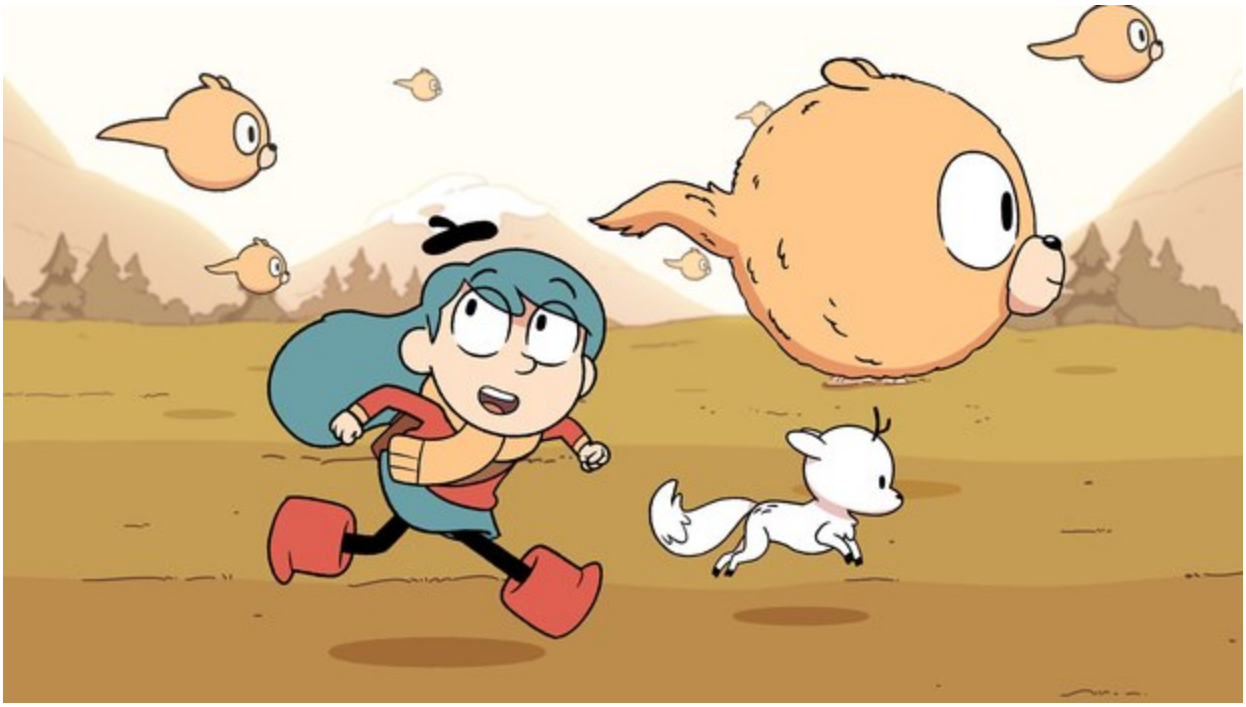
Hildacrypt Ransomware actively spreading in the wild

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:

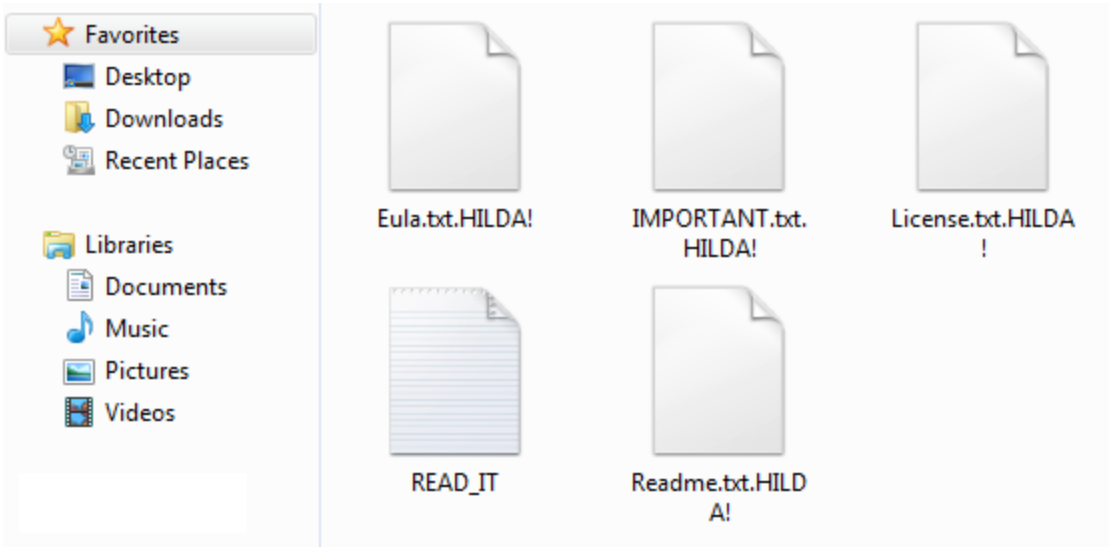
Malware.exe

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

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

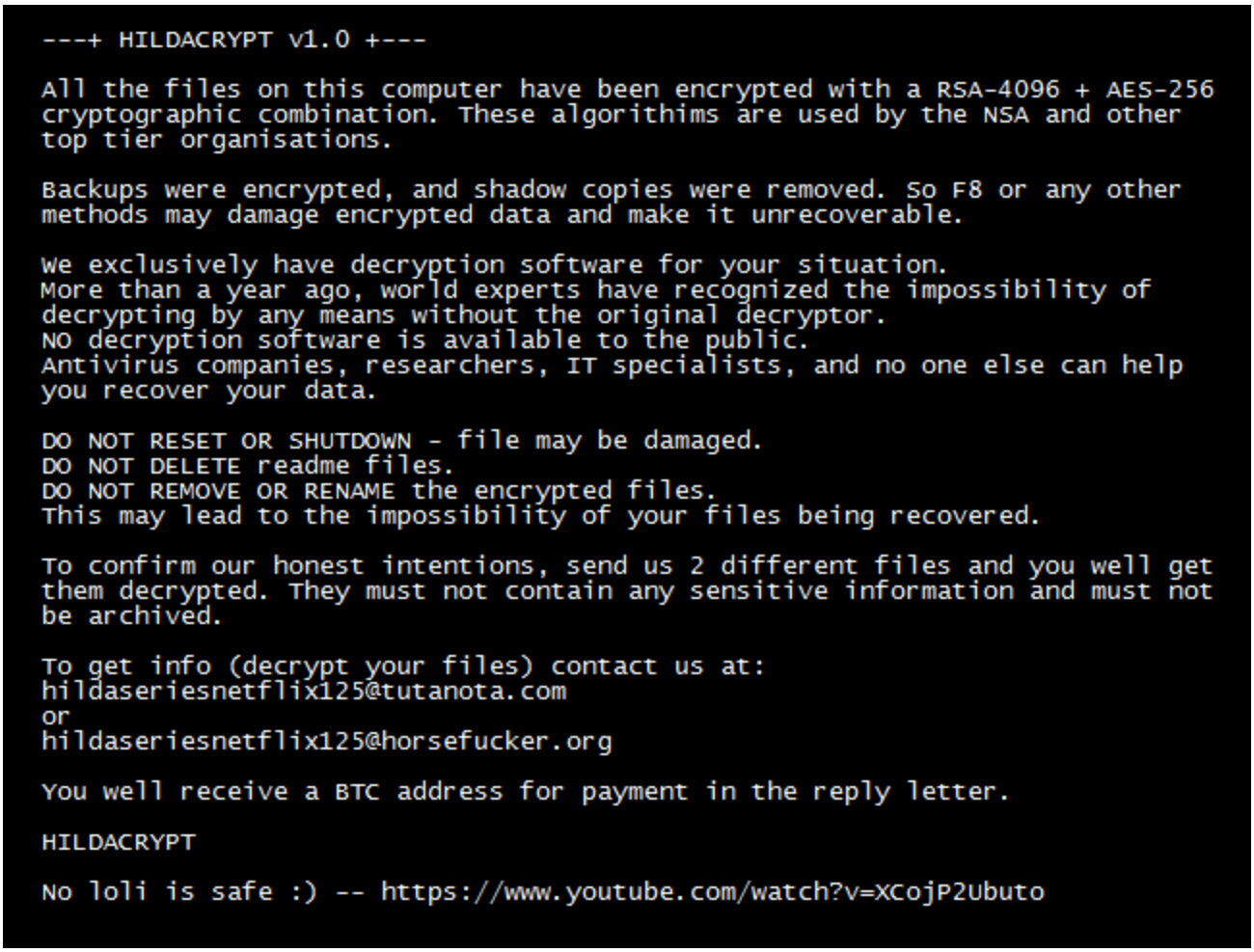
Malware.exe (2544)	Microsoft PDF Do...	"C:\Users\windows7\Desktop\Malware.exe"	Microsoft Corporation
net.exe (2120)	Net Command	"net.exe" /stop WinDefend /y	Microsoft Corporation
net1.exe (2336)	Net Command	C:\Windows\system32\net1 /stop WinDefend /y	Microsoft Corporation
net.exe (1872)	Net Command	"net.exe" /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.



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.