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 economic development since the first extortion application was born.

Ransomware has become 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 cannot 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 Ransomware

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.

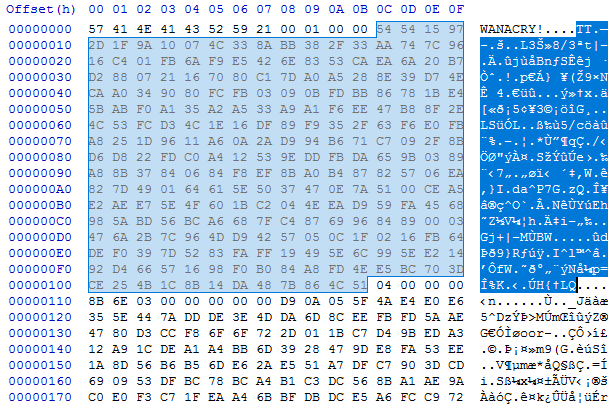
As the table1 provided by[cutting the Gordian knot], 5.37% of the ransomware sample implemented encryption mechanisms during the attack, however it is important to point out that three out of these four families are developed after 2012 and for most ransomware samples which developed before 2012 are lacking of encryption function, the novel type of ransomware attack was commencing. The infamous Cryptodefense( also known as Cryptowall) appeared in late February 2014, Tor network and Bitcoin was employed to the ransomware for anonymity, and RSA with 2048-bits key encryption scheme provide a strong invasive power to mask victim files. Attacker behind ransomware has turned theire attention to produce more powerful crypto-ransomware families that incorporating new innovations, platforms and more complex encryption schemes.

[process flow

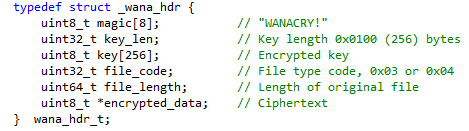
Graph + bullet point]

Characteristics of ransomware

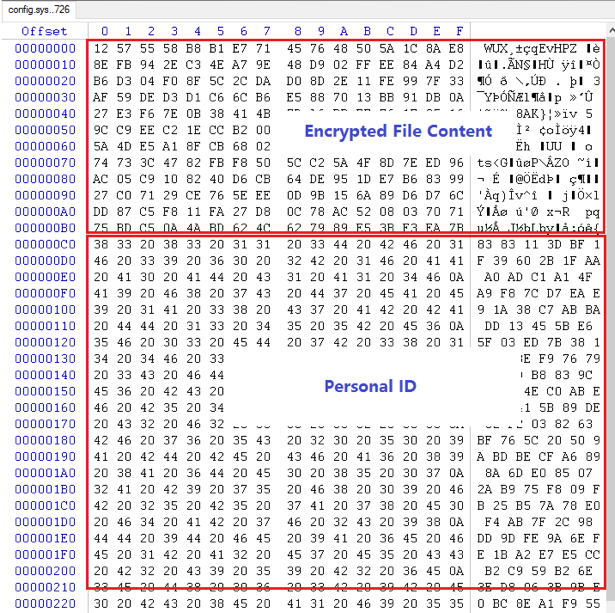
This section is aim to explain ransomware process activities, discuss general mitigation process against them in the following section.

Encryption Mechanism. Encryption is applied on files in the compromised devices after ransomware is installed and initialised but not all files get encrypted. For example, Globelmposter maintains two exclusion lists, one contains specific directories and the other one keeps a list of file extensions, while the ransomware encrypts all files on the machine, it skips files in the directory folder and all file extensions from second list. Others like WannaCry has a hard-coded binary file containing all targeted file extensions. The encrypted file normally has a designated format or a prepended a header to encrypted file for malware to identify encrypted files and future decryption. 

Wannacry file header



Header structure.



Globelmposter, encrypted file. Personal ID is later send to attacker for decryption key.

The exclusion lists for Globelmposter are as follow:

*Folder exclusion list: (44 in total)*

*Windows, Microsoft, Microsoft Help, Windows App Certification Kit, Windows Defender, ESET, COMODO, Windows NT, Windows Kits, Windows Mail, Windows Media Player, Windows Multimedia Platform, Windows Phone Kits, Windows Phone Silverlight Kits, Windows Photo Viewer, Windows Portable Devices, Windows Sidebar, WindowsPowerShell, Temp, NVIDIA Corporation, Microsoft.NET, Internet Explorer, Kaspersky Lab, McAfee, Avira, spytech software, sysconfig, Avast, Dr.Web, Symantec, Symantec\_Client\_Security, system volume information, AVG, Microsoft Shared, Common Files, Outlook Express, Movie Maker, Chrome, Mozilla Firefox, Opera, YandexBrowser, ntldr, Wsus, ProgramData.*

*Extension exclusion list: (170 in total)*

*.$er .4db .4dd .4d .4mp .abs .abx .accdb .accdc .accde .accdr .accdt .accdw .accft .adn .adp .aft .ahd .alf .ask .awdb .azz .bdb .bib .bnd .bok .btr .cdb .cdb .cdb .ckp .clkw .cma .crd .daconnections .dacpac .dad .dadiagrams .daf .daschema .db .db-shm .db-wa .db2 .db3 .dbc .dbf .dbf .dbk .dbs .dbt .dbv .dbx .dcb .dct .dcx .dd .df1 .dmo .dnc .dp1 .dqy .dsk .dsn .dta .dtsx .dx .eco .ecx .edb .emd .eq .fcd .fdb .fic .fid .fi .fm5 .fmp .fmp12 .fmps .fo .fp3 .fp4 .fp5 .fp7 .fpt .fzb .fzv .gdb .gwi .hdb .his .ib .idc .ihx .itdb .itw .jtx .kdb .lgc .maq .mdb .mdbhtm .mdf .mdn .mdt .mrg .mud .mwb .myd .ndf .ns2 .ns3 .ns4 .nsf .nv2 .nyf .oce .odb .oqy .ora .orx .owc .owg .oyx .p96 .p97 .pan .pdb .pdm .phm .pnz .pth .pwa .qpx .qry .qvd .rctd .rdb .rpd .rsd .sbf .sdb .sdf .spq .sqb .sq .sqlite .sqlite3 .sqlitedb .str .tcx .tdt .te .teacher .tmd .trm .udb .usr .v12 .vdb .vpd .wdb .wmdb .xdb .xld .xlgc .zdb .zdc*

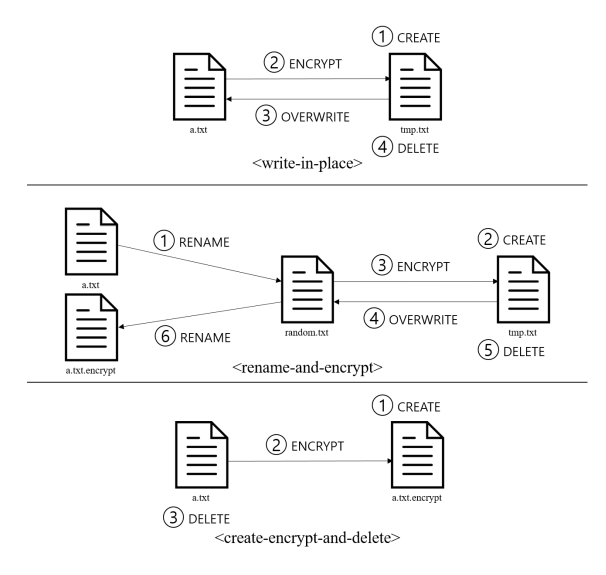
Furthermore, not only victim files are being encrypted, the attacker protects their delicate malware application by encrypting or hashing resources used by the ransomware, static value such as ransom demanding message, bitcoin address, hard-coded extension table, control and command server address and for what is the most important RSA public key (and/or AES key if AES is in use.) as well as the dynamic resources such as customised encryption algorithm and libraries. This procedures will slow down the malware analysts from understanding the true intent of the malware and making static analysis hard to proceed because the key values are not directly readable by human.

Both symmetric encryption scheme and asymmetric encryption scheme is found in ransomware families and in some ransomware family both encryption schemes are coupled together serving different purposes. For example in WannaCry, an embedded RSA public key (or a freshly generated RSA key pair) is used to protect the AES encryption key generated for each file encrypted by this AES key.

WNCRY DATA flow graph.

File system activity. It is inevitable for a ransomware to interact with file system of victim to perform fulfil its goal, therefore looking at the file system activity is necessary to detect and identify a ransomware. For cryptographic ransomware such as WannaCry, Critroni and TeslaCrypt, the ransomware will enumerate and traverse through entire mounted file system to find all files with specific extension which is stored in a predefined extension list in the malware, the directory of these files are recorded and later will be encrypted or amended(If ransomware is aiming to change MBR or Simply change system behaviour).

To perform encryption to targeted files ransomware will have to generate I/O request to the system, a I/O request could be read, write or delete. There are three common methods found in existing Ransomwares:

As observed on the graph, creating a copy of original file needs ransomware to read the original file then overwrite the original file and finally drop the original file. The dataset used in the experiment contains information about the I/O requests on every files interacted and related operation. I/O requests on files are important for analysing the behaviour of a ransomware and also proven to be one valid and relevant feature for dynamic analysis.(cite daniel RHUL)

MBR changing. Some ransomware families are developed to change the Master boot record. MBR contains the executable boot code and the partition table for the operating system and file system, ransomware such as MATSNU will modify registries to enable itself to execute in every system start and disable some of the processes such as registry editor and task manager. It also deletes registries to prevent user from entering safe mode, and it has capability of locking computer for ransom through command sent through C&C communication. PETYA utilise the same vulnerability as WannaCry-EnternalBlue to effectively infect MBR, overwrite the Windows boot loader to trigger computer to reboot, upon reboot, the master file be encrypted and ransom notes displayed to victim.

Detecting ransomware

Honeypot, signature, static string, file extension

Identifying Ransomware

behavioral analysis

I/O file

Entropy of procedures

API monitoring

Defending ransomware

Ad-Hoc procedures

dump ransomware samples