HARYANA GOVERNMENT / हरियाणा सरकार

Haryana State Information Security Management Office

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

INFORMATION SECURITY

HRY-ISMO/2016/CISO/ 3667

04 July 2016

CS/ 23 PHE
Diary No. 596
Date 12/07/16

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. Sumanth

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

Public Health Branch
Diary No. 596
Date 15-07-16

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

Endst. No. 68667-68737/PHE/CD-23 Dated: 28/07/2016.

A copy of the above is forwarded to the following along with CERT-in special advisory (indicated above) for information and necessary action:-

1. All Superintending Engineer, Public Health Engineering Circles.
2. All Executive Engineer, Public Health Engineering Divisions.
3. Chief Engineer, (Rural/ Prog./ Project/ Urban/ Mech.) & Chief Engineer-Cum-Dir.(WSSO), Public Health Engineering Deptt.
4. All Superintending Engineer / Executive Engineer, PHED Head office, Panchkula.
5. All other officers and Branch In-charges in Head Office.

DA/As above

28/7/16

Executive Engineer (Coord)
For Engineer-in-Chief, Haryana

27/7/16

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.

- 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