CryptoLuck Ransomware being Malvertised via RIG-E Exploit Kits

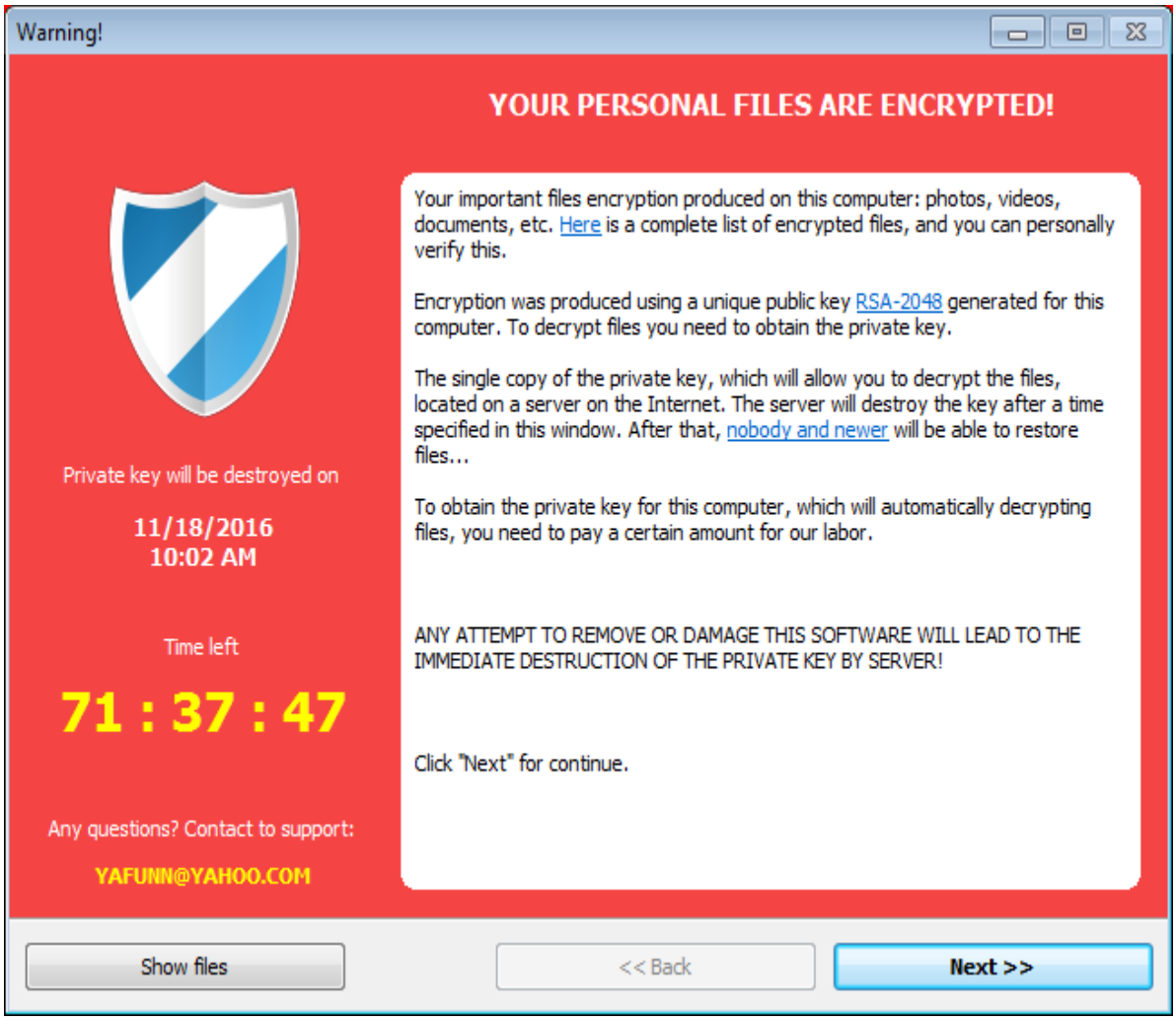
By Lawrence Abrams

November 15, 2016 03:46 PM

http://www.bleepingcomputer.com/news/security/cryptoluck-ransomware-being-malvertised-via-rig-e-exploit-kits/

A new ransomware called CryptoLuck has been discovered by Proofpoint security researcher and exploit kit expert Kafeine that is being distributed via the RIG-E exploit kit. While it has become common to see new ransomware variants being distributed daily, it is not as common to find new ransomware infections being distributed via exploit kits. Seeing this type of activity typically indicates that a particular ransomware will see much wider distribution and thus a larger amount of victims.

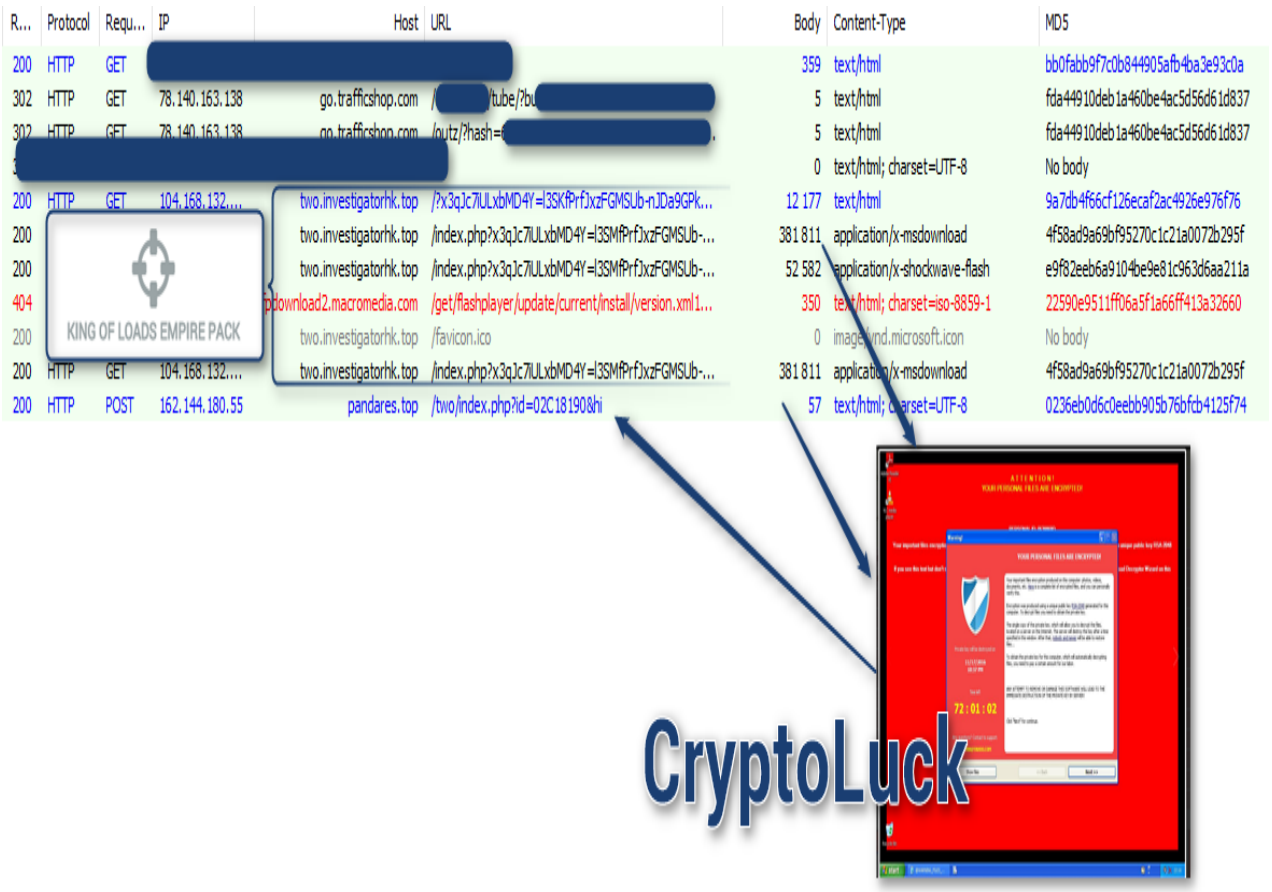
CryptoLuck also utilizes an interesting method of infecting a victim through the legitimate GoogleUpdate.exe executable and DLL hijacking. Once infected, a victim's data will be encrypted and then be given a 72 hour countdown to pay a 2.1 bitcoin, or approximately $1,500 USD, ransom payment.



CryptoLuck

CryptoLuck distributed via Exploit kits after Redirection from Compromised Websites and Malvertising Chains

According to Kafeine, CryptoLuck has been spotted being distributed via the RIG-E (Empire) exploit kit through malvertising. While Kafeine only specifically saw this sample through advertising in the Adult web site space, he said there is a good possibility of it also being distributed through other sources such as compromised sites.

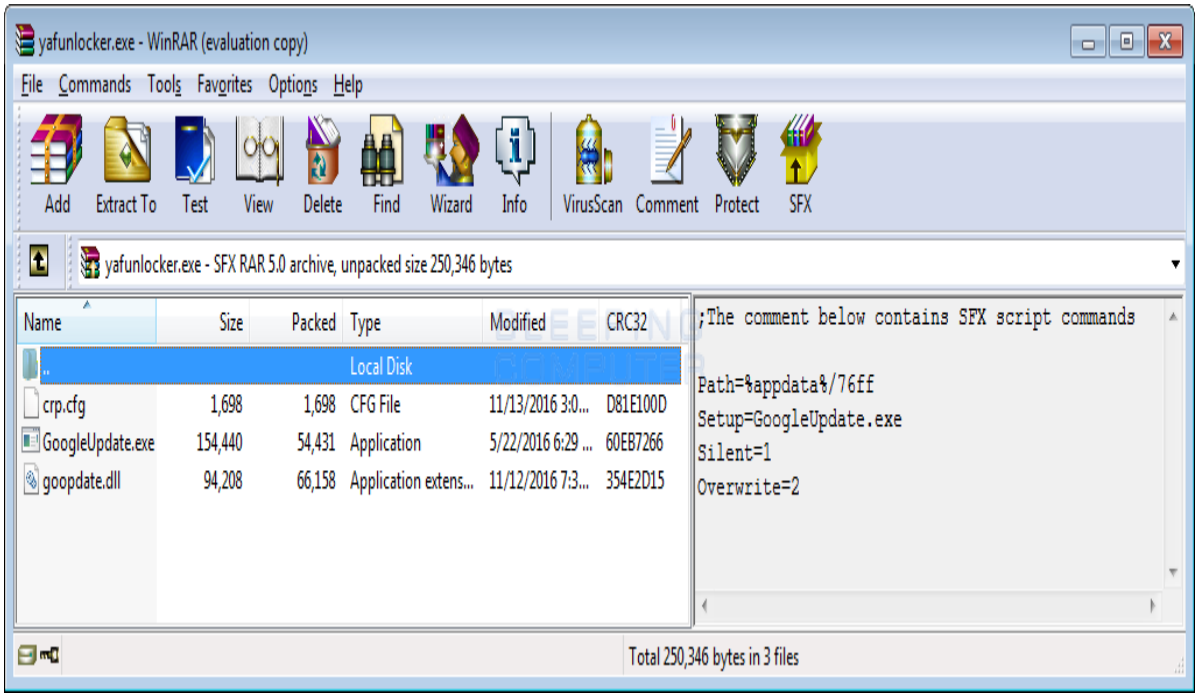


RIG-E Exploit Kit installing CryptoLuck
Source: Kafeine

CryptoLuck installed via bundled Googleupdate.exe and DLL Hijacking

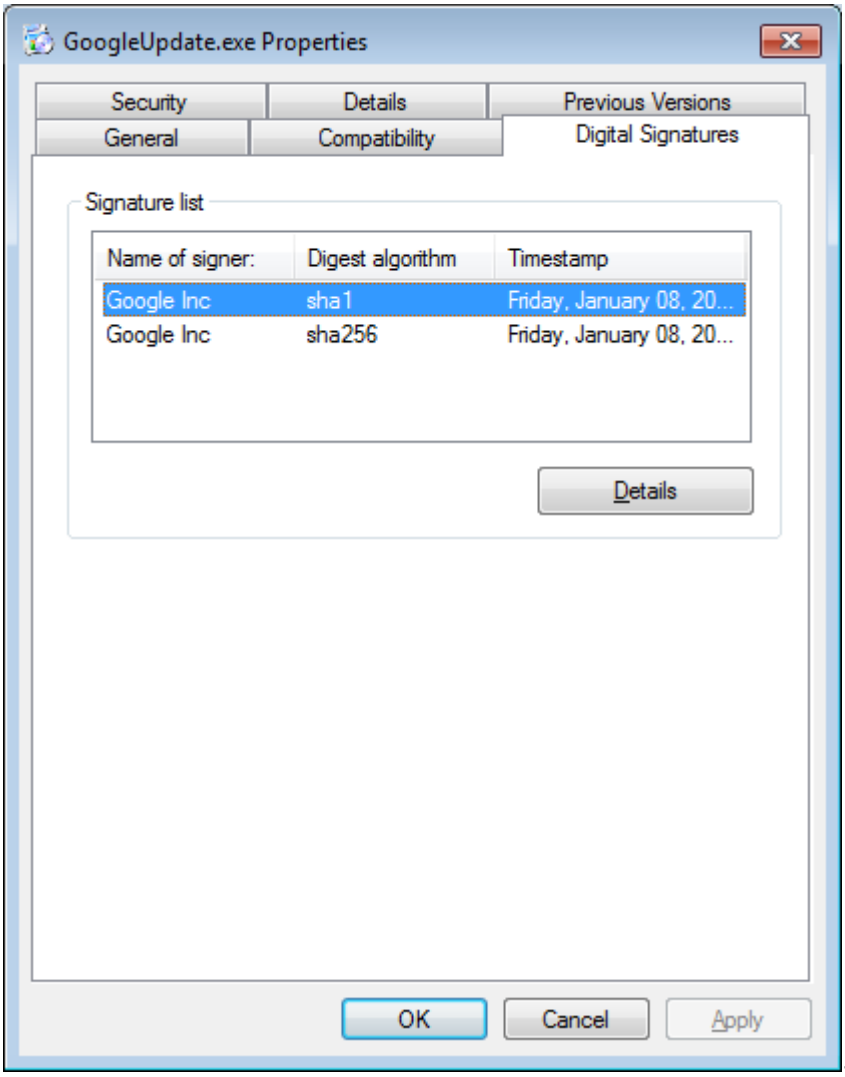
An interesting feature of CryptoLuck is that it uses a legitimate and code signed program from Google called GoogleUpdate.exe and DLL hijacking to install the ransomware. To understand how this works, we need to take a look at how the ransomware is installed.

This ransomware is distributed using a RAR SFX file that includes the crp.cfg, GoogleUpdate.exe, and goopdate.dll files. The SFX file also contains instructions that when it is executed it will extract these files into the %AppData%\76ff folder and then silently execute the GoogleUpdate.exe program.



CryptoLuck RAR SFX File

The GoogleUpdate.exe is a legitimate Google program that is signed by Google as shown below.



Signed Google Executable

When the GoogleUpdate.exe program is run, it will look for a DLL file called goopdate.dll file and load it. The problem is that it will first look for this file in the same folder that the GoogleUpdate.exe resides in. This allows a malware developer to create their own malicious goopdate.dll file and have it loaded by GoogleUpdate.

This is the case with the CryptoLuck developer, who had put all of the ransomware related code into their own malicious goopdate.dll file. Then when the legitimate GoogleUpdate.exe file is executed it loads the malicious DLL rather than the legitimate one normally used by Google.

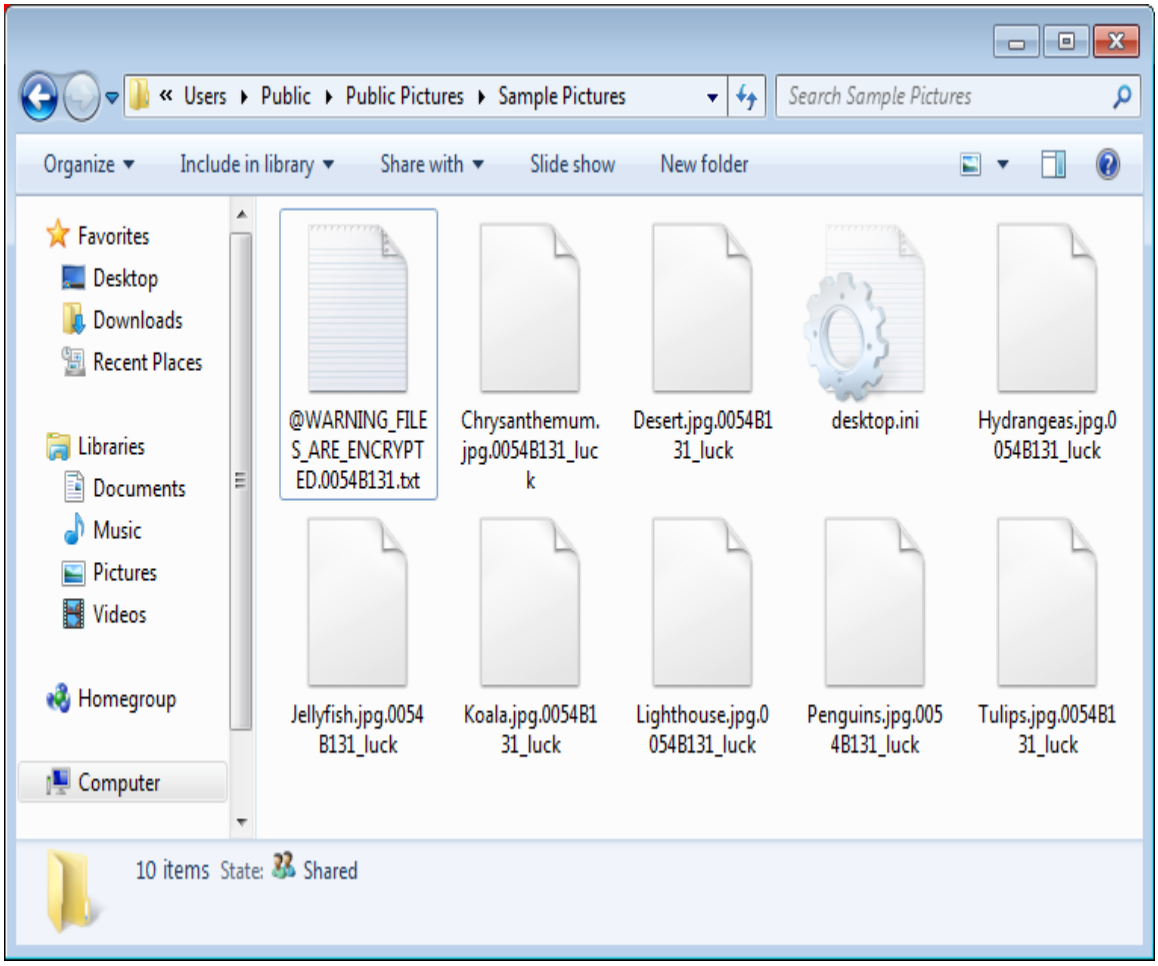
How CryptoLuck Encrypts your Files

When CryptoLuck infects a computer it will first check to see if it is being run within a virtual machine, and if it is, the process will terminate. Otherwise, it will scan the computer, its mounted drives, and unmapped network shares for files that contain certain file extensions. According to Fabian Wosar of Emsisoft, when it detects a targeted file it will generate a unique AES encryption key for that file and encrypt the file using AES-256 encryption. This file's encryption key is then encrypted with an embedded public RSA key and the resulting encrypted AES key is embedded in the encrypted file.

The current public RSA encryption key for CryptoLuck is:

```
-----BEGIN PUBLIC KEY-----
MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAnoamWzd2h7DKzMKYAhdJ
qoQDpVAd0mirVhWElZsstWdTVfb4WxYMftVJx1CN2MG0FxSF7Rp825Iokm/6MWry
cXeaafM5vK/AD7j9X/4oxuxZI1zb+BJBvN/kzThDeH2oSmVsSuvT1JlIqn7iGfrG
D93Ej7ENL53r0SVFXFFB6WhOji54eJlLTkJGH2cYubsREvobBQ4SytKUxEkxbaHp
6kOM9l3UOaJm6tEepeQmiW4ZaGJmGLGgc1dL0cw+YPooz8egLuLSvLGnBw4W+RyN
VHKamYLN7JX11rzw5ZnhknS7BFKcSY0nV0tD+CgcQsaaM06qMmsMTT1vW9wtotDX
FwIDAQAB
-----END PUBLIC KEY-----
```

When files are encrypted they will have the **.[victim_id]_luck** extension appended to filename. For example, if a victim had an ID of 0054B131 and a file called test.jpg was encrypted by CryptoLuck its new name would be test.jpg.0054B131_luck. The original name of each encrypted file is then added as an entry under the HKCU\Software\sosad_[victim_idfile]\files key.



CryptoLuck Encrypted Files

The files targeted by CryptoLuck are:

```
.3ds .3fr .4db .4dd .7z .7zip .accdb .accdt .aep .aes .ai .apk .
arch00 .arj .arw .asset .bar .bay .bc6 .bc7 .big .bik .bkf .bkp
 .blob .bpw .bsa .cas .cdr .cer .cfr .cr2 .crp .crt .crw .csv .d
3dbsp .das .dazip .db0 .dba .dbf .dbx .dcr .der .desc .dmp .dng
 .doc .docm .docx .dot .dotm .dotx .dwfx .dwg .dwk .dxf .dxg .em
l .epk .eps .erf .esm .fdb .ff .flv .forge .fos .fpk .fsh .gdb .
gho .gpg .gxk .hkdb .hkx .hplg .hvpl .ibank .icxs .idx .ifx .in
dd .iso .itdb .itl .itm .iwd .iwi .jpe .jpeg .jpg .js .kdb .kdbx
 .kdc .key .kf .ksd .layout .lbf .litemod .lrf .ltx .lvl .m2 .ma
p .max .mcmeta .mdb .mdbackup .mddata .mdf .mef .menu .mlx .mpd
 .mpp .mpqge .mrwref .msg .myo .nba .nbf .ncf .nrw .nsf .ntl .nv
2 .odb .odc .odm .odp .ods .odt .ofx .orf .p12 .p7b .p7c .pak .p
db .pdd .pdf .pef .pem .pfx .pgp .pkpass .ppj .pps .ppsx .ppt .p
ptm .pptx .prproj .psd .psk .pst .psw .ptx .py .qba .qbb .qbo .q
bw .qdf .qfx .qic .qif .r3d .raf .rar .raw .rb .re4 .rgss3a .rim
 .rofl .rtf .rw2 .rwl .saj .sav .sb .sdc .sdf .sid .sidd .sidn .
sie .sis .sko .slm .snx .sql .sr2 .srf .srw .sum .svg .sxc .sync
```

```
db .t12 .t13 .tar .tax .tbl .tib .tor .txt .upk .vcf .vcxproj .v
df .vfs0 .vpk .vpp_pc .vtf .w3x .wallet .wb2 .wdb .wotreplay .w
pd .wps .x3f .xf .xlk .xls .xlsb .xlsm .xlsx .xxx .zip .ztmp
```

Last, but not least, when CryptoLuck scans for files to encrypt, it will skip files whose names contain the following strings:

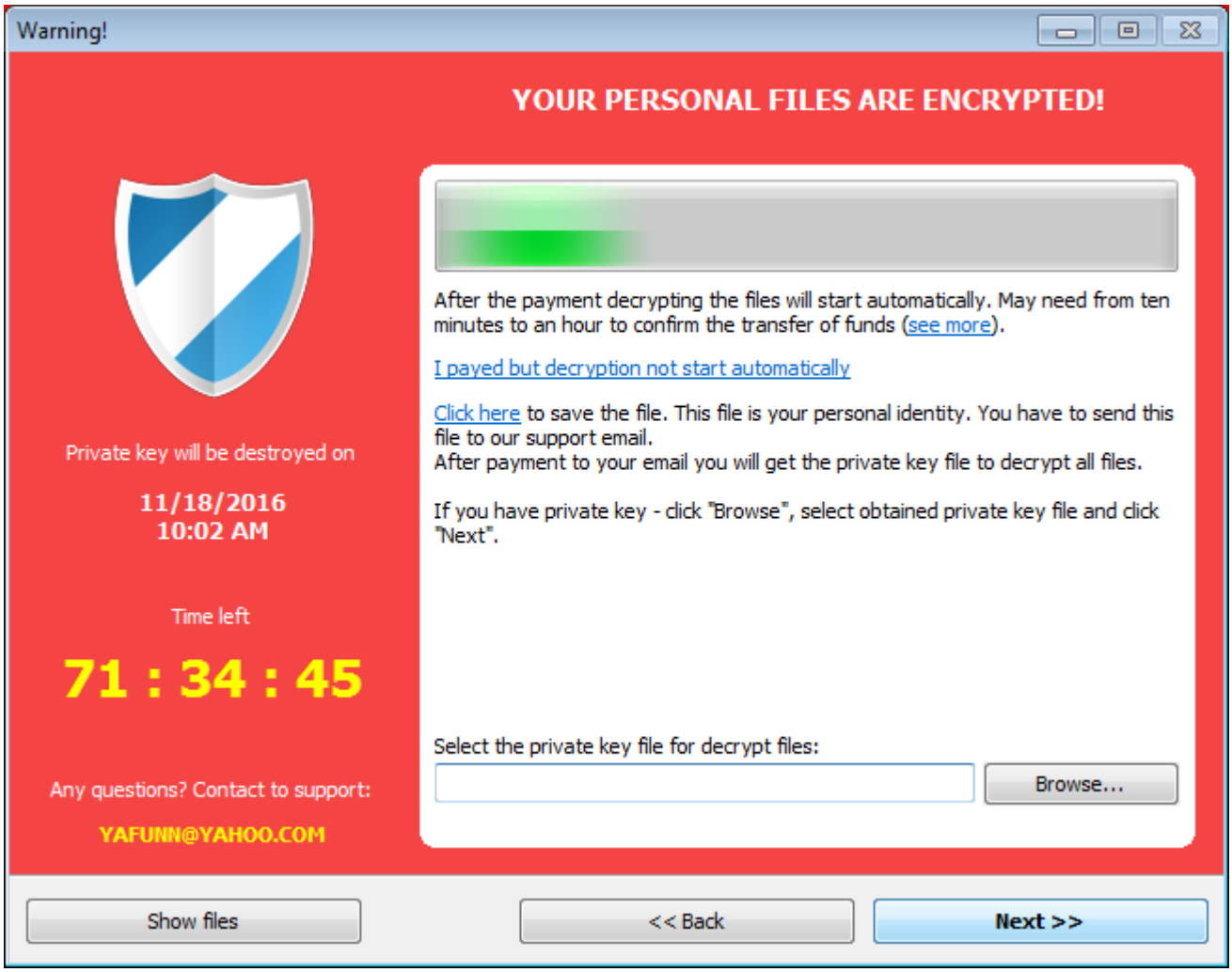
```
Windows

Program Files

Program Files (x86)

ProgramData

AppData

Application Data

Temporary Internet Files

Temp

Games

nvidia

intel

$Recycle.Bin

Cookies
```

When it has finished encrypting the files and available network shares, it will display a ransom note named **%AppData%\@WARNING_FILES_ARE_ENCRYPTED.[victim_id].txt**. This ransom note will contain instructions on how to download the decryptor and make the ransom payment. The text of this ransom note is:

```
A T T E N T I O N !

YOUR PERSONAL FILES ARE ENCRYPTED!

PERSONAL ID: 0054B131


Your important files encryption produced on this computer: phot
os, videos, documents, etc. Encryption was produced using a uni
```

```
que public key RSA-2048 generated for this computer. To decrypt
 files you need to obtain the private key.


If you see this text but don't see Decryptor Wizard window - ple
ase, disable any Firewalls and antivirus products, and download
 Decryptor Wizard on this URL:

http://dropmefiles.com/304718



You have 72 hours for payment.

After this time the private key will be destroyed.




For more info and support, please, contact us at this email add
ress:

YAFUNN@YAHOO.COM
```

The victim will then be shown a Decryption Wizard that walks the victim through making a payment and then waits for the payment to be made. If a ransom payment is made, the decryptor states it will automatically decrypt the victim's files.



Waiting for Payment

Unfortunately, as each file is encrypted using their own unique AES key and only the malware developer knows the master RSA decryption key, this ransomware is not currently decryptable. For those who are looking for further support or who have questions regarding CryptoLuck, you can ask in the CryptoLuck Help and Support Topic.

Files associated with CryptoLuck:

```
%AppData%\@WARNING_FILES_ARE_ENCRYPTED.0054B131.txt
%AppData%\info_[vicitm_id].info
%AppData%\76ff\
%AppData%\76ff\crp.cfg
%AppData%\76ff\GoogleUpdate.exe
```

```
%AppData%\76ff\goopdate.dll
```

Registry entries associated with CryptoLuck:

```
HKCU\Software\Microsoft\Windows\CurrentVersion\Run\GoogleUpdate.exe  %AppData%\76ff\GoogleUpdate.exe

HKCU\Software\sosad_[victim_id]
```

IOCs:

```
SHA256: d399d7eb0e02123a5262549f822bb06e27b4bc8749260363788a5e39a0ce5c2a
```

Network Communication:

```
http://pandares.top/two/index.php
```

http://www.bleepingcomputer.com/news/security/cryptoluck-ransomware-being-malvertised-via-rig-e-exploit-kits/