Thousands Of Linux Servers Infected By Lilu (Lilocked) Ransomware

fossbytes.com/lilocked-ransomware-infected-linux-servers/

Anmol Sachdeva September 7, 2019

A new strain of ransomware named Lilocked or Lilu has affected thousands of Linux-based servers all over the world. The ransomware started infecting servers back in mid-July but in the last two weeks, the attacks have become more frequent.

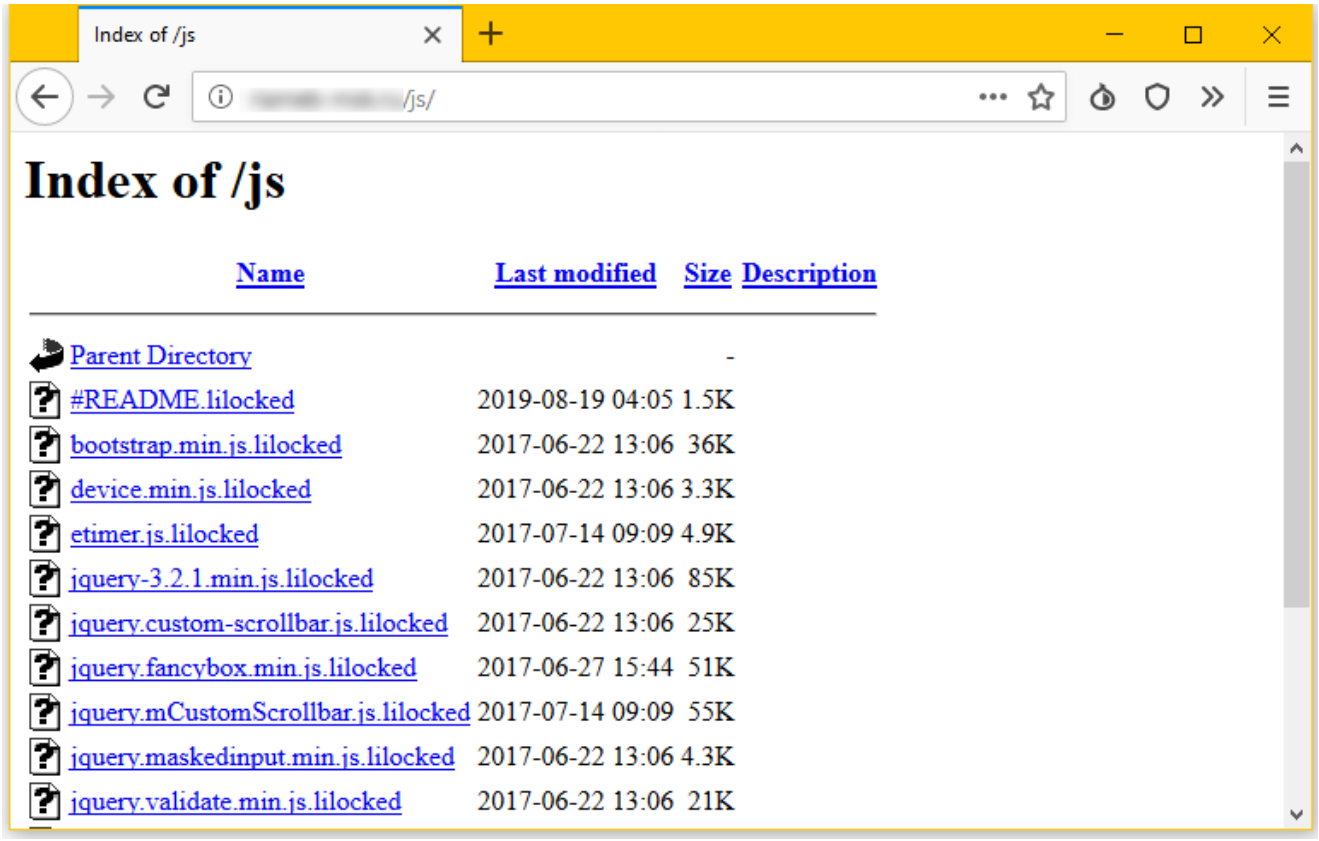
The very first case of Lilocked ransomware came to light when a user uploaded a ransomware note on ID Ransomware, a website used for identifying the name of ransomware from the ransomware note or demand specified in the attack.

It targets servers and gains its root access. The mechanism behind how it gets access in unknown yet.

According to a Russian forum, bad actors might be targeting Linux-based servers that are running defunct Exim software.

Demand – 0.03 Bitcoin

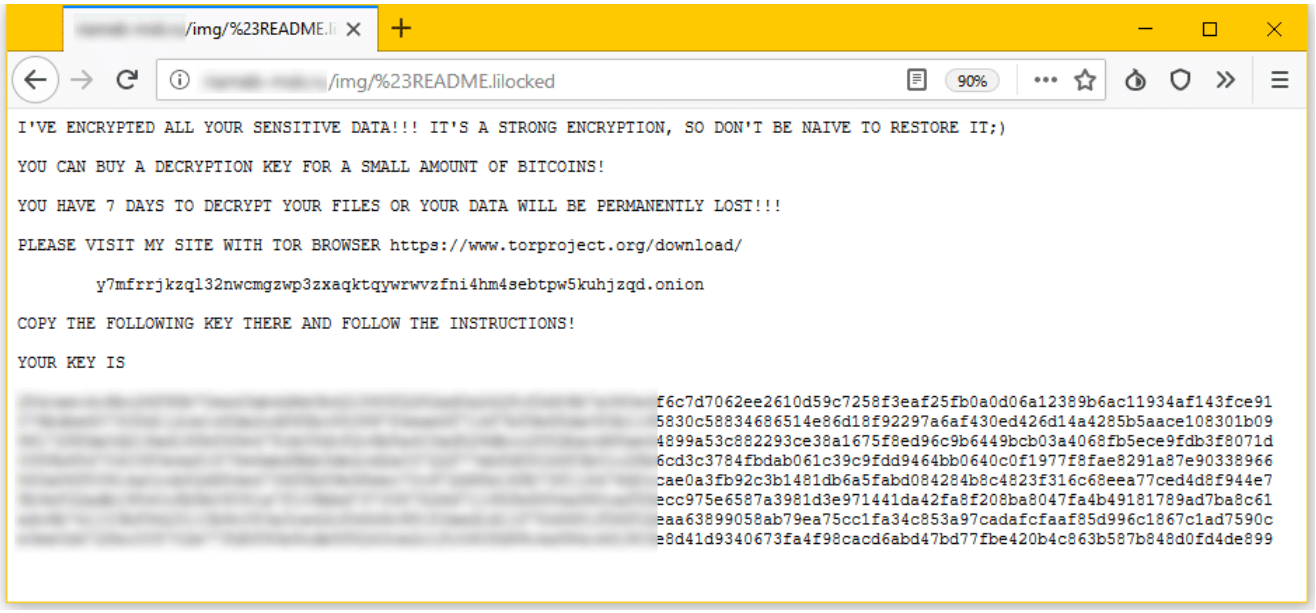
After a server has been attacked, the files are locked with ".lilocked" file extension.



ZDNet

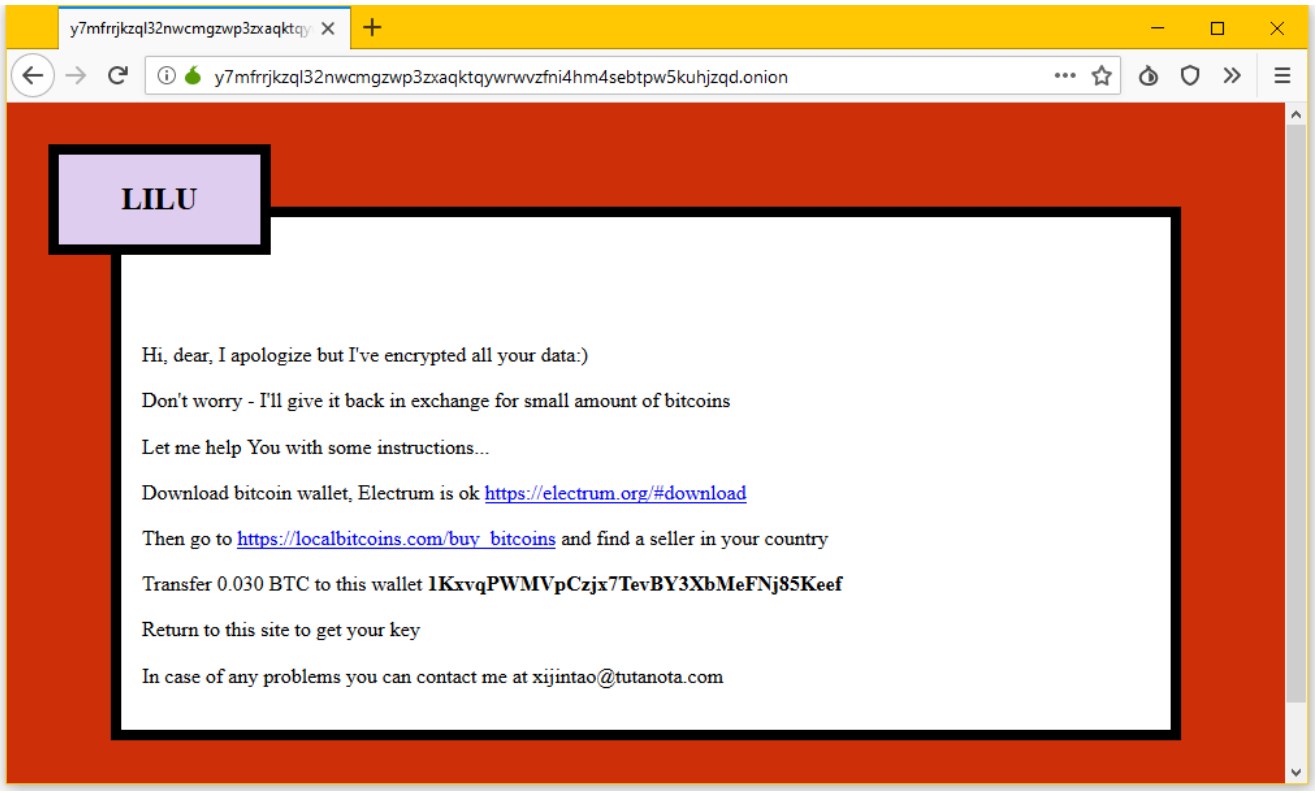
The note accompanied with the encrypted files reads: "*I've encrypted all your sensitive data!!! It's a strong encryption, so don't be naive to restore it;)*"

Find your dream job



ZDNet

Upon clicking the link in the note, users are redirected to a website on the dark web, prompting them to enter the key in the note. When the affected user enters the key, they are asked to deposit 0.03 bitcoin or $325 in the Electrum wallet to get their files decrypted.



ZDNet

Linux Ransomware Does Not Affect System Files

Lilock ransomware does not affect system files but files with extensions including HTML, SHTML, JS, CSS, PHP, INI, and other image formats. Since system files are not affected, Linux systems are running normally.

As per Benkow, a French security researcher, Lilock ransomware has affected 6,700 servers to date. Most of these servers are cached in Google search results. However, the number of infected servers could be much more as there are many infected Linux servers that are not indexed on Google.

Since the mechanism behind the ransomware is not known yet, there isn't a security advisory. You might evade this attack by keeping strong passwords and updating the apps as and when security patches arrive.

> Also Read: Apple Hits Back Hard At Google And Defends iOS Security