Locky Ransomware Returns, but Targets Only Windows XP & Vista

bleepingcomputer.com/news/security/locky-ransomware-returns-but-targets-only-windows-xp-and-vista/

Catalin Cimpanu

By
Catalin Cimpanu

- June 22, 2017
- 03:48 AM
- 1

The Locky ransomware is back, spreading via a massive wave of spam emails distributed by the Necurs botnet, but the campaign appears to be a half-baked effort because the ransomware is not able to encrypt files on modern Windows OS versions, locking files only on older Windows XP & Vista machines.

Locky's return to action is surprising but makes perfect sense. There have been numerous clues hinting that the same group behind the Necurs botnet was also behind the Locky ransomware, and more recently, the Jaff ransomware, which many have considered Locky's successor.

As Necurs slowly switched to Jaff, the Necurs group stopped spreading Locky spam in May, most likely preferring the newer Jaff ransomware instead of the older Locky.

Locky's return may be tied to Jaff's fall

The Necurs group's long-term plan was foiled last week after security researchers from Kaspersky Labs found a flaw in Jaff's encryption routine and created a free utility to help infected victims recover their files without paying the ransom.

This was unexpected, as researchers were never able to crack Locky's encryption method, and many thought Jaff to be just as tough, if not harder.

Kaspersky's feat appears to have taken the Necurs group by surprise as well. As soon as the free decrypter was made available, Jaff spam went down, and beginning yesterday, the Necurs group started distributing Locky once more. This switch most likely happened because Locky's encryption was never cracked, and operators have a better chance of extorting ransom from infected hosts.

Windows DEP security feature mitigates new Locky variant

The new spam waves were detected by a large number of security researchers. All reported that they had trouble infecting themselves on their test machines.

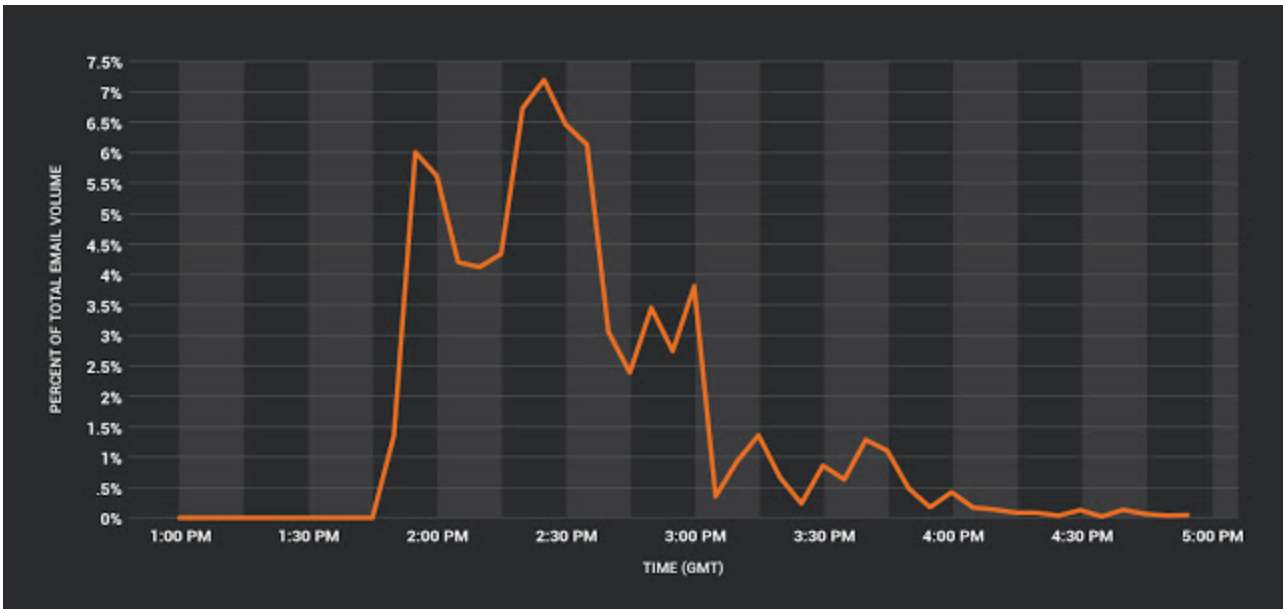
It was Cisco's Talos division that discovered why. According to the company's experts, the Locky authors rushed to replace the decrypted Jaff version with Locky and made several errors in their deployment.

"Upon further investigation, we determined that on systems running Windows 7 or later with Data Execution Prevention (DEP) would cause the unpacker to fail," said Cisco Talos experts. This means that only older OS versions such as XP and Vista are affected.

In their rush, the Locky authors most likely didn't notice this bug, as they put considerable resources into the ransomware's distribution, something they might not have done if they knew its ineffectiveness.

Locky spam accounted for 7.2% of all email spam

Cisco says spam for this new Locky variant accounted for nearly 7.2% of the Internet's entire email spam traffic. That's an insanely massive spam wave for a ransomware that only targets less than 10% of the entire Windows userbase.



Necurs spam wave distributing new Locky version [Source: Cisco Talos]

Furthermore, this Locky version comes with minimal changes from the version researchers spotted the last time, in May. This Locky variant still uses the LOTPR extension at the end of encrypted files, and the same URL structure for C&C servers. This confirms the theory that the Necurs operators rushed to deploy Locky after Kaspersky published the Jaff decrypter.

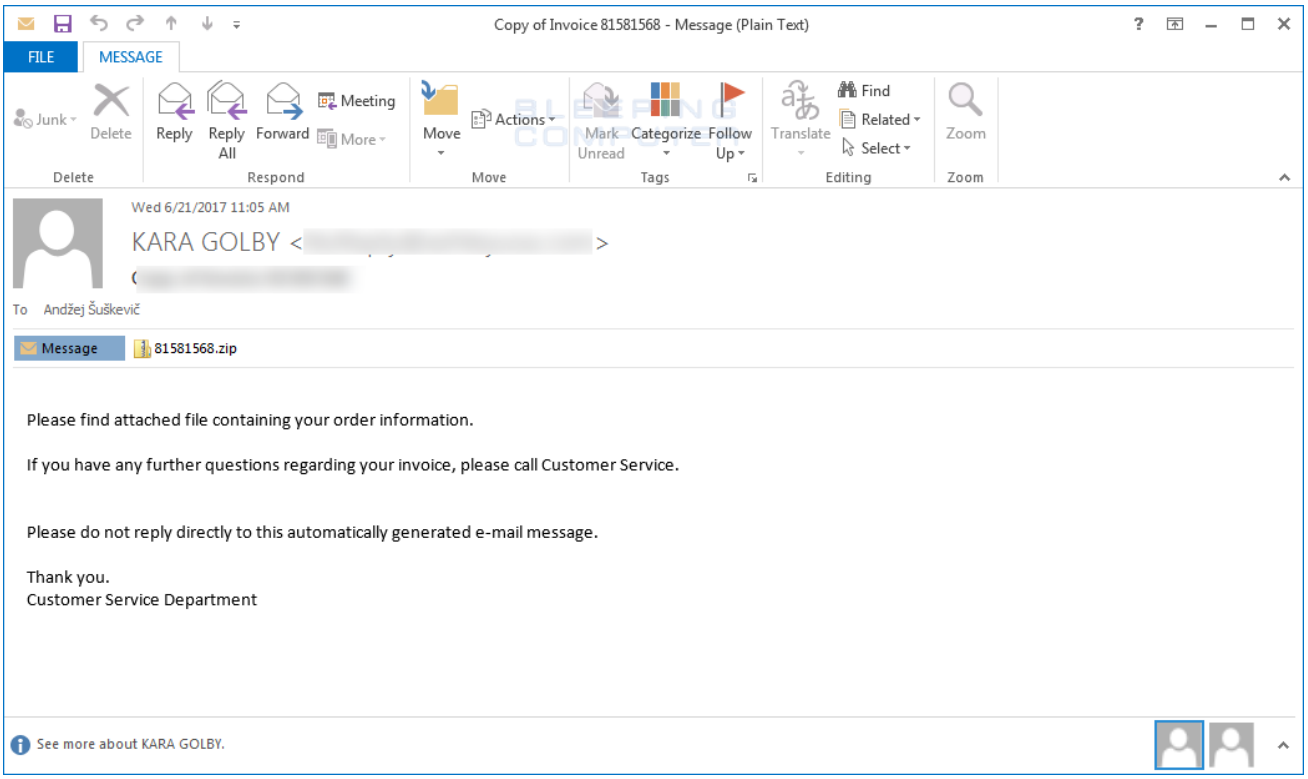
Locky's new tactics

But there are also new wrinkles in this new Locky spam wave as well. Vitaly Kremez, Flashpoint Director of Research, discovered that Locky uses a new method of launching the infected binary on targeted hosts.

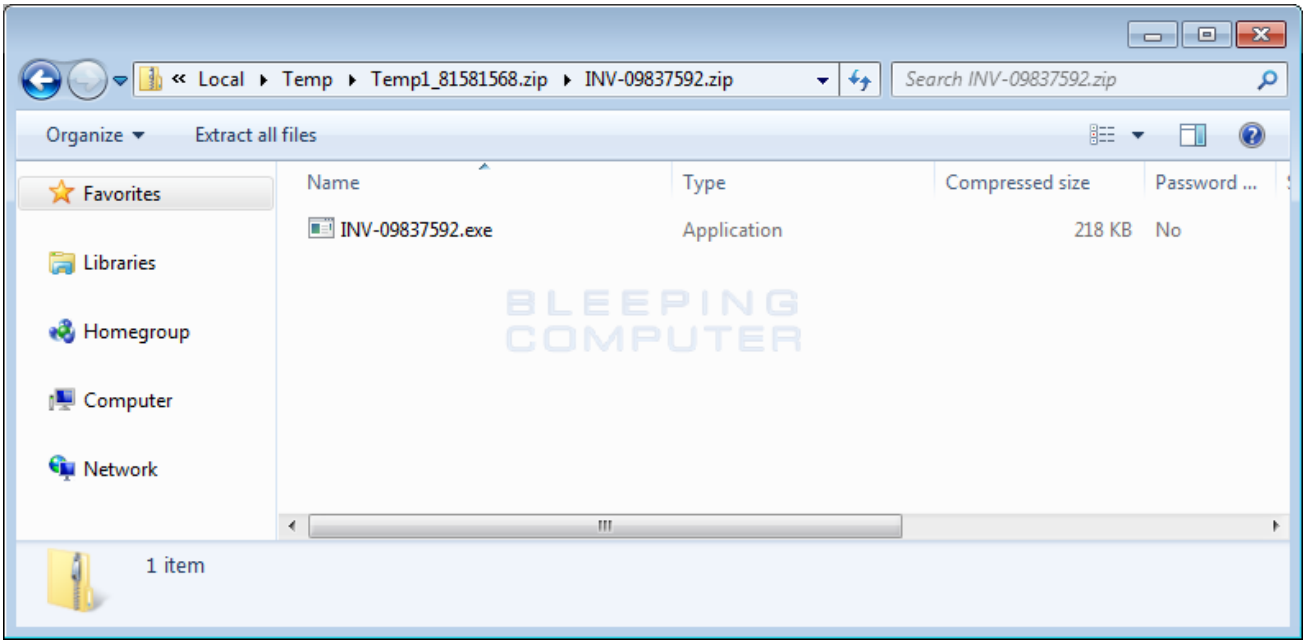
> Still vetting but wanted to share -> #Locky has a seemingly new execution method using ddeexec & Shortcut execution via "locky.exe" "%1" pic.twitter.com/61Ei0X4F6o
>
> — Vitali Kremez (@VK_Intel) June 21, 2017

In addition, the Locky spam emails use new texts for the email subjects and body content, albeit they still pretend to be invoices, payment receipts, order confirmations, and so on.

These emails also packed file attachments differently, utilizing a double-nested ZIP structure. The emails Bleeping Computer analyzed deliver a ZIP file with names in the format of eight random digits (e.g.: 38017832.zip). This initial ZIP file contains another ZIP file, which in turns contains an EXE file that runs Locky when executed.



Emails spreading new Locky version



Content of second ZIP file delivered via recent Locky spam

Last but not least, this Locky version also added some anti-debugging protections that prevent the ransomware from running in virtual machines and other debug environments, which explains why researchers had a hard time analyzing it for the first few hours.

Overall, this particular Locky spam run seems to be a rushed effort, but we can expect the ransomware's operators to correct their flaws and start delivering a fixed version in the following days.

Below are other indicators of compromise for this latest Locky variant.

Hash:

```
49184047c840287909cf0e6a5e00273c6d60da1750655ad66e219426b3cf9cd8
```

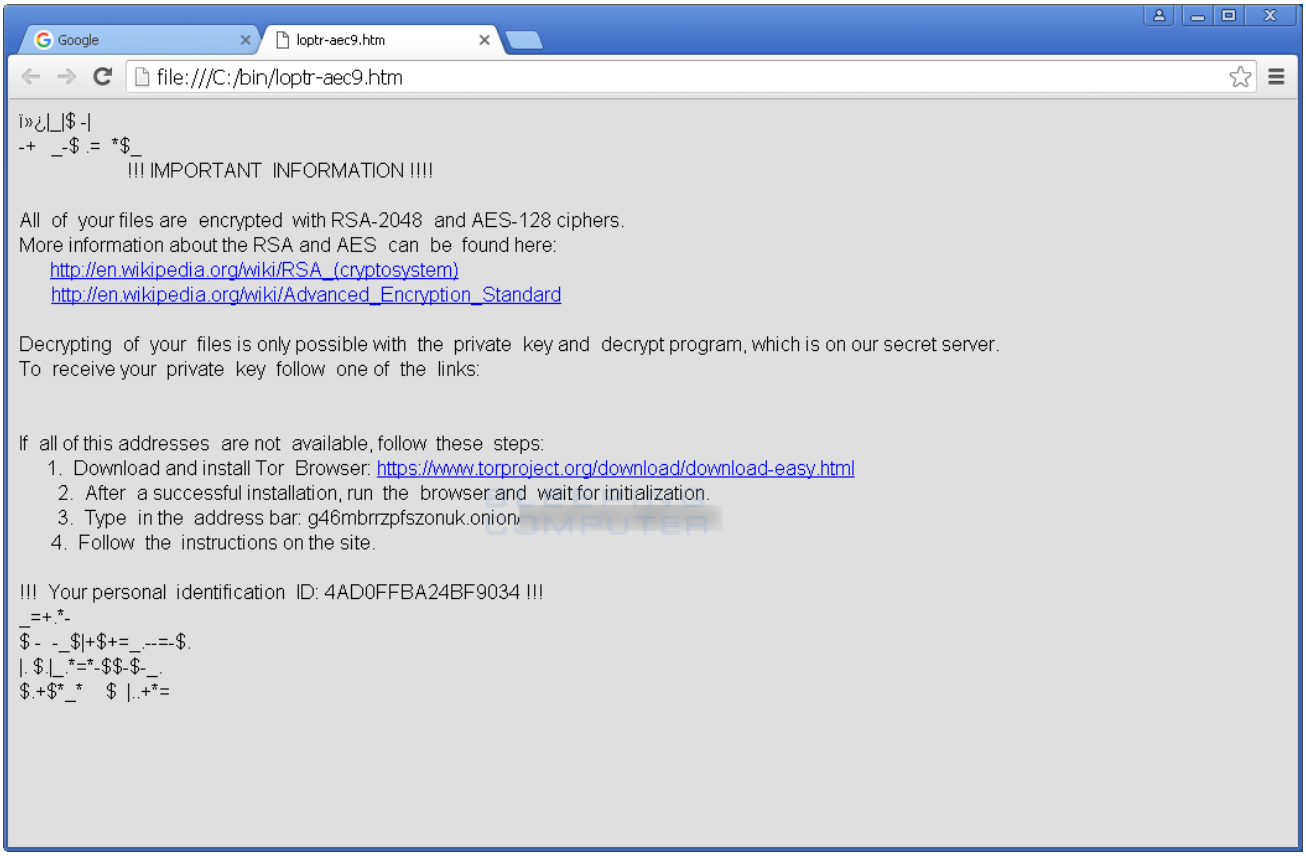
Extension:

```
.loptr
```

Ransom note:

```
loptr-[random_4_chars].htm
```

Ransom Note:



```
-+ _-$ .= *$_
      !!! 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:


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: g46mbrrzpfszonuk.onion/4AD0FFBA24BF9034
 4. Follow the instructions on the site.

!!! Your personal identification ID: 4AD0FFBA24BF9034 !!!
_=+.*-
$ - -_$|+$+=_.--=-$.
|. $.|_.*=*-$$-$-_.
$.+$*_* $ |..+*=
```

Whitelisted folders:

```
tmp
winnt
Application Data
AppData
Program Files (x86)
Program Files
temp
thumbs.db
$Recycle.Bin
System Volume Information
Boot
Windows
```

Extensions:

```
.yuv, .ycbcra, .xis, .wpd, .tex, .sxg, .stx, .srw, .srf, .sqlitedb, .sqlite3,
.sqlite, .sdf, .sda, .s3db, .rwz, .rwl, .rdb, .rat, .raf, .qby, .qbx, .qbw, .qbr,
.qba, .psafe3, .plc, .plus_muhd, .pdd, .oth, .orf, .odm, .odf, .nyf, .nxl, .nwb,
.nrw, .nop, .nef, .ndd, .myd, .mrw, .moneywell, .mny, .mmw, .mfw, .mef, .mdc, .lua,
.kpdx, .kdc, .kdbx, .jpe, .incpas, .iiq, .ibz, .ibank, .hbk, .gry, .grey, .gray,
.fhd, .ffd, .exf, .erf, .erbsql, .eml, .dxg, .drf, .dng, .dgc, .des, .der, .ddrw,
.ddoc, .dcs, .db_journal, .csl, .csh, .crw, .craw, .cib, .cdrw, .cdr6, .cdr5, .cdr4,
.cdr3, .bpw, .bgt, .bdb, .bay, .bank, .backupdb, .backup, .back, .awg, .apj, .ait,
.agdl, .ads, .adb, .acr, .ach, .accdt, .accdr, .accde, .vmxf, .vmsd, .vhdx, .vhd,
.vbox, .stm, .rvt, .qcow, .qed, .pif, .pdb, .pab, .ost, .ogg, .nvram, .ndf, .m2ts,
.log, .hpp, .hdd, .groups, .flvv, .edb, .dit, .dat, .cmt, .bin, .aiff, .xlk, .wad,
.tlg, .say, .sas7bdat, .qbm, .qbb, .ptx, .pfx, .pef, .pat, .oil, .odc, .nsh, .nsg,
.nsf, .nsd, .mos, .indd, .iif, .fpx, .fff, .fdb, .dtd, .design, .ddd, .dcr, .dac,
.cdx, .cdf, .blend, .bkp, .adp, .act, .xlr, .xlam, .xla, .wps, .tga, .pspimage,
.pct, .pcd, .fxg, .flac, .eps, .dxb, .drw, .dot, .cpi, .cls, .cdr, .arw, .aac, .thm,
.srt, .save, .safe, .pwm, .pages, .obj, .mlb, .mbx, .lit, .laccdb, .kwm, .idx,
.html, .flf, .dxf, .dwg, .dds, .csv, .css, .config, .cfg, .cer, .asx, .aspx, .aoi,
.accdb, .7zip, .xls, .wab, .rtf, .prf, .ppt, .oab, .msg, .mapimail, .jnt, .doc,
.dbx, .contact, .mid, .wma, .flv, .mkv, .mov, .avi, .asf, .mpeg, .vob, .mpg, .wmv,
.fla, .swf, .wav, .qcow2, .vdi, .vmdk, .vmx, .wallet, .upk, .sav, .ltx, .litesql,
.litemod, .lbf, .iwi, .forge, .das, .d3dbsp, .bsa, .bik, .asset, .apk, .gpg, .aes,
.ARC, .PAQ, .tar.bz2, .tbk, .bak, .tar, .tgz, .rar, .zip, .djv, .djvu, .svg, .bmp,
.png, .gif, .raw, .cgm, .jpeg, .jpg, .tif, .tiff, .NEF, .psd, .cmd, .bat, .class,
.jar, .java, .asp, .brd, .sch, .dch, .dip, .vbs, .asm, .pas, .cpp, .php, .ldf, .mdf,
.ibd, .MYI, .MYD, .frm, .odb, .dbf, .mdb, .sql, .SQLITEDB, .SQLITE3, .pst, .onetoc2,
.asc, .lay6, .lay, .ms11 (Security copy), .sldm, .sldx, .ppsm, .ppsx, .ppam, .docb,
.mml, .sxm, .otg, .odg, .uop, .potx, .potm, .pptx, .pptm, .std, .sxd, .pot, .pps,
.sti, .sxi, .otp, .odp, .wks, .xltx, .xltm, .xlsx, .xlsm, .xlsb, .slk, .xlw, .xlt,
.xlm, .xlc, .dif, .stc, .sxc, .ots, .ods, .hwp, .dotm, .dotx, .docm, .docx, .DOT,
.max, .xml, .txt, .CSV, .uot, .RTF, .pdf, .XLS, .PPT, .stw, .sxw, .ott, .odt, .DOC,
.pem, .csr, .crt, .key
```

Related Articles:

BlackCat/ALPHV ransomware asks $5 million to unlock Austrian state

Windows 11 KB5014019 breaks Trend Micro ransomware protection

Industrial Spy data extortion market gets into the ransomware game

New ‘Cheers’ Linux ransomware targets VMware ESXi servers

SpiceJet airline passengers stranded after ransomware attack

- Jaff
- Locky
- Ransomware
- Spam
- Windows Vista
- Windows XP

Catalin Cimpanu

Catalin Cimpanu is the Security News Editor for Bleeping Computer, where he covers topics such as malware, breaches, vulnerabilities, exploits, hacking news, the Dark Web, and a few more. Catalin previously covered Web & Security news for Softpedia between May 2015 and October 2016. The easiest way to reach Catalin is via his XMPP/Jabber address at campuscodi@xmpp.is. For other contact methods, please visit Catalin's author page.

- Previous Article
- Next Article

Comments

steventaylor86 - 4 years ago

-
-

There is no stopping it. Feels really unsafe now. After recent attack of WannaCry ransomware, Semantic team said there is 2nd wave is still to come and attacks has increased drastically in past 2 years. From 2015 to 2016, the number of ransomware attacks were total 2 million and rose 17.7 % from the previous year as per gotowebsecurity - http://gotowebsecurity.com/ransomware-getting-worse/. It really dangerous to see such attacks. Most of the offices still using older version and still struggling to adopt new technology. Its really bad.

Post a Comment Community Rules

You need to login in order to post a comment

Not a member yet? Register Now

You may also like: