Indian Computer Emergency Response Team
Ministry of Electronics and Information Technology
Government of India
सत्यमेव जयते

CURRENT ACTIVITIES

Locky ransomware spreading through massive spam campaign

Original Issue Date:September 02, 2017

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" attachements 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.

For details regarding Locky ransomware, please refer to alert regarding Locky ransomware issued in February 2016 here:
http://www.cyberswachhtakendra.gov.in/alerts/locky_ransomware.html

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 Bitcoins"

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 HoeflerText font". 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.

Indicators of Compromise:
(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/imageload.cgi

Fake dropbox sites:

- hxxp://albion-cx22.co[.]uk/dropbox.html
- hxxp://ambrogiauto[.]com/dropbox.html
- hxxp://arthurdenniswilliams[.]com/dropbox.html
- hxxp://autoecoleathena[.]com/dropbox.html
- hxxp://autoecoleboisdesroches[.]com/dropbox.html
- hxxp://autoecoledufrene[.]com/dropbox.html
- hxxp://avtokhim[.]ru/dropbox.html
- hxxp://bayimpex[.]be/dropbox.html
- hxxp://binarycousins[.]com/dropbox.html
- hxxp://charleskeener[.]com/dropbox.html
- hxxp://campusvoltaire[.]com/dropbox.html
- hxxp://dar-alataa[.]com/dropbox.html
- hxxp://flooringforyou.co[.]uk/dropbox.html
- hxxp://gestionale-orbit[.]it/dropbox.html
- hxxp://griffithphoto[.]com/dropbox.html
- hxxp://jakuboweb[.]com/dropbox.html
- hxxp://jaysonmorrison[.]com/dropbox.html
- hxxp://patrickreeves[.]com/dropbox.html
- hxxp://potamitis[.]gr/dropbox.html
- hxxp://tasgetiren[.]com/dropbox.html
- hxxp://willemshoeck[.]nl/dropbox.html

Note: For update on latest Indicators of Compromises, please see references to security vendors given in references section

Countermeasures and Best Practices for prevention

Users and administrators are advised to take the following preventive measures to protect their computer networks from ransomware infection/ attacks:

- 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.

References

https://blog.appriver.com/2017/08/locky-ransomware-attacks-increase/
https://www.webroot.com/blog/2017/08/17/locky-ransomware-resurges-diablo-lukitus/
https://isc.sans.edu/forums/diary/Malspam+pushing+Locky+ransomware+tries+HoeflerText+notifications+for+Chrome+and+FireFox/22776/
http://www.zdnet.com/article/this-giant-ransomware-campaign-just-sent-millions-of-malware-spreading-emails/
https://www.forbes.com/sites/leemathews/2017/08/31/massive-ransomware-attack-unleashes-23-million-emails-in-24-hours/#30cc2155394b
https://www.databreachtoday.com/blogs/locky-ransomware-returns-two-new-variants-p-2528
https://twitter.com/peterkruse/status/903538736599891969

Contact Information

Email:info@cert-in.org.in
Phone: +91-11-24368572

Postal Address

Indian Computer Emergency Response Team (CERT-In)
Ministry of Electronics and Information Technology
Government of India
Electronics Niketan
6, CGO Complex, Lodhi Road,
New Delhi - 110 003
India