2016. 12. 06

Tech Report

Locky Ransomware Variants Cropping Up Continuously

AhnLab

220, Pangyoyeok-ro, Bundang-gu, Seongnam-si, Gyeonggi-do, South Korea

Tel: +82-31-722-8000 | Fax: +82-31-722-8901 | www.ahnlab.com

Table of Content

Introduction

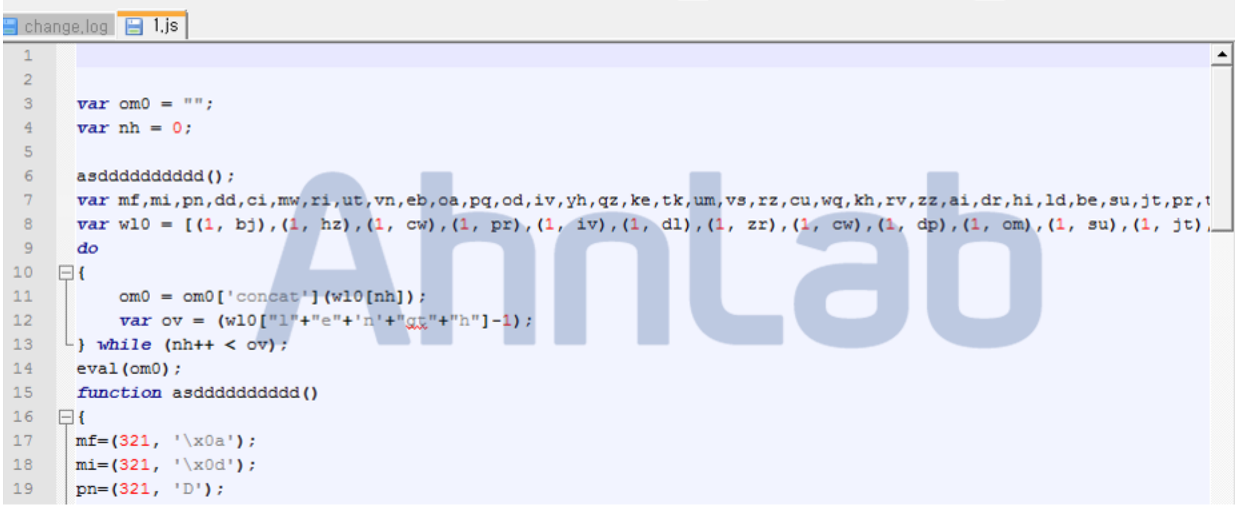
Locky ransomware is proving to be disturbingly resilient. First spotted in February of 2016, Locky is not only extremely active but continuously evolving. Locky is being distributed as attachments to mass spam emails via the Necurs botnet. These attachments have diversified beyond the previous .DOCX format to include JS (JavaScript), WSF (Windows Script File), HTA (Hyper-Text Application), and most recently LNK (Windows shortcut) files.

The extensions added to the encrypted files of the infected PCs have continued to change as well. The files were initially renamed with the .locky extension, then to .zepto in late June and .odin in late September, with a recent variant found in late October changing the affected file's extension to the lamentable ".shit". It took four months for the extension to change from locky to zepto, an even shorter period of three months to change into odin, and a single month for the newest extension to appear.

This report presents two recent variants of the Locky ransomware and the most practical ransomware response strategy for both individual users and corporations.

Findings #1. Locky ransomware that turns file extension to .shit

This recent variant of Locky, like older versions, is distributed as a JS (JavaScript) file. They are generally compressed as ZIP files, and the infection occurs when the ZIP file is decompressed and the user clicks on the JS file contained within.



```


var om0 = "";
var nh = 0;

asdddddddddd();
var mf,mi,pn,dd,ci,mw,ri,ut,vn,eb,oa,pq,od,iv,yh,qz,ke,tk,um,vs,rz,cu,wq,kh,rv,zz,ai,dr,hi,ld,be,su,jt,pr,t
var wl0 = [(1, bj),(1, hz),(1, cw),(1, pr),(1, iv),(1, dl),(1, zr),(1, cw),(1, dp),(1, om),(1, su),(1, jt),
do
{
    om0 = om0['concat'](wl0[nh]);
    var ov = (wl0["l"+"e"+'n'+"gt"+"h"]-1);
} while (nh++ < ov);
eval(om0);
function asdddddddddd()
{
mf=(321, '\x0a');
mi=(321, '\x0d');
pn=(321, 'D');
```

[Figure 1] Ransomware downloader in obfuscated JavaScript

Once the obfuscated downloader script is executed, the malware accesses the IP/URL shown below to download the DLL file.

coreywallace.com/qjkrlxp
74.220.199.24:80

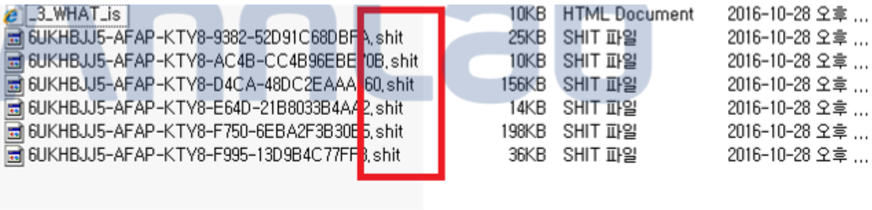
[Table 1] URL and IP of the DLL file location

The DLL file is written in the path below, and, similar to other existing Locky variants, loads the DLL with rundll32.exe to begin the file encryption process.

C:\Documents and Settings\Administrator\Local Settings\Temp\VFVGY7may1.dll

[Table 2] File location where the DLL file is stored

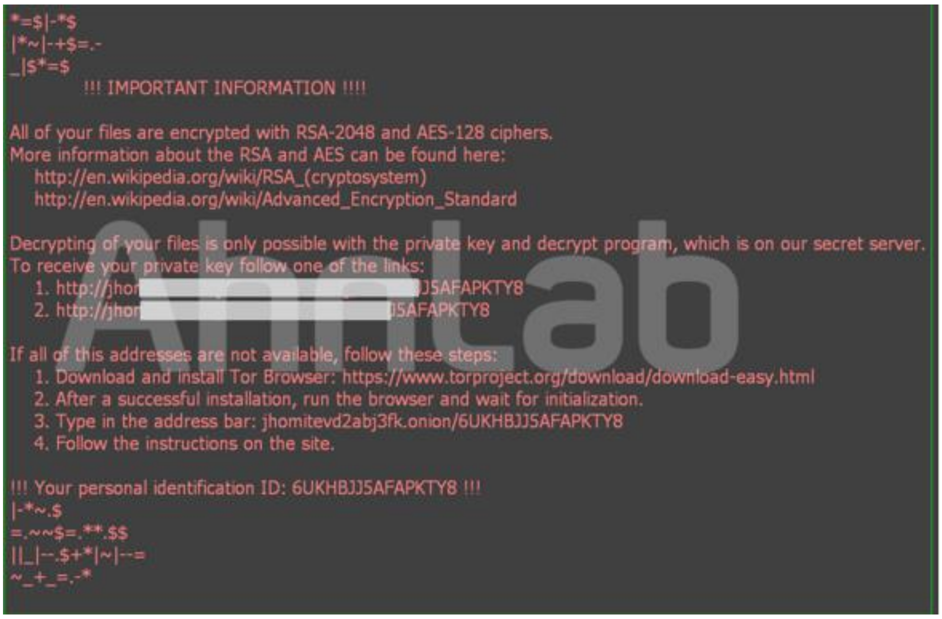
Once the encryption is complete, the file names and extensions are altered. The file names are changed into a 32 character-long string, with the first 16 characters kept uniform to apparently serve as a unique identifier of the infected PC. Whereas older variants added ".odin" as the new extension, the newer strain adds the extension ".shit".



```
_3_WHAT_is                                      10KB   HTML Document   2016-10-28 오후 ...
6UKHBJJ5-AFAP-KTY8-9382-52D91C68DBFA.shit       25KB   SHIT 파일        2016-10-28 오후 ...
6UKHBJJ5-AFAP-KTY8-AC4B-CC4B96EBE70B.shit       10KB   SHIT 파일        2016-10-28 오후 ...
6UKHBJJ5-AFAP-KTY8-D4CA-48DC2EAAA60.shit       156KB   SHIT 파일        2016-10-28 오후 ...
6UKHBJJ5-AFAP-KTY8-E64D-21B8033B4AA2.shit       14KB   SHIT 파일        2016-10-28 오후 ...
6UKHBJJ5-AFAP-KTY8-F750-6EBA2F3B30E5.shit      198KB   SHIT 파일        2016-10-28 오후 ...
6UKHBJJ5-AFAP-KTY8-F995-13D9B4C77FFB.shit       36KB   SHIT 파일        2016-10-28 오후 ...
```

[Figure 2] New extensions added after encryption

The ransom note that is displayed following the Locky infection shows little difference when compared to those of other variants.

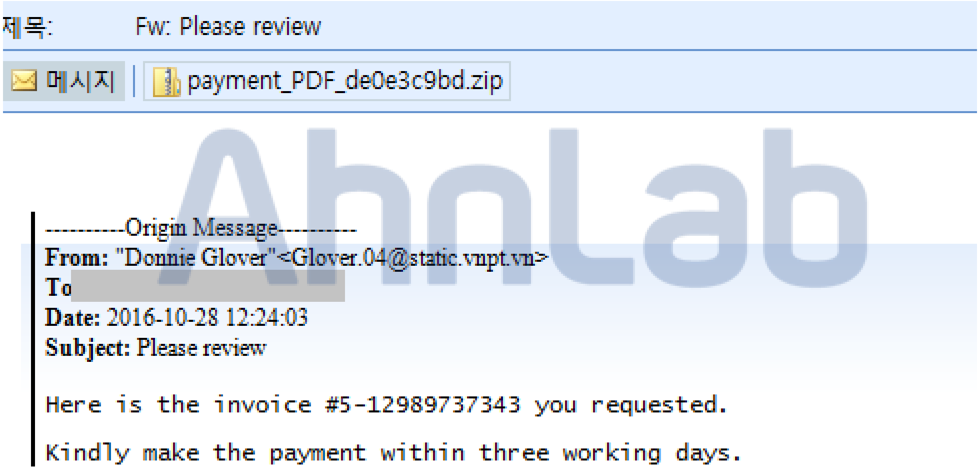


```
*=$|-*$
|*~|-+$=.-
_|$*=$
        !!! IMPORTANT INFORMATION !!!!

All of your files are encrypted with RSA-2048 and AES-128 ciphers.
More information about the RSA and AES can be found here:
    http://en.wikipedia.org/wiki/RSA_(cryptosystem)
    http://en.wikipedia.org/wiki/Advanced_Encryption_Standard

Decrypting of your files is only possible with the private key and decrypt program, which is on our secret server.
To receive your private key follow one of the links:
    1. http://jhor[redacted]J5AFAPKTY8
    2. http://jhor[redacted]J5AFAPKTY8

If all of this addresses are not available, follow these steps:
    1. Download and install Tor Browser: https://www.torproject.org/download/download-easy.html
    2. After a successful installation, run the browser and wait for initialization.
    3. Type in the address bar: jhomitevd2abj3fk.onion/6UKHBJJ5AFAPKTY8
    4. Follow the instructions on the site.

!!! Your personal identification ID: 6UKHBJJ5AFAPKTY8 !!!
|-*~.$
=.~~$=.**.$$
||_|--.$+*|~|--=
~_+_=.-*
```

[Figure 3] Pay-up warning dialogue of .shit Locky

Findings #2. Locky variant that changes the file extension to .thor

Only days after the appearance of the Locky variant that changes the extension of affected files to .shit, a new Locky variant was discovered that attaches the new extension .thor. Like other variants, the ransomware was disseminated as ZIP file attachments of spam emails.



제목: Fw: Please review

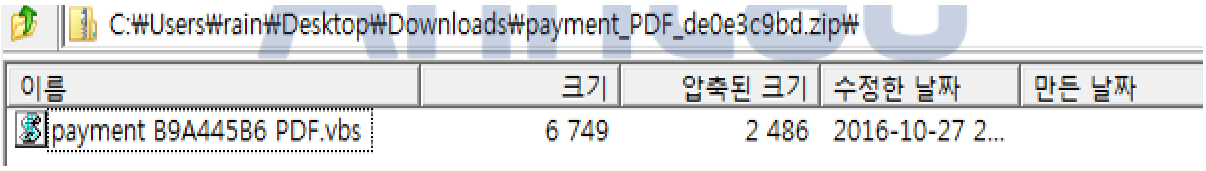
----------Origin Message----------
From: "Donnie Glover"<Glover.04@static.vnpt.vn>
To [redacted]
Date: 2016-10-28 12:24:03
Subject: Please review

Here is the invoice #5-12989737343 you requested.

Kindly make the payment within three working days.

[Figure 4] Distribution as a spam email attachment

Unlike the ".shit Locky" ransomware that contains a JS (JavaScript) file in the attachment, “.thor Locky” contains a VBS (Visual Basic Script) file.

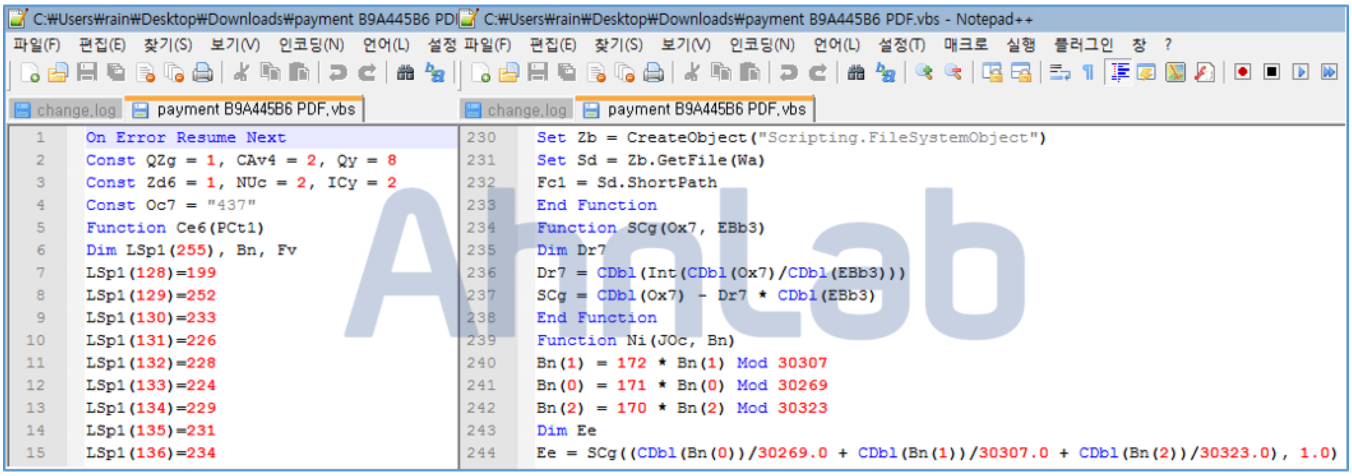


C:₩Users₩rain₩Desktop₩Downloads₩payment_PDF_de0e3c9bd.zip₩

이름	크기	압축된 크기	수정한 날짜	만든 날짜
payment B9A445B6 PDF.vbs	6 749	2 486	2016-10-27 2...	

[Figure 5] VBS file contained in the ZIP file attachment

Like the JavaScript file in other variants, the VBS file contained in the ZIP file is obfuscated to evade recognition.



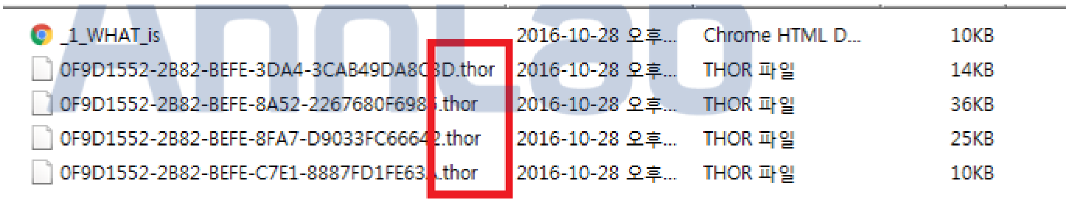
C:₩Users₩rain₩Desktop₩Downloads₩payment B9A445B6 PDF.vbs - Notepad++
파일(F) 편집(E) 찾기(S) 보기(V) 인코딩(N) 언어(L) 설정(T) 매크로 실행 플러그인 창 ?
change.log
payment B9A445B6 PDF.vbs

```
On Error Resume Next
Const QZg = 1, CAv4 = 2, Qy = 8
Const Zd6 = 1, NUc = 2, ICy = 2
Const Oc7 = "437"
Function Ce6(PCt1)
Dim LSp1(255), Bn, Fv
LSp1(128)=199
LSp1(129)=252
LSp1(130)=233
LSp1(131)=226
LSp1(132)=228
LSp1(133)=224
LSp1(134)=229
LSp1(135)=231
LSp1(136)=234
```

```
Set Zb = CreateObject("Scripting.FileSystemObject")
Set Sd = Zb.GetFile(Wa)
Fc1 = Sd.ShortPath
End Function
Function SCg(Ox7, EBb3)
Dim Dr7
Dr7 = CDbl(Int(CDbl(Ox7)/CDbl(EBb3)))
SCg = CDbl(Ox7) - Dr7 * CDbl(EBb3)
End Function
Function Ni(JOc, Bn)
Bn(1) = 172 * Bn(1) Mod 30307
Bn(0) = 171 * Bn(0) Mod 30269
Bn(2) = 170 * Bn(2) Mod 30323
Dim Ee
Ee = SCg((CDbl(Bn(0))/30269.0 + CDbl(Bn(1))/30307.0 + CDbl(Bn(2))/30323.0), 1.0)
```

[Figure 6] Obfuscated ransomware downloader in VBS format

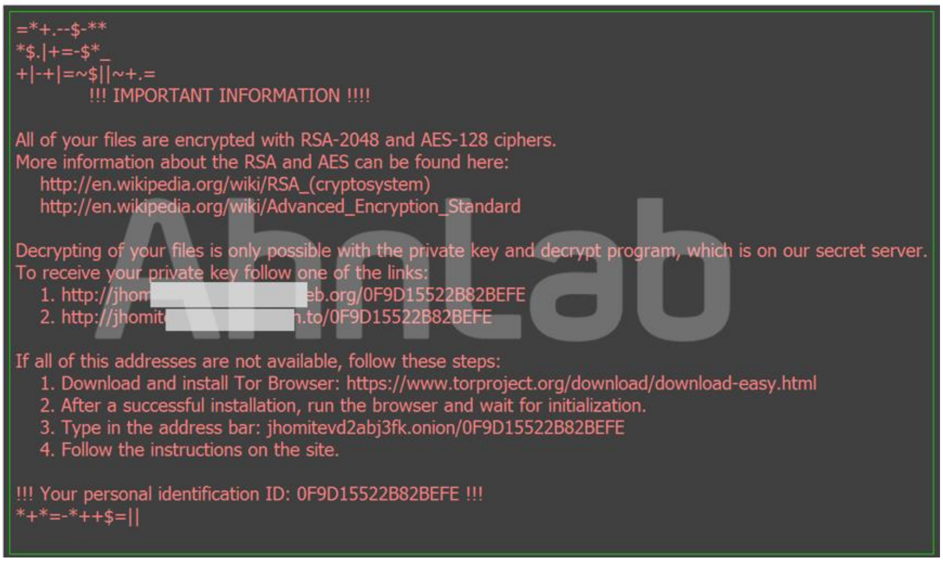
Once the encryption of the files in the infected PC is complete, the extensions are changed, this time, to ".thor". Another common feature this strain shares with other variants is the alteration of the file name to a string composed of 32 characters. The first 16 are again fixed, seemingly representing the unique ID of the infected PC.



```
_1_WHAT_is                                    2016-10-28 오후...   Chrome HTML D...   10KB
0F9D1552-2B82-BEFE-3DA4-3CAB49DA8C3D.thor     2016-10-28 오후...   THOR 파일           14KB
0F9D1552-2B82-BEFE-8A52-2267680F6985.thor     2016-10-28 오후...   THOR 파일           36KB
0F9D1552-2B82-BEFE-8FA7-D9033FC66642.thor     2016-10-28 오후...   THOR 파일           25KB
0F9D1552-2B82-BEFE-C7E1-8887FD1FE63A.thor     2016-10-28 오후...   THOR 파일           10KB
```

[Figure 7] New .thor extensions given to encrypted files

The ransom note for this particular variant, like the other example cited earlier, is unchanged from older Locky variants.



```
=*+.--$-**
*$.|+=-$*_
+|-+|=~$||~+.=
         !!! IMPORTANT INFORMATION !!!!

All of your files are encrypted with RSA-2048 and AES-128 ciphers.
More information about the RSA and AES can be found here:
   http://en.wikipedia.org/wiki/RSA_(cryptosystem)
   http://en.wikipedia.org/wiki/Advanced_Encryption_Standard

Decrypting of your files is only possible with the private key and decrypt program, which is on our secret server.
To receive your private key follow one of the links:
   1. http://jhom[redacted]eb.org/0F9D15522B82BEFE
   2. http://jhomit[redacted]n.to/0F9D15522B82BEFE

If all of this addresses are not available, follow these steps:
   1. Download and install Tor Browser: https://www.torproject.org/download/download-easy.html
   2. After a successful installation, run the browser and wait for initialization.
   3. Type in the address bar: jhomitevd2abj3fk.onion/0F9D15522B82BEFE
   4. Follow the instructions on the site.

!!! Your personal identification ID: 0F9D15522B82BEFE !!!
*+*=-*++$=||
```

[Figure 8] Pay-up warning dialogue of .thor Locky

The relevant aliases of these Locky variants identified by V3 products, AhnLab's anti-virus program, are shown below:

<Aliases identified by V3 products>
Trojan/Win32.Locky (2016.10.25.03)
JS/Obfus.S158 (2016.10.25.05)
Trojan/Win32.Locky (2016.10.28.03)
Downloader/VBS.Agent (2016.10.29.00)

Conclusion: Practical Ransomware Response Strategy

Locky is proving to be just one of a wide variety of advanced ransomware that continues to proliferate around the world. Like legitimate software programs, ransomware also continuously upgrades into new versions and are increasingly evolving into advanced persistent threats (APTs) that utilize a wide range of attack methods in order to evade detection by antivirus programs. These trends are making it increasingly difficult for traditional security solutions to detect these newer types of ransomware and protect systems.

These latest ransomware attacks show that ransomware also target endpoints. With this in view, AhnLab provides a viable ransomware countermeasure strategy by the interoperation of V3 Internet Security (V3), AhnLab's anti-virus program, with AhnLab MDS, an APT protection solution. V3 provides cloud-feed as well as signature- and reputation-based malware detection to identify and block ransomware as well as their variants. V3 also employs behavior-based technology to detect the entire stages of ransomware activity, from initial infiltration to activation and encryption. In June, 2016, AhnLab newly applied decoy honeypot technology to bolster V3's ransomware detection capability, which has been followed by continuous updates and refinements.

AhnLab MDS (Malware Defense System), an APT protection solution, collects and detects flies being infiltrated at the network level and conducts sandbox-based static and dynamic analysis for new and unknown malware and exploits. MDS provides an agent-based "Execution Holding" function that actively prevent ransomware from wreaking havoc. Execution holding is a feature that prevents a file from being executed while being analyzed by MDS, preventing a potentially harmful file from damaging the system. Execution holding prevents ransomware-suspected files from carrying out destructive activities such as encrypting the PC's documents, photos and videos, protecting the initial victim from harm as well as considerably reducing the damage caused by ransomware by employing precise analysis to determine whether a file is malicious.