Lilocked Ransomware Actively Targeting Servers and Web Sites

bleepingcomputer.com/news/security/lilocked-ransomware-actively-targeting-servers-and-web-sites/

Lawrence Abrams

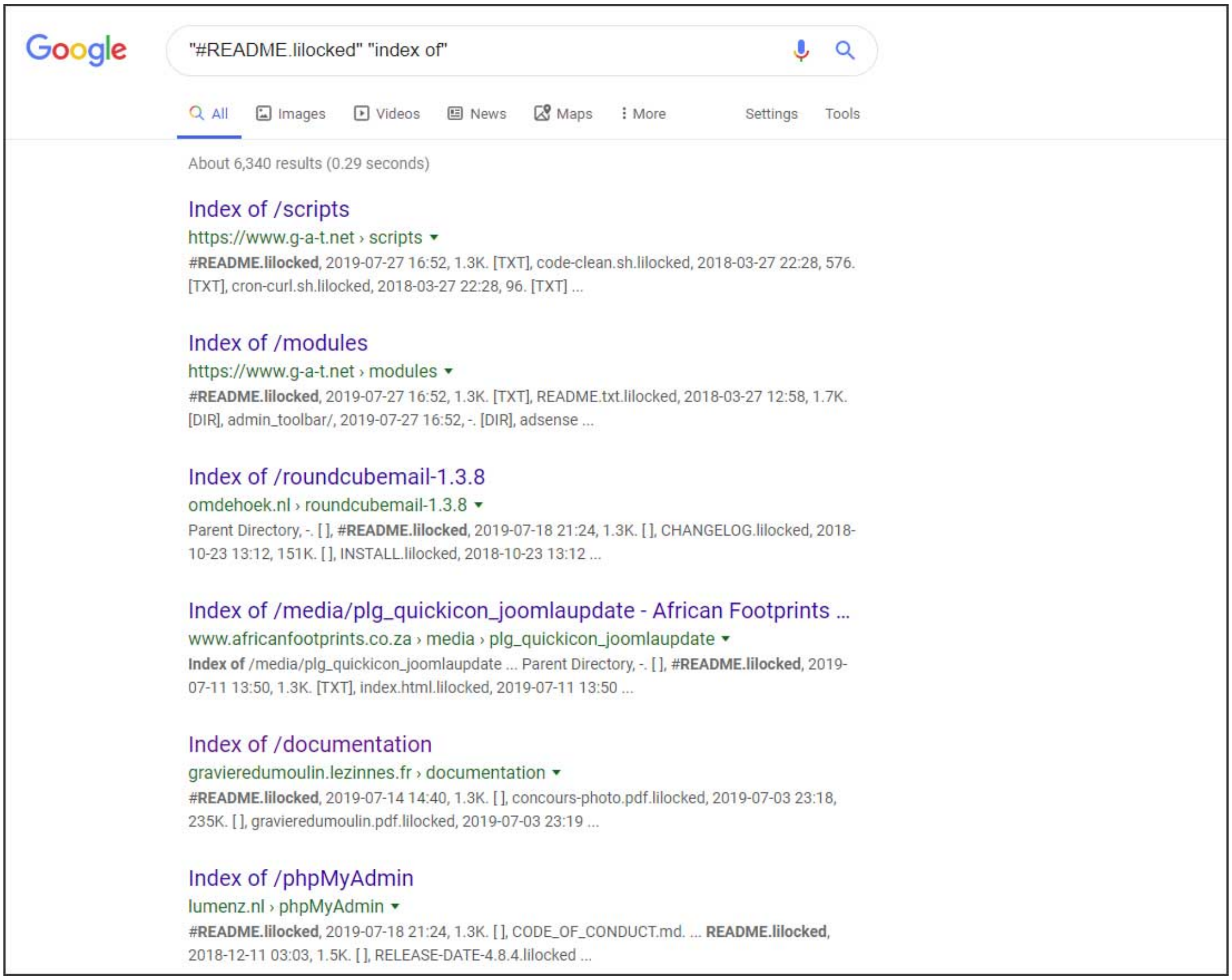
By
Lawrence Abrams

- September 6, 2019
- 10:19 AM
- 0

A relatively new ransomware named Lilocked by researchers and Lilu by the developers is actively targeting servers and encrypting the data located on them. All of the known infected servers are web sites, which is causing the encrypted files to show up in Google search results.

We first reported about Lilu in our The Week in Ransomware article on July 26th, 2019 when Michael Gillespie saw a sample uploaded to his ID Ransomware service. It was spotted again yesterday by security researcher Benkow who tweeted about it.

Google reports over 6,000 search results with web servers that have been encrypted by this ransomware and having their files renamed with a .lilocked extension. It should be noted that many of these results are for the same web sites.



"#README.lilocked" "index of"

About 6,340 results (0.29 seconds)

Index of /scripts
https://www.g-a-t.net › scripts ▾
#README.lilocked, 2019-07-27 16:52, 1.3K. [TXT], code-clean.sh.lilocked, 2018-03-27 22:28, 576. [TXT], cron-curl.sh.lilocked, 2018-03-27 22:28, 96. [TXT] ...

Index of /modules
https://www.g-a-t.net › modules ▾
#README.lilocked, 2019-07-27 16:52, 1.3K. [TXT], README.txt.lilocked, 2018-03-27 12:58, 1.7K. [DIR], admin_toolbar/, 2019-07-27 16:52, -. [DIR], adsense ...

Index of /roundcubemail-1.3.8
omdehoek.nl › roundcubemail-1.3.8 ▾
Parent Directory, -. [ ], **#README.lilocked**, 2019-07-18 21:24, 1.3K. [ ], CHANGELOG.lilocked, 2018-10-23 13:12, 151K. [ ], INSTALL.lilocked, 2018-10-23 13:12 ...

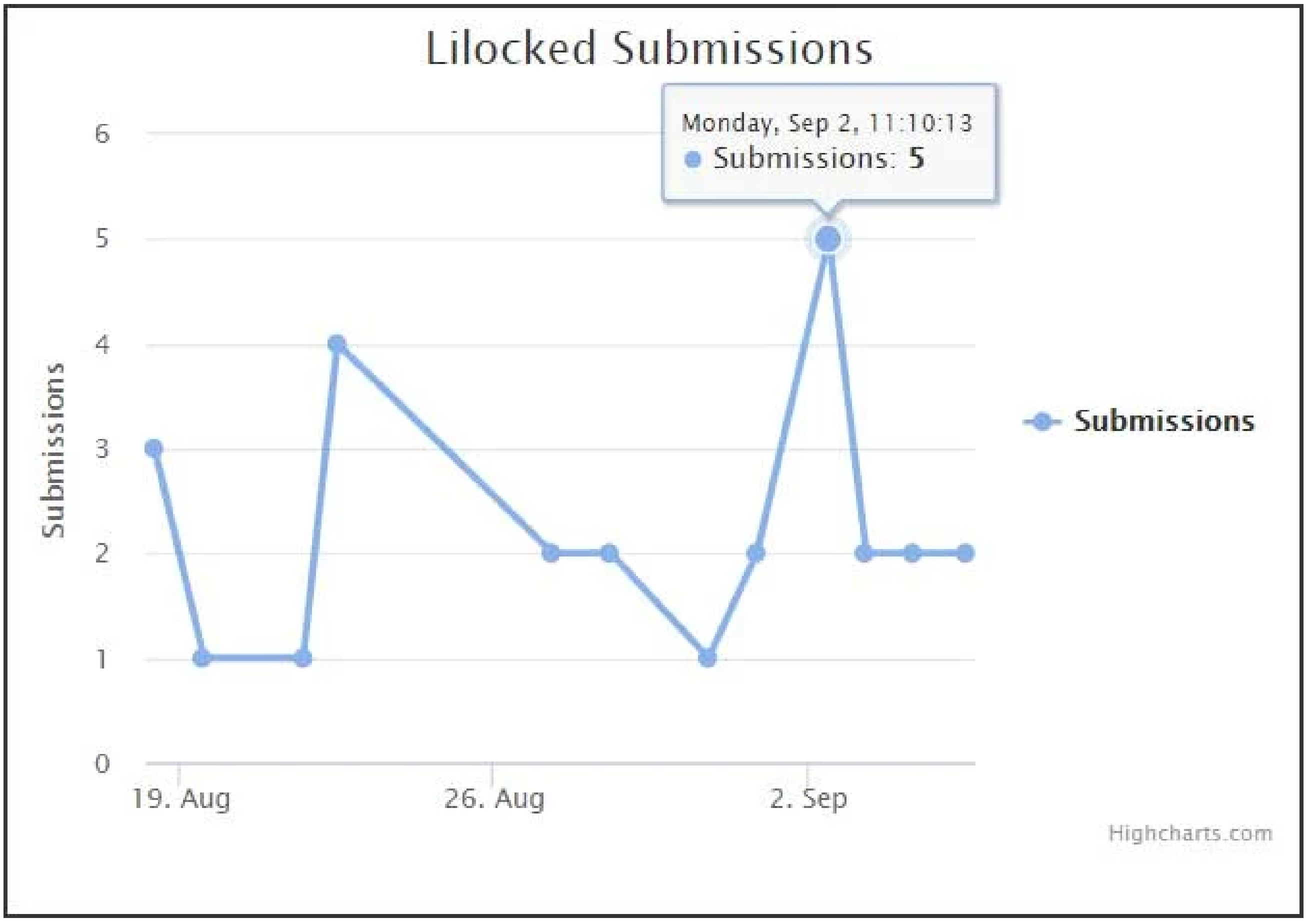
Index of /media/plg_quickicon_joomlaupdate - African Footprints ...
www.africanfootprints.co.za › media › plg_quickicon_joomlaupdate ▾
Index of /media/plg_quickicon_joomlaupdate ... Parent Directory, -. [ ], **#README.lilocked**, 2019-07-11 13:50, 1.3K. [TXT], index.html.lilocked, 2019-07-11 13:50 ...

Index of /documentation
gravieredumoulin.lezinnes.fr › documentation ▾
#README.lilocked, 2019-07-14 14:40, 1.3K. [ ], concours-photo.pdf.lilocked, 2019-07-03 23:18, 235K. [ ], gravieredumoulin.pdf.lilocked, 2019-07-03 23:19 ...

Index of /phpMyAdmin
lumenz.nl › phpMyAdmin ▾
#README.lilocked, 2019-07-18 21:24, 1.3K. [ ], CODE_OF_CONDUCT.md. ... **README.lilocked**, 2018-12-11 03:03, 1.5K. [ ], RELEASE-DATE-4.8.4.lilocked ...

Google search results showing infected servers

Furthermore, submissions stats from ID Ransomware show that this infection has a low volume, but steady, amount of submissions ot the ransomware identification service.

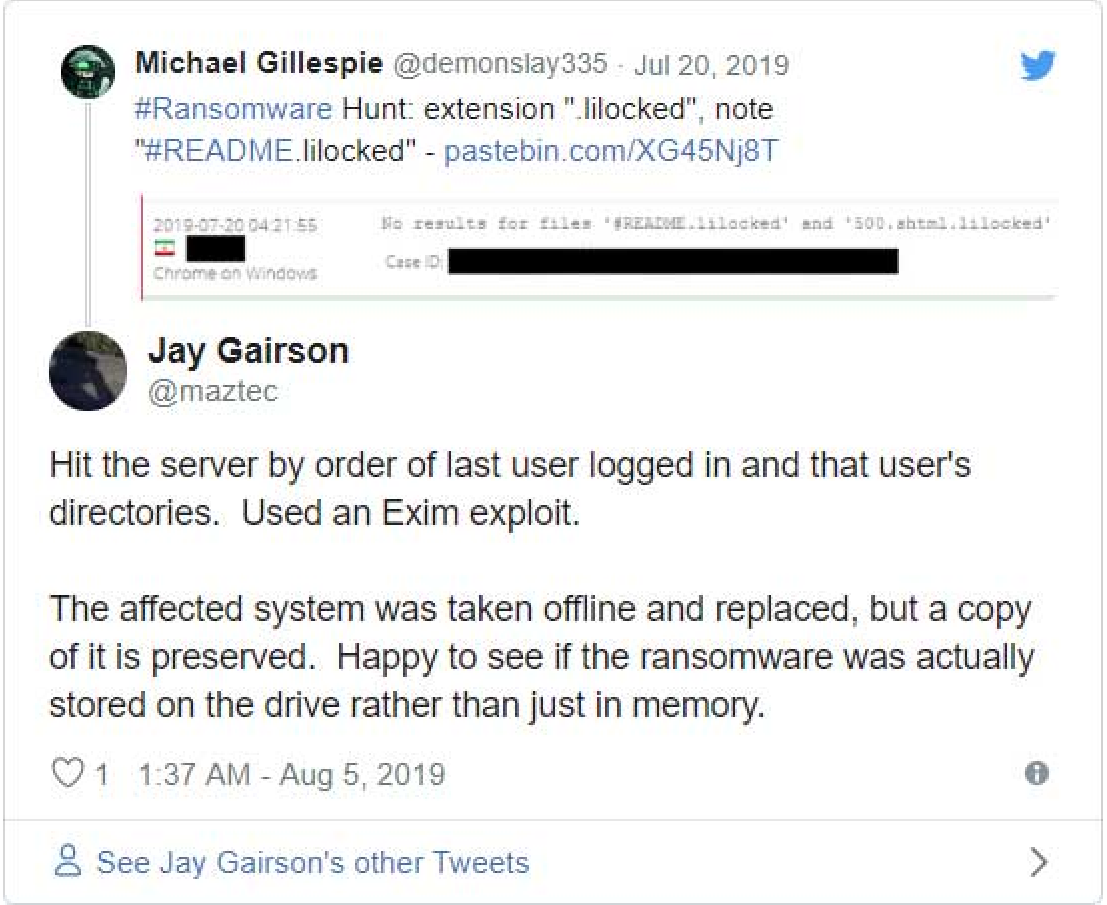


ID Ransomware submission stats

It is not known if Lilu is specifically targeting web servers, but most of the submitted files seen by BleepingComputer are related to web sites. When reviewing the submitted files, there does not seem to be a pattern such as WordPress, Magento, or other commonly hacked CMS sites.

Attackers possibly using exploits to gain access

In response to Gillespie's tweet, one user reported that the attacker gained access to their web server using an Exim exploit. Gillespie further told BleepingComputer that another victim felt that they were infected through an outdated WordPress installation.



Michael Gillespie @demonslay335 · Jul 20, 2019

#Ransomware Hunt: extension ".lilocked", note "#README.lilocked" - pastebin.com/XG45Nj8T

2019-07-20 04:21:55
[redacted]
Chrome on Windows

No results for files '#README.lilocked' and '500.shtml.lilocked'

Case ID: [redacted]

Jay Gairson
@maztec

Hit the server by order of last user logged in and that user's directories. Used an Exim exploit.

The affected system was taken offline and replaced, but a copy of it is preserved. Happy to see if the ransomware was actually stored on the drive rather than just in memory.

♡ 1 1:37 AM - Aug 5, 2019

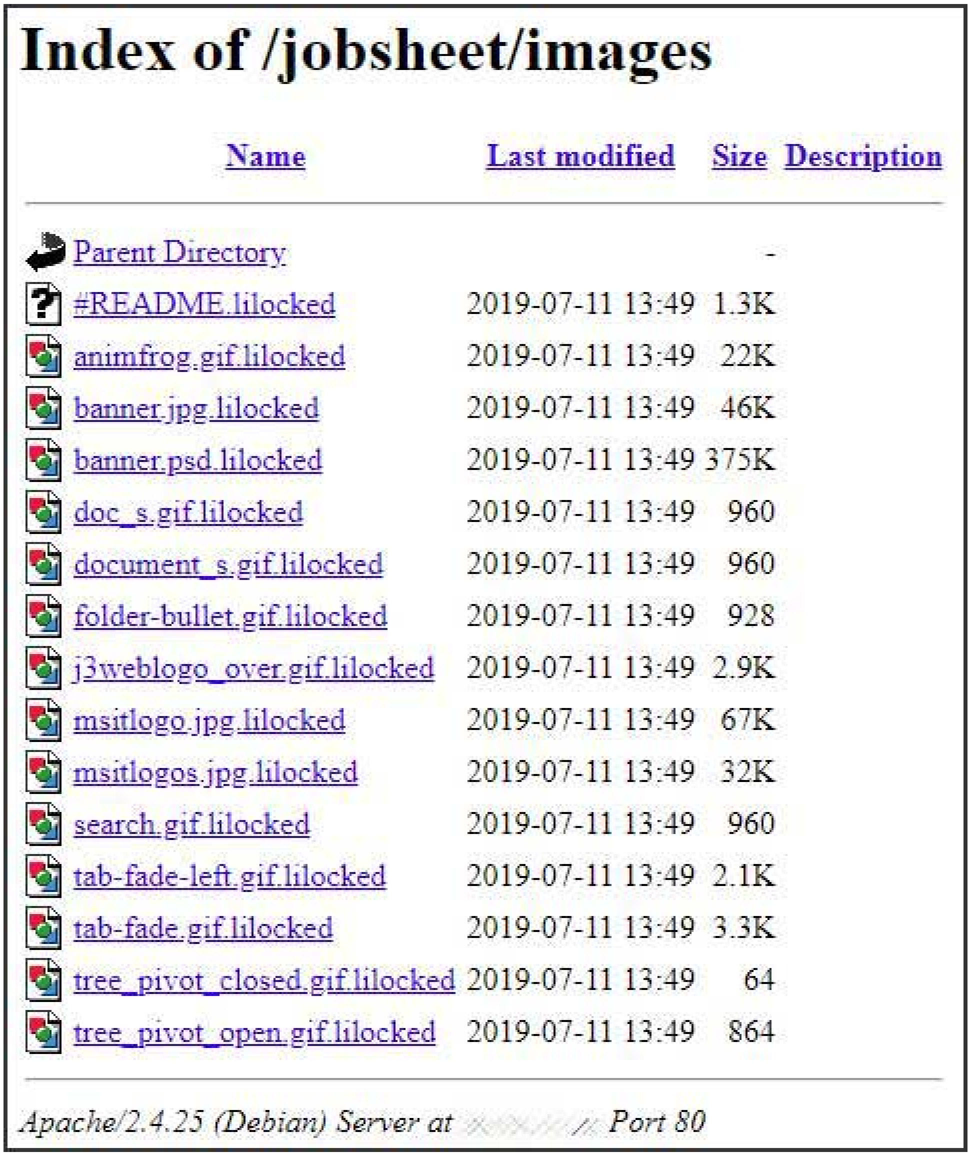
BleepingComputer has not been able to independently confirm if the attacker is using exploits to hack into the sites.

What's known about the Lilocked encryption process

Unfortunately, a sample has never been found for the Lilocked, or Lilu, Ransomware, so not much is known about it other than what we can see in the wild.

When a machine is infected, the ransomware will encrypt a file and then append the **.lilocked** extension to the file name. For example, apple-icon.png would be encrypted and renamed to apple-icon.png.lilocked.

For each folder that is encrypted, Lilocked will also drop a ransom note named **#README.lilocked**.



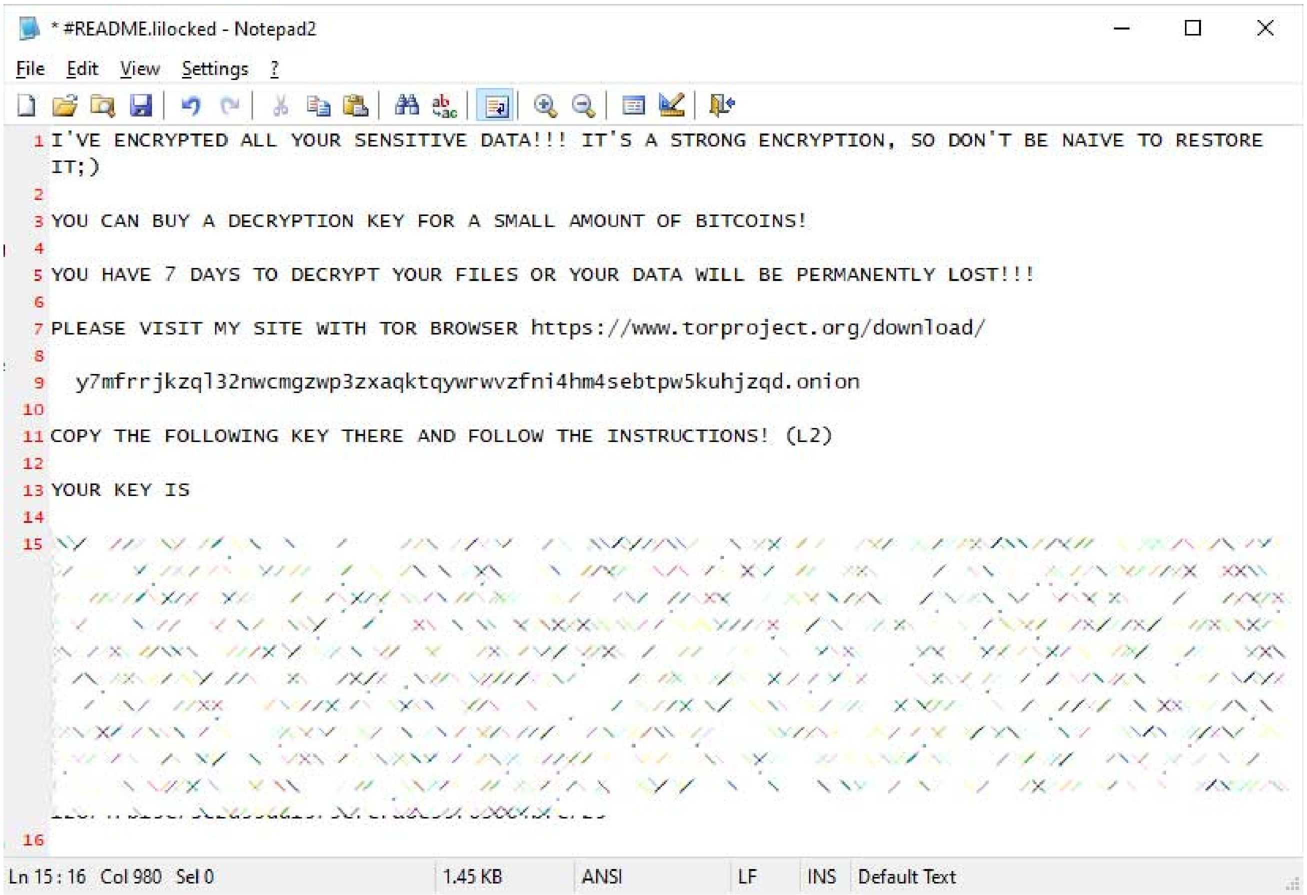
Index of /jobsheet/images

Name	Last modified	Size	Description
Parent Directory		-	
#README.lilocked	2019-07-11 13:49	1.3K	
animfrog.gif.lilocked	2019-07-11 13:49	22K	
banner.jpg.lilocked	2019-07-11 13:49	46K	
banner.psd.lilocked	2019-07-11 13:49	375K	
doc_s.gif.lilocked	2019-07-11 13:49	960	
document_s.gif.lilocked	2019-07-11 13:49	960	
folder-bullet.gif.lilocked	2019-07-11 13:49	928	
j3weblogo_over.gif.lilocked	2019-07-11 13:49	2.9K	
msitlogo.jpg.lilocked	2019-07-11 13:49	67K	
msitlogos.jpg.lilocked	2019-07-11 13:49	32K	
search.gif.lilocked	2019-07-11 13:49	960	
tab-fade-left.gif.lilocked	2019-07-11 13:49	2.1K	
tab-fade.gif.lilocked	2019-07-11 13:49	3.3K	
tree_pivot_closed.gif.lilocked	2019-07-11 13:49	64	
tree_pivot_open.gif.lilocked	2019-07-11 13:49	864	

Apache/2.4.25 (Debian) Server at [redacted] Port 80

Encrypted server in search results

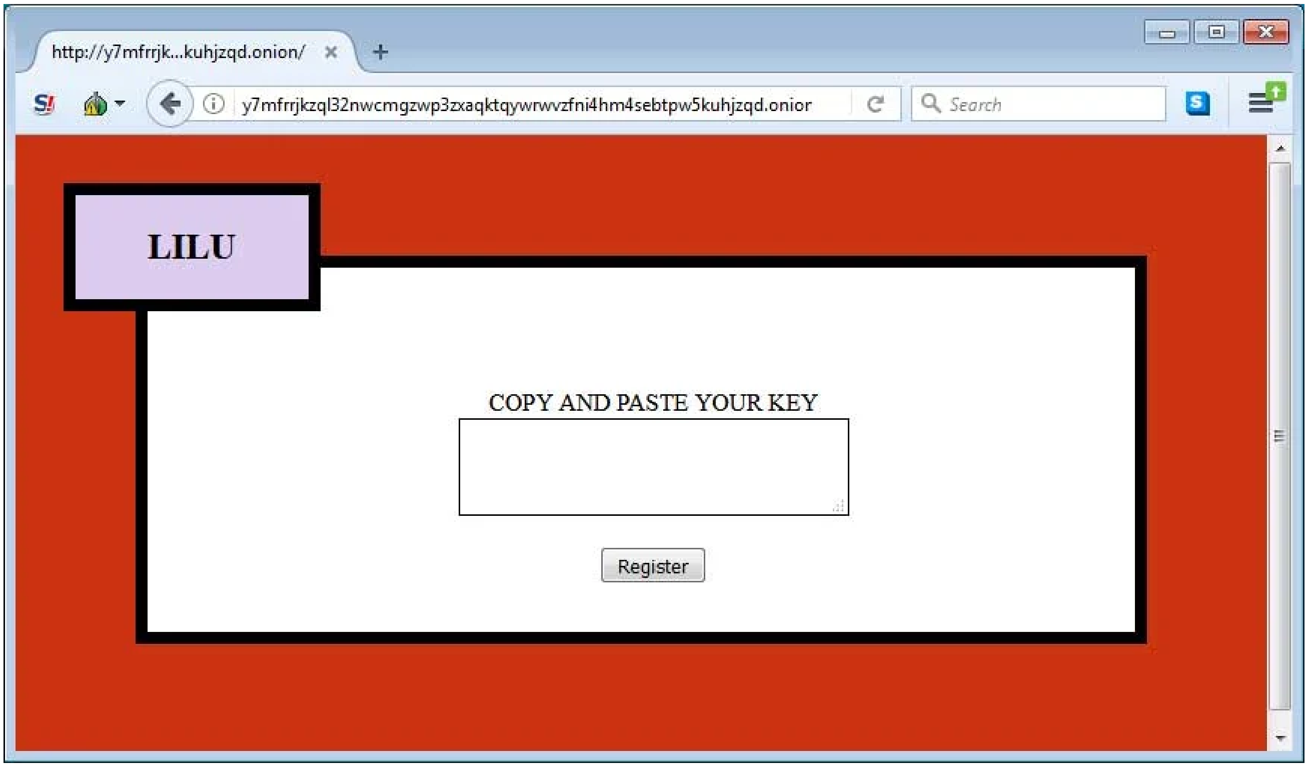
The #README.lilocked ransom note tells the victim that their data has been encrypted and that they must go to the attacker's Tor payment site in order to pay a ransom. This ransom note includes a key that is needed to login to the payment site.



```
I'VE ENCRYPTED ALL YOUR SENSITIVE DATA!!! IT'S A STRONG ENCRYPTION, SO DON'T BE NAIVE TO RESTORE
IT;)

YOU CAN BUY A DECRYPTION KEY FOR A SMALL AMOUNT OF BITCOINS!

YOU HAVE 7 DAYS TO DECRYPT YOUR FILES OR YOUR DATA WILL BE PERMANENTLY LOST!!!

PLEASE VISIT MY SITE WITH TOR BROWSER https://www.torproject.org/download/

  y7mfrrjkzql32nwcmgzwp3zxaqktqywrwvzfni4hm4sebtpw5kuhjzqd.onion

COPY THE FOLLOWING KEY THERE AND FOLLOW THE INSTRUCTIONS! (L2)

YOUR KEY IS

[redacted]

```

Lilu ransom note

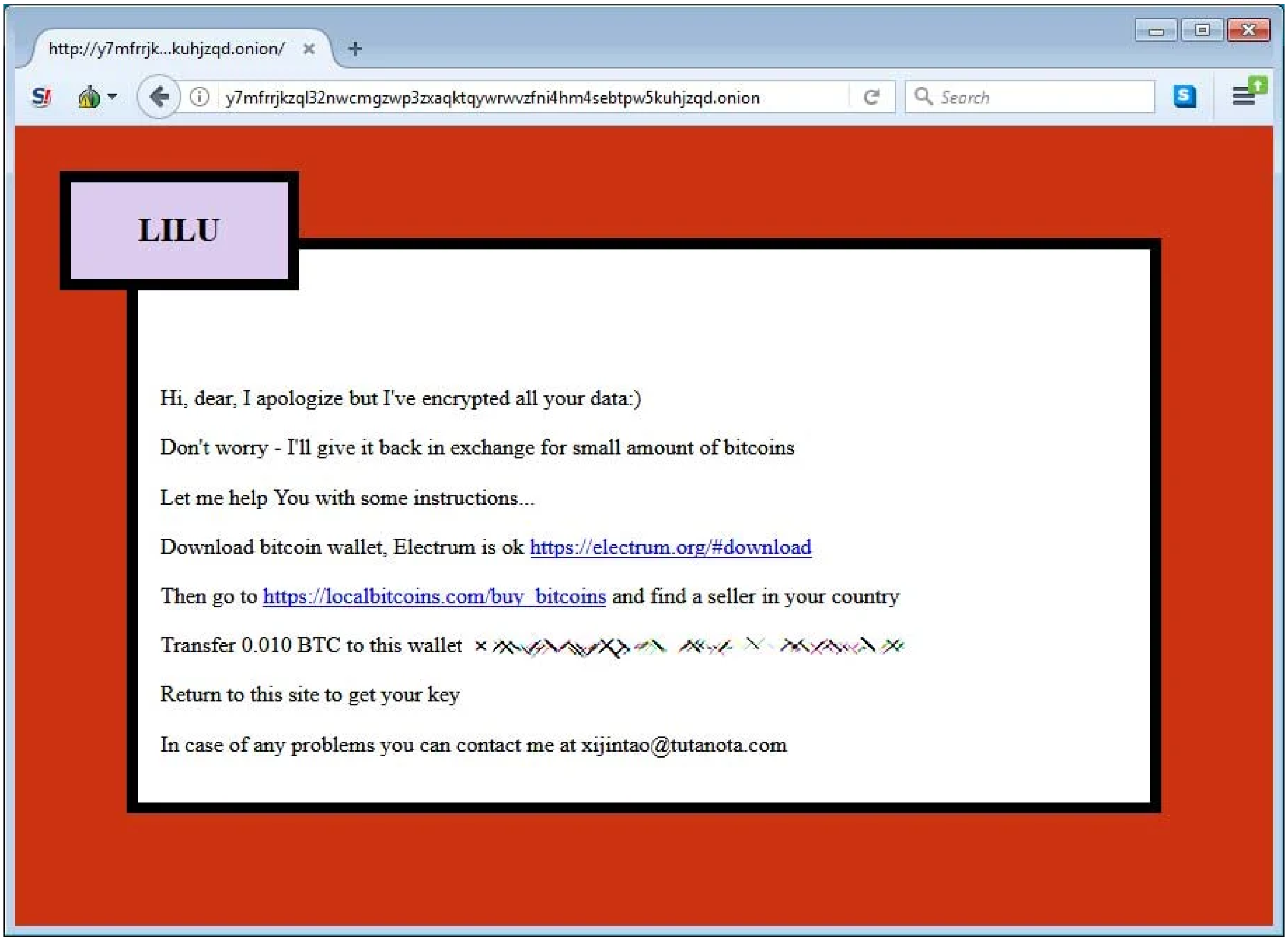
If a victim goes to the site, they will be presented with a page asking them to enter their key.



http://y7mfrrjk...kuhjzqd.onion/
y7mfrrjkzql32nwcmgzwp3zxaqktqywrwvzfni4hm4sebtpw5kuhjzqd.onior
Search
LILU
COPY AND PASTE YOUR KEY
Register

Lilu Tor payment site login

Once the key is entered, they will be shown a page with instructions on how to pay the ransom. These instructions include a bitcoin address and ransom amount, which is 0.010 BTC or approximately $100 USD from the ransom demands seen by BleepingComputer.


http://y7mfrrjk...kuhjzqd.onion/
y7mfrrjkzql32nwcmgzwp3zxaqktqywrwvzfni4hm4sebtpw5kuhjzqd.onion
Search
LILU

Hi, dear, I apologize but I've encrypted all your data:)

Don't worry - I'll give it back in exchange for small amount of bitcoins

Let me help You with some instructions...

Download bitcoin wallet, Electrum is ok https://electrum.org/#download

Then go to https://localbitcoins.com/buy_bitcoins and find a seller in your country

Transfer 0.010 BTC to this wallet [redacted]

Return to this site to get your key

In case of any problems you can contact me at xijintao@tutanota.com

Lilu payment instructions

At this time, there is no known way to decrypt files encrypted by Lilu, but if a sample is discovered that may change.

BleepingComputer has also reached out to the contact email listed on the Tor site with questions, but had not heard back at the time of this publication.

IOCs:

Associated Files:

```
#README.lilocked
```

Associated email:

```
xijintao@tutanota.com
```

Tor Payment Site:

```
y7mfrrjkzql32nwcmgzwp3zxaqktqywrwvzfni4hm4sebtpw5kuhjzqd.onion
```

Ransom Note Text:

```
I'VE ENCRYPTED ALL YOUR SENSITIVE DATA!!! IT'S A STRONG ENCRYPTION, SO DON'T BE
NAIVE TO RESTORE IT;)

YOU CAN BUY A DECRYPTION KEY FOR A SMALL AMOUNT OF BITCOINS!

YOU HAVE 7 DAYS TO DECRYPT YOUR FILES OR YOUR DATA WILL BE PERMANENTLY LOST!!!

PLEASE VISIT MY SITE WITH TOR BROWSER https://www.torproject.org/download/

        y7mfrrjkzql32nwcmgzwp3zxaqktqywrwvzfni4hm4sebtpw5kuhjzqd.onion

COPY THE FOLLOWING KEY THERE AND FOLLOW THE INSTRUCTIONS! (L2)

YOUR KEY IS

[key]
```

- Lilocked
- Lilu
- Ransomware

Lawrence Abrams

Lawrence Abrams is the owner and Editor in Chief of BleepingComputer.com. Lawrence's area of expertise includes Windows, malware removal, and computer forensics. Lawrence Abrams is a co-author of the Winternals Defragmentation, Recovery, and Administration Field Guide and the technical editor for Rootkits for Dummies.

- Previous Article
- Next Article

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: