Dairy No. 1534
Date 12-7-16

HARYANA GOVERNMENT / हरियाणा सरकार

Haryana State
Information Security Management Office

Society for IT Initiative Fund for e-Governance,
Department of Electronics & Information Technology, Haryana

हरियाणा
INFORMATION SECURITY

HRY-ISMO/2016/CISO/ 3667

04 July 2016

Dear Sir / Madam:

Subject: *Rise of Ransomware attacks* – Important for Information Security.

Government of India has released a special advisory on Ransomware attacks on Computer Systems, which is attached herewith for your information & necessary action. The advisory is self explanatory as regards Ransomware attacks and its remedial measures. You are requested to circulate this advisory within your organization for prompt action by all concerned.

Yours truly,

R. Suman Thy

Chief Information Security Officer
Haryana State ISMO

Encl:

1. CERT-In special advisory CISA-2016-001

All Administrative Secretaries
All Heads of Departments
All Boards, Corporations and Institutions
State Informatics Officer, NIC
Head – SeMT, Haryana
cc: Nodal Officer – Amit Beniwal, Haryana ISMO
email – amitbeniwal@haryanaismo.gov.in

Bays 73-76, Hartron Bhawan, Sector 2, Panchkula. 134151
Chairman, E.C.: 2740009, MSEC.: 2741547, Ad.O: 2748142, Fax:0172-2749985
ciso@haryanaismo.gov.in www.haryanait.gov.in

निदेशालय औद्योगिक प्रशिक्षण विभाग हरियाणा चण्डीगढ़।
पृ0 क0 टीए/16/सरकूलर/तालमेल/6020 दिनांक 1/8/16

उपरोक्त कि एक प्रति निम्नलिखित को सूचनार्थ एवं आवश्यक कार्यवाही हेतु भेजी जाती है:–

1. निजी सहायक/निदेशक।
2. स्टैनों टू अतिरिक्त निदेशक (प्रशासन)।
3. सभी अधिकारी/अनुभागों के प्रभारी मुख्यालय पर।
4. सभी उप–कार्यालय हरियाणा राज्य में।
5. सहायक निदेशक विभागीय वेबसाईट।

सहायक निदेशक (तालमेल)
कृते: निदेशक औद्योगिक प्रशिक्षण विभाग
हरियाणा चण्डीगढ़।

Subject: Ransomware attacks – remedial measures

1. Background:

It has been observed that "Ransomware malware" attacks are on rise on financial institutions, businesses and academic institutions in the country. Ransomware are type of malicious software (malware) that scramble the contents of a computer or server (associated network shares and removable media) and demands payment/ransom to unlock it "usually by anonymous decentralized virtual currency BITCOINS". Ransomware usually causes temporary or permanent loss of sensitive or proprietary information, financial losses, disruption to regular operations and potential harm to an organization's reputation.

This Advisory is intended to provide further information about Ransomware, its main characteristics, the proliferation mechanisms and to provide prevention and mitigation information.

2. Modus Operandi of attacks

Ransomware is typically spread **through spear phishing emails** that contain malicious attachments and **drive-by download**. Drive-by downloading occurs when a user unknowingly visits an infected website and malware is downloaded and installed without the user's knowledge or when user clicks on links spread through Web-based instant messaging applications.

Ransomware attempts to extort money from victims by displaying an extortion alert indicating that their computer has been locked or all files have been encrypted, and demand that a ransom is paid to restore access.

The authors of ransomware instill fear and panic into their victims by deleting the windows restore points, causing them to click on a link or pay a ransom. Paying the ransom does not guarantee the encrypted files will be released; it only guarantees that the malicious actors receive the victim's money, and in some cases, their banking information. In addition, decrypting files does not mean the malware infection itself has been removed.

It has also been reported that attackers have gone one level deeper by typically targeting the backend databases / backup which stores critical financial data. In contrast with the conventional ransomware methodology, wherein "IN-ONE-GO" encryption of the files /documents is carried out, in the latest attacks, attacker tampers specific fields / records of databases which are sensitive in nature and subsequently demand ransom, an indication of persistent access to the critical assets of an enterprise network.

Cyber security companies are working on decryption tools for such encrypted files, but, till date decrypting the files has not been possible, as there is no way to retrieve the private key that can be used to decrypt the files. Brute forcing the decryption key is not realistic due to the length of time required to break this type of cryptography. Restoring to earlier operating system state may fail as the malware may delete the volume shadow copies (restore points in windows) as the first step immediately after infection.

Some of the prevalent and destructive ransomware variants observed in Indian cyber spaces are CryptoLocker, Reveton, CTB-Locker, Cryptowall, TeslaCrypt. Ransomware are evolving in their methods of propagation, encryption, and the targets sought. Recently, "ransom32" - a javascript based *Ransomware as Service* is being offered in the underground market to facilitate the whole extortion process.

CERT-In has issued alerts on ransomware such as Cryptolocker, Locky etc. The same may be seen on website www.cert-in.org.in

3. Best Practices and remedial measures

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.
- 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
- 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.
- Keep the operating system third party applications (MS office, browsers, browser Plugins) up-to-date with the latest patches.
- Application whitelisting/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.
- 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.
- 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.
- If not required consider disabling, PowerShell /windows script hosting.
- Restrict users' 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