



Metropolitan Stock Exchange of India Limited

Department: Technology

Segment: ALL

Circular No: MSE/IT/5489/2017

Date : Sep 4, 2017

Subject: Locky ransomware spreading through massive spam campaign

To All Members,

In regards of the recent Communique from Cert-in all members are hereby notified and requested to undertake appropriate actions as applicable to their environment. A brief description and immediate steps to be taken are mentioned below.

MSE has taken all the counter measures required to protect its systems and services.

Description of the threat:

It has been reported that a new wave of spam mails are circulating with common to spread variants of Locky ransomware. Reports indicate that over 23 million messages have been sent in this campaign. The messages contain common subjects like "please print", "documents", "photo", "Images", "scans" and "pictures". However the subject texts may change in targeted spear phishing campaigns. The messages contain "zip" attachments with Visual Basic Scripts (VBS) embedded in a secondary zip file. The VBS file contains a downloader which polls to domain "greatesthits[dot]mygoldmusic[dot]com" (please do not visit this malicious website) to download variants of Locky ransomware.

If the system is infected by Locky all files are encrypted and string with random numbers with extension "[.]lukitus" or "[.]diablo6" is appended to the encrypted files. It may be noted that earlier variants of Locky add extension ".locky" to the encrypted files. After encryption, desktop background is changed with instructions and a ".htm" file with a name "Lukitus[dot]htm". The instructions contain installation of TOR browser and visiting ".onion" sites and demanding ransom of ".5 Bit coins"

It is also reported that a spam campaign showing links to fake dropbox sites is being used to spread Locky variants.

If the pages are viewed in Chrome or Firefox, they show a fake notification stating "you don't have the HoeflerTextfont". These fake notifications had an "update" button that returns a malicious JavaScript (.js) file. Users are advised to exercise caution while opening emails and organizations are advised to deploy anti spam solutions and update spam block lists.

Key actions to be taken to mitigate the threat:

- Block the below malicious domains/IPs at the perimeter
 - greatesthits[dot]mygoldmusic[dot]com
 - files with extension "[.]lukitus" or "[.]diablo6"
 - file Win[.]JSFontlib09[.]js
 - hxxp://geocean.co[.]id/657erikftgvb??pGDIWEKDHD=Pgdiwekdhd
 - Locky ransomware post-infection URL: hxxp://46.183.165.45/load.cgi

▪ Fake dropbox sites:

- <http://albion-cx22.co.uk/dropbox.html>
 - <http://ambrogiauto.com/dropbox.html>
 - <http://arthurdenniswilliams.com/dropbox.html>
 - <http://autoecoleathena.com/dropbox.html>
 - <http://autoecoleboisdesroches.com/dropbox.html>
 - <http://autoecoledufrene.com/dropbox.html>
 - <http://avtokhim.ru/dropbox.html>
 - <http://bayimpex.be/dropbox.html>
 - <http://binarycousins.com/dropbox.html>
 - <http://charleskeener.com/dropbox.html>
 - <http://campusvoltaire.com/dropbox.html>
 - <http://dar-alataa.com/dropbox.html>
 - <http://flooringforyou.co.uk/dropbox.html>
 - <http://gestionale-orbit.it/dropbox.html>
 - <http://griffithphoto.com/dropbox.html>
 - <http://jakuboweb.com/dropbox.html>
 - <http://jaysonmorrison.com/dropbox.html>
 - <http://patrickreeves.com/dropbox.html>
 - <http://potamitis.gr/dropbox.html>
 - <http://tasgetiren.com/dropbox.html>
 - <http://willemshoeck.nl/dropbox.html>
-
- Perform regular backups of all critical information to limit the impact of data or system loss and to help expedite the recovery process. Ideally, this data should be kept on a separate device, and backups should be stored offline.
 - Keep the operating system third party applications (MS office, browsers, browser Plugins) up-to-date with the latest patches.
 - Maintain updated Antivirus software on all systems.
 - Don't open attachments in unsolicited e-mails, even if they come from people in your contact list, and never click on a URL contained in an unsolicited e-mail, even if the link seems benign. In cases of genuine URLs close out the e-mail and go to the organization's website directly through browser
 - Follow safe practices when browsing the web. Ensure the web browsers are secured enough with appropriate content controls.
 - Establish a Sender Policy Framework (SPF) for your domain, which is an email validation system designed to prevent spam by detecting email spoofing by which most of the ransomware samples successfully reaches the corporate email boxes.
 - Check regularly for the integrity of the information stored in the databases.
 - Regularly check the contents of backup files of databases for any unauthorized encrypted contents of data records or external elements, (backdoors /malicious scripts.)
 - Ensure integrity of the codes /scripts being used in database, authentication and sensitive systems
 - Application white listing/Strict implementation of Software Restriction Policies (SRP)to block binaries running from %APPDATA% and %TEMP% paths. Ransomware sample drops and executes generally from these locations.
 - Network segmentation and segregation into security zones - help protect sensitive information and critical services. Separate administrative network from business processes with physical controls and Virtual Local Area Networks.
 - Disable ActiveX content in Microsoft Office applications such as Word, Excel, etc.
 - Disable remote Desktop Connections, employ least-privileged accounts. Limit users who can log in using Remote Desktop, set an account lockout policy. Ensure proper RDP logging and configuration.

- Restrict access using firewalls and allow only to selected remote endpoints, VPN may also be used with dedicated pool for RDP access
- Use strong authentication protocol, such as Network Level Authentication (NLA) in Windows.
- Additional Security measures that may be considered are
 - Use RDP Gateways for better management
 - Change the listening port for Remote Desktop
 - Tunnel Remote Desktop connections through IPSec or SSH
 - Two-factor authentication may also be considered for highly critical systems
- If not required consider disabling, PowerShell / windows script hosting.
- Restrict user's abilities (permissions) to install and run unwanted software applications.
- Enable personal firewalls on workstations.
- Implement strict External Device (USB drive) usage policy.
- Employ data-at-rest and data-in-transit encryption.
- Consider installing Enhanced Mitigation Experience Toolkit, or similar host-level anti-exploitation tools.
- Block the attachments of file types, exe|pif|tmp|url|vb|vbe|scr|reg|cer|pst|cmd|com|bat|dll|dat|hlp|hta|js|wsf
- Carry out vulnerability Assessment and Penetration Testing (VAPT) and information security audit of critical networks/systems, especially database servers from CERT-IN empaneled auditors. Repeat audits at regular intervals.
- Individuals or organizations are not encouraged to pay the ransom, as this does not guarantee files will be released. Report such instances of fraud to CERT-In and Law Enforcement agencies.

Disclaimer:

- a) The information contained in this notice has been extracted from public sources and has been published only as guidance to members. As the future course of events with regards to this threat are not known, members are advised to keep a close watch on their systems to identify timely detection and remediation of this threat
- b) Members shall act upon this notice at their own discretion after conducting appropriate impact/risk analysis to their specific environment
- c) This circular is for informational purpose only.

Trading Members / Stock Brokers are advised to take suitable necessary actions / measures in view of the aforementioned Advisory and Vulnerability Note of CERT-In. Trading Members / Stock Brokers may also bring the aforementioned Advisory and Vulnerability Note of CERT-In to the notice of their Sub Brokers / Clients.

Trading Members / Stock Brokers are advised to report us and CERT-In regarding Incident(s) of breach, if any due to Advanced Software Script (Malware) attack on their systems.

Copies of the advisories attached:

- CERT-In Note on Locky - September 02, 2017
- Cyber Swachhta Kendra_ LOCKY Ransomware
- Cyber Swachhta Kendra_ Prevention of Ransomware Infections

For and on behalf of
Metropolitan Stock Exchange of India Limited

Kundan Zamvar
Chief Information Security Officer