Locky Ransomware Virus Delivered by Actor Behind Dridex | Proofpoint US

By February 16, 2016 Proofpoint Staff

Published: 2016-02-17 · Archived: 2026-04-05 14:55:27 UTC

Locky Ransomware Overview

Proofpoint researchers have discovered a new ransomware named "Locky" being distributed via MS Word documents with malicious macros. While a variety of new ransomware has appeared since the end of 2015, Locky ransomware stands out because it is being delivered by the same actor behind many of the Dridex malware campaigns we have tracked over the last year.

Locky Spam Distribution

As with most malware campaigns this year, actors are distributing Locky ransomware through document attachments spam. In this campaign, messages from random senders with the subject "ATTN: Invoice J-12345678" deliver an attachment "invoice_J-12345678.doc". The attachments are MS Word documents containing macros which download and install the Locky ransomware, first observed by Proofpoint on February 16, 2016.

The botnet (a group of infected machines running a spam bot) delivering the spam is the same botnet that distributes the vast majority of messages bearing the Dridex banking Trojan. In the past, this botnet delivered Dridex botnet IDs 120, 122, 123, 220, 223, 301 (among others), as well as some other non-Dridex malware such as Ursnif (for example on 1-5-2016), Nymaim (12-15-2015), TeslaCrypt (12-14-2015), and Shifu (10-07-2015).

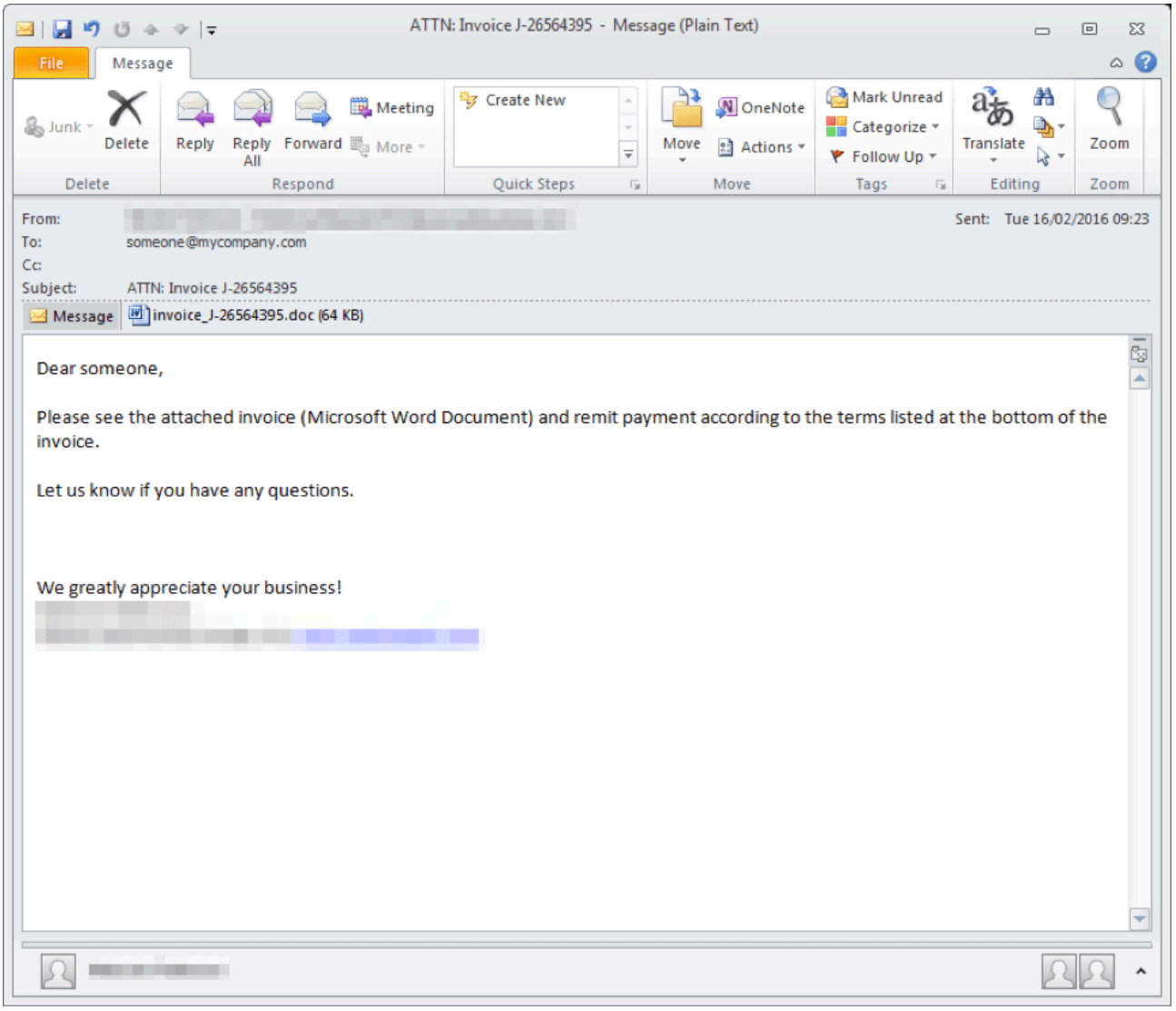

Figure 1 : Email lure associated with Locky

The actors behind the Locky ransomware attack are clearly taking a cue from the Dridex playbook in terms of distribution. Just as Dridex has been pushing the limits of campaign sizes, now we're seeing even higher volumes with Locky, rivaling the largest Dridex campaigns we have observed to date.

Coincidentally, the same day we tracked the large spam campaign, we also spotted Locky ransomware being distributed in a Neutrino thread usually spreading Necurs. When run on the same virtual machine, the document from both the Neutrino drop and the spam emails generate the same individual ID, point to the same Bitcoin wallet, and appear to use the same infrastructure. This can be explained either by a common actor or, more likely, by a distribution in affiliate mode.

#	Result	IP	Protocol	Req...	Host	URL	Body	Content-Type	Comments
5	200	92. .204	HTTP	GET	sid.nussvital.com.ar	/js/script.js	159	text/javascript	
13	200	89. .118	HTTP	GET	wg .gshout.top	/brain/d2NzbGVhYnlxZA	708	text/html	Neutrino : Landing
14	200	89. .118	HTTP	GET	wg .gshout.top	/tense/dGZ4Z3dkaGNh.swf	98 318	application/x-shockwave-flash	Neutrino : Flash Bundle
15	200	89. .118	HTTP	GET	wg .gshout.top	/flush/lamp-animal-unicorn-14180807	31	text/html	Neutrino
18	200	89. .118	HTTP	GET	wg .gshout.top	/maid/YWFiaWpidWRyZg	101 938	application/octet-stream	Neutrino : dropping Locky
19	200	86. .144	HTTP	POST	86. .144	/main.php	292	text/html; charset=UTF-8	Locky calling Home
20	200	86. .144	HTTP	POST	86. .144	/main.php	1 149	text/html; charset=UTF-8	Locky calling Home

Figure 2 : Locky being dropped by the Neutrino EK

When users open the attached document, they must enable macros to be infected.

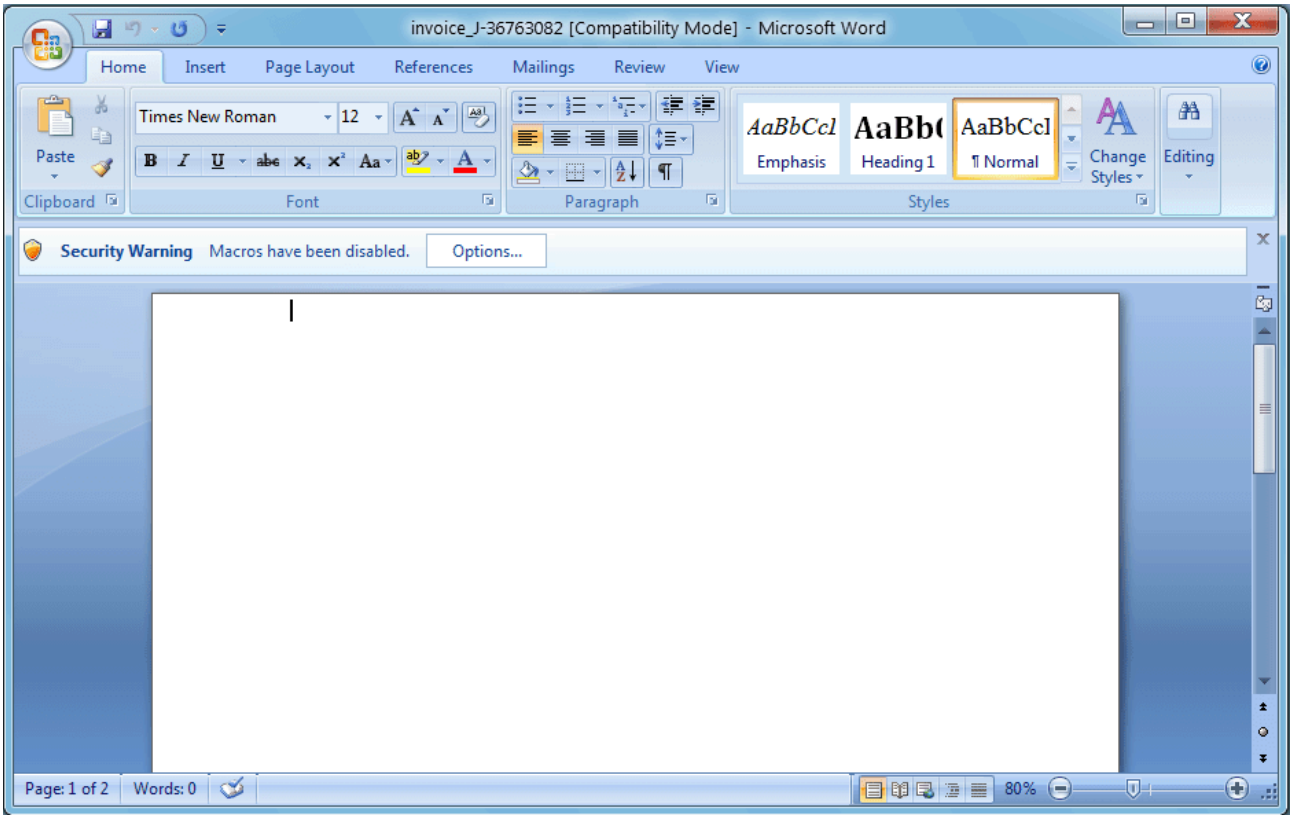

Figure 3: Attachment showing macro enabling

Locky Ransomware

The ransomware encrypts files based on their extension and uses notepad to display the ransom message (Figure 5). Additionally, it replaces the Desktop background with the ransom message (Figure 4). If the user visits the .onion (or tor2web) links specified in the ransom message, s/he is instructed to buy Bitcoins, send them to a certain Bitcoin address, and then refresh the page to wait for the decryptor download. We have not confirmed if the decryptor will actually be provided if the user pays.

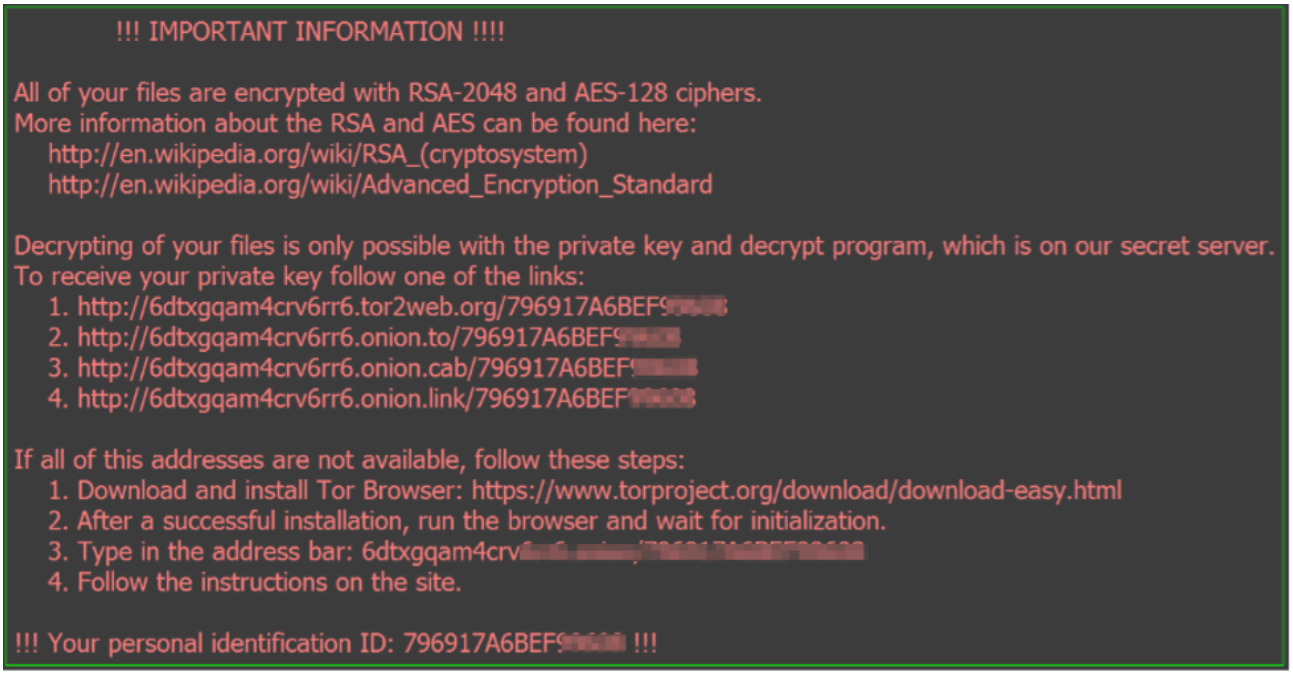

Figure 4: Desktop background after Locky is installed

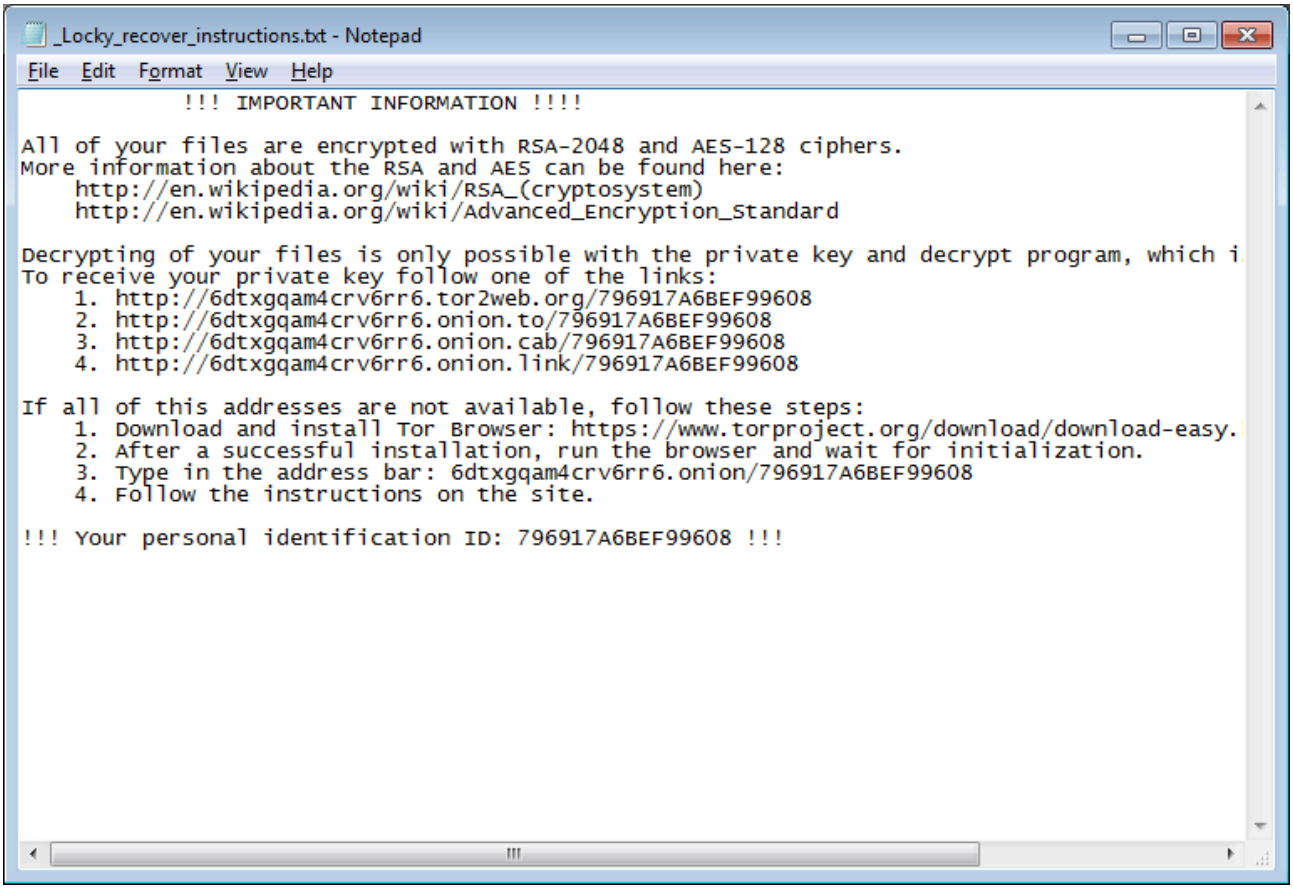

Figure 5: Ransom message displayed in notepad

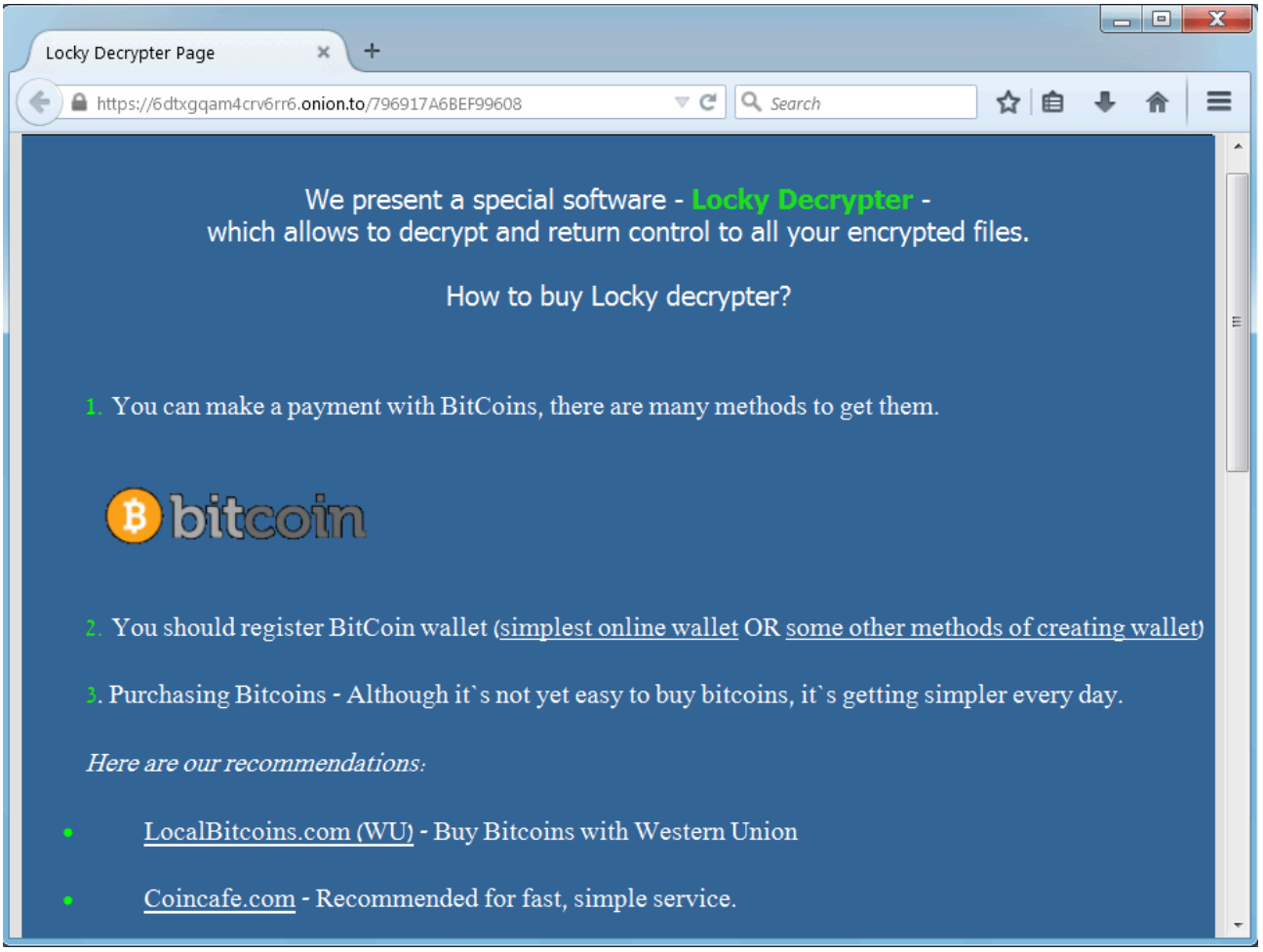

Figure 6: Decryption website

Locky ransomware encrypts most of the useful file formats on the user's local disk drives; some reports are emerging that Locky also encrypts files on mapped shared drives. The affected file formats are listed below:

.m4u | .m3u | .mid | .wma | .flv | .3g2 | .mkv | .3gp | .mp4 | .mov | .avi | .asf | .mpeg | .vob | .mpg | .wmv | .fla | .swf | .wav | .mp3 | .qcow2 | .vdi | .vmdk | .vmx | .gpg | .aes | .ARC | .PAQ | .tar.bz2 | .tbk | .bak | .tar | .tgz | .gz | .7z | .rar | .zip | .djv | .djvu | .svg | .bmp | .png | .gif | .raw | .cgm | .jpeg | .jpg | .tif | .tiff | .NEF | .psd | .cmd | .bat | .sh | .class | .jar | .java | .rb | .asp | .cs | .brd | .sch | .dch | .dip | .pl | .vbs | .vb | .js | .asm | .pas | .cpp | .php | .ldf | .mdf | .ibd | .MYI | .MYD | .frm | .odb | .dbf | .db | .mdb | .sql | .SQLITEDB | .SQLITE3 | .asc | .lay6 | .lay | .ms11 (Security copy) | .ms11 | .sldm | .sldx | .ppsm | .ppsx | .ppam | .docb | .mml | .sxm | .otg | .odg | .uop | .potx | .potm | .pptx | .pptm | .std | .sxd | .pot | .pps | .sti | .sxi | .otp | .odp | .wb2 | .123 | .wks | .wk1 | .xltx | .xltm | .xlsx | .xlsm | .xlsb | .slk | .xlw | .xlt | .xlm | .xlc | .dif | .stc | .sxc | .ots | .ods | .hwp | .602 | .dotm | .dotx | .docm | .docx | .DOT | .3dm | .max | .3ds | .xml | .txt | .CSV | .uot | .RTF | .pdf | .XLS | .PPT | .stw | .sxw | .ott | .odt | .DOC | .pem | .p12 | .csr | .crt | .key

Locky also appears to generate DGA traffic for command and control (the list of domains below were unregistered at the time of investigation):

vkrdbsrqpi[.]de
jaomjlyvwxgdt[.]fr

wpogw[.]it
ofhhoowfmnuihyd[.]ru

We detected several filesystem IOCs (files, registry keys used for persistence, etc):

Registry: HKCU\Software\Microsoft\Windows\CurrentVersion\Run\Locky
Registry: HKCU\Software\Locky\id
Registry: HKCU\Software\Locky\pubkey
Registry: HKCU\Software\Locky\paytext
File: C:\Users\(username)\AppData\Local\Temp\ladybi.exe
File: C:\Users\(username)\Documents_Locky_recover_instructions.txt
Command: vssadmin.exe Delete Shadows /All /Quiet
Command: "C:\Windows\system32\NOTEPAD.EXE" C:\Users\Admin\Desktop_Locky_recover_instructions.txt

As both endpoint and network protection measures become increasingly capable of handling the ransomware that made headlines in the last couple of years (CryptoLocker, CryptoWall, etc.), new variants and strains will continue to emerge. Check back later this week for a complete rundown of several new ransomwares that are making the rounds in the wild.

Locky Malware IOCs

Sample hashes
e95cde1e6fa2ce300bf778f3e9f17dfc6a3e499cb0081070ef5d3d15507f367b (Neutrino EK)
5466fb6309bfe0bbbb109af3ccfa0c67305c3464b0fdffcec6eda7fcb774757e (attachment)

Filesystem IOCs (files, registry keys used for persistence, etc):
Registry: HKCU\Software\Microsoft\Windows\CurrentVersion\Run\Locky
Registry: HKCU\Software\Locky\id
Registry: HKCU\Software\Locky\pubkey
Registry: HKCU\Software\Locky\paytext
File: C:\Users\(username)\AppData\Local\Temp\ladybi.exe
File: C:\Users\(username)\Documents_Locky_recover_instructions.txt
Command: vssadmin.exe Delete Shadows /All /Quiet
Command: "C:\Windows\system32\NOTEPAD.EXE" C:\Users\Admin\Desktop_Locky_recover_instructions.txt

Payloads downloaded by macro:
[hxxp://www.iglobali[.]com/34gf5y/r34f3345g.exe]
[hxxp://www.southlife[.]church/34gf5y/r34f3345g.exe]
[hxxp://www.villaggio.airwave[.]at/34gf5y/r34f3345g.exe]
[hxxp://www.jesusdenazaret[.]com.ve/34gf5y/r34f3345g.exe]
[hxxp://66.133.129[.]5/~chuckgilbert/09u8h76f/65fg67n]
[hxxp://173.214.183[.]81/~tomorrowhope/09u8h76f/65fg67n]
[hxxp://iynus[.]net/~test/09u8h76f/65fg67n]

Locky C2:

[hxxp://109.234.38[.]35/main.php]

[hxxp://lneqqkvxxogomu[.]eu/main.php]

[hxxp://qpdar[.]pw/main.php]

[hxxp://ydbayd[.]de/main.php]

[hxxp://ssojravpf[.]be/main.php]

[hxxp://gioaqjklhoxf[.]eu/main.php]

[hxxp://txlmnqnunppnpuq[.]ru/main.php]

Payment URIs (Locky asks user to click these links):

[hxxp://6dtxgqam4crv6rr6.tor2web[.]org]

[hxxp://6dtxgqam4crv6rr6.onion[.]to]

[hxxp://6dtxgqam4crv6rr6.onion[.]cab]

[hxxp://6dtxgqam4crv6rr6.onion[.]link]

[hxxps://6dtxgqam4crv6rr6[.]onion]
