भारतीय डाक

Zero Day Exploit Advisory

India Post

Overview:

This is a general advisory regarding a zero-day infection which is spreading currently which we have received from our sources of information. Here the attacker is using a Trojan as a medium to perform recon activity on system & retrieves the system information and sends it to a CNC hosted in AWS. A zero day exploit is a cyber attack that occurs on the same day a weakness is discovered in software. It's exploited before a fix becomes available from its creator. Usually the program creators are quick to create a fix that improves program protection, however, sometimes hackers hear about the flaw first and are quick to exploit it. Hence, the zero day exploits are vulnerable until a fix is released against them by the concerned team so as to block that particular loophole or backdoor. It is advised to the users to perform full scan of the system and up to date all the systems with latest antivirus signature.

Release Date: 11th September, 2019

Targeted OS: Windows system, Network Devices

Distribution Method: Trojan, Phishing

India Post

Mitigation Measures:

1. Users should follow the best practices to defend against the ransomware:

- The system and applications should be patched and updated.
- Regularly backup the files.
- Enforce the principle of least privilege
- Defence in depth implementation is required, so that security solutions can protect at each layer like gateways, routers, servers and endpoints.

2. Users should follow the best practices to defend against the malware:

- Keep software and security patches up to date by downloading the latest software releases and updates. Installing security patches fixes bugs that the previous version may have missed.
- Enforce the principle of least privilege.
- Defence in depth implementation is required, so that security solutions can protect at each layer like gateways, routers, servers and endpoints.
- Ensure the most current AV signatures are applied.
- Web scanning should be performed so as to prevent access to malicious process and detect malware used in the attack.
- Install a proactive and comprehensive security software to help block known and unknown threats to vulnerabilities.

Prevention Measures:

Following are the basic steps the users can follow as of now, if we found any discrepancies later than we will surely release further information:-

- Upgrade your systems with the latest security patches.
- 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.)
- Keep the operating system third party applications (MS office, browsers, browser Plugins) up-to-date with the latest patches.
- 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.
- 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.
- Set remote access restrictions.
- Restrict users' abilities (permissions) to install and run unwanted software applications.
- By regulating, monitoring, and controlling the use of RDP and addressing vulnerabilities, it is possible to reduce risk and prevent Remote Desktop Protocol attacks.
- Configure Windows to show file extensions and keep the macros disabled.
- Scan while using External Device (USB drive) usage policy.

For any queries kindly contact us: 0821-2300717 / 738 or itsecuritycept@indiapost.gov.in

IT Security Team,
CEPT, Mysore- 570010