

Forum:[Hack Forums](#)

Thread: [New TeslaCrypt Ransomware sets its scope on video gamers](#)

Meow - February 28, 2015, 3:24 pm

A new ransomware called TeslaCrypt was discovered by Fabian Wosar of Emsisoft that encrypts your files using AES encryption and then demands a ransom payment in order to decrypt your files. What makes TeslaCrypt different than other ransomware is its attempt to cash in on the \$81 billion game market by placing a strong emphasis on encrypting video game related files. Unlike other ransomware that typically target images, documents, videos, and applications databases, TeslaCrypt also targets over 40 different video game related files. The game files being targeted belong to games such as RPG Maker, Call of Duty, Dragon Age, StarCraft, MineCraft, World of Warcraft, World of Tanks, and Steam.

Another major difference with this ransomware is that for the first time this type of infection not only accepts bitcoins as a ransom payment, but also accepts PayPal My Cash cards. PayPal My Cash cards are cards that can be purchased at popular US store chains and then filled with money that can then be transferred to a PayPal account using the PIN on the card. Paying the ransom with PayPal My Cash cards, though, comes at a premium of \$1,000, while paying the ransom with bitcoins is half that price at \$500 USD. This higher price for using the Cash cards is probably due to the higher risk of the illegal gains being confiscated by PayPal.

At this point it is unknown as to how TeslaCrypt is distributed, but once a computer is infected it will scan all drives on a computer and encrypt certain file types using AES encryption. Any files that are encrypted will have the .ecc extension added to the end of the filename. The file types encrypted by the TeslaCrypt ransomware are:

Quote:

```
.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;.mdbbackup;.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;.lvi;.snx;.cfr;.ff;.vpp_pc;.lrf;.m2;.mcmeta;.vfs0;.mpqge;.kdb;.db0;.DayZProfile;.rofl;.hxx;.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;
```

Unlike other ransomware, TeslaCrypt pays peculiar attention to files used by popular games such as Dragon Age, Call of Duty, StarCraft 2, RPG Maker, World of Warcraft, World of Tanks, Minecraft, DayZ, and League of Legends. This targeting of video game related files is a new development in ransomware. Once all of your data has been encrypted, it will run the following command to delete all Shadow Volume Copies and restore points from your computer. This is done so you are unable to restore your data from System Restore Points.

Quote:vssadmin delete shadows /all

Finally, the ransomware will change your Desktop wallpaper to a ransom note and create another ransom note called HELP_TO_DECRYPT_YOUR_FILES.txt on your desktop. A lock screen will then appear that explains your data was encrypted and that you have 3 days to make payment. This

lock screen contains buttons that allow you to check whether a payment has been accepted, the ability to enter your decryption keys, and a link to a TOR payment site where you can perform a free file decryption as a test.

[img]http://www.bleepstatic.com/swr-guides/t/teslacrypt-ransomware/teslacrypt-screen.jpg[/img]

TeslaCrypt's TOR site provides instructions on how you can make your ransom payment in bitcoins or PayPal My Cash Cards. The site also allows you to decrypt one file for free to prove that they can indeed decrypt your files. Last, but not least, the site includes a message system that allows a victim to communicate privately with the malware developers.

Unfortunately, at this time there is no known method of decrypting your files for free. As always we recommend that you do not pay the ransom if you can avoid it. Instead restore files from a backup or try restoring your files using Shadow Explorer or with a file recovery tool like R-Studio, Photorec, or Recuva. None of these restoration methods are guaranteed to work, but it is worth trying as people have reported success with malware like TeslaCrypt in the past.

Known TeslaCrypt Ransomware Files:

Quote:%AppData%\<random>.exe

%AppData%\key.dat

%AppData%\log.html

%Desktop%\CryptoLocker.lnk

%Desktop%\HELP_TO_DECRYPT_YOUR_FILES.bmp

%Desktop%\HELP_TO_DECRYPT_YOUR_FILES.txt

Known TeslaCrypt Ransomware Registry keys:

Quote:

HKCU\Software\Microsoft\Windows\CurrentVersion\Run\crypto13 %AppData%\<random>.exe

I DID NOT WRITE THIS,ORIGINAL POST CAN BE FOUND HERE:

<http://www.bleepingcomputer.com/forums/t/568525/new-teslacrypt-ransomware-sets-its-scope-on-video-gamers/>

-Hyperion - February 28, 2015, 5:55 pm

Finally a good malware idea from them

The Frost - March 14, 2015, 4:26 pm

This is going a bit too far in my opinion. \$500 to decrypt it? Anyone knows how this ransomware is being spreaded?

Meow - March 15, 2015, 4:25 am

(Mar 14, 2015 04:26 PM)The Frost Wrote: [\[CITE\]](#) This is going a bit too far in my opinion. \$500 to decrypt it? Anyone knows how this ransomware is being spreaded?

Probably with those "free steam games" stuff or something like that,not sure tho. ?

Nigissimo - March 15, 2015, 3:40 pm

Is it just me, or is targeting Gamers with Ransom Ware is bizarre at best. What 14 year old playing Minecraft will fork over 500\$ to get his saves back? And what stops a user from just reformatting the drive and redownloading the games through steam or reinstalling them through a disk. Especially when many games now upload saves to the cloud.

EagleEye - March 16, 2015, 2:40 am

thats going too far in this shit malware , 500\$ why ??

before it was fake FBI warning now this

scirpkiddie - March 16, 2015, 2:44 am

have if i ever got this i would just reformat the hard drive then restore my games with a back up i have disconnected from my pc :'L

Little Girls - March 17, 2015, 5:06 am

Isn't this that Zeus game over bot, and if it is your files will be deleted unless you pay, but I suggest getting someone to decrypt the files instead of paying.

Nyan~

Ghanem - March 17, 2015, 6:54 am

(Mar 17, 2015 05:06 AM)Little Girls Wrote: [CITE](#) Isn't this that Zeus game over bot, and if it is your files will be deleted unless you pay, but I suggest getting someone to decrypt the files instead of paying.

Nyan~

I probably missed something here but how do you expect someone to decrypt the files?

I mean, ransomwares are pretty tough when it's about encrypting the files.

(Unless the retarded developpers let the decryption key on the machine.)

sunnyrabbit2 - March 19, 2015, 2:12 pm

who would pay for this though?

You can literally wipe your hard drive then reinstall the games, steam is free. All it takes is for you to securely wipe the HD and then log on to steam, install the setup, install steam, and install your games.