- News
  - Featured
  - Latest
    - 

      Help BleepingComputer Defend Freedom of Speech
    - 

      Emsisoft Releases a Decrypter for HydraCrypt and UmbreCrypt Ransomware

- 

  New TeslaCrypt variant now uses the .MP3 Extension

- 

  Hidden Tear Ransomware Developer Blackmailed by Malware Developers using his Code

- 

  PadCrypt: The first ransomware with Live Support Chat and an Uninstaller

- 

  Emsisoft Releases a Decrypter for HydraCrypt and UmbreCrypt Ransomware

- 

  Affiliate Spam is not only Annoying but can offer Costly Advice

- 

  New TeslaCrypt variant now uses the .MP3 Extension

- Downloads
  - Latest
  - Most Downloaded
  - 

    Malwarebytes Anti-Ransomware Beta

  - 

    Free Clipboard Viewer

  - 

    Unchecky Beta

  - 

FurMark

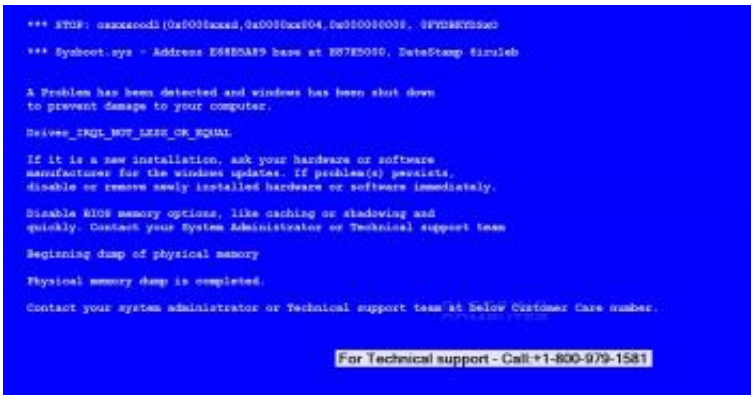
ComboFix

AdwCleaner

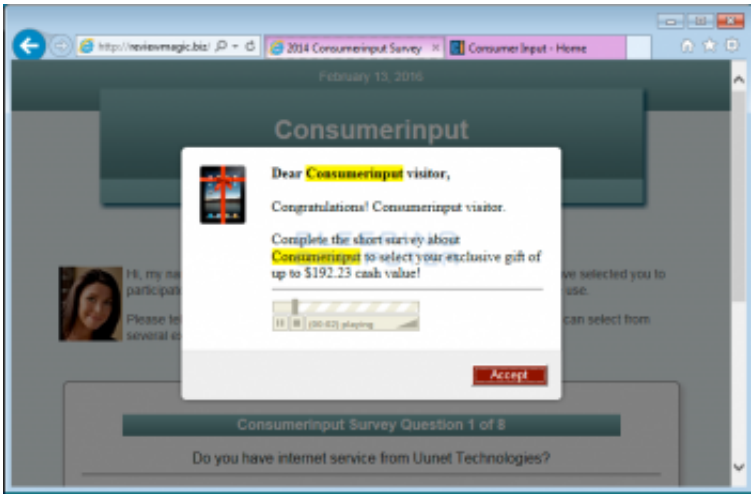
RKill

Junkware Removal Tool

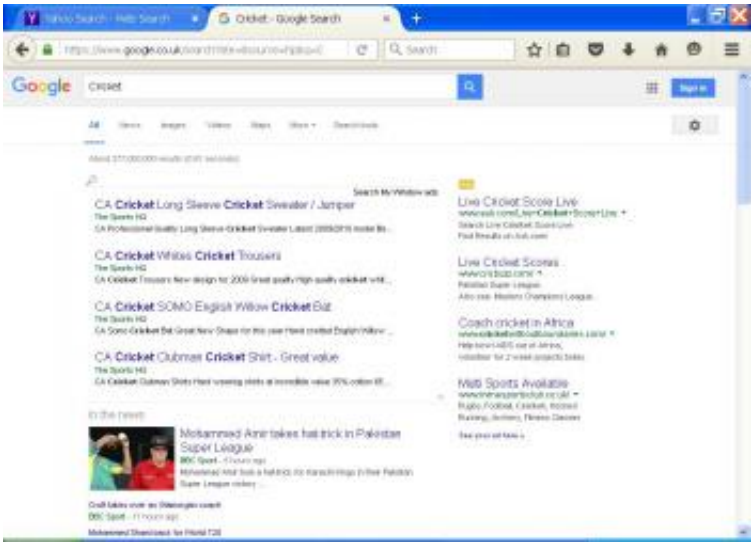
- Virus Removal Guides
  - Latest
  - Most Viewed
  - Ransomware



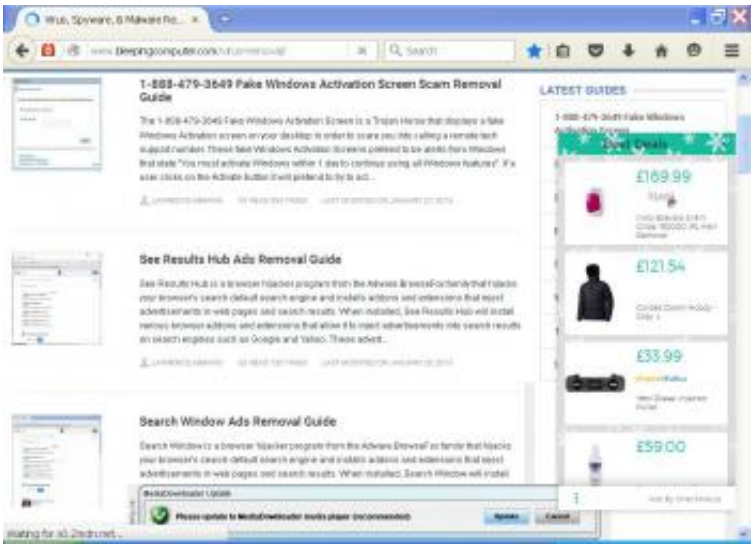
- [Weather Wizard or Fake Sysboot.sys Crash Screen Removal Guide]



- [ConsumerInput Removal Guide]



- [Search My Window Ads Removal Guide]

- 

[CheckMeUp Ads Removal Guide]

- 

[Remove Security Tool and SecurityTool (Uninstall Guide)]

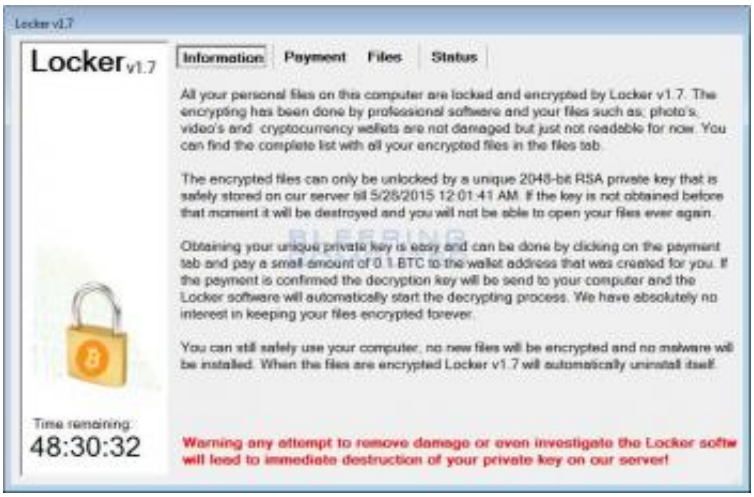
- 

[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]

- 

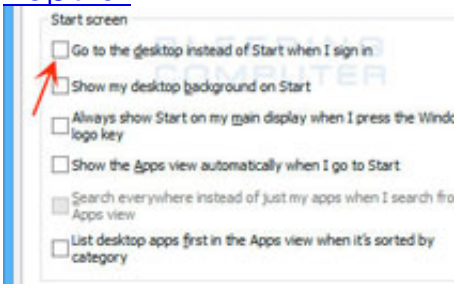
[Locker Ransomware Information Guide and FAQ]

- 

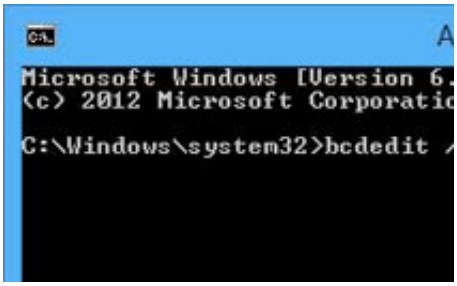
[TorrentLocker (fake CryptoLocker) Ransomware Information Guide and FAQ]

- 

[The CoinVault Ransomware Information Guide and FAQ]

- Tutorials
  - Latest
  - Popular
    - 

      [How to sign in directly to the Windows 8.1 desktop]

    - 

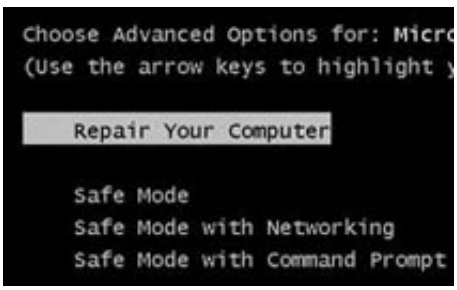
      [How to enable the F8 key to start Safe Mode in Windows 8]

    - 

      [How to change email storage folder in Windows Live Mail]

    - 

      [How to create a command-line toolkit for Windows]

    - 

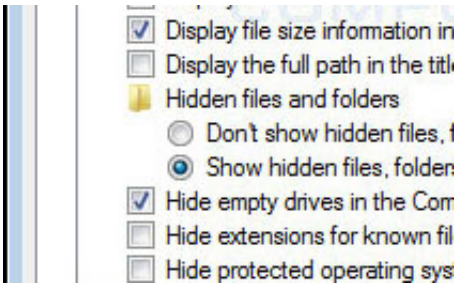
[How to start Windows in Safe Mode](#)

- 

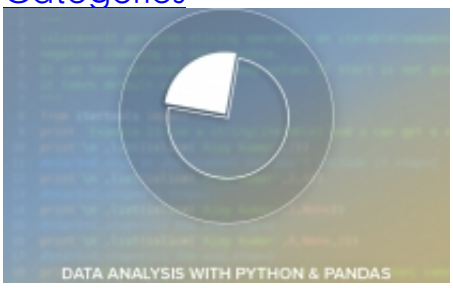
[How to remove a Trojan, Virus, Worm, or other Malware](#)

- 

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

- 

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

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

[Python Programming Pro Bundle](#)

- 

  [Cyber Security Hacker Training & Certification Bundle]

- 

  [Linux Learner e-Learning Bundle]

- 

  [Xbox Live Gold: 12-Month Subscription]

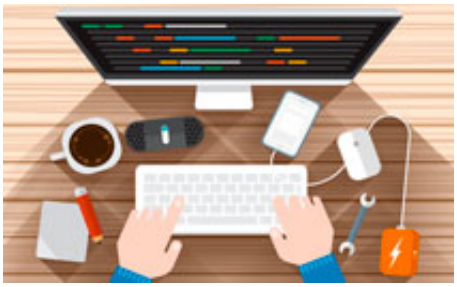
- 

  [Genie Timeline Pro for PC]

- 

  [Complete White Hat Hacking & Penetration Testing Bundle]

NES30 Pro Bluetooth Game Controller



eLearning

IT Certification Courses

Gear + Gadgets

Security

- Forums

PadCrypt: The first ransomware with Live Support Chat and an Uninstaller

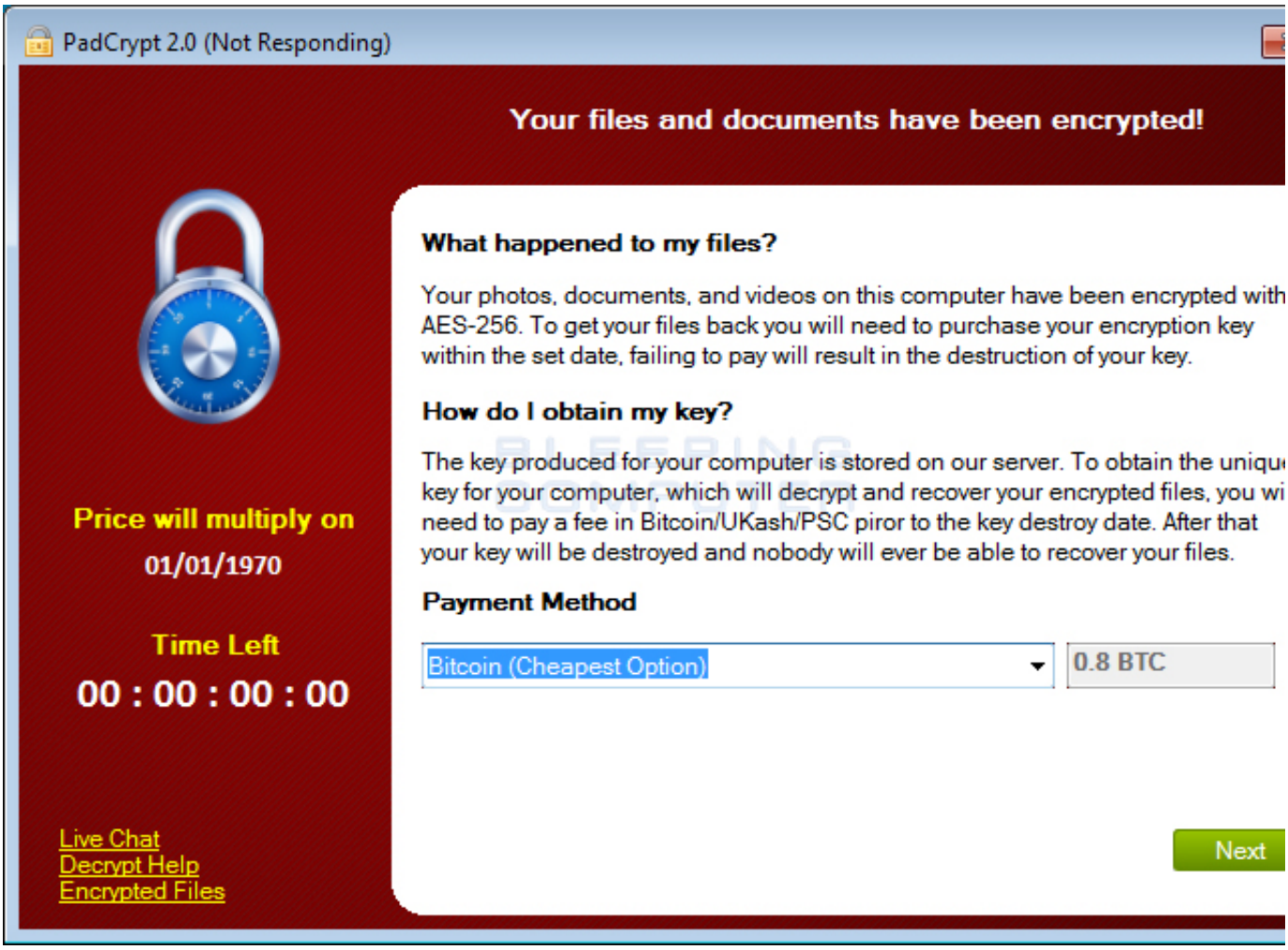
Lawrence Abrams

- February 14, 2016
- 01:50 PM
- Read 1,882 times
- 2

A new ransomware was discovered by @abuse.ch and further analyzed by MalwareHunterTeam called PadCrypt that offers for the first time a live support chat feature and an uninstaller for its victims. CryptoWall was the first ransomware to provide customer support on their payment sites, but PadCrypt's use of live chat allows victims to interact with malware developers in real time. A feature like this could potentially increase the amount of payments as the victim can receive "support" and be guided on the confusing process of making a payment.

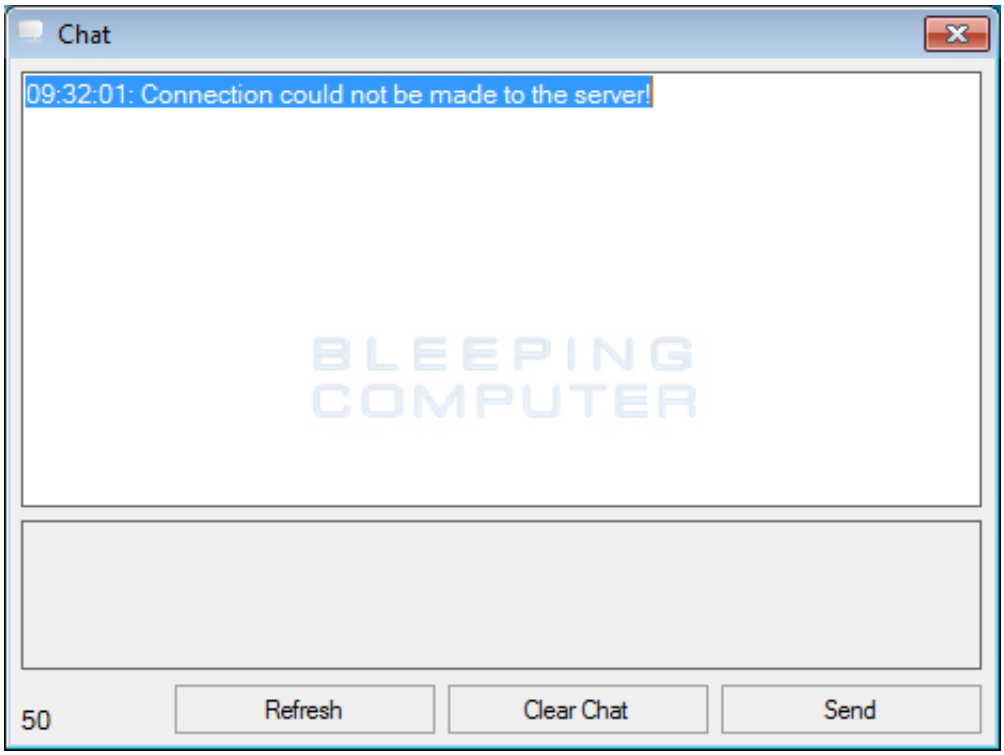
PadCrypt offers a Live Support Chat Feature

With the release of PadCrypt, customer support is taken to a new level by the malware developers offering live chat. In the main screen for the PadCrypt ransomware there is a link called **Live Chat** as shown in the image below.



PadCrypt Ransomware Screen

If a user clicks on the Live Chat option, it will open up another screen that allows the victim to send a message to the developers. When the developers respond, their reply will be shown in the same screen.



Live Chat feature of PadCrypt

At this time, the Command & Control servers for PadCrypt are offline, so the ransomware will not actually encrypt anything even though it shows you the ransomware screen. Furthermore, as the live support chat requires an active C2 server, the live chat functionality is broken as well.

PadCrypt makes it easy to remove the infection

For those who wish to remove the infection, PadCrypt makes it easy by also downloading and installing an uninstaller. We recently have seen a ransomware that allows you to enable and disable the autorun for it, but this is the first time we have seen a ransomware that provides an uninstall program as well. When PadCrypt is installed, an uninstaller will also be downloaded and installed at %AppData%\PadCrypt\unistl.exe. Once the uninstaller is executed, it will remove all ransom notes and files associated with the PadCrypt infection. Unfortunately, all encrypted files will remain.

Ransomware developers love CryptoWall

There is something about CryptoWall that other ransomware developers just love to imitate it. This is also the case with PadCrypt as the executable has numerous references to CryptoWall in it. For example, the PDB for the PadCrypt executable is:

```
C:\Users\user\Documents\Visual Studio 2013\Projects\Cryptowall 2.0\Cryptowall\bin\Debug
```

There are also numerous references to CryptoWall within the C# project for this ransomware. For example, one of the namespaces for the ransomware is called Cryptowall.

Form1 Form2

```
1   using ...
13
14  namespace Cryptowall
15  {
16      public class Form2 : Form
17      {
18          private ListBox listBox_0;
19
20          private Label label_0;
21
22          private Label label_1;
23
24          private readonly static Array array_0;
25
26          private readonly static object object_0;
27
28          private readonly static Array array_1;
29
30          internal static byte byte_0;
31
32          internal IContainer icontainer_0 = null;
33
34          internal Label label_2;
35
36          internal Button button_0;
37
38          [SecuritySafeCritical]
39          static Form2() ...
54
55          public Form2() ...
```


CryptoWall Namespace

PadCrypt Encryption Process

PadCrypt is distributed via SPAM that contains a link to a zip archive that contains what appears to be a PDF file with a name like DPD_11394029384.pdf.scr. This PDF file, though, is actually an executable renamed to have the .scr .extension that when executed downloads the package.pdcr and unistl.pdcr files from the now disabled Command & Control servers. The known C2 servers used by this ransomware include annaflowersweb.com, subzone3.2fh.co, and cloudnet.online. The package.pdcr is the PadCrypt executable and the uninstl.pdcr is the uninstaller. Both of these files will be stored in the %AppData%\PadCrypt folder.

When the main PadCrypt.exe file is executed, it will scan the local drives for any files that match certain extensions and encrypt them using AES encryption. Any file that is encrypted will have the .ENC extension appended to the filename. PadCrypt will also record the name of any encrypted file in the %AppData%\PadCrypt\files.txt file. The list of targeted extensions are:

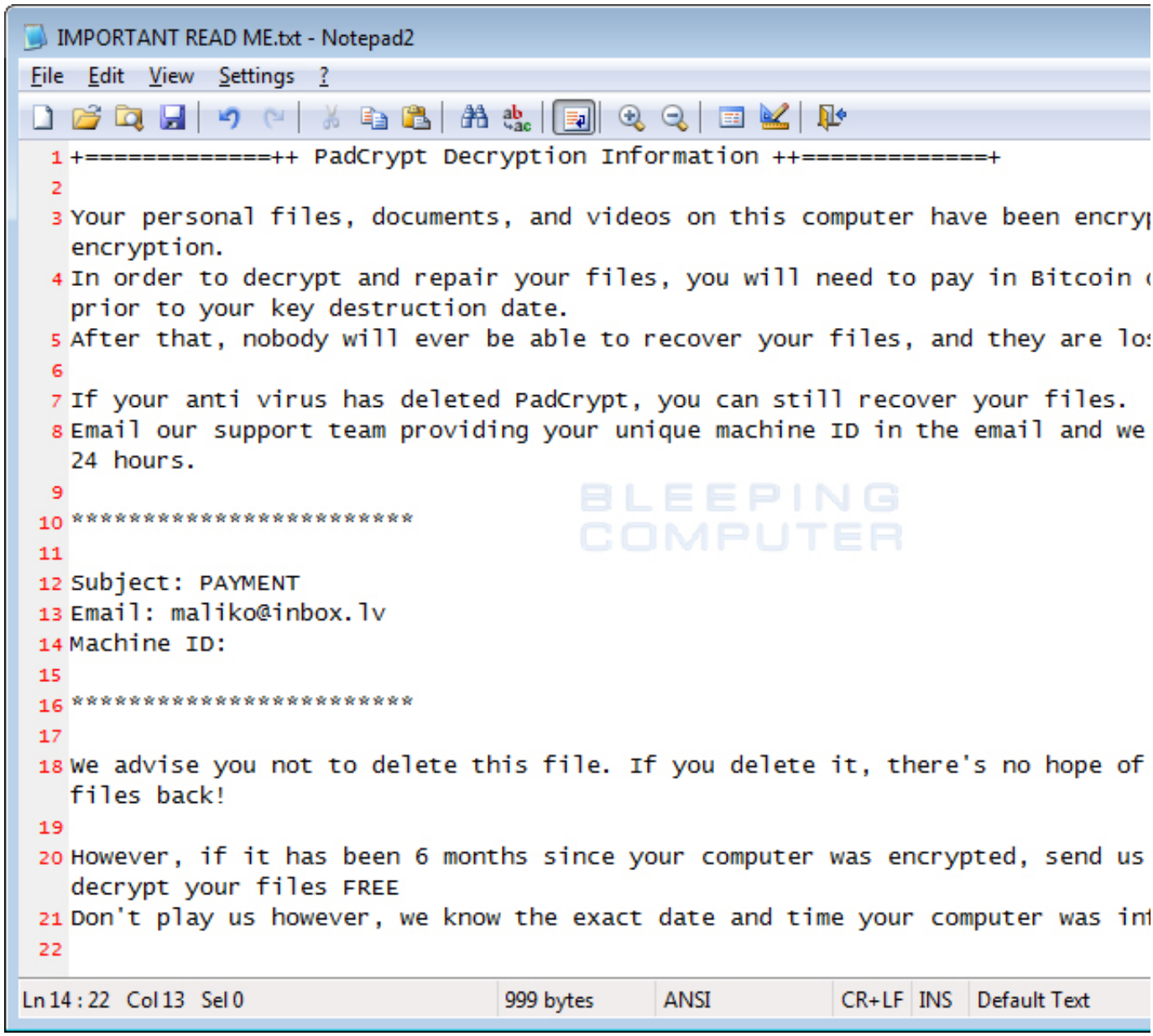
```
pdf, gif, bmp, jpeg, jpg, png, doc, docx, ppt, ptx, psd, pdn
```

During the encryption process, PadCrypt will also delete the Shadow Volume Copies on

the computer by executing the following command:

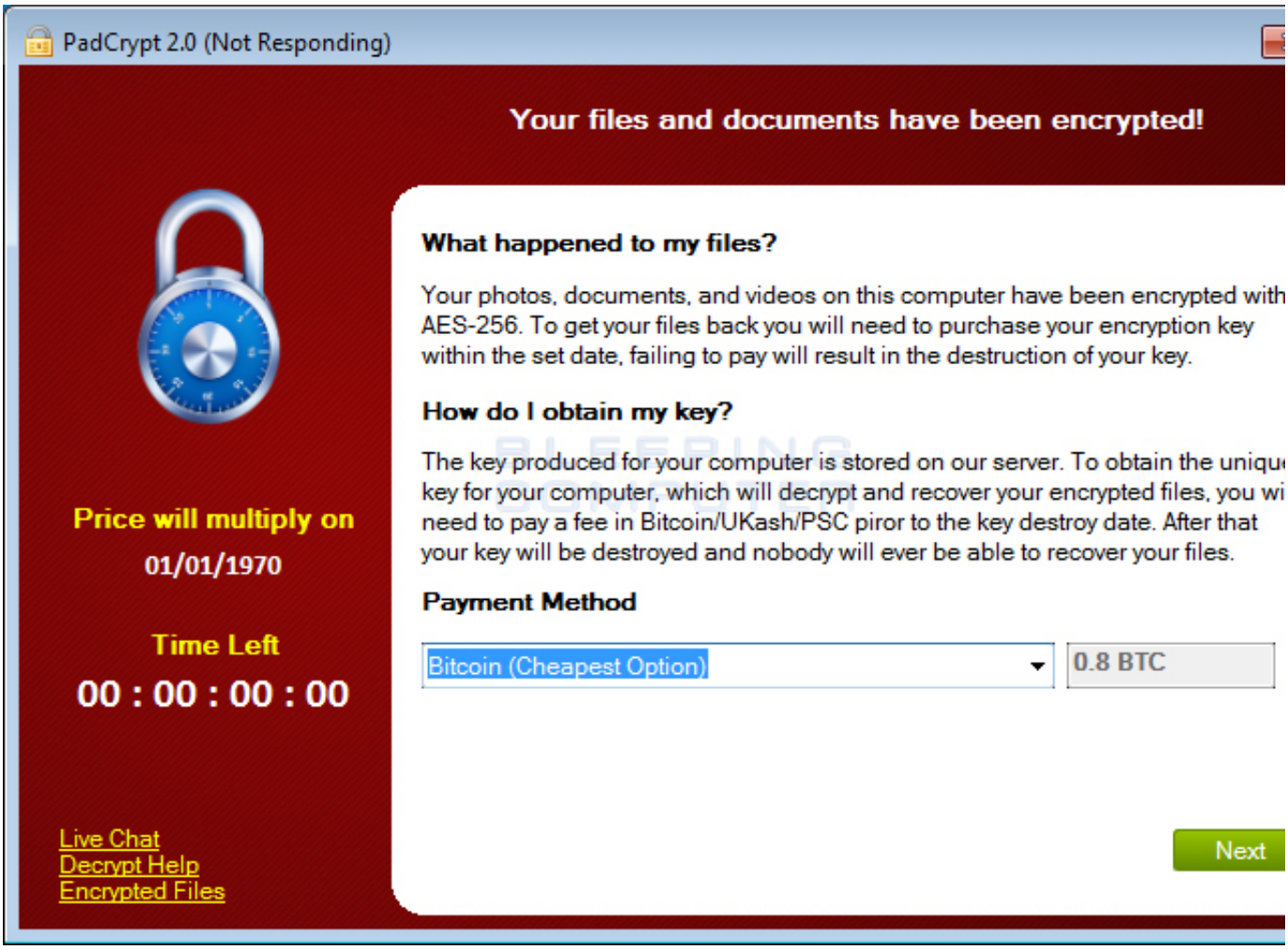
```
vssadmin delete shadows /for=z: /all /quiet
```

When it has finished encrypting the data it will create a IMPORTANT READ ME.txt file on the desktop that contains ransom instructions as shown below.



IMPORTANT READ ME.txt

Finally, it will show the ransom screen as shown below.



PadCrypt Ransomware Screen

This ransom screen will provide instructions on how to make .8 bitcoin payment or a ~$350 payment via PaySafeCard or Ukash. The instructions also state that you have 96 hours to make payment or the key will be destroyed.

At this time, it is currently unknown if there is a way to decrypt these files for free, but if we learn anything further we will be sure to post it.

Files associated with PadCrypt

```
%Desktop%\IMPORTANT READ ME.txt
%AppData%\PadCrypt\unistl.exe
%AppData%\PadCrypt\decrypted_files.dat
%AppData%\PadCrypt\File Decrypt Help.html
%AppData%\PadCrypt\PadCrypt.exe
%AppData%\PadCrypt\Files.txt
```

Registry entries associated with PadCrypt

```
HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Run "PadCrypt" = "%AppData%
HKEY_CURRENT_USER\Control Panel\Desktop "Wallpaper" = "%AppData%\PadCrypt\Wallpaper.bmp
HKEY_CURRENT_USER\Control Panel\Desktop "WallpaperStyle" = 1
```

```
HKEY_CURRENT_USER\Control Panel\Desktop "TileWallpaper" = 0
```


- PadCrypt
- Ransomware

- Previous Article

Comments

- 

  ScathEnfys - 14 hours ago

  -
  -

  I'm hoping that the reason the C2 is disabled for the moment is that they found some sort of flaw in the code... A flaw we may be able to use to decrypt the files without paying the ransom or at least study this interesting piece of malware more than the developers intended.

- 

  Angoid - 1 hour ago

-
-

Until the C&C servers come online, the malware is ineffective anyway by the looks of things:
From the article:

"At this time, the Command & Control servers for PadCrypt are offline, so the ransomware will not actually encrypt anything even though it shows you the ransomware screen."

So all you need to do if you suspect you're infected is to back all your data up (or ensure your backup is up-to-date) and rip the ransomware out (Lawrence says that the uninstaller is downloaded at install time, and if this is from the same C&C servers then it won't be available).

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

- Emsisoft Releases a Decrypter for HydraCrypt and UmbreCrypt Ransomware

- New TeslaCrypt variant now uses the .MP3 Extension

- 

  Help BleepingComputer Defend Freedom of Speech

- 

  UmbreCrypt Ransomware manually installed via Terminal Services

Latest forum topics

- How Event Managers use Technology

  ashleyalex in Apple iOS
- Audio Distortion

  hopper15 in Windows 8 and Windows 8.1
- http://onlinefitnesszone.co.uk/biofusion-eye-cream/

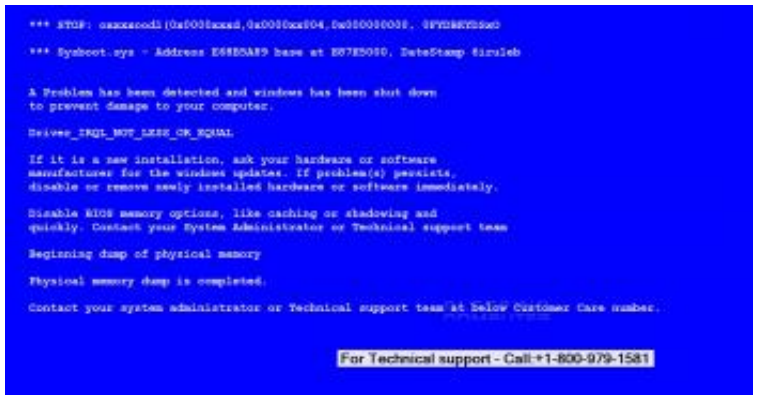
  panglioc in Windows 95/98/ME

Newsletter Sign Up

To receive periodic updates and news from BleepingComputer, please use the form below.

Email Address... Submit

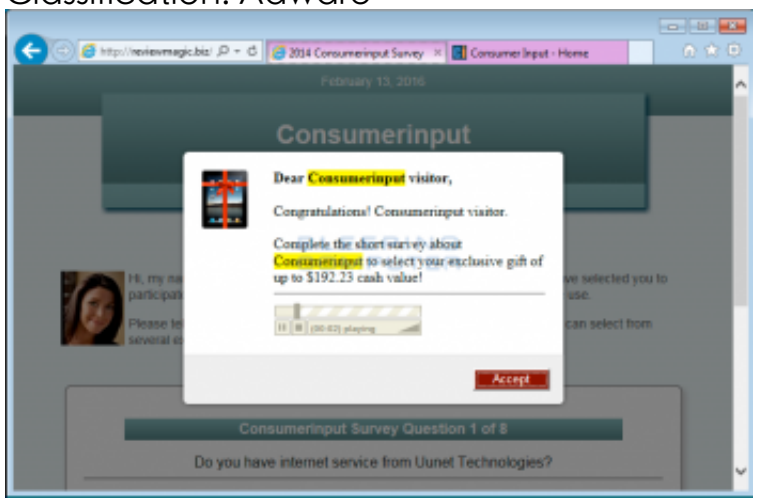
Latest virus removal guides



- [Weather Wizard or Fake Sysboot.sys Crash Screen Removal Guide]

  - Lawrence Abrams
  - Read 833 times

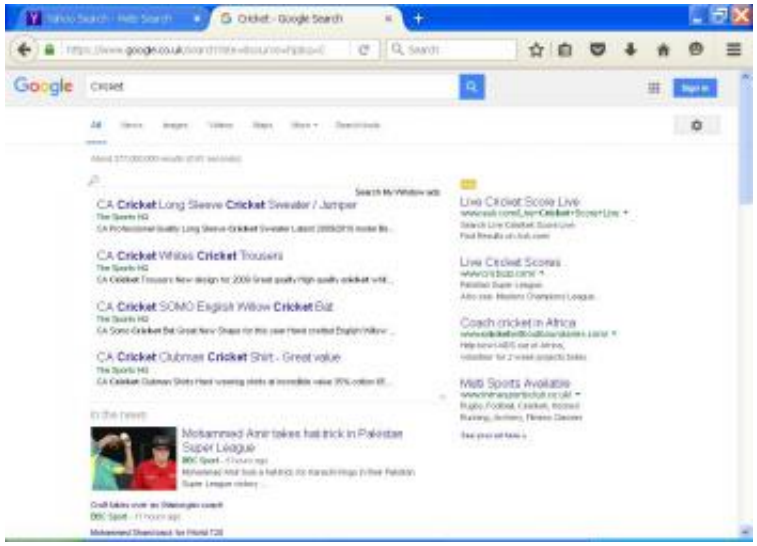
Classification: Adware



- [ConsumerInput Removal Guide]

  - Lawrence Abrams
  - Read 539 times

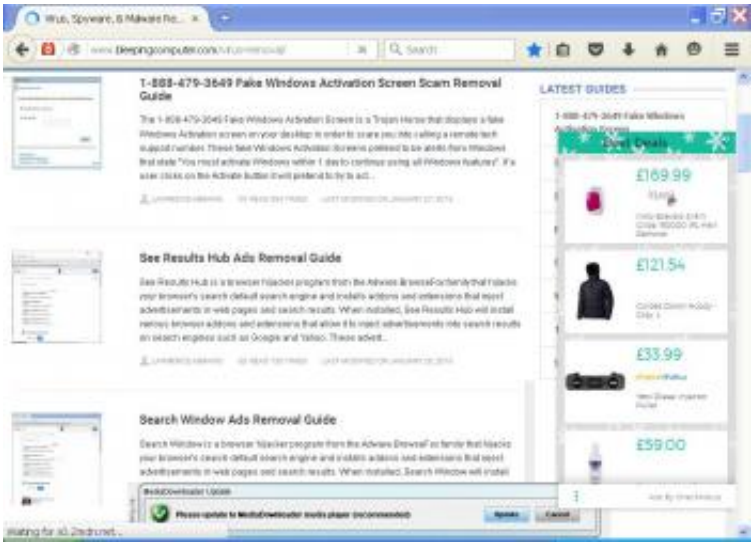
Classification: Adware



- [Search My Window Ads Removal Guide]

- Lawrence Abrams
- Read 607 times

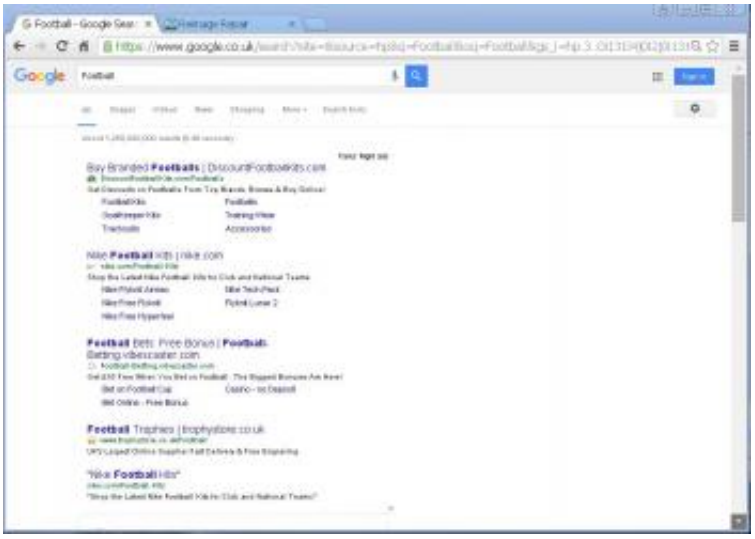
Classification: Adware



- CheckMeUp Ads Removal Guide

- Lawrence Abrams
- Read 464 times

Classification: Adware



- Facts Right Ads Removal Guide

- Lawrence Abrams
- Read 729 times

Classification: Adware

Latest Downloads

- Windows Repair (All In One)

Version: 3.8.2
635,762 *Downloads*

- 

  Process Explorer

  Version: 16.12.0.0
  48,651 *Downloads*

- 

  Panda USB Vaccine

  Version: 1.0.1.16
  6,100 *Downloads*

- 

  Malwarebytes Anti-Rootkit

  Version: 1.9.3.1001
  370,332 *Downloads*

- 

  Malwarebytes Anti-Exploit

  Version: 1.8.1.1045
  101,294 *Downloads*

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