

## Lilocked Ransomware Actively Targeting Servers and Web Sites

By Lawrence Abrams

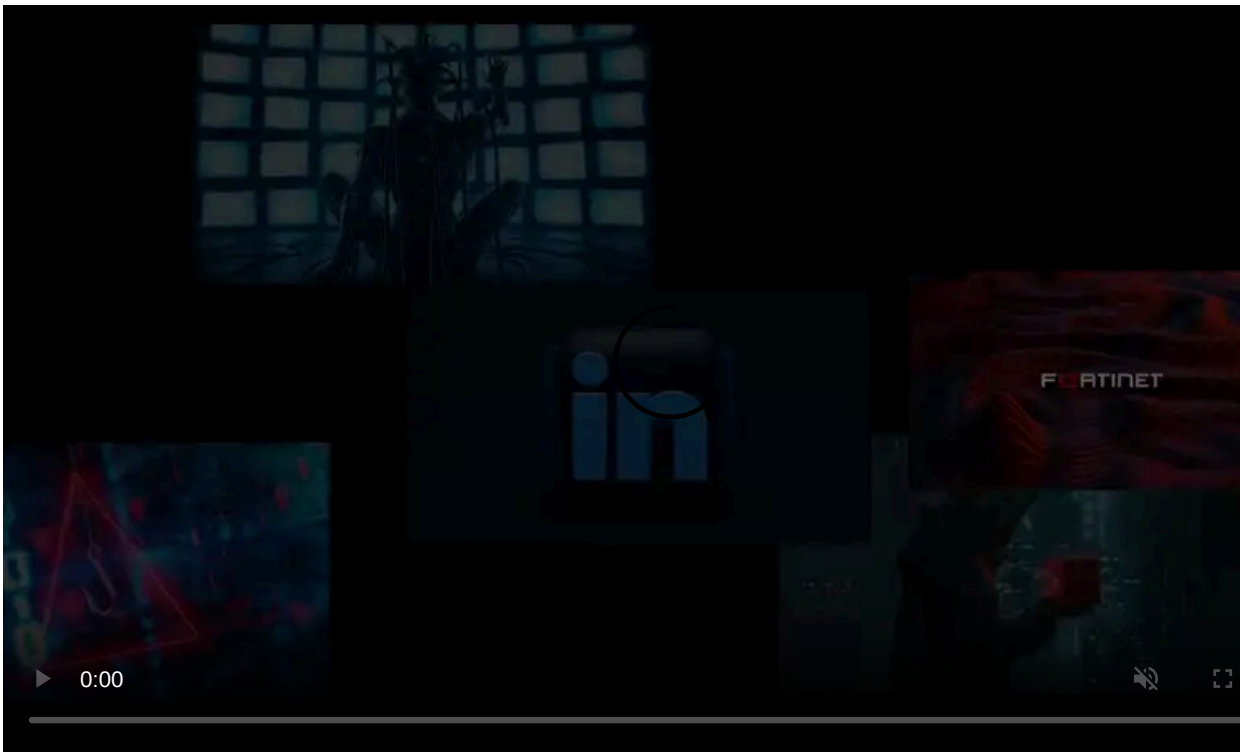
Published: 2019-09-06 · Archived: 2026-04-05 20:04:01 UTC



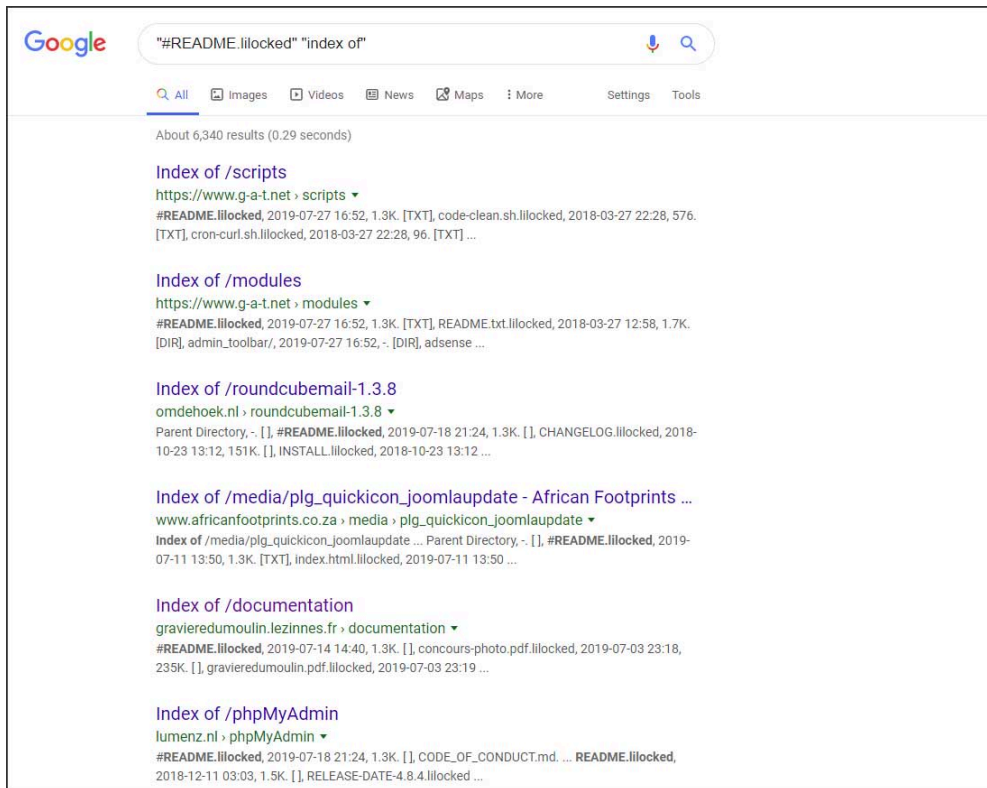
A relatively new ransomware named Lilocked by researchers and Lilu by the developers is actively targeting servers and encrypting the data located on them. All of the known infected servers are web sites, which is causing the encrypted files to show up in Google search results.

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.

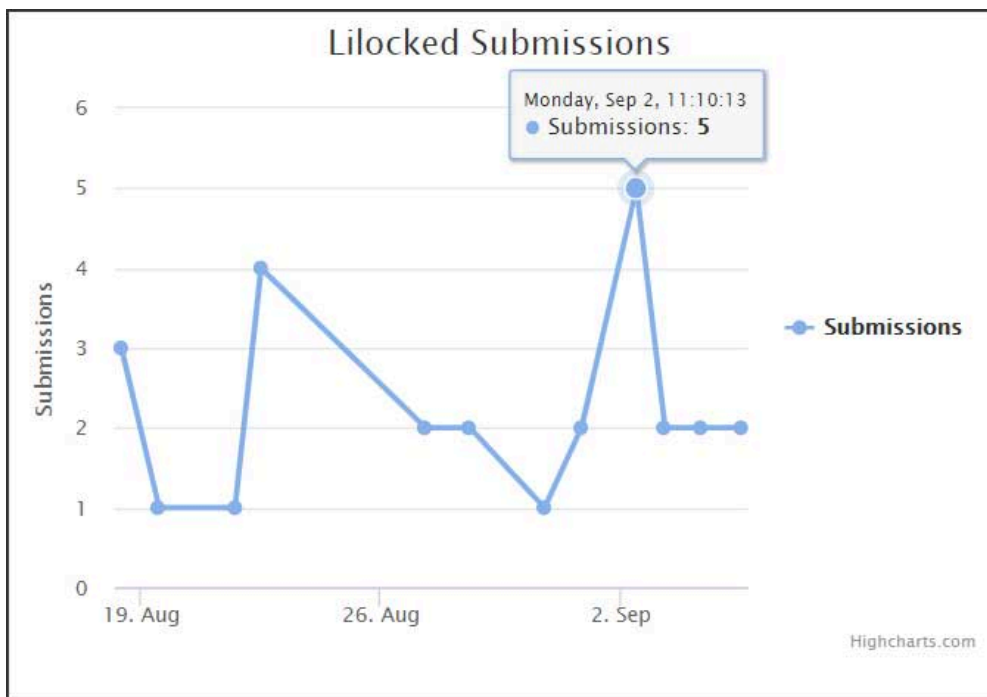


Visit Advertiser website [GO TO PAGE](#)



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 of the ransomware identification service.



ID Ransomware submission stats

It is not known if Lilo 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 Gillespie further told BleepingComputer that another victim felt that they were infected through an outdated WordPress installation.



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**.

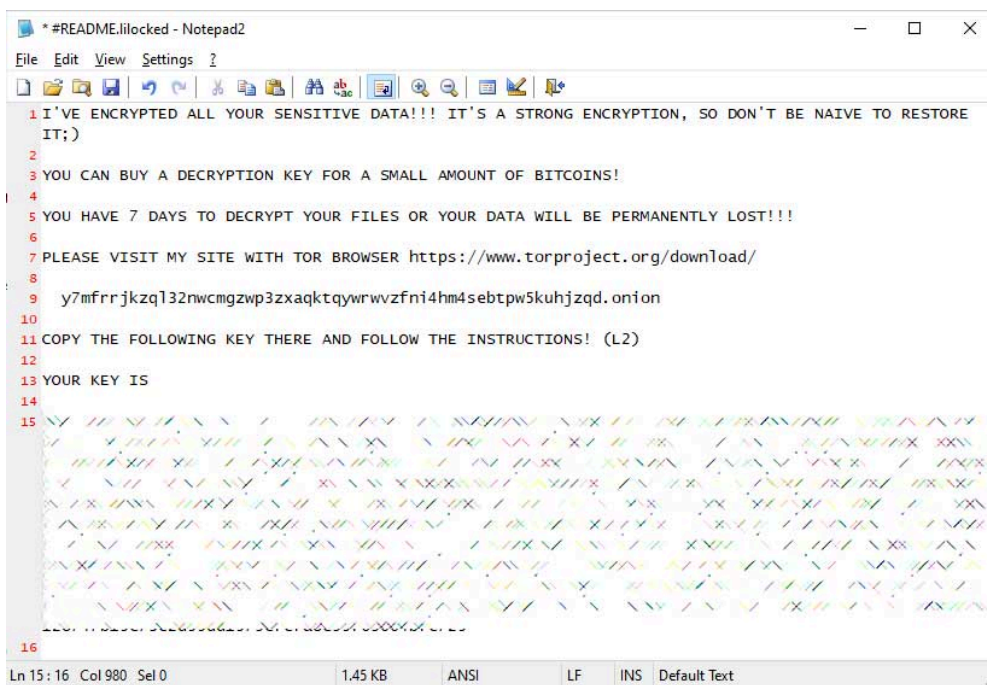
## Index of /jobsheet/images

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

Apache/2.4.25 (Debian) Server at // // Port 80

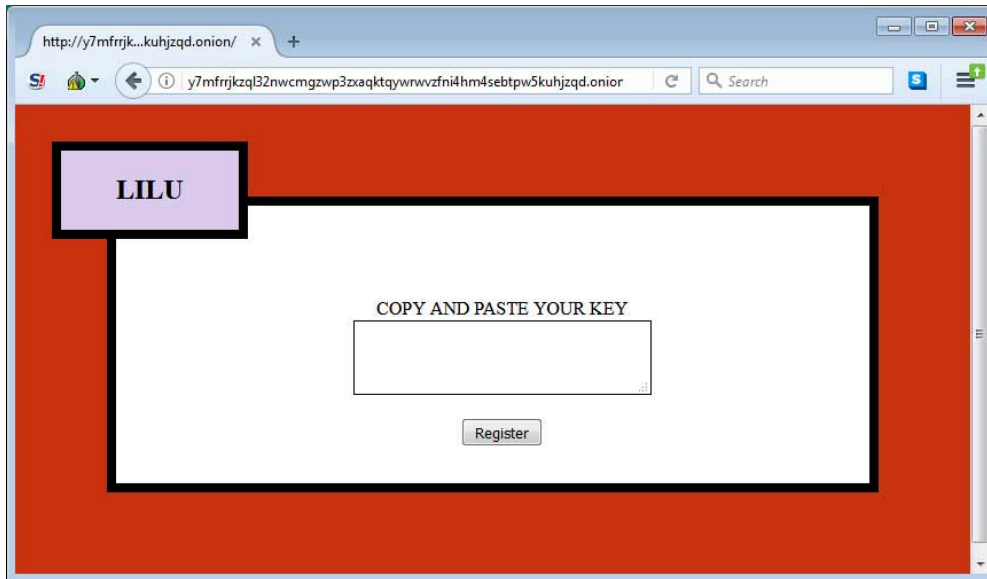
### Encrypted server in search results

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.



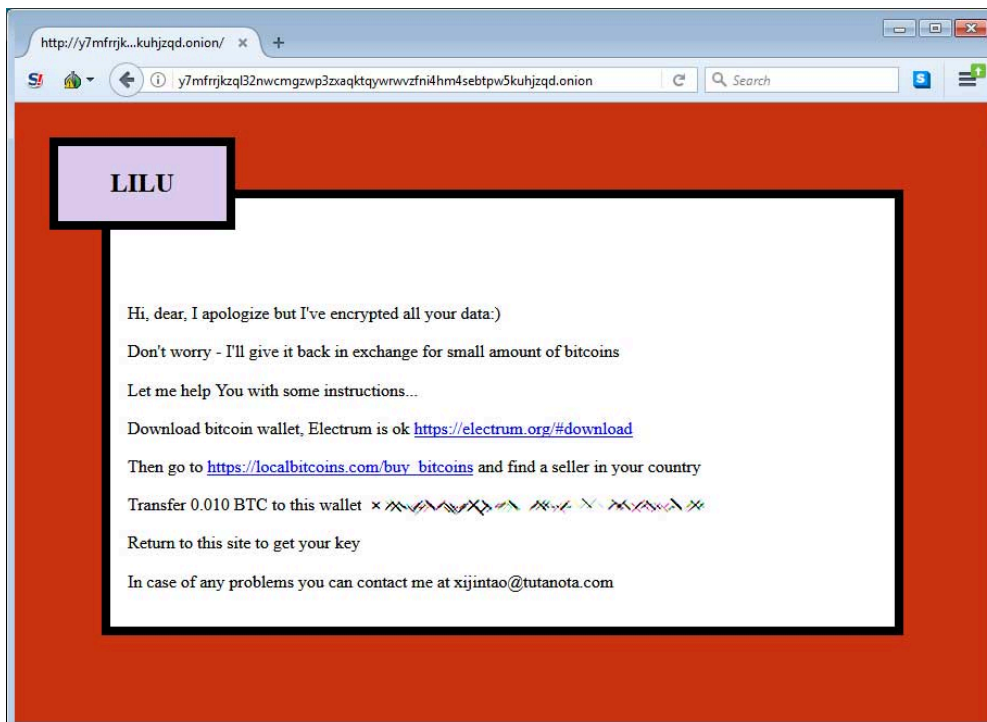
### Lilu ransom note

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



**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.



**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:**

y7mfrjrkzql32nwcmgzwp3zxaqktqyrrwvzfni4hm4sebtpw5kuhjzqd.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!!!

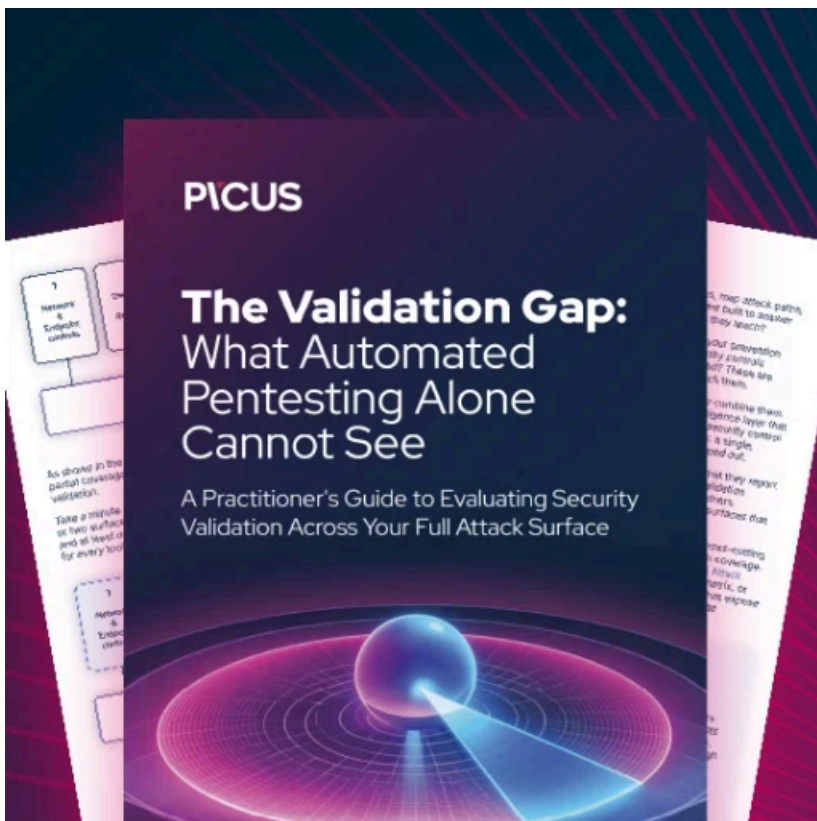
PLEASE VISIT MY SITE WITH TOR BROWSER <https://www.torproject.org/download/>

y7mfrjrkzql32nwcmgzwp3zxaqktqyrrwvzfni4hm4sebtpw5kuhjzqd.onion

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

YOUR KEY IS

[key]



## **Automated Pentesting Covers Only 1 of 6 Surfaces.**

Automated pentesting proves the path exists. BAS proves whether your controls stop it. Most teams run one without the other.

This whitepaper maps six validation surfaces, shows where coverage ends, and provides practitioners with three diagnostic questions for any tool evaluation.

---

Source: <https://www.bleepingcomputer.com/news/security/llocked-ransomware-actively-targeting-servers-and-web-sites/>