





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 Cont	tents
SECURITY ISSUE	"Osiris" Ransomware Rises from the Grave	04
ANALYSIS-IN-DEPTH	VenusLocker Presenting Serious Throat for 2017	10

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



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.



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

					Í		hsrj	iWg`	ľ₩,z	:k							
WgTW																	
t(h) 00	0 01	02	03	04	05	06	07	08	09	0.4	ов	oc	OD	OE	OF		Ξzÿÿ
es 0000	9 29	Å6	4E	61	49	58	42	54	70	64	73	C9	B1	69	49);NjIXBTpdsɱiI	
0010 EO	0 42	50	70	64	73	36	4E	29	49	58	42	50	70	64	73	àBPpds6N) IXBPpds	È
0020 36	5 4E	69	49	58	42	50	70	64	73	36	4E	69	49	58	42	6NiIXBPpds6NiIXB	LÍ!Th
0030 50	0 70	64	73	36	4E	69	49	58	42	50	70	AC	73	36	4E	Ppds6NiIXBPp¬s6N	is program canno
0040 67	7 56	E2	4C	50	C4	6D	BE	17	F6	68	05	95	63	04	18	gVâLPĂm%.öh. c	t be run in DOS
0050 OD	00 0	16	ЗE	1B	26	3F	30	31	1D	44	10	57	20	07	26	>. &201.D.W .&	mode\$
0060 2C	C 62	32	15	44	01	43	20	49	20	36	62	14	3F	37	53	,b2.D.C I 6b.?7S	KÜCEEE
0070 5B	8 21	OD	2C	76	4F	5D	7Å	40	73	36	4E	69	49	58	42	[!., v0] z8s6NiIXB	E:#E.%-E'0'E.%-E
0080 1B	B AC	27	65	39	F3	44	oc	57	FF	7D	35	6B	CE	1B	OB	.¬'e9óD.₩ÿ)5kÎ	`0) E. H-EVZ>E. H-E
0090 E5	5 E8	7B	07	58	CD	49	36	56	EC	4E	0C	5C	FF	7D	35	åè(.XÍI6VìN.\ÿ)5	9>SE.H-EPigh.H-E
0010 04	4 D1	1F	OB	64	F4	75	07	06	EE	5Å	36	34	F3	44	oc	.ÑdóuîZ64óD.	PE.L
00B0 61	1 D9	76	35	48	CE	1B	OB	3B	20	ЗB	2 A	5F	CD	49	36	aÙv5HÎ; ;* ÍI6	.cgx
0000 36	5 4E	69	49	58	42	50	70	34	36	36	4E	25	48	5D	42	6NiIXBPp466N%H]B	
000 36	5 4E	69	49	40 58	42	50	70	34	36	36	4E	25	48	49 5D	42	6N1IXBPp466N%H]B	.çgx~

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

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.

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.



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.

5	200	HTTP	royaloakripon.co.uk	/8eecjblke	146,568	max-ag	text/plain	wscript
6	200	HTTP	Tunnel to	translate.googleapis.com:	0			chrome
7	200	HTTP	Tunnel to	clients4.google.com:443	0			chrome
38	200	HTTP	Tunnel to	clients3.google.com:443	0			chrome
i 9	502	HTTP	owudguyilz	1	534	no-cac	text/html; c	chrome
10	502	HTTP	ozgjiker	1	534	no-cac	text/html; c	chrome
11	502	HTTP	yifnfkia	_	534	no-cac	text/html; c	chrome

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 Accept-Encoding: gzip, deflate User-Agent: Mozilla/5.0 (Windows NT Entity Content-Length: 0 Transport Host: owudguyilz Proxy-Connection: keep-alive	Client Accept-Encoding: gzip, deflate User-Agent: Mozila/S.0 (Windows NT Entity Content-Length: 0 Transport Host: ozgiker Proxy-Connection: keep-alive	Client Accept-Encoding: gzip, deflate User-Agent: Mozilla/S.0 (Windows NT Entity Content-Length: 0 Transport Host: yifnfkia Proxy-Connection: keep-alive	
Figure 1–6 HTTP HE	AD requests		

After these preliminary steps are out of the way and the files are encrypted, a notice indicating ransomware infection appears on the PC, as shown in Figure 1–7. It is noticeable that the extensions of encrypted files have been altered from *.zk* to *.osiris* as shown in Figure 1–8.



	374I660JCBIUYT5G5EA1D4B9B5A26D7064CD.osiris
	374I660JCBIUYT5G9BC1897683F314534261.osiris
	374I660JCBIUYT5G421BED27927C06605B6A.osiris
	374I660JCBIUYT5G12705AF014A1E67A1A1B.osiris
	374I660JCBIUYT5G560014E60010363BD670.osiris
	374I660JCBIUYT5GC83AEA2D972C77D719D5.osiris
	374I660JCBIUYT5GE6B4A662408C4B433A3C.osiris
D	374I660JCBIUYT5GFCF80D371D0E8FD53F80.osiris

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

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

Analysis-In-Depth

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.



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=u1X002hOybNdRvZb9SGGnm 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 <i>VenusLocker</i>'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: <i>VenusLf</i>, <i>VenusLf</i>, <i>VenusLfS</i> 2. Partial encryption: <i>Venusp</i>, <i>VenusLp</i>, <i>VenusLpS</i>

Ahnlab

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, wrx, 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, pf, 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, d

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.

Yo	our are hacked	Your personal files are encrypted What happened Payment	
Your KI 2017-0	KEY will be destroyed on 03-30 Ω.≑ 4:35:59	What happened to my files Your presonal files, including your photos, documents, videos and other important files on this computer, have been encrypted with RSA 2048, a strong encryption algorithm RSA algorithm generates a public key and a private key for your computer. The public key was used to encrypt your files a moment ago. The private key is necessary for you to decrypt and recover your files. Now, your private key is stored on our secret Internet server. And there is no doubt that no one can recover your files who your private key. How to decrypt my files To decrypt and recover your files, you have to pay SOU US Dollars For the private key in the original file subject them the topic of the private key and decryption service. Note that you have ONLY 72 hours To decrypt my files SOU US Dollars For the private key them the private key and decryption service. Note that you have only our service All you files, when your permet if your permet directed on the completed within time first, your private key with a dolled a difficult time first, your service All you files. How to pay for my private key The security of timesactions, all the payment must be completed via Blocin network. Thus, you need to exchange 500 USD (or exavised to cal carrencies) to Blocins, and then served these files to be following receiving address.	you have Warning e your in files vourd better not close this window. If you close it, you will not able to see it again. Are you sure? Cancel all the o Bitcoins. and then send these Bitcoins (about 0.86 BTC) to the following rece
	Time Left 71:58:18	TO/9YnMiciNgaKuy2Kynygu7n821tvV80D For further information about BTC, please refer to the next "Payment Tab". 2. After making a payment with BTC, please send your personal ID to our official email. Vour Personal D is Ba87833be81ac710113af4de9262250d4 3. You will receive a decryptor and your private key to recover all your files within one working day. Please keep checking your email. For detailed information, you can also read the file "ReadMe.txt" on your desktop.	1Dj9YnMiciNgaKuyzKynygu7nB21tvV6QD
Figure 2–3 Infecti	ion notice (le	eft) and pop-up warning if the user attempt	s 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.

QWRvYmUucGRm.VenusLp	VENUSLP 파일	12KB
v6K8v8XXvbrGrl9FeGNlbC54bHN4.VenusL	.f VENUSLF 파일	10KB
VFhUX05vX1BhZGRpbmcudHh0.VenusLf	VENUSLF 파일	1KB
Word_패팅.dock.Venusits	VENUSLFS 파일	14KB
x9Gx2y5od3A=.VenusLf	VENUSLF 파일	10KB
xdi9usauX1BhZGRpbmcudHh0.VenusLf	VENUSLF 파일	1KB
	Ŷ	
이름	유형	크기
🛃 [512]Adobe.pdf	Adobe Acrobat Document	12KB
📜 [1024]Adobe.pdf	Adobe Acrobat Document	12KB
TXT_No_Padding.txt	텍스트 문서	1KB
🕙 Word_패팅.docx	Microsoft Word 문서	14KB
에셀테스트_Excel.xlsx	Microsoft Excel 워크시트	10KB

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.

W1RFU1RdUERGLnBkZg==.VenusLp
[5T2][TEST]PDF.pdf

Figure	2-5
--------	-----

Files created during recovery of partially encrypted files

ſ	1012(1157)POFed Addre Aurobat Reader DC Rig 82 x27(m) 5000 £6800 S 5.7 [512](1157)POFed x Image: I	2 🗣
	O コ ギンビー アンパル あたき きゃうちゅう シンシー ジェル あり たきふま またらいた. C	eve re
	① 이 파철은 POI/A 표준을 준수하여 수정할 수 없도록 읽기 전용으로 열렸습니다. 한 전	전집 사용
	Recovery succe Interview (Dummy) [Text] [T	ess

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.

0000h:	58 5	6 65	62	75	73 .	IC (8 6	3 63	3 65	72	20	52	61 62		(Venu	aro	cker R	lan	0	000h:	58	5.6	65	62	75	73	10	65	63	68 (65 7	72 2	0 5	2 61	1.62	[Ve	nua	Lock	cer R	a:
0010h:	73 4	T 62	77	61	72 (65 5	D O	D 03	58	44	75	6D	6D 71	1	SOUND	ize].	. [Dum	wy 👘	0	010h:	73	67	60	77	61	72	65	5D	0D	OA :	18 1	44 7	5 6	D 60	0 79	808	INA.	e]	[Dum	m)
0020h:	5D 0	D CA	58	54	65 1	73 7	4 5	D						1	1 [7	(est)			0	020h:	50	00	0A	58	54	65	73	74	5D	00 00	00 0	00 0	0 0	0 00	00 0	1	[Te	at].		
																			0	030h:	00	00	00	00	00	00	00	00	00	00 0	00 0	00 0	0 0	0 00	00 0					
																			0	040h	00	00	00	00	00	00	00	00	00	00 0	00 0	00 0	0 0	0 00	00 0					
																			0	050h:	00	00	00	00	00	00	00	00	00	00 0	00 0	00 0	0 0	0 00	00 0					
																			0	060h	00	00	00	00	00	00	00	00	00	00 0	00 0	00 0	0 0	0.00	00 0					
																	Δŀ		10	0		00	00	00	00	00	00	00	00	00 0	00 0	00 0	0 0	0 00	00 0					
																					6	00	00	00	00	00	00	00	00	00 0	00 0	00 0	0.0	0 00	00					
																			0	090h:	00	00	00	00	00	00	00	00	00	00 0	00 0	00 0	0 0	0 00	00 0					
																			0	03.0h;	00	00	00	00	00	00	00	00	00	00 0	00 0	00 0	0 0	0 00	00					
																			0	OB0h:	00	00	00	00	00	00	00	00	00	00 0	00 0	00 0	0 0	0 00	00 0					
																			0	ocoh:	00	00	00	00	00	00	00	00	00	00 0	00 0	00 0	0 0	0 00	00 0					
																			0	opoh:	00	00	00	00	00	00	00	00	00	00 0	00 0	00 0	0 0	0 00	00 0					
																			0	OE0h:	00	00	00	00	00	00	00	00	00	00 0	00 0	00 0	0 0	0 00	00 0					
																			0	OFOh:	00	00	00	00	00	00	00	00	00	00 0	00 0	00 0	0 0	0 00	00 0					

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 Q1 2017

Ahnlab

ContributorsASEC ResearchersEditorContent Creatives TeamDesignDesign Team

Publisher Al Website gl Email gl

AhnLab, Inc. global.ahnlab.com global.info@ahnlab.com

Disclosure to or reproduction for others without the specific written authorization of AhnLab is prohibited.

©AhnLab, Inc. All rights reserved.