(http://www.cert-in.org.in/)

Ministry of Electronics and Information Technology Government of India

सत्यमेव जयते

(http://meity.gov.in/)

साइबर स्वच्छता केन्द्र

CYBER SWACHHTA KENDRA

Botnet Cleaning and Malware Analysis Centre

(..\index.html)

Home (../index.html) | About Us (../about.html) | CERT-In (http://www.cert-in.org.in/)

Security Tools (../security-tools.html) | Alerts (../alerts.html) | Security Best Practices (../security-best-practices.html)

Partners (../partners.html) | FAQ's (../faq.html) | Contact Us (../contact.html)

(http

(http

## LOCKY Ransomware

Original Issue Date:-February 25, 2016
Virus Type:- Ransomware

Ransomware-Locky is a ransomware that scramble the contents of a computer or server (associated network shares ,both mapped and unmapped and removable media) and demands payment to unlock it "usually by anonymous decentralized virtual currency BITCOINS".

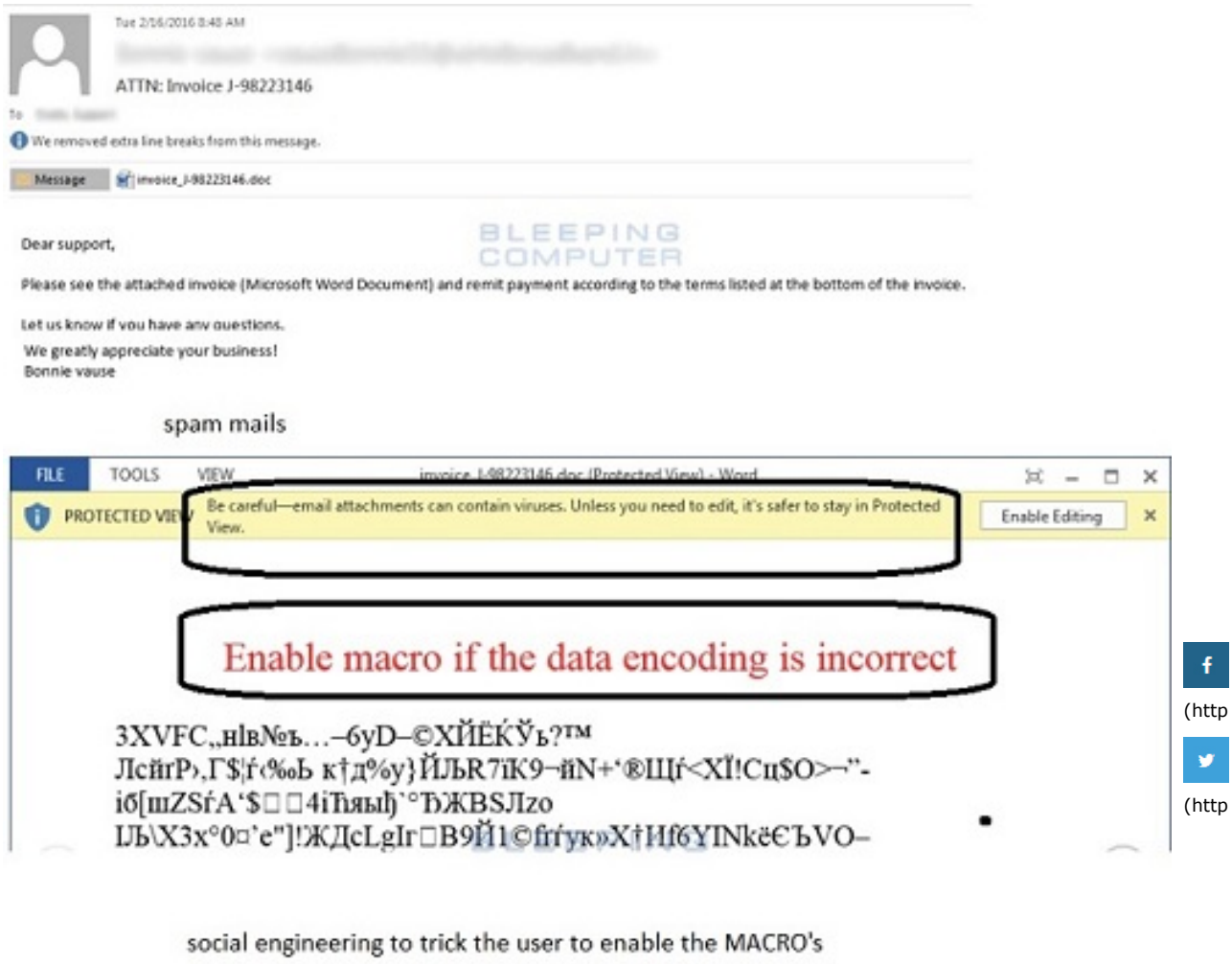
**Locky features:**

- Domain Generation Algorithm (DGA)
- Mapped / Unmapped Network share discovery
- Restore point deletion

The contents of the original files are encrypted (renamed to .locky) using an RSA-2048 and AES-1024 algorithm.The compromised user has to pay the attacker to get the files decrypted.

**Propagation Methods**

The primary modus operandi of Locky is via spammed emails that come with an attachment in the form of a MACRO ENABLED Microsoft Office document file with catchy subjects similar to **ATTN: Invoice J-98223146 / invoice_J-12345678.doc / Rechnung-54-110090.xls**



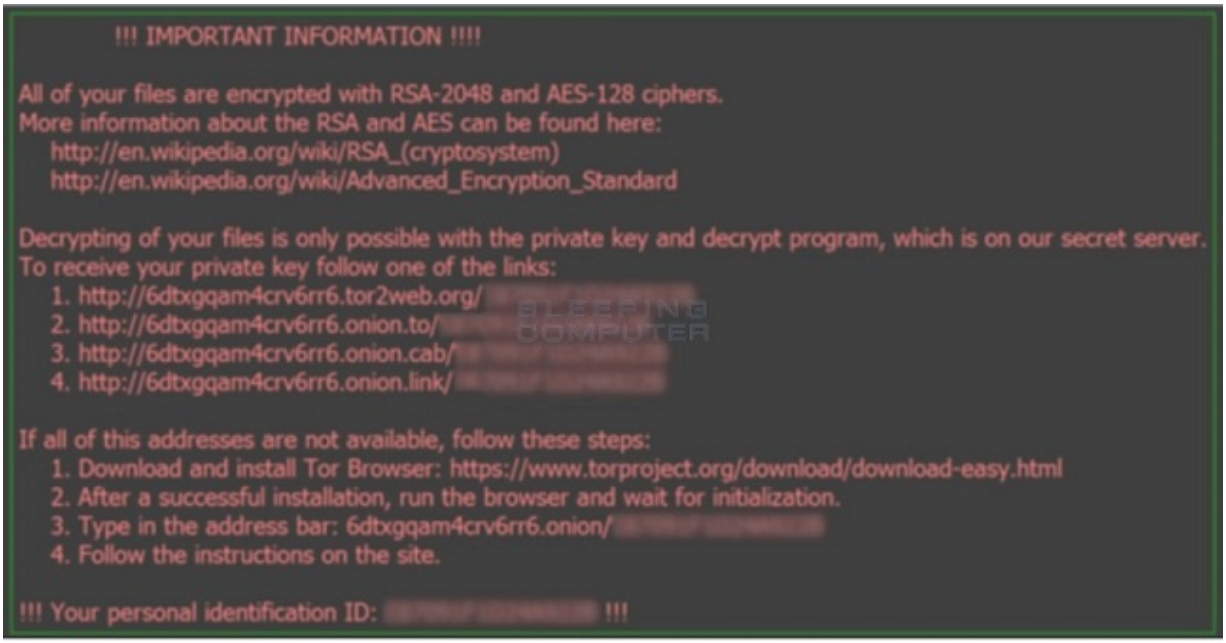

Once MACROS are trick to be enabled, the embedded downloads Locky, stores it in the Temp folder and executes it. Once installed Locky scraps the file systems (and unmapped shares also), with certain extensions (.pptx, .pptm, .dotm, .dotx, .docm, .docx, .RTF,. DOC, **.pem,.crt, .key, wallet.dat**,.pdf, .XLS, .PPT,,tar.bz2, .bak, .tar, .tgz, .rar, .zip, .bmp, .png, .gif, .jpeg, .jpg, .tif, .tiff, .bat, .class, .jar, .java, .asp, .vbs,.cpp, .php,.sql etc) and scrambles it and renaming it to **[unique_id][identifier].locky** As part of the initial infection process, Locky **deletes** the **volume shadow copy files** hence preventing **restoring** the system to an earlier steady state by "vssadmin.exe Delete Shadows /All /Quiet"

**Major File System Changes**

- **Files created** %temp%.exe
- %user Desktop%/_Locky_recover_instructions.bmp
- %user Desktop%/_Locky_recover_instructions.txt

**Presence of registry keys**

- HKEY_CURRENT_USER\ Software\Microsoft\Windows\CurrentVersion\Run "Locky" = "LOCKY PATH"
- HKCU\Software\Locky\id - The unique ID assigned to the victim.
- HKCU\Software\Locky\pubkey - The RSA public key.
- HKCU\Software\Locky\paytext - The text that is stored in the ransom notes.
- HKCU\Software\Locky\completed - Whether the ransomware finished encrypting the computer
- HKCU\Control Panel\Desktop\Wallpaper "%UserProfile%\Desktop_Locky_recover_instructions.bmp"




LOCKY EXTROTION MESSAGE

Locky [leverages Domain Generation Algorithm (DGA] is reported as making network connection to the following :

185.14.30.97, 195.154.241.208, 195.22.28.196, 195.22.28.198, 31.41.47.37, 95.181.171.58, avp-mech.ru, bebikiask.bc00.in, cgavqeodnop.it, cms.insviluppo.net, dltvwp.it, kqlxtqptsmys.in, neways-eurasia.com.ua, premium34.tmweb.ru, pvwinlrmwvccuo.eu, sso.anbtr.com, test.rinzo.biz, tramviet.vn, uponor.otistores.com, uxvvm.us, wblejsfob.pw

A detailed list of Indicators of compromise including domains, IP's, Malware HASH listed IOC here File-I (../documents/IOC-I.pdf) - File-II (../documents/IOC-II.pdf)

### Recommendations:

- Block connections to the IPS/ domains aforementioned.
  Note:
  - Blocking IP addresses should always be carefully considered and only when subject to the business needs.
  - Connection to unexpected domains should be categorically monitored /blocked since Locky employs DGA
- Create SRP rules to block execution of the executables listed in the IOC section.
- 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.
- Disable Macro in Microsoft Office applications. Macros can run in Office applications only if Macro Settings are set to "Enable all macros" or if the user manually enables a macro. By default, it will be in a disabled state. The recommended setting is to select the option "Disable all macros with notification" in "Macro Settings".
- 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 you think it looks safe. Instead, close out the e-mail and go to the organization's website directly.
- Practice and Enforce Least privilege Policy. Lock down all open network shared to the lowest permissions.
- Follow safe practices when browsing the web. Ensure the web browsers are secured enough with best practices.
- 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.
- Application whitelisting/Strict implementation of Software Restriction Policies (SRP) to block binaries running from %APPDATA% and %TEMP% paths
- Disable ActiveX content in Microsoft Office applications such as Word, Excel, etc.
- Disable remote Desktop Connections, employ least-privileged accounts.
- Restrict users' abilities (permissions) to install and run unwanted software applications.
- Enable personal firewalls on workstations.
- 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.
- Keep your operating system, browsers, browser plugins & Antivirus Software up-to-date with the latest patches.