

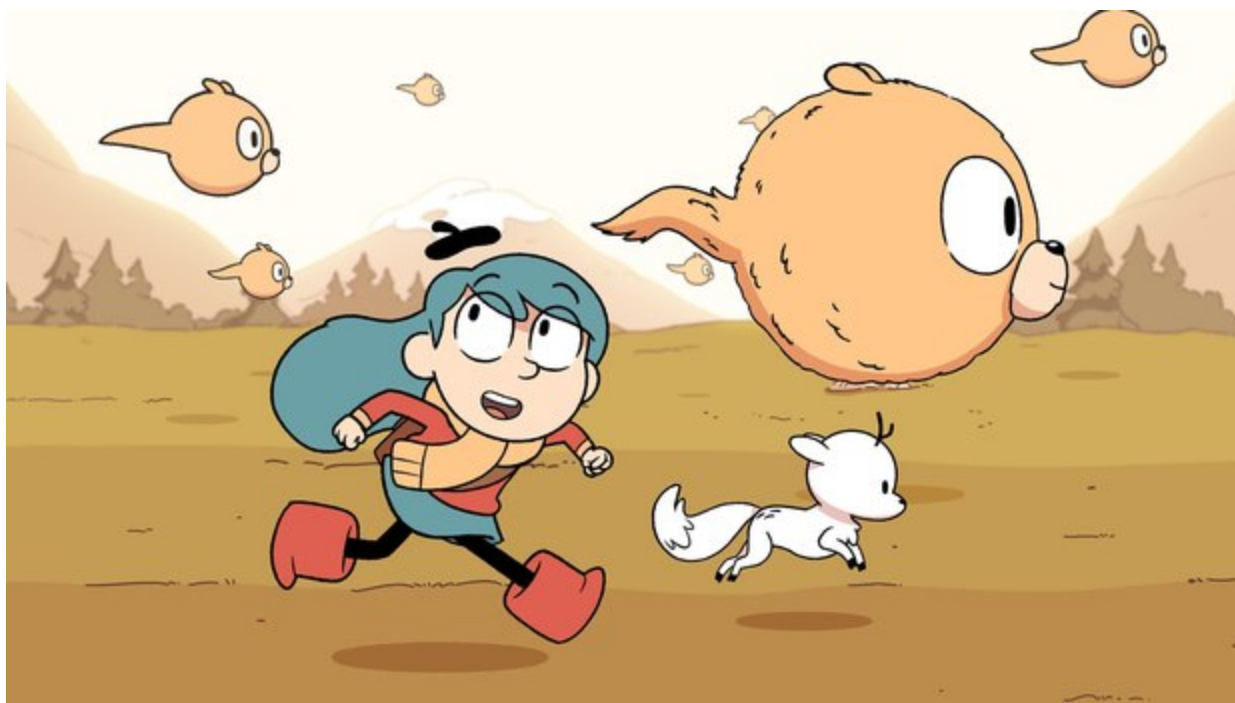
# Hildacrypt Ransomware actively spreading in the wild

 [securitynews.sonicwall.com/xmlpost/hildacrypt-ransomware-actively-spreading-in-the-wild/](https://securitynews.sonicwall.com/xmlpost/hildacrypt-ransomware-actively-spreading-in-the-wild/)



September 4, 2019

The SonicWall Capture Labs Threat Research Team observed reports of a new variant family of **Hildacrypt ransomware [Hildacrypt.RSM]** actively spreading in the wild.



The **Hildacrypt** ransomware encrypts the victim's files with a strong encryption algorithm until the victim pays a fee to get them back.

### Infection Cycle:

The ransomware adds the following files to the system:

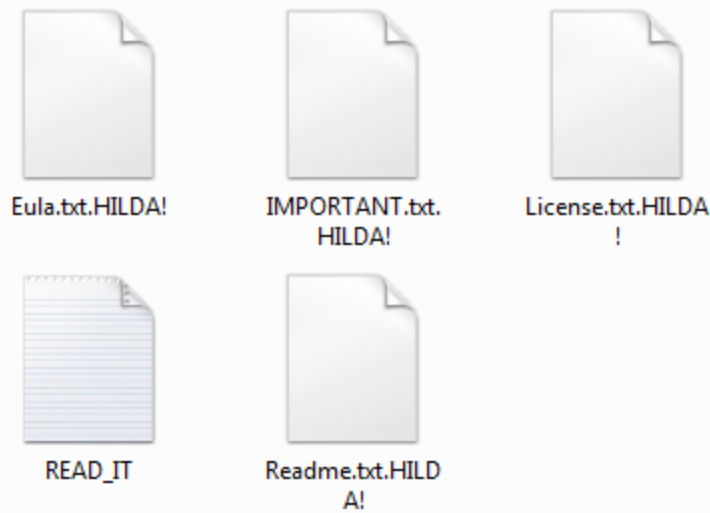
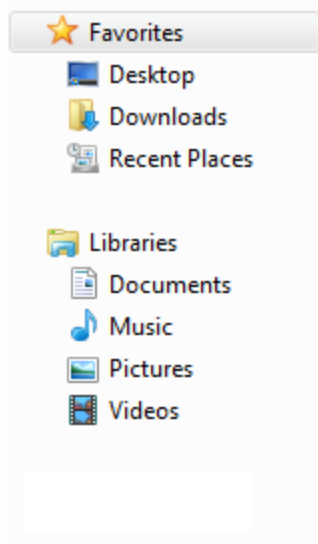
#### Malware.exe

- o % App.path%\ **TXT**  
Instruction for recovery
- o %App.path%\ [Name]. **HILDA!**

Once the computer is compromised, the ransomware runs the following commands:

Malware.exe (2544)	Microsoft PDF Do... "C:\Users\windows7\Desktop\Malware.exe"	Microsoft Corporation
net.exe (2120)	Net Command "net.exe" /stop WinDefend /y	Microsoft Corporation
net1.exe (2336)	Net Command C:\Windows\system32\net1 /stop WinDefend /y	Microsoft Corporation
net.exe (1872)	Net Command "net.exe" /stop MBAMService /y	Microsoft Corporation
net1.exe (2272)	Net Command C:\Windows\system32\net1 /stop MBAMService /y	Microsoft Corporation
vssadmin.exe (1136)	Command Line Int... "vssadmin.exe" Delete Shadows /All /Quiet	Microsoft Corporation

The ransomware encrypts all the files and appends the **[.HILDA!]** extension onto each encrypted file's filename.



Malware.exe	CreateFile	C:\Program Files\DVD Maker\Shared\DvdStyles\Circle_SelectionSubpictureA.png.HILDA!
Malware.exe	CreateFile	C:\Program Files\DVD Maker\Shared\DvdStyles\Circle_SelectionSubpictureB.png.HILDA!
Malware.exe	CreateFile	C:\Program Files\DVD Maker\Shared\DvdStyles\Circle_VideoInset.png.HILDA!
Malware.exe	CreateFile	C:\Program Files\DVD Maker\Shared\DvdStyles\Dot.png.HILDA!
Malware.exe	CreateFile	C:\Program Files\DVD Maker\Shared\DvdStyles\Heart_ButtonGraphic.png.HILDA!
Malware.exe	CreateFile	C:\Program Files\DVD Maker\Shared\DvdStyles\Heart_SelectionSubpicture.png.HILDA!
Malware.exe	CreateFile	C:\Program Files\DVD Maker\Shared\DvdStyles\Heart_VideoInset.png.HILDA!
Malware.exe	CreateFile	C:\Program Files\DVD Maker\Shared\DvdStyles\menu_style_default_Thumbnail.png.HILDA!
Malware.exe	CreateFile	C:\Program Files\DVD Maker\Shared\DvdStyles\NavigationLeft_ButtonGraphic.png.HILDA!
Malware.exe	CreateFile	C:\Program Files\DVD Maker\Shared\DvdStyles\NavigationLeft_SelectionSubpicture.png.HILDA!
Malware.exe	CreateFile	C:\Program Files\DVD Maker\Shared\DvdStyles\NavigationRight_ButtonGraphic.png.HILDA!
Malware.exe	CreateFile	C:\Program Files\DVD Maker\Shared\DvdStyles\NavigationRight_SelectionSubpicture.png.HILDA!
Malware.exe	CreateFile	C:\Program Files\DVD Maker\Shared\DvdStyles\NavigationUp_ButtonGraphic.png.HILDA!
Malware.exe	CreateFile	C:\Program Files\DVD Maker\Shared\DvdStyles\NavigationUp_SelectionSubpicture.png.HILDA!
Malware.exe	CreateFile	C:\Program Files\DVD Maker\Shared\DvdStyles\photoedge_buttongraphic.png.HILDA!
Malware.exe	CreateFile	C:\Program Files\DVD Maker\Shared\DvdStyles\photoedge_selectionsubpicture.png.HILDA!
Malware.exe	CreateFile	C:\Program Files\DVD Maker\Shared\DvdStyles\photoedge_videoinset.png.HILDA!
Malware.exe	CreateFile	C:\Program Files\DVD Maker\Shared\DvdStyles\Postage_ButtonGraphic.png.HILDA!
Malware.exe	CreateFile	C:\Program Files\DVD Maker\Shared\DvdStyles\Postage_SelectionSubpicture.png.HILDA!
Malware.exe	CreateFile	C:\Program Files\DVD Maker\Shared\DvdStyles\Postage_VideoInset.png.HILDA!
Malware.exe	CreateFile	C:\Program Files\DVD Maker\Shared\DvdStyles\shadowonlyframe_buttongraphic.png.HILDA!
Malware.exe	CreateFile	C:\Program Files\DVD Maker\Shared\DvdStyles\shadowonlyframe_selectionsubpicture.png.HILDA!
Malware.exe	CreateFile	C:\Program Files\DVD Maker\Shared\DvdStyles\shadowonlyframe_videoinset.png.HILDA!

After encrypting all personal documents, the ransomware shows the following text file containing a message reporting that the computer has been encrypted and to contact its developer for unlock instructions.

---+ HILDACRYPT v1.0 +---

All the files on this computer have been encrypted with a RSA-4096 + AES-256 cryptographic combination. These algorithms are used by the NSA and other top tier organisations.

Backups were encrypted, and shadow copies were removed. So F8 or any other methods may damage encrypted data and make it unrecoverable.

We exclusively have decryption software for your situation. More than a year ago, world experts have recognized the impossibility of decrypting by any means without the original decryptor. NO decryption software is available to the public. Antivirus companies, researchers, IT specialists, and no one else can help you recover your data.

DO NOT RESET OR SHUTDOWN - file may be damaged.  
DO NOT DELETE readme files.  
DO NOT REMOVE OR RENAME the encrypted files.  
This may lead to the impossibility of your files being recovered.

To confirm our honest intentions, send us 2 different files and you will get them decrypted. They must not contain any sensitive information and must not be archived.

To get info (decrypt your files) contact us at:  
hildaseriesnetflix125@tutanota.com  
or  
hildaseriesnetflix125@horsefucker.org

You will receive a BTC address for payment in the reply letter.

HILDACRYPT

No loli is safe :) -- <https://www.youtube.com/watch?v=XCojP2Ubuto>

**SonicWall Capture Labs provides protection against this threat via the following signature:**

**GAV: Hildacrypt.RSM (Trojan)**

This threat is also detected by SonicWALL Capture ATP w/RTDMI and the Capture Client endpoint solutions.