6G6Z1012 Information and Network Security

The Design and Development of a new Crypto-ransomware

Mark Bellingham

14032098

14032098@stu.mmu.ac.uk

Questions to be answered about each ransomware program

Q1. What files will it encrypt?

Q2. Describe how to search for local and network drives?

Q3. How to get files from the drive?

Q4. What are the supported file extensions?

Q5. How does it encrypt files?

a) A description of the algorithm design explaining the operations that are performed at each processing stage, their input and output and processing flow.
b) A description of key generation and preparation at each processing stage
c) A schematic diagram that depicts the components of the algorithm, their running order (processing flow), interaction between components, inputs and outputs and number of rounds

Q6. Is there a way to decrypt the files? or identify, detect and remove the ransomware?

Q7. What are the payment instructions like?

Cryptowall 3.0

Q1.
The files it encrypts are the most common files found on the average user's PC. They include documents that are important for productivity and files that would have great personal value to the user such as photos and videos

Q2.
It scans all the drive letters that are not optical drives using the "GetLogicalDriveStrings" API on the infected computer.

Q3.
For each drive that it finds in the process above, a separate program thread is launched.

Q4.
.sql, .mp4, .7z, .rar, .m4a, .wma, .avi, .wmv, .csv, .d3dbsp, .zip, .sie, .sum, .ibank, .t13, .t12, .qdf, .gdb, .tax, .pkpass, .bc6, .bc7, .bkp, .qic, .bkf, .sidn, .sidd, .mddata, .itl, .itdb, .icxs, .hvpl, .hplg, .hkdb, .mdbackup, .syncdb, .gho, .cas, .svg, .map, .wmo, .itm, .sb, .fos, .mov, .vdf, .ztmp, .sis, .sid, .ncf, .menu, .layout, .dmp, .blob, .esm, .vcf, .vtf, .dazip, .fpk, .mlx, .kf, .iwd, .vpk, .tor, .psk, .rim, .w3x, .fsh, .ntl, .arch00, .lvl, .snx, .cfr, .ff, .vpp_pc, .lrf, .m2, .mcmeta, .vfs0, .mpqge, .kdb, .db0, .dba, .rofl, .hkx, .bar, .upk, .das, .iwi, .litemod, .asset, .forge, .ltx, .bsa, .apk, .re4, .sav, .lbf, .slm, .bik, .epk, .rgss3a, .pak, .big, wallet, .wotreplay, .xxx, .desc, .py, .m3u, .flv, .js, .css, .rb, .png, .jpeg, .txt, .p7c, .p7b, .p12, .pfx, .pem, .crt, .cer, .der, .x3f, .srw, .pef, .ptx, .r3d, .rw2, .rwl, .raw, .raf, .orf, .nrw, .mrwref, .mef, .erf, .kdc, .dcr, .cr2, .crw, .bay, .sr2, .srf, .arw, .3fr, .dng, .jpe, .jpg, .cdr, .indd, .ai, .eps, .pdf, .pdd, .psd, .dbf, .mdf, .wb2, .rtf, .wpd, .dxg, .xf, .dwg, .pst, .accdb, .mdb, .pptm, .pptx, .ppt, .xlk, .xlsb, .xlsm, .xlsx, .xls, .wps, .docm, .docx, .doc, .odb, .odc, .odm, .odp, .ods, .odt
(Pilici, 2015)

Q5.

a) The program spawns one encryption thread for each volume that is not an optical drive.
b) The program creates an MD5 hash identifying the computer by gathering the system information, which is combined with the computer's IP address and sent back to the Cryptowall Command and Control centre. The Cryptowall server responds with a 3 digit number, which acts as a signal to start the main thread. The public key is generated using a combination of a crypt element and the MD5 hash.
c) - -

Q6.
It is relatively easy to remove this ransomware by deleting the executables and removing the registry keys. Decrypting the files is harder since the required key is stored on the creator's server. It is possible to restore files from the Volume Shadow Copies, assuming that they have not yet been overwritten.

Q7.
Older versions use a website only accessible through Tor. Payment is Bitcoin at a rate of 1.09XBC = $500 if the ransom is paid early, otherwise it rises to $2.18XBC = $1000

CryptoLocker

Q1.
It encrypts files such as documents, spreadsheets and images. The list is not as extensive as for Cryptowall but will still cover all of the most important files for the majority of people.

Q2.
It only scans drives that are either local or mapped. It does not scan network drives.

Q3.
It periodically scans for new files even after the initial encryption.

Q4.
*.odt, *.ods, *.odp, *.odm, *.odc, *.odb, *.doc, *.docx, *.docm, *.wps, *.xls, *.xlsx, *.xlsm, *.xlsb, *.xlk, *.ppt, *.pptx, *.pptm, *.mdb, *.accdb, *.pst, *.dwg, *.dxf, *.dxg, *.wpd, *.rtf, *.wb2, *.mdf, *.dbf, *.psd, *.pdd, *.pdf, *.eps, *.ai, *.indd, *.cdr, *.jpg, *.jpe, img_*.jpg, *.dng, *.3fr, *.arw, *.srf, *.sr2, *.bay, *.crw, *.cr2, *.dcr, *.kdc, *.erf, *.mef, *.mrw, *.nef, *.nrw, *.orf, *.raf, *.raw, *.rwl, *.rw2, *.r3d, *.ptx, *.pef, *.srw, *.x3f, *.der, *.cer, *.crt, *.pem, *.pfx, *.p12, *.p7b, *.p7c
(Hassell, 2013)

Q5.

a) It uses Microsoft's CryptoAPI rather than its own custom cipher.
b) It uses RSA AES public private key pair which are generated on the Command and Control server after the program sends a short request code.
c) - -

Q6.
Possible to extend the time limit by setting the BIOS clock back but once the time limit has run out the program uninstalls and it is impossible to recover the files by reinstalling Cryptolocker. The makers did offer a service whereby you send them a sample encrypted file and they would search for your key. This service cost 5 times as much as the original ransom demand. In 2014 security researchers at FireEye and Fox-IT obtained the private keys used by the program and reverse-engineered the program. In August of that year they published a free website where people could submit a sample encrypted file and receive a recovery program and master key by email.

Q7.
Once payment has been made, the countdown screen disappears and it displays a payment activation window. This checks every 15 minutes to see if payment has been accepted.

Locky

Q1.
The files it will encrypt can be divided into 11 different categories and 160 different file types. Office/Document files, scripts, media files, graphic or images, databases, archives, CAD/CAM/3D files, certificates, virtual HDD, data encryption (AES and GPG), virtual currency.

Q2.
It encrypts files that are on RAM disk drives, removable drives and fixed drives, newer versions can target remote drives and network file sources with no assigned drive letter. It does not encrypt computers whose locale is set to Russia.

Q3.
The program deletes information from the Volume Shadow Copy Service so that System Restore cannot rewind the files back to before encryption. It sets a registry value at *Software\Microsoft\Windows\CurrentVersion\Run* (“A closer look at the Locky ransomware,” 2016) *so that it can* continue encrypting after the computer has been restarted.

Q4.
.123, .602, .CSV, .dif, .DOC, .docb, .docm, .docx, .DOT, .dotm, .dotx, .hwp, .mml, .odg, .odp, .ods, .odt, .otg, .otp, .ots, .ott, .pdf, .pot, .potm, .potx, .ppam, .pps, .ppsm, .ppsx, .PPT, .pptm, .pptx, .RTF, .sldm, .sldx, .slk, .stc, .std, .sti, .stw, .sxc, .sxd, .sxi, .sxm, .sxw, .txt, .uop, .uot, .wb2, .wk1, .wks, .xlc, .xlm, .XLS, .xlsb, .xlsm, .xlsx, .xlt, .xltm, .xltx, .xlw, .xml, .asm, .asp, .bat, .brd, .c, .class, .cmd, .cpp, .cs, .dch, .dip, .h, .jar, .java, .js, .pas, .php, .pl, .rb, .sch, .sh, .vb, .vbs, .3g2, .3gp, .asf, .avi, .fla, .flv, .m3u, .m4u, .mid, .mkv, .mov, .mp3, .mp4, .mpeg, .mpg, .swf, .vob, .wav, .wma, .wmv, .bmp, .cgm, .djv, .djvu, .gif, .jpeg, .jpg, .NEF, .png, .psd, .raw, .svg, .tif, .tiff, .db, .dbf, .frm, .ibd, .ldf, .mdb, .mdf, .MYD, .MYI, .odb, .onenotec2, .sql, .SQLITE3, .SQLITEDB, .7z, .ARC, .bak, .gz, .PAQ, .rar, .tar, .bz2, .tbk, .tgz, .zip, .3dm, .3ds, .asc, .lay, .lay6, .max, .ms11, .ms11 (Security copy), .crt, .csr, .key, .p12, .pem, .qcow2, .vdi, .vmdk, .vmx, .aes, .gpg, wallet.dat
(“A closer look at the Locky ransomware,” 2016)

Q5.

a) The program uses RSA-2048+AES-128 encryption with ECB mode. It only encrypts after obtaining the RSA public key from the C & C server and while the computer is connected to the internet. All files that have been encrypted are given a new name in the format [userid][random hash].locky User ID is generated from a MD5 hash of the volume mount point GUID of the HDD. (“A closer look at the Locky ransomware,” 2016)
b) Locky generates a new 128-bit key for each file and encrypts it using AES-128 in CTR mode. It appends data to the end of the file containing the key, also encrypted using RSA-2048, and other relevant information.
c) - -

Q6.
It is not currently possible to decrypt files without paying the ransom. Files may be recovered using Volume Shadow Copy, the Previous Version feature in some apps

although Locky is capable of deleting these files, or by using data recovery programs which check for deleted files.

Q7.
Once encryption has been completed it sets an image as the desktop picture with instructions for the victim. Like other ransomware the website that the program directs its victim to is located inside the Tor network and payment is only in Bitcoins. The ransom amount is probably linked to how many files are encrypted.

Cerber

Q1.
Cerber targets the largest range of files of all the Ransomware programs in this study. Almost every type of file that could have any kind of importance is included.

Q2.
The program is capable of scanning for Windows shares on the victim's network and encrypting them, even if those locations are not mapped to the infected computer.

Q3.
The program bypasses the User Access Control in Windows so that it can run with elevated privileges. It does this by using a very sophisticated method to hijack another program in the Windows/System32 folder

Q4.

```
accdb,.mdb,.mdf,.dbf,.vpd,.sdf,.sqlitedb,.sqlite3,.sqlite,.sql,.sd
b,.doc,.docx,.odt,.xls,.xlsx,.ods,.ppt,.pptx,.odp,.pst,.dbx,.wab,.
tbk,.pps,.ppsx,.pdf,.jpg,.tif,.pub,.one,.rtf,.csv,.docm,.xlsm,.ppt
m,.ppsm,.xlsb,.dot,.dotx,.dotm,.xlt,.xltx,.xltm,.pot,.potx,.potm,.
xps,.wps,.xla,.xlam,.erbsql,.sqlite-shm,.sqlite-
wal,.litesql,.ndf,.ost,.pab,.oab,.contact,.jnt,.mapimail,.msg,.prf
,.rar,.txt,.xml,.zip,.1cd,.3ds,.3g2,.3gp,.7z,.7zip,.aoi,.asf,.asp,
.aspx,.asx,.avi,.bak,.cer,.cfg,.class,.config,.css,.dds,.dwg,.dxf,
.flf,.flv,.html,.idx,.js,.key,.kwm,.laccdb,.ldf,.lit,.m3u,.mbx,.md
,.mid,.mlb,.mov,.mp3,.mp4,.mpg,.obj,.pages,.php,.psd,.pwm,.rm,.saf
e,.sav,.save,.srt,.swf,.thm,.vob,.wav,.wma,.wmv,.3dm,.aac,.ai,.arw
,.c,.cdr,.cls,.cpi,.cpp,.cs,.db3,.drw,.dxb,.eps,.fla,.flac,.fxg,.j
ava,.m,.m4v,.max,.pcd,.pct,.pl,.ppam,.ps,.pspimage,.r3d,.rw2,.sldm
,.sldx,.svg,.tga,.xlm,.xlr,.xlw,.act,.adp,.al,.bkp,.blend,.cdf,.cd
x,.cgm,.cr2,.crt,.dac,.dcr,.ddd,.design,.dtd,.fdb,.fff,.fpx,.h,.ii
f,.indd,.jpeg,.mos,.nd,.nsd,.nsf,.nsg,.nsh,.odc,.oil,.pas,.pat,.pe
f,.pfx,.ptx,.qbb,.qbm,.sas7bdat,.say,.st4,.st6,.stc,.sxc,.sxw,.tlg
,.wad,.xlk,.aiff,.bin,.bmp,.cmt,.dat,.dit,.edb,.flvv,.gif,.groups,
.hdd,.hpp,.m2ts,.m4p,.mkv,.mpeg,.nvram,.ogg,.pdb,.pif,.png,.qed,.q
cow,.qcow2,.rvt,.st7,.stm,.vbox,.vdi,.vhd,.vhdx,.vmdk,.vmsd,.vmx,.
vmxf,.3fr,.3pr,.ab4,.accde,.accdr,.accdt,.ach,.acr,.adb,.ads,.agdl
,.ait,.apj,.asm,.awg,.back,.backup,.backupdb,.bank,.bay,.bdb,.bgt,
.bik,.bpw,.cdr3,.cdr4,.cdr5,.cdr6,.cdrw,.ce1,.ce2,.cib,.craw,.crw,
.csh,.csl,.db_journal,.dc2,.dcs,.ddoc,.ddrw,.der,.des,.dgc,.djvu,.
dng,.drf,.dxg,.eml,.erf,.exf,.ffd,.fh,.fhd,.gray,.grey,.gry,.hbk,.
ibank,.ibd,.ibz,.iiq,.incpas,.jpe,.kc2,.kdbx,.kdc,.kpdx,.lua,.mdc,
.mef,.mfw,.mmw,.mny,.moneywell,.mrw,.myd,.ndd,.nef,.nk2,.nop,.nrw,
.ns2,.ns3,.ns4,.nwb,.nx2,.nxl,.nyf,.odb,.odf,.odg,.odm,.orf,.otg,.
oth,.otp,.ots,.ott,.p12,.p7b,.p7c,.pdd,.mts,.plus_muhd,.plc,.psafe
3,.py,.qba,.qbr,.qbw,.qbx,.qby,.raf,.rat,.raw,.rdb,.rwl,.rwz,.s3db
,.sd0,.sda,.sr2,.srf,.srw,.st5,.st8,.std,.sti,.stw,.stx,.sxd,.sxg,
.sxi,.sxm,.tex,.wallet,.wb2,.wpd,.x11,.x3f,.xis,.ycbcra,.yuv,.mab,
.json,.msf,.jar,.cdb,.srb,.abd,.qtb,.cfn,.info,.info_,.flb,.def,.a
```

`tb,.tbn,.tbb,.tlx,.pml,.pmo,.pnx,.pnc,.pmi,.pmm,.lck,.pm!,.pmr,.usr,.pnd,.pmj,.pm,.lock,.srs,.pbf,.omg,.wmf,.sh,.war,.ascx,.k2p,.apk,.asset,.bsa,.d3dbsp,.das,.forge,.iwi,.lbf,.litemod,.ltx,.m4a,.re4,.slm,.tiff,.upk,.xxx,.money,.cash,.private,.cry,.vsd,.tax,.gbr,.dgn,.stl,.gho,.ma,.acc,.db`
(Abrams, 2016)

Q5.

a) Much of the program has not yet been deciphered but it is known that it checks for anti-malware software running on the computer. It can generate a log when sued in debug mode. There is a configuration file which can be used to customise options. The program is able to bypass User Access Control.
b) It can run the encryption in offline mode, it does not need to contact the C & C server to get the keys. It is likely that the file is appended to with the RSA encrypted AES key because the file size increases by about 384 bytes. The RSA public key is included in the program.
c) - -

Q6.

It is not currently possible to decrypt the files without paying the ransom. The creators of this program are still very active, releasing new and more capable versions on a regular basis. It might be possible to use System Restore if you act in time before the ransomware has corrupted them.

Q7.

Website for the ransom demand can only be accessed through Tor. Initially the ransom amount is 1.24 Bitcoins but after 7 days this doubles to 2.48 Bitcoins. The ransom note on the computer is only in English but the version on the TOR website has been translated into several languages.

Petya

Q1.
This program encrypts the Master File Table to prevent normal access to the files. It also overwrites the Master Boot record with its own custom one. It does not encrypt the entire disk despite claiming to do so.

Q2.
This program only targets the local machine.

Q3.
It does not automatically give itself elevated privileges so when the program is run, Windows will display the UAC dialogue. Once it has completed the first stage, it intentionally crashes the computer then runs through a fake CHKDISK routine while it encrypts the Mater Boot Record.

Q4.
This program does not target specific file extensions.

Q5.

a) It uses encryption algorithms from the public library mbedtls (formerly polarssl). It remains in RAM once created and not saved to the hard drive.
b) The key is generated through a series of several different encryption steps utilising a combination of AES, XOR, random data, SHA512 and public/private keys
c) - -

Q6.
Leo Stone has developed a program that generates a decryption key. If the user notices a problem quickly enough and switches off their computer, the only damage done is through 1-byte XOR and it is possible for a specialist to recover from this. The user identifier is decrypted to find out the file decryption key. All of this information is held in the program, no data is sent to the C & C server.

Q7.
The user is confronted with a flashing red page and a skull and crossbones picture. They are then instructed to download the Tor browser and visit an onion website where they have to enter their unique code. This screen also has text entry for the purchased key. Payment is in Bitcoins. The payment page tries to scare the user further by stating that RSA encryption has been used, when it has not.

Questions for the designed ransomware

Q1. Distribution scheme

Q2. Obfuscation

Q3. Command and Control (C&C) Communications

Q4. What files will it encrypt?

Q5. Describe how to search for local and network drives?

Q6. How to get files from the drive?

Q7. What are the supported file extensions?

Q8. How does it encrypt files?

a. A description of the algorithm design explaining the operations that are performed at each processing stage, their input and output and processing flow.
b. A description of key generation and preparation at each processing stage
c. A schematic diagram that depicts the components of the algorithm, their running order (processing flow), interaction between components, inputs and outputs and number of rounds

Q9. Is there a way to decrypt the files? or identify, detect and remove the ransomware?

Q10. What are the payment instructions like?

Q1.
The program should be distributed by means of an attachment with an email. Document and spreadsheet files are zipped containers with files and subfolders for objects such as images, settings and styles, amongst other things. A python script can be embedded within this structure as a macro. When the document is opened by the victim, if their security settings are set low enough they may be asked if they want to enable macros, which if they do would let the program run and do its damage.

To guard against this threat, users should set the macro security in the Office program's security settings to high and only open documents that they are expecting and from people they know and trust. Even then, if the document contains a macro, they should check with the sender whether or not the document can be trusted.

Q2.
One way of obfuscating the program's identity is to hide in plain sight. Giving the program the same or similar name as a relatively common or system program helps to avoid suspicion. The program in this project is designed to encrypt the user's Home space. This will help it to avoid detection by virus scanners because the user has permission to modify files in these folders. Yet it will also cause significant damage since this is where the user's personal files and program settings are stored.

Q3.
The program should generate a random key, which is sent to the Command and Control server and stored in a database along with a string that uniquely identifies this particular computer. The server uses the ransom key to generate a public and private key. The public key is returned to the computer and used to encrypt the files using RSA encryption. The private key is stored in the database and only retrieved if the ransom is paid. This type of encryption is unbreakable, meaning that the victim has only two options. Pay the ransom or lose their files.

Q4.
The program is designed to encrypt text files However this can encompass a wide range of different file types including text-based program files and program settings. The program will ignore any file types that it cannot encrypt, such as binary files.

Q5.
In Python, if the option to follow links in os.walk is set to True, the program will discover drives and directories that have been mounted in the user's home space. If the program is run with administrator permissions, the program can discover other drives and partitions in /dev/sdx or /mnt but this is more difficult to program since it normally requires a password.

Q6.
The program uses a Python module called os.walk, which traverses through the folder structure, touching upon each sub-folder and file as it encounters them. For each file it finds it checks the extension against the list of supported extensions. If the file is not supported, it is ignored, otherwise the filename is added to the path of the current location and passed to the encrypt or decrypt section depending on the selected mode.

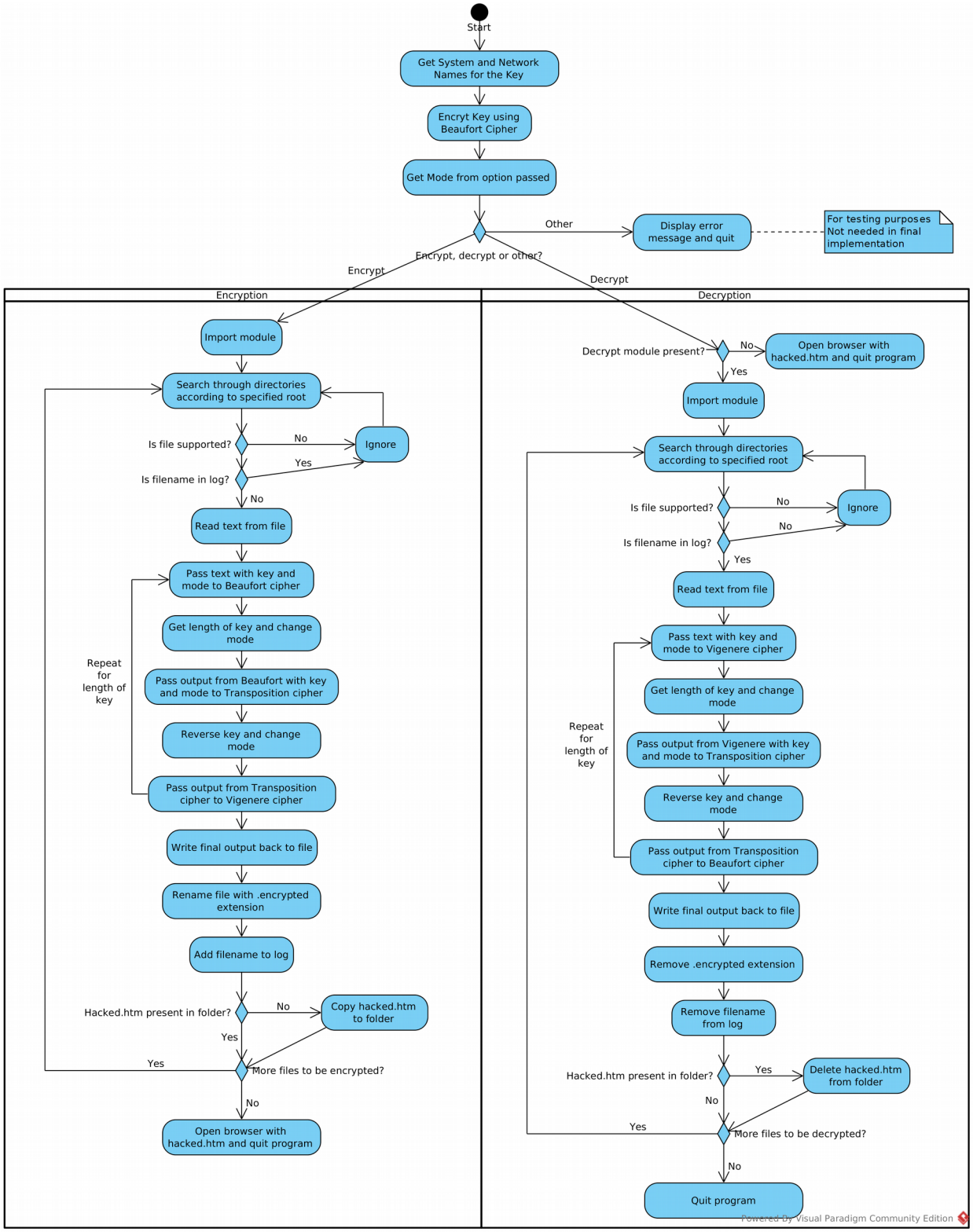
Q7.
The actual file types that this program is designed to target is listed below.

'.txt', '.xhtml', '.html', '.htm', '.css', '.php', '.sql', '.java', '.jsp', '.js', '.xml', '.xsl', '.xsd', '.xslt', '.xlog', '.json', '.py', '.rtf', '.srt', '.sub', '.csv', '.conf', '.log', '.manifest', '.lrc', '.html5', '.linux', '.sha1', '.sha512', '.err', '.readme', '.man', '.encrypted'

‘.encrypted’ is included so that the program can locate these files in order to decrypt them.

Q8.

a) The encryption algorithm combines 3 of the classic text ciphers into a product cipher, Beaufort, Transposition and Vigenère. Each cipher takes three arguments, the text from the file, the key and the mode. The file is first read into memory and the text passed to the Beaufort cipher with the key and mode. The output from this is passed to the Transposition cipher, and the mode is changed from encrypt to decrypt in order to strengthen the cipher. The result from the Transposition cipher is passed to the Vigenère cipher, for which the mode is changed back to encrypt. This algorithm is repeated x number of times, where x is the length of the key. Once encryption has completed, the text is written back out to the file and it is renamed with the .encrypted extension and the filename is also added to the log file.
b) The key is generated by concatenating the system and network names of the computer. It is then reversed using the Reverse cipher and the two variables are passed as string and key into the Beaufort cipher to be encrypted. This constitutes the key for the first cipher in the encryption algorithm. The second cipher takes the length of the key and for the third cipher the key is reversed.



c)

Q9.

The designed program is also able decrypt files that it has encrypted. The encryption and decryption modules are separate and the program can operate if either is not present. If

the decrypt module is not present, the program will display the message of how to pay the ransom and then exit cleanly.

Some online backup services such as Dropbox provide version history, so if your files are automatically backed up to the cloud and those are subsequently encrypted as well, it is possible to revert to a previous version. This approach should not be relied upon as a

Q10.
The program will copy a html file called hacked.htm into each folder that contains encrypted files. This file contains details of what has happened to the victim's files and how to get them back. The victim is instructed to first download the TOR browser because the address that contains details of where to send the ransom is a onion address which can only be reached through TOR. The TOR network hides the location of the server containing the website, which makes it more difficult for the police to track or remove the website. Payment is made using Bitcoin, which is a peer-to-peer transaction system. While Bitcoin transaction are always tracked, it is very difficult to discover who owns the bitcoin address that the transaction is sent to.

Most security experts advise against paying the ransom. It only serves to encourage more attacks of this type and there is no guarantee that those demanding payment will keep their word and provide means of decryption. The best defence against this type of attack is to regularly backup files in a location that is kept physically and logically separate from the host computer.

Appendix

The top five ransomware were chosen by analysing a number of security blogs and counting how many times each one was mentioned. Below is a screenshot of the spreadsheet used to count and sort this data.

	Cryptowall	CryptoLocker	Locky	Cerber	Petya	TorrentLocker	CTB-Locker	TeslaCrypt	AlphaCrypt	Reveton	PowerWare	Surprise	Bit Cryptor	CryptXXX	Chimera	Zev3n	Samas	Tox Ransomware	Jigsaw	Shade	KeRanger	Zepto	Fairware	Wildfire	TorrentWall	OphionLocker	VaultCrypt
http://technofaq.org	1	1	1		1																1						
https://cyware.com				1	1																	1	1	1			
http://news.softpedia	1		1	1		1		1																			
http://www.compuerwee	1		1		1		1	1																			
http://www.symantec.c			1	1										1													
http://www.datto.com/	1	1																							1		
https://blog.varonis.	1	1	1			1	1		1			1			1	1	1									1	
https://en.wikipedia.	1	1				1				1																	
http://www.computerwo	1	1	1	1	1						1																
http://www.darkreadin	1	1								1																	
http://cfoc.org/top-1		1							1				1					1									
https://www.trendmicr	1	1	1	1							1	1							1								
http://www.zdnet.com/	1	1											1														
https://securelist.co	1					1	1													1							
https://www.trendmicr			1	1	1									1		1	1		1	1							
http://www.darkreadin	1														1			1									
http://www.mcafee.com	1	1				1	1	1																			
Total	13	10	8	6	5	5	4	3	2	2	2	2	2	2	2	2	2	2	2	2	1	1	1	1	1	1	

References

Abrams, L. (2016). *The Cerber Ransomware not only Encrypts Your Data But Also Speaks to You*. [online] BleepingComputer. Available at: https://www.bleepingcomputer.com/news/security/the-cerber-ransomware-not-only-encrypts-your-data-but-also-speaks-to-you/ [Accessed 16 Dec. 2016].

Abrams, L. (2016). *Petya Ransomware skips the Files and Encrypts your Hard Drive Instead*. [online] BleepingComputer. Available at: https://www.bleepingcomputer.com/news/security/petya-ransomware-skips-the-files-and-encrypts-your-hard-drive-instead/ [Accessed 16 Dec. 2016].

AG, G. (2016). *Ransomware Petya encrypts hard drives - G DATA*. [online] Blog.gdatasoftware.com. Available at: https://blog.gdatasoftware.com/2016/03/28213-ransomware-petya-encrypts-hard-drives [Accessed 16 Dec. 2016].

Berghoff, T. (n.d.). *Ransomware Petya - a technical review - G DATA*. [online] Blog.gdatasoftware.com. Available at: https://blog.gdatasoftware.com/2016/03/28226-ransomware-petya-a-technical-review [Accessed 16 Dec. 2016].

Bitcoin, (2016). *Bitcoin - Open source P2P money*. [online] Bitcoin.org. Available at: https://bitcoin.org/en/ [Accessed 16 Dec. 2016].

Blog.avast.com. (2016). *A closer look at the Locky ransomware*. [online] Available at: https://blog.avast.com/a-closer-look-at-the-locky-ransomware [Accessed 16 Dec. 2016].

Blue, V. (2013). *CryptoLocker's crimewave: A trail of millions in laundered Bitcoin | ZDNet*. [online] ZDNet. Available at: http://www.zdnet.com/article/cryptolockers-crimewave-a-trail-of-millions-in-laundered-bitcoin/ [Accessed 16 Dec. 2016].

Bourez, C. (2015). *Interface-oriented programming in OpenOffice / LibreOffice : automate your office tasks with Python Macros*. [online] Christopher5106.github.io. Available at: https://christopher5106.github.io/office/2015/12/06/openoffice-libreoffice-automate-your-office-tasks-with-python-macros.html [Accessed 16 Dec. 2016].

Chacos, B. (2014). *CryptoLocker decrypted: Researchers reveal website that frees your files from ransomware*. [online] PCWorld. Available at: http://www.pcworld.com/article/2462280/cryptolocker-decrypted-researchers-reveal-website-that-frees-your-files-from-ransomware.html [Accessed 16 Dec. 2016].

Ducklin, P. (2013). *Destructive malware “CryptoLocker” on the loose – here’s what to do*. [online] Naked Security. Available at: https://nakedsecurity.sophos.com/2013/10/12/destructive-malware-cryptolocker-on-the-loose/ [Accessed 16 Dec. 2016].

Engineer, J. (2016). *PETYA Crypto-ransomware Overwrites MBR to Lock Users Out of Their Computers - TrendLabs Security Intelligence Blog*. [online] TrendLabs Security Intelligence Blog. Available at: http://blog.trendmicro.com/trendlabs-security-intelligence/petya-crypto-ransomware-overwrites-mbr-lock-users-computers/ [Accessed 16 Dec. 2016].

Group, T. (2015). *Cryptowall 3.0: Back to the Basics*. [online] blogs@Cisco - Cisco Blogs. Available at: https://blogs.cisco.com/security/talos/cryptowall-3-0 [Accessed 16 Dec. 2016].

hasherezade, (2016). *Cerber Ransomware – New, But Mature*. [online] Malwarebytes Labs. Available at: https://blog.malwarebytes.com/threat-analysis/2016/03/cerber-ransomware-new-but-mature/ [Accessed 16 Dec. 2016].

hasherezade, (2016). *Petya – Taking Ransomware To The Low Level*. [online] Malwarebytes Labs. Available at: https://blog.malwarebytes.com/threat-analysis/2016/04/petya-ransomware/ [Accessed 16 Dec. 2016].

Hassell, J. (2013). *Cryptolocker: How to avoid getting infected and what to do if you are*. [online] Computerworld. Available at: http://www.computerworld.com/article/2485214/microsoft-windows/cryptolocker-how-to-avoid-getting-infected-and-what-to-do-if-you-are.html [Accessed 16 Dec. 2016].

Msdn.microsoft.com. (n.d.). *CryptEncrypt function (Windows)*. [online] Available at: https://msdn.microsoft.com/en-us/library/aa379924.aspx [Accessed 16 Dec. 2016].

Msdn.microsoft.com. (n.d.). *Example C Program: Encoding and Decoding Data (Windows)*. [online] Available at: https://msdn.microsoft.com/en-us/library/aa382052.aspx [Accessed 16 Dec. 2016].

Nabzsoftware.com. (n.d.). *Remove CryptoWall 3.0 virus: how to decrypt CryptoWall 3.0 encrypted files – Nabz Software*. [online] Available at: http://nabzsoftware.com/types-of-threats/cryptowall-3-0 [Accessed 16 Dec. 2016].

O'Brien, L. and Morparia, J. (2014). *Ransom.Cryptowall | Symantec*. [online] Symantec.com. Available at: https://www.symantec.com/security_response/writeup.jsp?docid=2014-061923-2824-99 [Accessed 16 Dec. 2016].

Pilici, S. (2015). *Remove CryptoWall 3.0 virus (Files Encrypted Ransomware)*. [online] MalwareTips Blog. Available at: https://malwaretips.com/blogs/remove-cryptowall-3-0-virus/ [Accessed 16 Dec. 2016].

Sconzo, M. (2016). *The Evolution of Cerber | RSA Link*. [online] Community.rsa.com. Available at: https://community.rsa.com/community/products/netwitness/blog/2016/09/27/the-evolution-of-cerber [Accessed 16 Dec. 2016].

Sinitsyn, F. (2016). *Locky: the encryptor taking the world by storm - Securelist*. [online] Securelist.com. Available at: https://securelist.com/blog/research/74398/locky-the-encryptor-taking-the-world-by-storm/ [Accessed 16 Dec. 2016].

Sinitsyn, F. (2016). *Petya: the two-in-one trojan - Securelist*. [online] Securelist.com. Available at: https://securelist.com/blog/research/74609/petya-the-two-in-one-trojan/ [Accessed 16 Dec. 2016].

Stone, L. (2016). *leo-stone/hack-petya*. [online] GitHub. Available at: https://github.com/leo-stone/hack-petya [Accessed 16 Dec. 2016].

Stoyanov, D. (2016). *Decrypt Locky Ransomware (.locky Extension) for Free*. [online] Virus Guides. Available at: http://virusguides.com/decrypt-locky-ransomware-locky-extension-for-free/ [Accessed 16 Dec. 2016].

The Tor Project, (2016). *Tor Project: Anonymity Online*. [online] Torproject.org. Available at: https://www.torproject.org/ [Accessed 16 Dec. 2016].