-
-
-
-

Search Site
Login Sign up

-
-
-
-

Search Site
Login Sign up

- [News](#)
  - [Featured](#)
  - [Latest](#)

[Gomasom .Crypt Ransomware Decrypted](#)

[Emsisoft releases Decrypter for the Randamant Ransomware Kit](#)

[CryptoWall 4 being distributed as a NSIS installer through Exploit Kits](#)

[Why Everyone Should disable VSSAdmin.exe Now!](#)

- New Adobe Flash Update fixes 19 Vulnerabilities

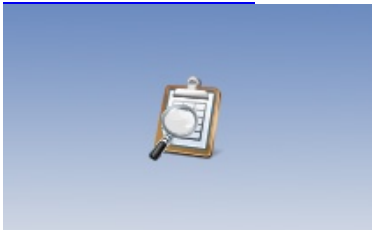- Radamant Ransomware Kit for sale on Exploit & Malware Sites

- Steam Caching Error leads to Account Disclosure

- New TeslaCrypt with Minor Changes and new Ransom Note

- Downloads
  - Latest
  - Most Downloaded

  - Free Clipboard Viewer

  - Unchecky Beta

FurMark

ShadowExplorer

ComboFix

AdwCleaner

RKill
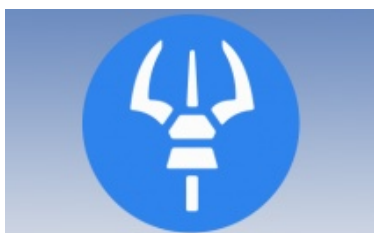
Junkware Removal Tool

- Virus Removal Guides
  - Latest
  - Most Viewed
  - Ransomware

How to remove Ads by Storm Alerts

Money Viking Removal Guide

TeslaCrypt and Alpha Crypt Ransomware Information Guide and FAQ

Oybtfpencref Removal Guide
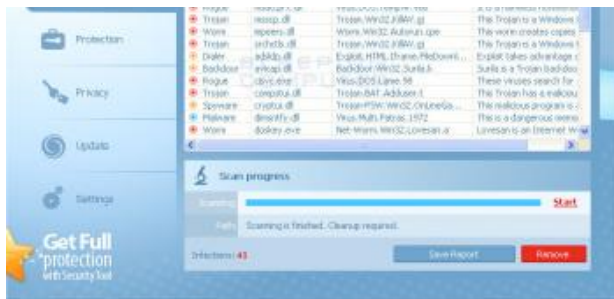
[Remove Security Tool and SecurityTool (Uninstall Guide)](#)

[How to remove Antivirus 2009 (Uninstall Instructions)](#)

[How to Remove WinFixer / Virtumonde / Msevents / Trojan.vundo](#)

[How to remove Google Redirects or the TDSS, TDL3, or Alureon rootkit using TDSSKiller](#)

[TeslaCrypt and Alpha Crypt Ransomware Information Guide and FAQ](#)

[Locker Ransomware Information Guide and FAQ](#)

[TorrentLocker (fake CryptoLocker) Ransomware Information Guide and FAQ](#)
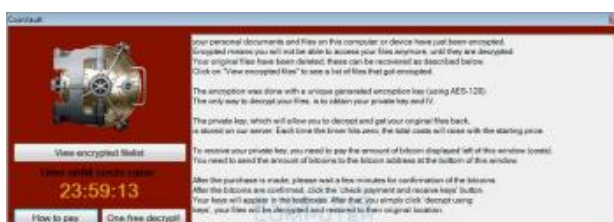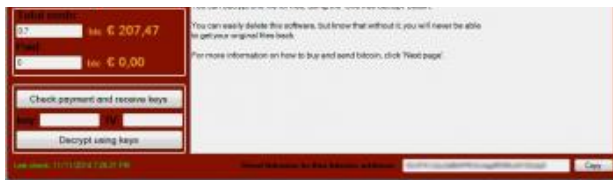
[The CoinVault Ransomware Information Guide and FAQ](#)

- Tutorials
  - [Latest](#)
  - [Popular](#)

[How to sign in directly to the Windows 8.1 desktop](#)
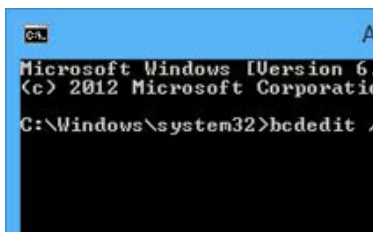
[How to enable the F8 key to start Safe Mode in Windows 8](#)
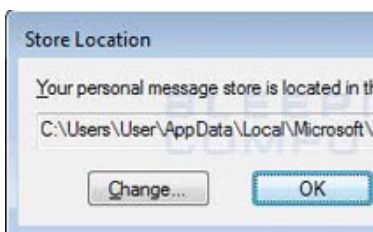
[How to change email storage folder in Windows Live Mail](#)

[How to create a command-line toolkit for Windows](#)
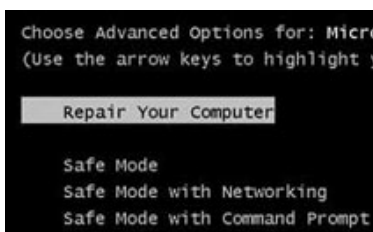
[How to start Windows in Safe Mode](#)
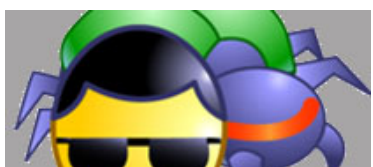
- [How to remove a Trojan, Virus, Worm, or other Malware](#)

- [How to see hidden files in Windows](#)
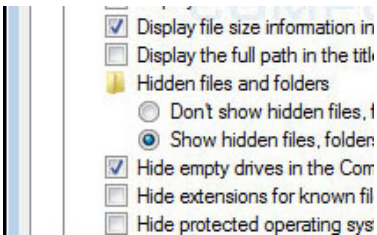
- [How to show hidden files in Windows 7](#)

- [Deals](#)
  - [Best Sellers](#)
  - [Latest](#)
  - [Categories](#)

  - [Cyber Security Hacker Training & Certification Bundle](#)
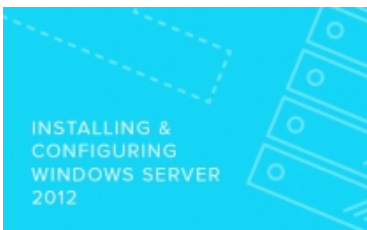
  - [Microsoft Certified Solutions Engineer: Server Infrastructure Bundle](#)

  - [CompTIA IT Certification Bundle](#)

[Linux Learner e-Learning Bundle](#)

[Cisco Certified Network Associate & Professional Certification Bund](#)

[Master OS X Yosemite Server Quickly & Easily](#)

[eLearning](#)

[IT Certification Courses](#)

[Gear + Gadgets](#)

Security

- Forums
- More
  - Startup Database
  - Uninstall Database
  - File Database
  - Glossary
  - Chat on IRC
  - Welcome Guide
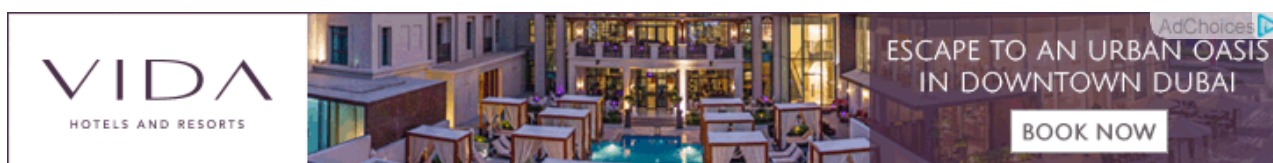
- Home
- News
- Security
- New TeslaCrypt with Minor Changes and new Ransom Note

- f 18 G+ in ✉
-
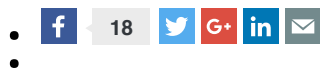
New TeslaCrypt with Minor Changes and new Ransom Note

Lawrence Abrams

- December 28, 2015
- 10:28 AM
- Read 447 times
- 0

A new variant of the TeslaCrypt ransomware was released a bit over a week ago that still refers to itself as version 2.2.0, but contains some minor changes compared to the previous release. The most noticeable change are the differences in the ransom notes. The ransom notes now include instructions to use translate.google.com if English is not the victim's native language. Some of the wording has also been changed, but the general gist is the same. The text version of the new ransom note can be seen below.

* Howto_Restore_FILES.TXT - Notepad2

File   Edit   View   Settings   ?

```
 1
 2  __!@#!@#!__!@#!@#!__!@#!@#!__!@#!@#!__!@#!@#!__!@#!@#!__!@#!@#!__!@#!@#!__!@#!@#!
 3
 4  NOT YOUR LANGUAGE? USE https://translate.google.com
 5
 6  What happened to your files ?
 7  All of your files were protected by a strong encryption with RSA-4096.
 8  More information about the encryption keys using RSA-4096 can be found here:
    http://en.wikipedia.org/wiki/RSA_(cryptosystem)
 9
10  How did this happen ?
11  !!! Specially for your PC was generated personal RSA-4096 KEY, both public and private.
12  !!! ALL YOUR FILES were encrypted with the public key, which has been transferred to your computer via the Internet.
13  Decrypting of your files is only possible with the help of the private key and decrypt program, which is on our
    secret server.
14
15  What do I do ?
16  So, there are two ways you can choose: wait for a miracle and get your price doubled, or start obtaining BTC NOW,
    and restore your data easy way.
17  If You have really valuable data, you better not waste your time, because there is no other way to get your files,
    except make a payment.
18
19  For more specific instructions, please visit your personal home page, there are a few different addresses pointing
    to your page below:
20  1. http://jf73ndna34df.ceorldess.com/XXXXXXXXXXXXXX
21  2. http://fqa4dnfh5fsk4.tarsfee.com/XXXXXXXXXXXXXX
22  3. http://hrdsjrnvskdjnt.pay4softrn.com/XXXXXXXXXXXXX
23  4. https://t7r67vsrpjcm5dfc.onion.to/XXXXXXXXXXXXX
24  5. https://t7r67vsrpjcm5dfc.tor2web.org/XXXXXXXXXXXXX
25  6. https://t7r67vsrpjcm5dfc.onion.cab/XXXXXXXXXXXXX
26
27  If for some reasons the addresses are not available, follow these steps:
28  1. Download and install tor-browser: http://www.torproject.org/projects/torbrowser.html.en
29  2. After a successful installation, run the browser and wait for initialization.
30  3. Type in the address bar: t7r67vsrpjcm5dfc.onion/XXXXXXXXXXXXX
31  4. Follow the instructions on the site.
32
33  !!! IMPORTANT INFORMATION:
34  !!! Your personal pages:
35  http://jf73ndna34df.ceorldess.com/XXXXXXXXXXXXXX
36  http://fqa4dnfh5fsk4.tarsfee.com/XXXXXXXXXXXXXX
37  http://hrdsjrnvskdjnt.pay4softrn.com/XXXXXXXXXXXXX
38  https://t7r67vsrpjcm5dfc.onion.to/XXXXXXXXXXXXX
39  !!! Your personal page in TOR Browser: t7r67vsrpjcm5dfc.onion/XXXXXXXXXXXXX
40  !!! Your personal identification ID: XXXXXXXXXXXXX
41  =======!!!!!=======!!!!!=======!!!!!=======!!!!!=======!!!!!=======!!!!!=======!!!!!
42
```

Ln 20 : 42 Col 38 Sel 0   2.32 KB   ANSI   CR+LF INS Default Text

The other change is the use of 0s (Zeros) for the first four bytes of the encrypted files. In the past the the first four bytes of the VVV encrypted files contained the DEADBEEF hexadecimal numbers. Now the first four bytes of the encrypted files have been changed to 00000000. You can see the first four bytes zeroed out in the image below.

010 Editor - C:\test\test_image.jpg.vvv

File Edit Search View Scripts Templates Tools Window Help

Edit As: Hex

test_image.jpg.vvv

```
            0  1  2  3   4  5  6  7   8  9  A  B   C  D  E  F   0123456789ABCDEF
0000h:     00 00 00 00  04 AA 67 9A  C4 AC 02 93  3C 22 EE 2D   .....ªgšÄ¬."<"î-
0010h:     9B 09 55 1A  38 96 70 19  56 82 DC 0E  85 BF EE 29   >.U.8–p.V‚Ü.…¿î)
0020h:     D1 4E 83 7C  99 27 87 03  6F AF C1 5E  7D 07 85 1C   ÑNƒ|™'‡.o¯Á^}.….
0030h:     06 84 93 D8  06 2A 70 1A  49 05 67 7B  46 3C 6B 34   .„"Ø.*p.I.g{F<k4
0040h:     29 21 34 CC  9B 33 41 41  41 43 33 43  30 38 44 41   )!4Ì›3AAAC3C08DA
0050h:     36 39 43 42  42 46 33 38  46 33 31 38  43 39 34 37   69CBBF38F318C947
0060h:     45 33 36 34  41 39 43 31  44 42 35 42  44 45 37 38   E364A9C1DB5BDE78
0070h:     36 36 43 38  38 39 45 44  39 31 32 32  34 38 43 46   66C889ED912248CF
0080h:     30 45 32 38  39 46 45 34  31 32 41 42  42 43 46 32   0E289FE412ABBCF2
0090h:     34 44 41 32  38 45 46 35  39 32 32 41  35 39 42 32   4DA28EF5922A59B2
00A0h:     34 36 45 46  41 34 36 46  42 39 33 42  31 42 36 39   46EFA46FB93B1B69
00B0h:     42 31 42 33  30 36 36 41  33 34 37 30  43 46 32 30   B1B3066A3470CF20
00C0h:     44 39 43 39  30 00 00 04  87 EB C1 7A  C9 EB 44 08   D9C90...‡ëÁzÉëD.
00D0h:     43 55 CB 33  5F EC D5 94  5F D2 7B 09  2F 5C 57 A0   CUË3_ìÕ"_Ò{./\W 
00E0h:     9A 89 BF 7A  F9 5E 49 1E  22 F1 DC 1C  6D 79 EE B7   š‰¿zù^I."ñÜ.myî·
00F0h:     19 EE 30 F0  13 07 35 3E  CF FD 59 DC  1F DE 47 5A   .î0ð..5>ÏýYÜ.ÞGZ
```

Selected: 4 bytes (Range: 0 to 3)   Start: 0 [0h]   Sel: 4 [4h]   Size: 925854 ANSI   LIT W OVR

If anything else is discovered, we will be sure to let you know as soon as possible.

- Ransomware
- TeslaCrypt
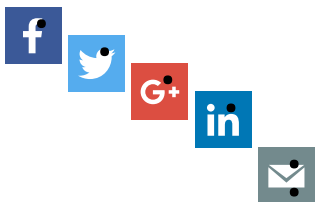
- Previous Article
- Next Article

Post a Comment Community Rules

You need to login in order to post a comment

Login

Not a member yet? Register Now

You may also like

Steam Caching Error leads to Account Disclosure

Gomasom .Crypt Ransomware Decrypted

New TeslaCrypt version adds the .VVV Extension to Encrypted Files

[Microsoft warns Adware Developers to stop using Man-in-the-Middle Attacks](#)

Latest forum topics

- [Need help to know where to begin.](#)

  [dayvolt](#) in [Am I infected? What do I do?](#)
- [Don't Know What I Want. Opinions Welcomed!](#)

  [ZeldaB](#) in [Questions and advice for Buying a New Computer](#)
- [Kaspersky detected HEUR:Trojan.Script.iframer or Iframer, .dll whitelisted](#)

  [wingardiumleviosa50](#) in [Am I infected? What do I do?](#)

Newsletter Sign Up

To receive periodic updates and news from [BleepingComputer](#), please use the form below.

[Email Address...] [Submit]

Latest virus removal guides

[How to remove Ads by Storm Alerts](#)

  - [Lawrence Abrams](#)
  - Read 2,704 times

Classification: Adware

Money Viking Removal Guide

- [Lawrence Abrams](#)
- Read 2,344 times

Classification: Adware

Oybtfpencref Removal Guide

- [Lawrence Abrams](#)
- Read 3,734 times

Classification: Adware

Computerhelper.site Security Help Page Removal Guide

- [Lawrence Abrams](#)
- Read 3,150 times

Classification: Adware

[Remove Ividi.org Browser Hijacker](#)

- [Lawrence Abrams](#)
- Read 3,685 times

Classification: Adware

Newsletter Sign Up

| Email Address... | Submit |

- Follow us:
-
-
-
-

Main Sections

- [News](#)
- [Downloads](#)
- [Virus Removal Guides](#)
- [Tutorials](#)
- [Startup Database](#)
- [Uninstall Database](#)
- [File Database](#)
- [Glossary](#)

Community

- [Forums](#)
- [Chat](#)

Useful Resources

- [Welcome Guide](#)
- [Sitemap](#)

Company

- [About BleepingComputer](#)
- [Contact Us](#)
- [Advertising](#)
- [Social & Feeds](#)
- [Changelog](#)

[User Agreement](#) - [Privacy Policy](#)

Login

Username [ ]
Password [ ]
☑ Remember Me
☐ Sign in anonymously

[Login]   [Sign in with Facebook](#)   [Sign in with Twitter](#)

Not a member yet? [Register Now](#)

Reporter

Help us understand the problem. What is going on with this comment?

- ◯ Spam
- ◯ Abusive or Harmful
- ◯ Inappropriate content
- ◯ Strong language
- ◯ Other

[Learn more](#) about what is not allowed to be posted.

[SUBMIT](#)