What is TeslaCrypt and AlphaCrypt?

TeslaCrypt and **Alpha Crypt** are file-encrypting ransomware programs that target all version of Windows including Windows XP, Windows Vista, Windows 7, and Windows 8. TeslaCrypt was first released around the end of February 2015 and Alpha Crypt was released at the end of April 2015. When you are first infected with TeslaCrypt or Alpha Crypt they will scan your computer for data files and encrypt them using AES encryption so they are no longer able to be opened. Once the infection has encrypted the data files on all of your computer drive letters it will display an application that contains instructions on how to get your files back. These instructions include a link to a Decryption Service site, which will inform you of the current ransom amount, the amount of files encrypted, and instructions on how to make your payment. The ransom cost starts at around $500 USD and is payable via bitcoins. The bitcoin address that you submit payment to will be different for every victim.

When TeslaCrypt or Alpha Crypt are first installed on your computer they will create a random named executable in the %AppData% folder. This executable will be launched and begin to scan all the drive letters on your computer for data files to encrypt. If a a supported data file is detected it will encrypt it and then append a new extension to the filename based on the particular variant you are infected with. When a new version of TeslaCrypt is released, it will use different file extensions for your encrypted files. The current list of extensions used by TeslaCrypt are **.ecc**, **.ezz**, **.exx**, .**xyz**, **.zzz**, **.aaa**, **.abc**, **.ccc**, and one version did not change your filename at all. Depending on the version of TeslaCrypt you were infected with, it may be possible to use the TeslaDecoder tool to decrypt your files for free.

The extensions targeted by TeslaCrypt are:

.7z, .rar, .m4a, .wma, .avi, .wmv, .csv, .d3dbsp, .sc2save, .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, .mcgame, .vdf, .ztmp, .sis, .sid, .ncf, .menu, .layout, .dmp, .blob, .esm, .001, .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, .DayZProfile, .rofl, .hkx, .bar, .upk, .das, .iwi, .litemod, .asset, .forge, .ltx, .bsa, .apk, .re4, .sav, .lbf, .slm, .bik, .epk, .rgss3a, .pak, .big, .unity3d, .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, .dbfv, .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

The extensions targeted by Alpha Crypt and newer versions of this family are:

.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,

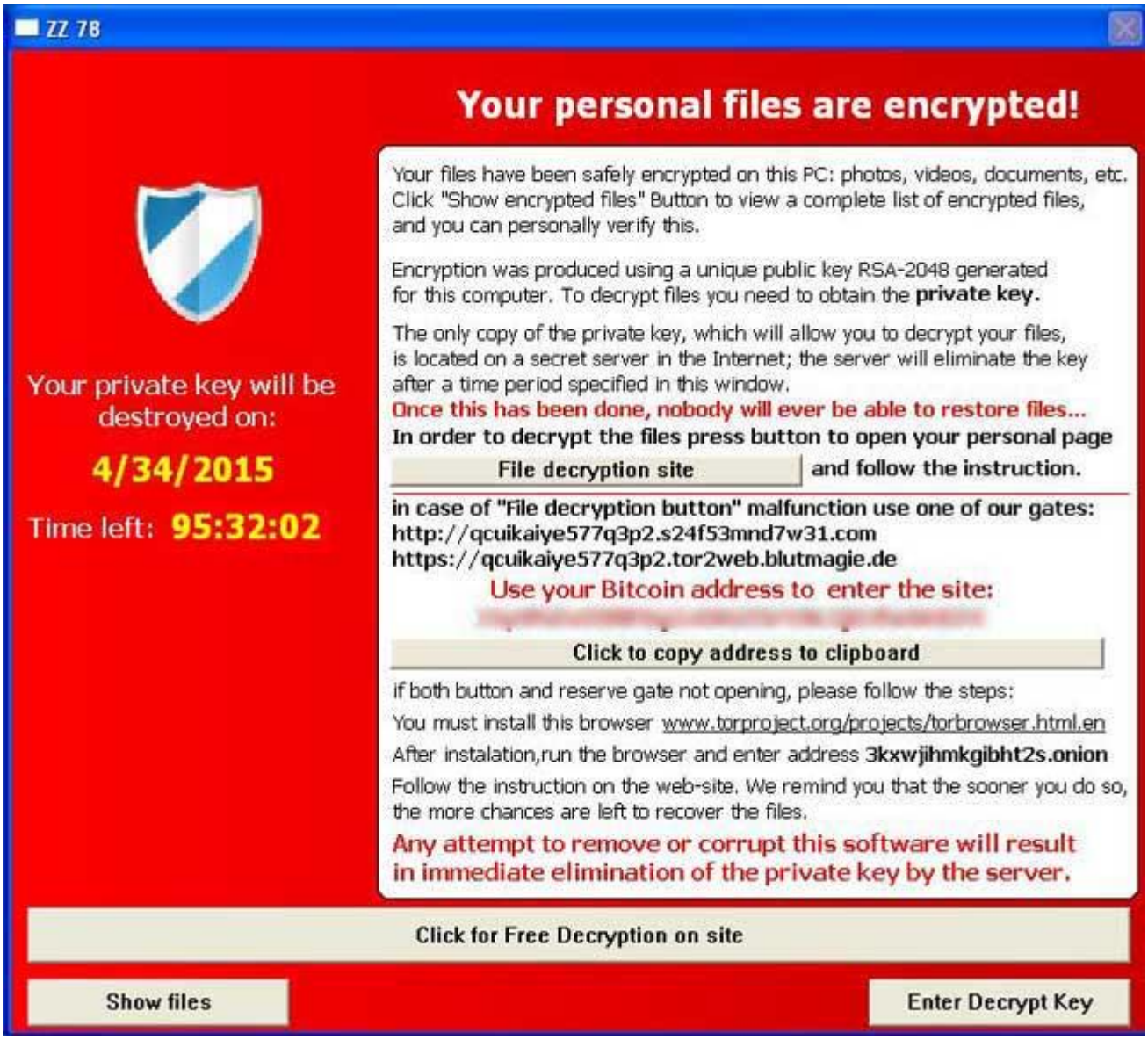
.db0, .dba, .rofl, .hkx, .bar, .upk, .das, .iwi, .litemod, .asset, .forge, .ltx, .bsa, .apk, .re4, .sav, .lbf, .slm, .bik, .epk, .rgss3a, .pak, .big, wallet, .wotreplay, .xxx, .desc, .py, .m3u, .flv, .js, .css, .rb, .png, .jpeg, .txt, .p7c, .p7b, .p12, .pfx, .pem, .crt, .cer, .der, .x3f, .srw, .pef, .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

It important to stress that both TeslaCrypt and Alpha Crypt will scan all drive letters on your computer including removable drives, network shares, and even DropBox mappings. In summary, if there is a drive letter on your computer it will be scanned for data files to encrypt by the ransomware

When the infection has finished scanning your computer it will also delete all of the Shadow Volume Copies that are on the affected computer. It does this so that you cannot use the shadow volume copies to restore your encrypted files. There are posts that state TeslaCrypt did not delete Shadow Volume Copies, but this is untrue. The command that is run to clear the Shadow Volumes is:

vssadmin delete shadows /all

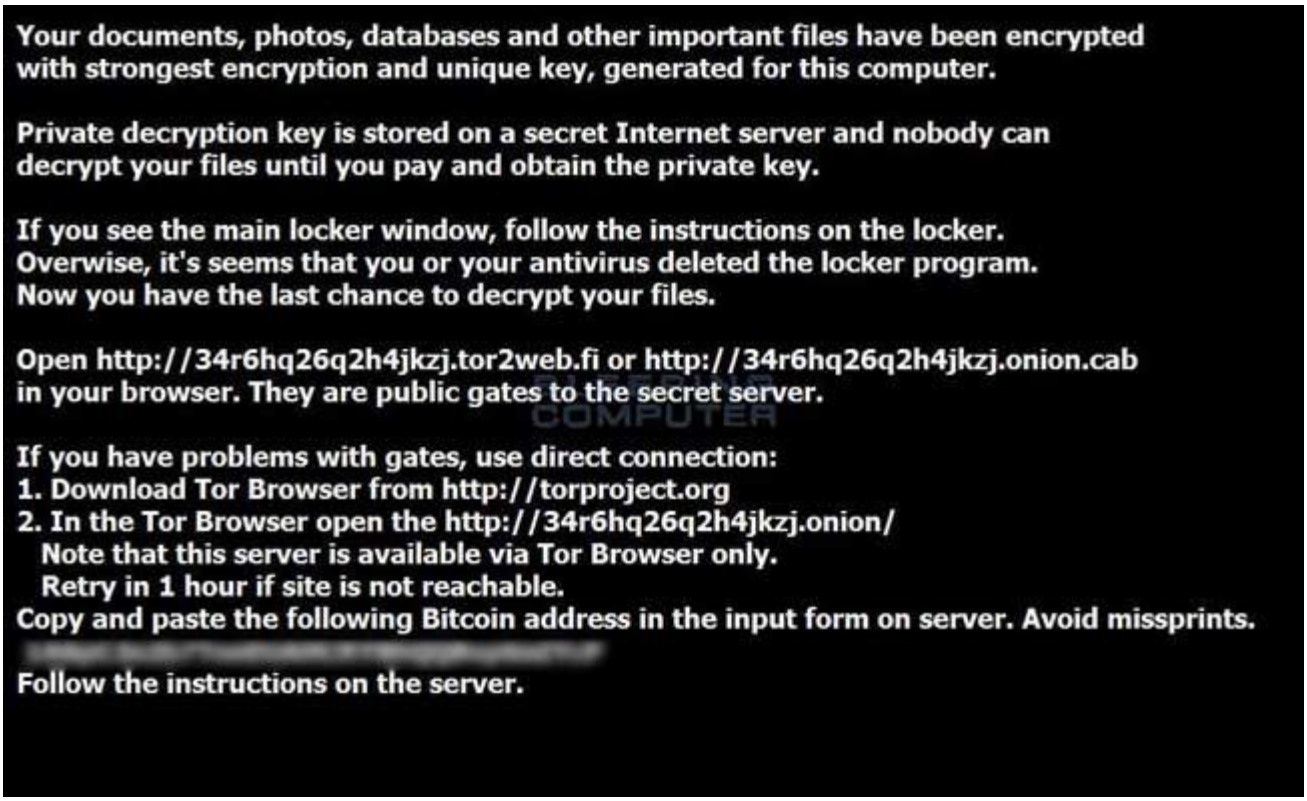
Now that your computer's data has been encrypted it will display the TeslaCrypt or Alpha Crypt application. For both of the ransomware variants the screens are identical other than the application title. The application title denotes the version of the ransomware.



Alpha Crypt Screen

While encrypting your files, this ransomware also create a text file ransom note in each folder that a file has been encrypted and on the Windows desktop. The ransomware will also change your Windows desktop wallpaper to a BMP file located on the Windows desktop. For TeslaCrypt the text ransom note is called **HELP_TO_DECRYPT_YOUR_FILES.txt** or **HELP_RESTORE_FILES.txt** and the BMP file is called **HELP_TO_DECRYPT_YOUR_FILES.bmp** or **HELP_RESTORE_FILES.bmp**. For Alpha Crypt the files are called **HELP_TO_SAVE_FILES.txt** and **HELP_TO_SAVE_FILES.bmp**.

Both the wallpaper and the text ransom note will contain the same information on how to access the payment site and get your files back. An example of the wallpaper can be seen below.



TeslaCrypt Wallpaper

When you go to the URLs listed in the ransom note you will be taken to a TOR site where you can learn how much your ransom is and how to make the payment. The payment site for TeslaCrypt is called the TeslaCrypt Decryption Service and for Alpha Crypt it is called the Alpha Tool Decryption Service. TeslaCrypt differs from most other ransomware as being the first to accept PayPal My Cash cards. With the release of AlphaCrypt, PayPal My Cash Cards were removed as a payment option. For more details about the Decryption Service, please skip to this section.

The text of the ransom application is:

All your important files are encrypted!

Your personal files(including those on the network disks, USB, etc) have been encrypted: photos, videos, documents, etc. Click "Show files" Button to view a complete list of encrypted files, and you can personally verify this.

Encryption was made using a unique strongest RSA-2048 public key generated for this computer. To decrypt files you need to acquire the private key.
The only copy of the private key, which will allow you to decrypt your files,is located on a secret TOR
server in the Internet; the server will eliminate the key after a time period specified in this

window.
Once this has been done, nobody will ever be able to restore files...

In order to decrypt files press button to open your personal page and follow the instruction. In case of "File decryption button" malfunction use one of public gates:
http://iq3ahijcfeont3xx.anfeua74x36.com or
https://iq3ahijcfeont3xx.tor2web.blutmagie.de

Use your Bitcoin address to enter the site: <bitcoin address>

if both button and reserve gates not opening, please follow these steps:
You must install TOR browser www.torproject.org/projects/torbrowser.html.en
After installation,run the browser and enter address iq3ahijcfeont3xx.onion
Follow the instructions on the web-site. We remind you that the sooner you do so, the more chances are left to recover the files.

There is no other way to restore your files except of making the payment.
Any attempt to remove or corrupt this software will result in immediate elimination of the private key by the server.

What should you do when you discover your computer is infected with TeslaCrypt or Alpha Crypt

If you discover that your computer is infected with TeslaCrypt you should immediately shutdown your computer and if possible create a copy, or image, of your hard drive. This allows you to save the complete state of your hard drive in the event that a free decryption method is developed in the future. For more information on how to do this, feel free to ask in the forums.

If you do not plan on paying the ransom and can restore from a backup, then scan your computer with an anti-virus or anti-malware program and let it remove everything. Unfortunately, most people do not realize TeslaCrypt or Alpha Crypt is on their computer until it displays the ransom note and your files have already been encrypted. The scans, though, will at least detect and remove any other malware that may have been installed along with the ransomware program.

As always we never recommend you pay the ransom, but if you do plan on doing so it is important that you do not delete anything from your computer. This is because the payment site may need certain files created by the infection to properly deliver you your key.

Some of the folders and file locations where associated malware have been found are:

%Temp%
C:\<random>\<random>.exe
%AppData%
%LocalAppData%

%ProgramData%
%WinDir%

How do you become infected with TeslaCrypt or Alpha Crypt?

A user is typically infected by TeslaCrypt or Alpha Crypt when they visit a hacked web site running an exploit kit and have outdated programs on their computer. In order to distribute their malware, developers will hack web sites and install a special software called an exploit kit that attempts to exploit vulnerabilities found in programs on your computer. The programs that are typically exploited include Java, Adobe Flash, Acrobat Reader, and Windows vulnerabilities. When an exploit kit successfully exploits your computer, it will install and start the ransomware without your knowledge.

Therefore, it is imperative that everyone keeps Windows and their installed programs up-to-date. You can use these tutorials for more information on keeping your Windows installation and installed programs updated:

How to update Windows
How to detect vulnerable and out-dated programs using Secunia Personal Software Inspector (PSI)

TeslaCrypt and it's targeting of Games

TeslaCrypt was the first ransomware to actively target data files used by PC video games. The game files being targeted belonged to games such as RPG Maker, Call of Duty, Dragon Age, StarCraft, MineCraft, World of Warcraft, Diablo, Fallout 3, Half Life 2, Skyrim, Day Z, League of Legends, World of Tanks, Steam, and many more. Though it is unknown if targetting games increased revenue for the malware developers, Alpha Crypt continues to target the same data files.

Though this was newsworthy, it is important to remember that TeslaCrypt and Alpha Crypt also happily encrypt your documents and images as well.

What you need to know about TeslaCrypt, Alpha Crypt, and Network Shares

TeslaCrypt and Alpha Crypt will encrypt data files on network shares only if that network share is mapped as a drive letter on the infected computer. If it is not mapped as a drive letter, then TeslaCrypt will not encrypt any files on a network share.

It is still strongly suggested that you secure all open shares by only allowing writable access to the necessary user groups or authenticated users. This is an important security principle that should be used at all times regardless of infections like these.

Decryption Service Site (TeslaCrypt and Alpha Crypt Payment Site)

The developers of TeslaCrypt created a TOR web site that victims can use to pay the ransom and decrypt their files. This web site is titled the **Decryption Service**, for TeslaCrypt, and the **Alpha Tool Decryption Service**, for Alpha Crypt. When you visit this site you will get information information about your encrypted files, learn how to pay the ransom, be given the ability to decrypt one file for free, and support page where you can receive "help" from the malware developers. Links to this site can be found in the **HELP_TO_SAVE_FILES.txt** and the **HELP_TO_DECRYPT_YOUR_FILES.txt** ransom notes that are found on your Windows desktop. Once you visit the site you can pay the ransom, which is currently between $300-$500 USD by sending Bitcoins to a specified address.