Tonga National Computer Emergency Response Team

Cert.to Advisory "Locky Ransomeware"

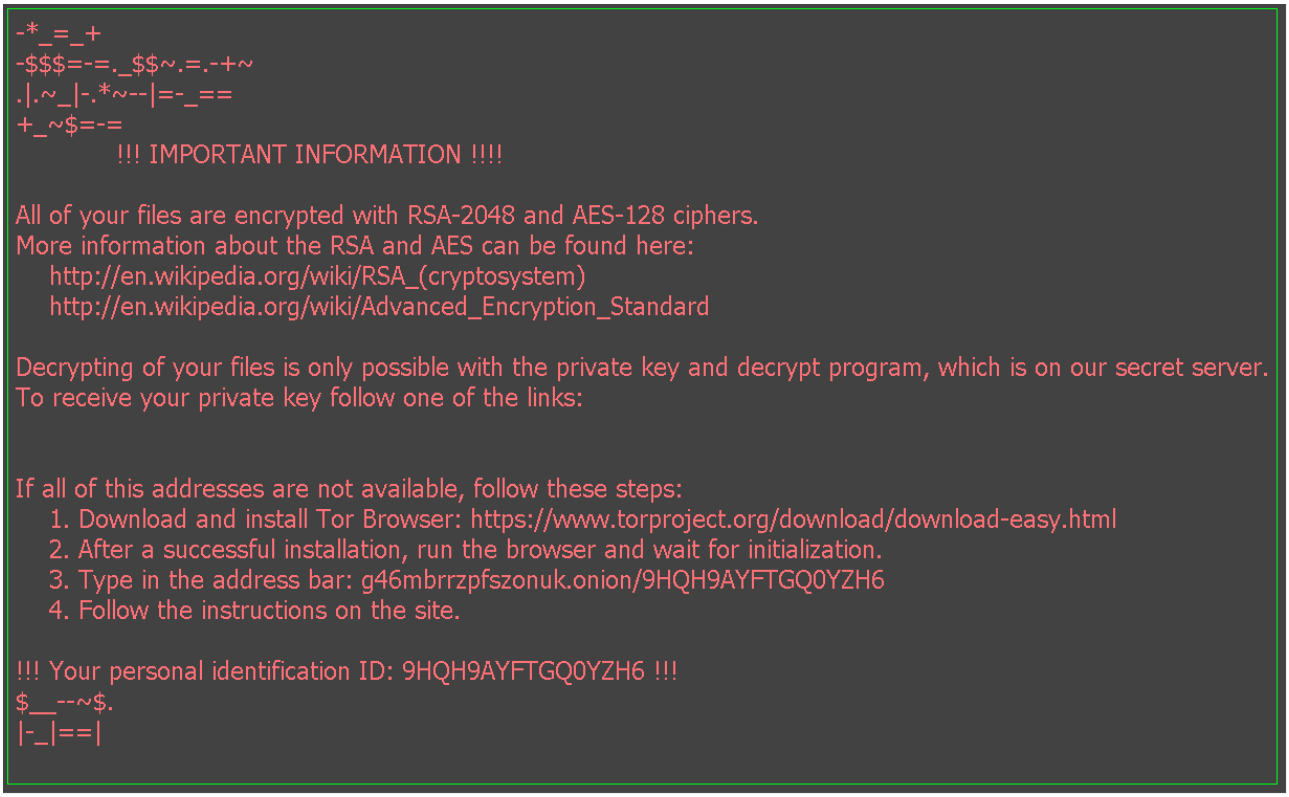
Dear Constituents,

Locky ransomware appear to be hard at work. Security experts have identified two new variants of Locky, dubbed *Diablo6* and *Lukitus*, being distributed in fresh attacks across the globe.

The malware is distributed by the usual method: spam emails. These messages will usually come with an attached Microsoft Office file or a ZIP attachment, which both contain malicious scripts. However, it appears this notorious attacks is back with distribution through the Necurs botnet, one of the largest botnets in use today.

How this attack is deployed

1. Locky Variant Diablo - is being distributed through spam emails and the body content **"Files attached. Thanks"** and the sender's email address had the same domain as the recipient's. The emails came with the .zip attachment "E 2017-08-09 (957).zip", which contained a VBScript downloader called "E 2017-08-09 (972).vbs".
2. Locky Variant Lukitus - is being distributed via spam emails with subject lines – "***No Subject" or Emailing - CSI-034183_MB_S_7727518b6bab2***.
3. Once the file has been downloaded an executed, it will start to encrypt the host computer's files.
4. Finally, it will append a ".lukitus" or ".diablo6" extension to all infected files. The downloaded program will disappear, and will be replaced by a file containing the ransom note as shown below that provides information on how to pay the ransom.



What to do?

- ***Backup regularly and keep a recent backup copy off-site.*** Encrypt your backup and you won't have to worry about the backup device falling into the wrong hands.
- ***Don't enable macros in document attachments received via email*.** Microsoft deliberately turned off auto-execution of macros by default many years ago as a security measure. A lot of malware infections rely on persuading you to turn macros back on, so don't do it!
- **Beware of Phishing emails.** Always be suspicious of uninvited documents sent over an email and never click on links inside those documents unless verifying the source.
- **Don't give yourself more login power than you need.** Most importantly, don't stay logged in as an administrator any longer than is strictly necessary, and avoid browsing, opening documents or other "regular work" activities while you have administrator rights.
- ***Patch early, patch often.*** Malware that doesn't come in via document macros often relies on security bugs in popular applications, including Office, your browser, Flash and more. The sooner you patch, the fewer open holes remain for the crooks to exploit.
- ***Keep your Antivirus software and system Up-to-date.*** Always keep your antivirus software and systems updated to protect against latest threats

Reference

- https://www.bleepingcomputer.com/news/security/the-week-in-ransomware-august-18th-2017-synccrypt-globeimposter-and-locky/
- http://thehackernews.com/2017/08/locky-mamba-ransomware.html
- http://www.zdnet.com/article/locky-ransomware-is-back-from-the-dead-again-with-new-diablo-variant/
- https://www.webroot.com/blog/2017/08/17/locky-ransomware-resurges-diablo-lukitus/
- https://hacked.press/2017/08/18/locky-ransomware-returned-with-diablo-and-lukitus-variants/
- https://blog.malwarebytes.com/cybercrime/2017/08/locky-ransomware-returns-to-the-game-with-two-new-flavors/

Please for more information you can contact us:

Tonga National CERT
Ministry of MEIDECC
OG Sanft Building Level 2
Nuku'alofa
Tel: 2378
email: cert@cert.to
web: www.cert.to