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

bleepingcomputer.com/news/security/padcrypt-the-first-ransomware-with-live-support-chat-and-an-uninstaller

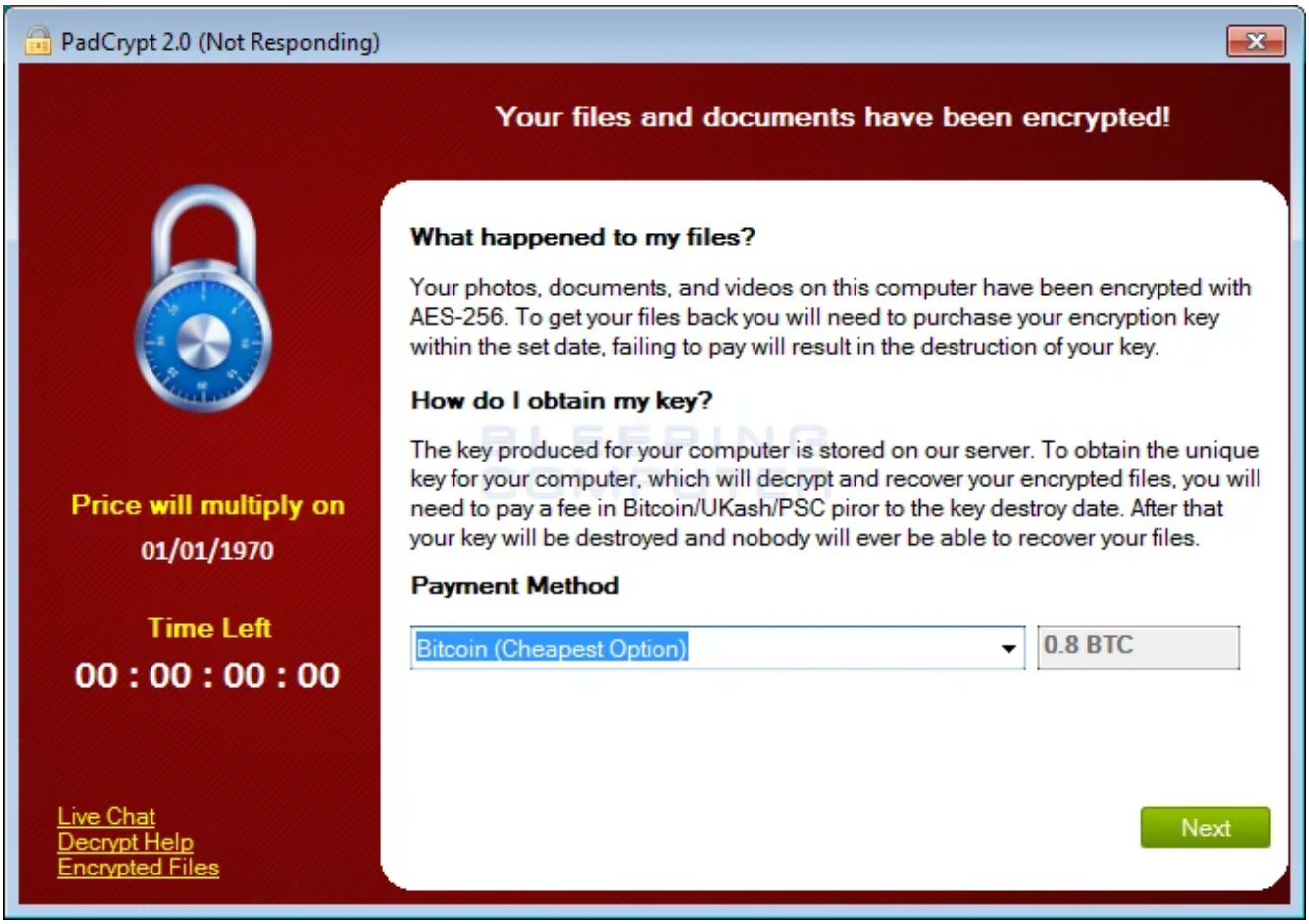
By
Lawrence Abrams

- February 14, 2016
- 01:50 PM
- 3

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.

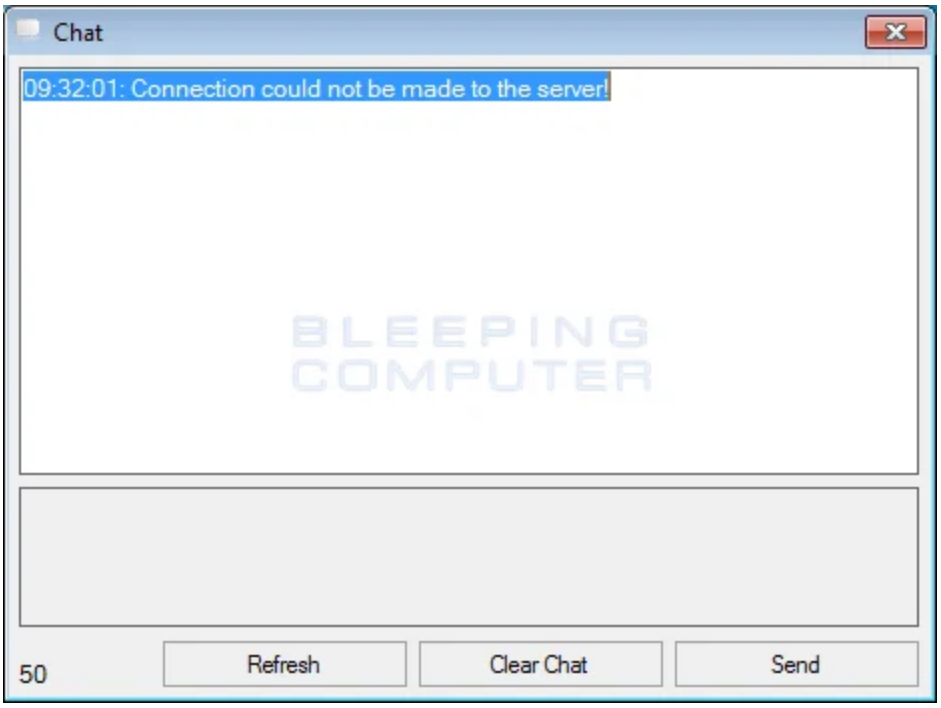
PadCrypt offers a Live Support Chat Feature

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

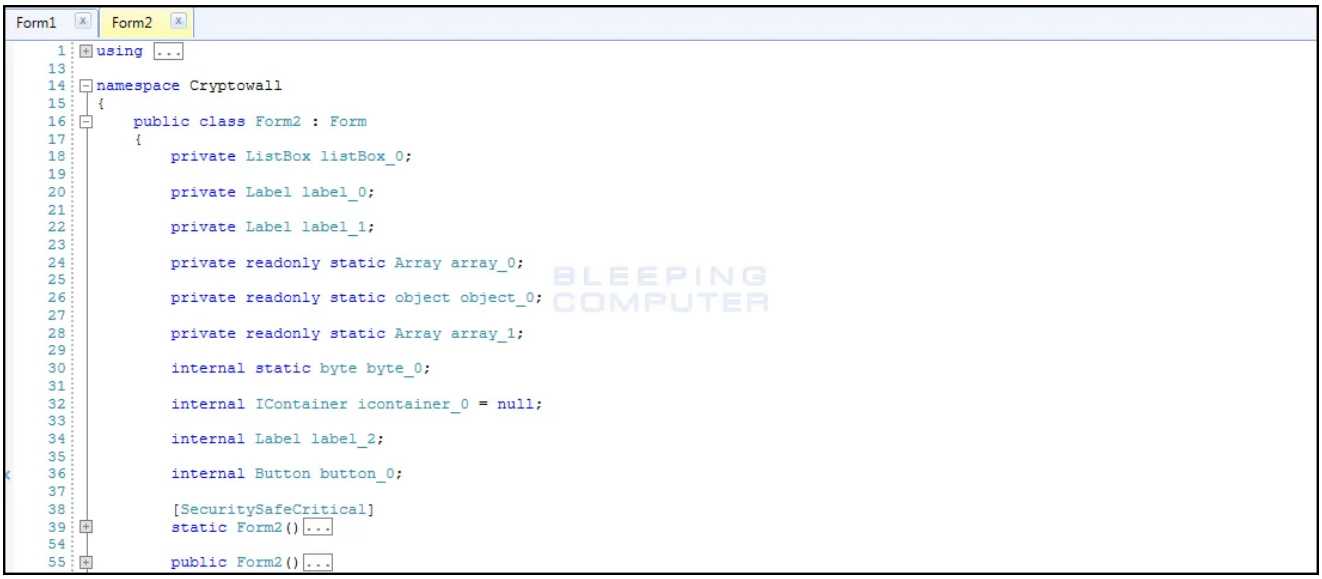
For those who wish to remove the infection, PadCrypt makes it easy by also downloading and installing an uninstaller. We recently have seen a ransomware that allows you to enable and disable the autorun for it, but this is the first time we have seen a ransomware that provides an uninstall program as 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\Obfuscated\PadCrypt.pdb
```

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.



CryptoWall Namespace

PadCrypt Encryption Process

Update on 2/15/16 with more information about the encryption process. Thx MalwareHunterTeam.

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 PadCrypt.exe encrypts files, it will encrypt any data files, regardless of extension, that are in the targeted folders. When encrypting a victim's files it starts by scanning and encrypting the following folders.

```
C:\Users\[login_name]\Downloads, C:\Users\[login_name]\Documents, C:\Users\
[login_name]\Pictures, and C:\Users\[login_name]\
```

When it has finished encrypting those folders it will then scan the **C:** drive and encrypt all files that are not located in the following folders or the contain the strings ProgramData, PerfLogs, Config.Msi, and $Recyle.Bin.

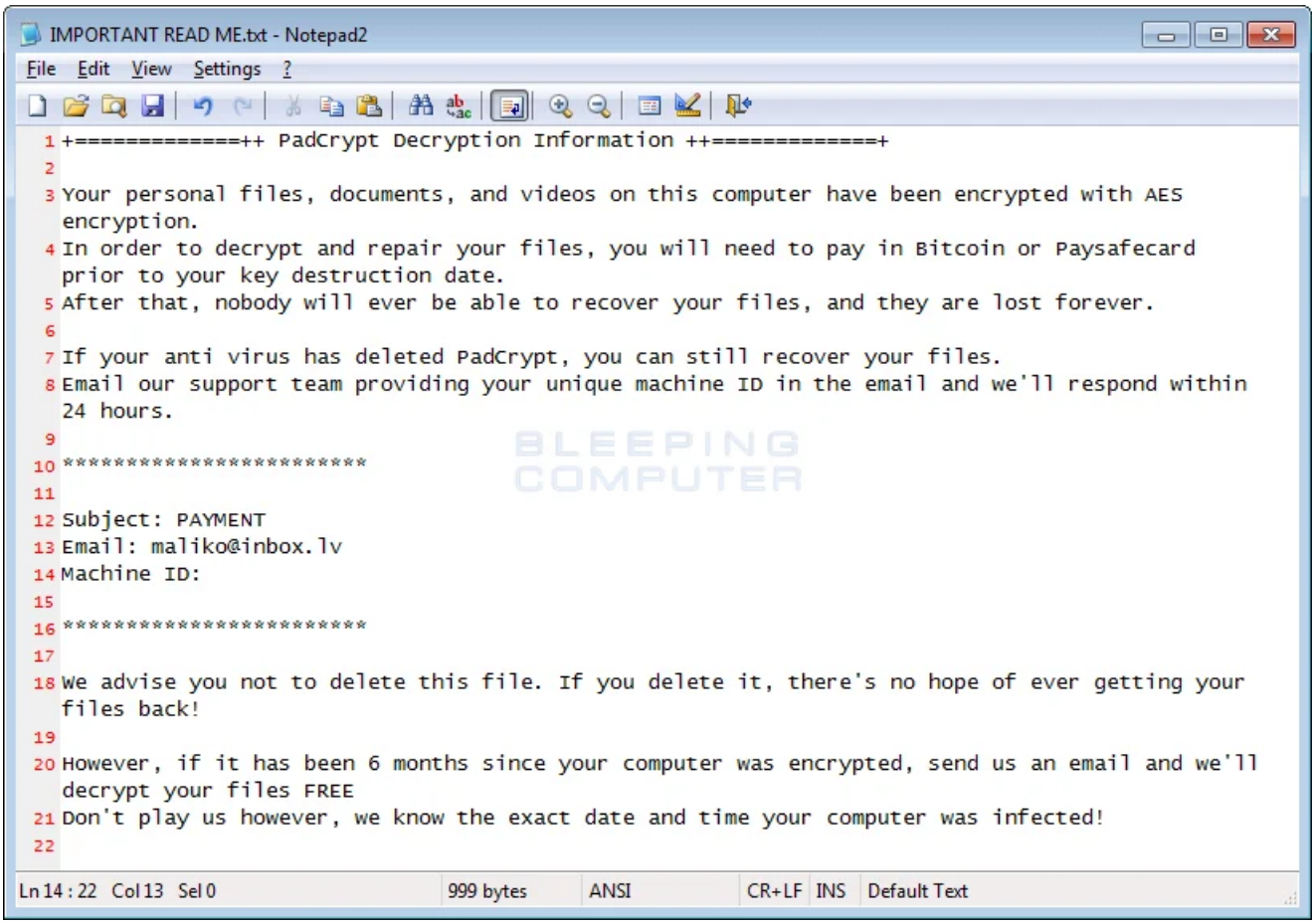
```
C:\Users, C:\NVIDIA, C:\Intel, C:\Documents and Settings, C:\Windows, C:\Program
Files, C:\Program Files (x86), C:\System Volume Information, and C:\Recycler
```

Finally, PadCrypt will enumerate all local drives and encrypt any files that are detected.

During the encryption process, PadCrypt will also delete the Shadow Volume Copies on the computer by executing the following command:

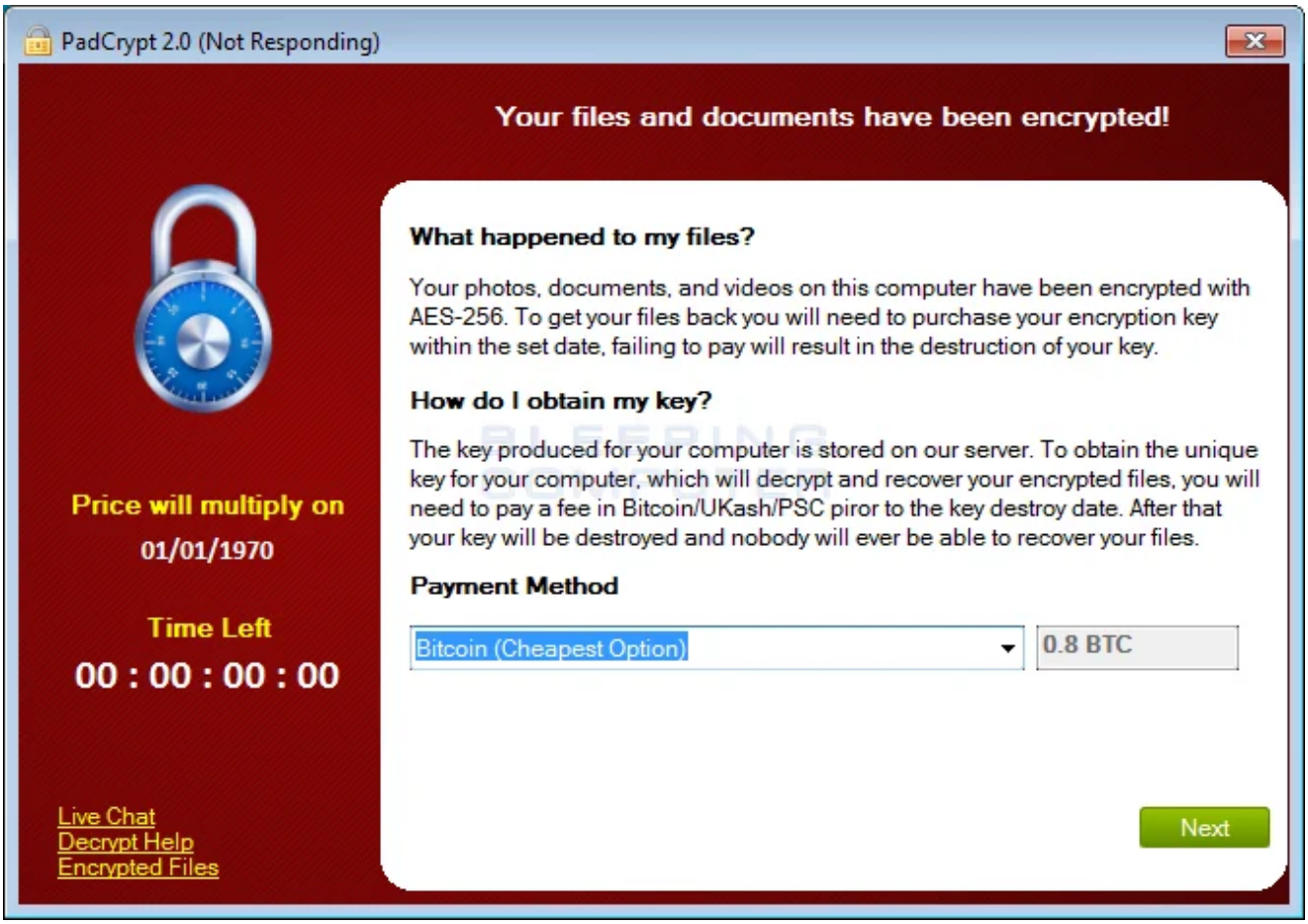
```
vssadmin delete shadows /for=z: /all /quiet
```

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.



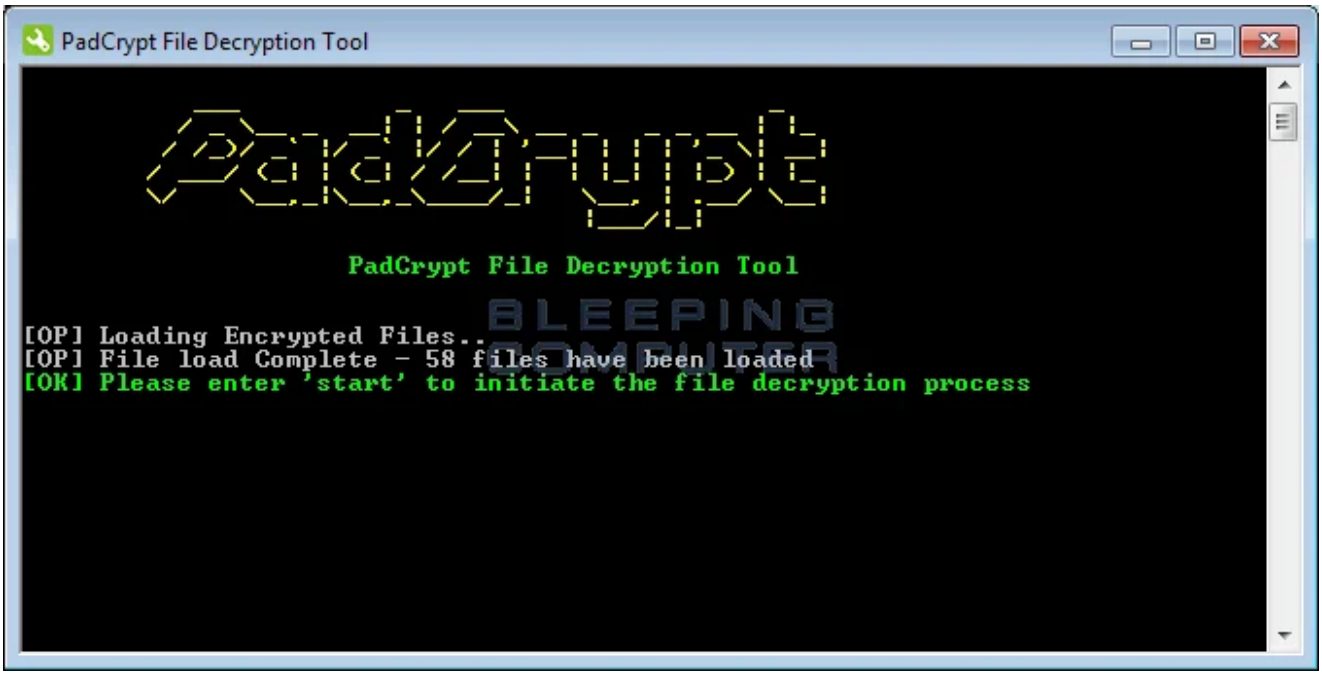
PadCrypt Ransomware Screen

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.

PadCrypt goes retro with its decrypter

PadCrypt is the ransomware with many surprises including its colorful retro decryption program. When run, the decrypter will import a list of encrypted files from **%AppData%\PadCrypt\Files.txt**.



PadCrypt Decrypter

When a victim types **start** and press enter, the decrypter will look for the decryption key in the **%AppData%\PadCrypt\data.txt** file. If one is detected it will decrypt any encrypted files listed in the files.txt file.

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 "Microsoft Corp" =
"%AppData%\PadCrypt\PadCrypt.exe"
HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Run "PadCrypt" =
"%AppData%\PadCrypt\PadCrypt.exe"
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
```

Related Articles:

Indian airline SpiceJet's flights impacted by ransomware attack

US Senate: Govt's ransomware fight hindered by limited reporting

New RansomHouse group sets up extortion market, adds first victims

Ransomware attack exposes data of 500,000 Chicago students

The Week in Ransomware - May 20th 2022 - Another one bites the dust

- PadCrypt
- Ransomware

Lawrence Abrams

Lawrence Abrams is the owner and Editor in Chief of BleepingComputer.com. Lawrence's area of expertise includes Windows, malware removal, and computer forensics. Lawrence Abrams is a co-author of the Winternals Defragmentation, Recovery, and Administration Field Guide and the technical editor for Rootkits for Dummies.

- Previous Article
- Next Article

Comments

- 

  ScathEnfys - 6 years 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 - 6 years 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).

- 

  julesPerox - 6 years ago

  Has anyone any solid advice on removal for a bit of a noob?! Had the SOS from the FinL this afternoon and tried first 'SpyHunter' software...I know... :(
  Appreciate any advice..download links to something that ACTUALLY works, and doesn't hint of being a virus itself?!
  Thanks all...

Post a Comment Community Rules

You need to login in order to post a comment

Not a member yet? Register Now

You may also like: