National Computer Board
Computer Emergency Response Team of Mauritius
(CERT-MU)

Advisory

Fake Google Chrome Update drops CTB-Locker Ransomware

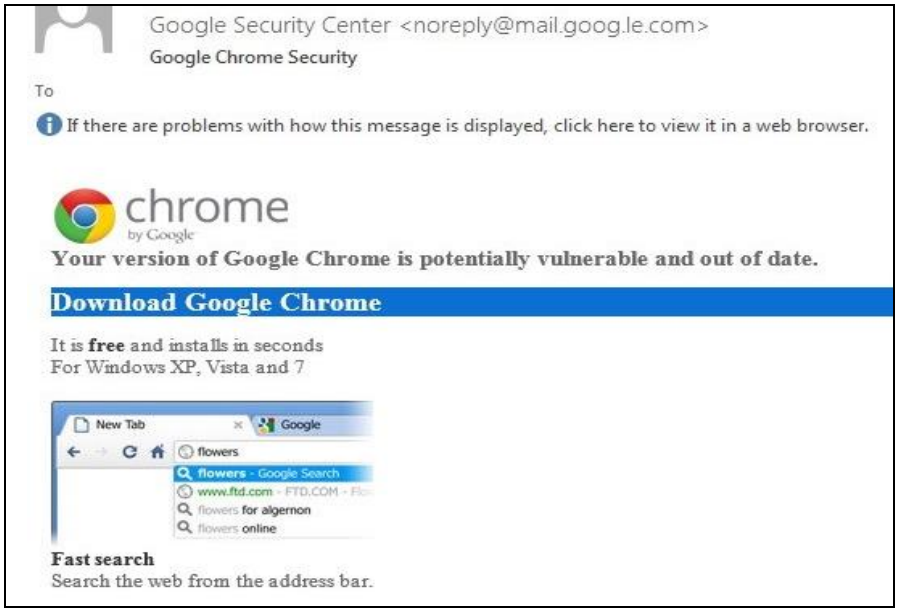
Issued on: 06 February 2015 **Severity Rating:** High

Description:

An email which seems to be originating from **Google Security Center** is making the rounds. The aim of the email is to trick users by posing as an update for the Chrome web browser. Users are prompted to click on a link provided in the message, which is supposedly the online location where the update is available. The malicious payload which is in fact a file encrypting malware is then downloaded from compromised websites. The malware is known as "Critroni" or CTB-Locker is a ransomware that encrypts the data on an affected system and then displays a message asking the victim for a fee in order to unlock the files. The malware has been detected as **Trojan.ZBAgent.NS.**

Methodology

1. The victim gets an email that appears to come from Google with the message *"Your version of Google Chrome is potentially vulnerable and out of date".*

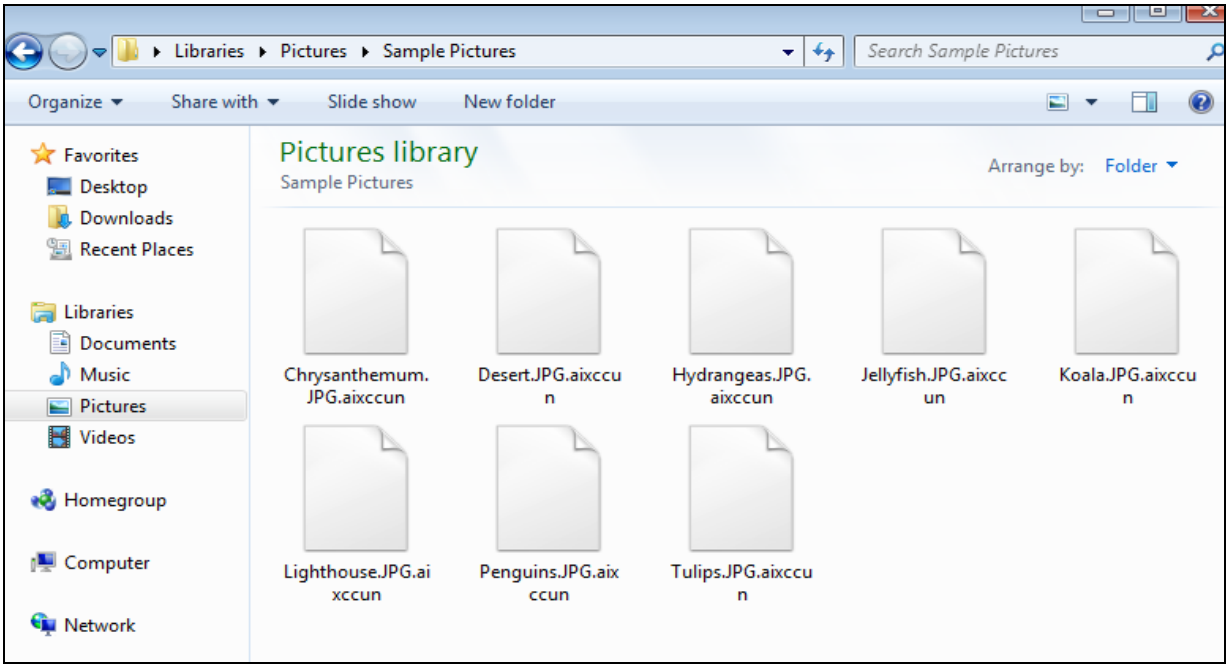


2. Upon **clicking on the link,** the victim is redirected to a compromised website. The payload is not attached to the email but instead gets downloaded from various websites that appear to have been compromised. One particular domain that seems to serve as the dynamic redirection mechanism is ***assetdigitalmarketing.com/redirect.php.*** It then directs the user to one of the following sites where the fake installer is hosted:

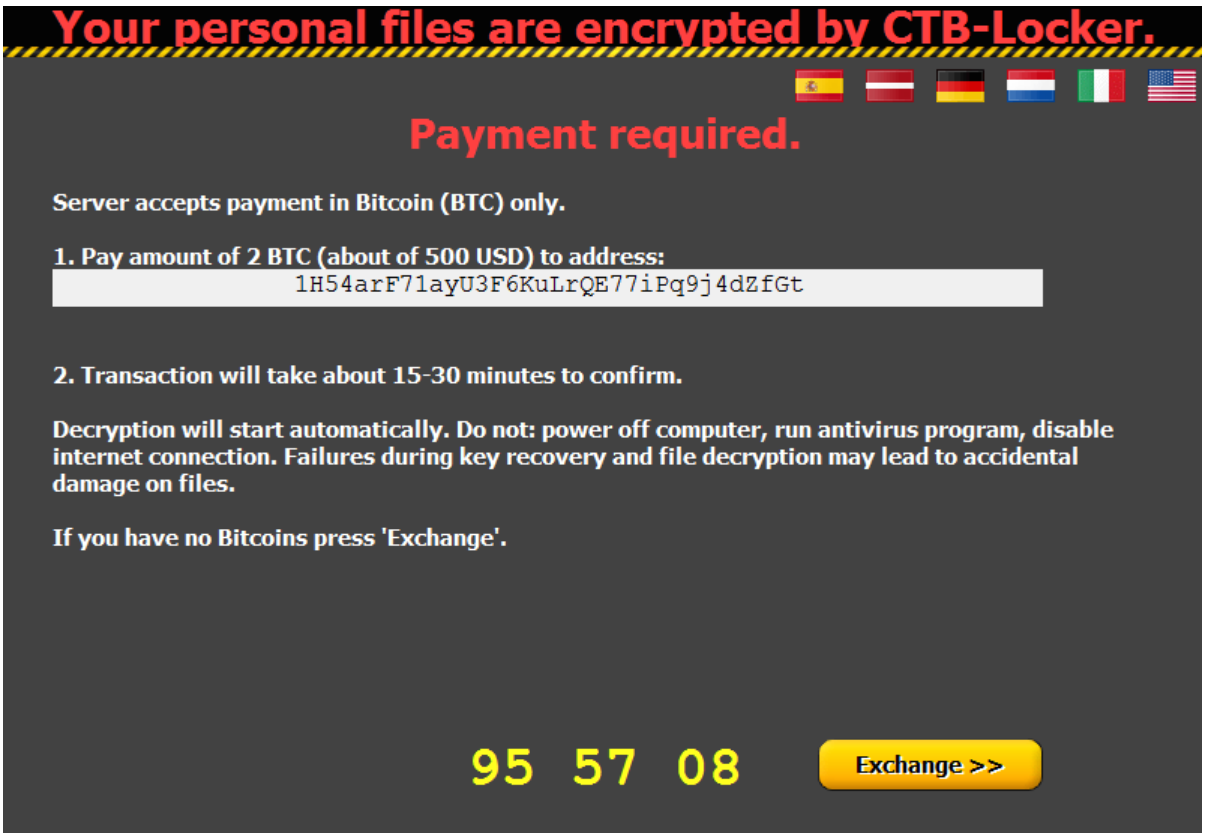
hxxp://www.thelastxmas.com/ChromeSetup.exe
hxxp://www.baddadsclub.com/ChromeSetup.exe
hxxp://cognacbrown.co.uk/ChromeSetup.exe
hxxp://www.geordie.land/ChromeSetup.exe
hxxp://www.goodtobeloved.com/ChromeSetup.exe

3. The victim receives a file (ChromeSetup.exe) pretending to be an installer for Google Chrome. Once launched, the encryption process begins and the ransom message is served when the operation completes.

4. The files on the system are encrypted:



5. A ransom is demanded (to be paid using Bitcoins) to decrypt the files:



Workarounds / Recommendations:

It is to be noted that Google Chrome updates automatically in the background without user intervention. Notifications about a new update **are not delivered by email** and most of the time there are in-program alerts. CERT-MU advises users to check with the vendor before applying any updates received via email.

In case of an infection, it is possible to retrieve the data without paying the ransom **only** if the malware is an **older variant** of the CTB-Locker. This is because it does not delete the shadow copies of the files created by the Windows Volume Shadow Service.

CERT-MU recommends users to be cautious in case they receive such email.

For more information please contact CERT-MU team on:

Hotline No: (+230) 800 2378

Fax No: (+230) 208 0119

Gen. Info. : contact@cert.ncb.mu

Incident: incident@cert.ncb.mu

Website: www.cert-mu.org.mu