taken regularly and tested (the backup process should be able to detect ransomware encrypted data and not overwrite existing unencrypted backup). Backup process should be tweaked to address potential issues associated with ransomware

Please report any incidents to Abu Dhabi Security Operation Center (SOC) at soc@adsic.abudhabi.ae to allow better collaboration and coordination of security incidents and response.

If you have any questions or comments, regarding this document or have any ideas for future topics, please email us at AD-InfoSec@adsic.abudhabi.ae.

References:

United Arab Emirates (UAE) Information Assurance (IA) Standards

San Francisco Transit Agency Earns Praise For Denying Ransom Request – http://www.darkreading.com/endpoint/san-francisco-transit-agency-earns-praise-for-denying-ransom-request/d/d-id/1327574?

SANS Security Awareness Newsletter – https://securingthehuman.sans.org/newsletters/ouch/issues/OUCH-201608_en.pdf

Abu Dhabi Security Operation Centre
soc@adsic.abudhabi.ae
02-696-1611
0566866677