Malware Advisory
Smoke Loader

भारतीय डाक
Indian Post

Overview:

Smoke Loader is trojan-type malware used to proliferate various other viruses. Cyber criminals proliferate Smoke Loader using spam emails (malicious attachments). Therefore, it typically infiltrates systems without users' consent. After successful infiltration, the malware performs a number of actions, such as:

1) self-updating; 2) removing all traces, and 3) downloading other viruses.

The new campaign of this malware variant uses "Stunnel", an open source application that acts as a proxy and universal TLS or SSL tunneling service. The attacker main aim to target Python-based shareware application which "Convert PDF to Word Plus" Organizations should consider adopting security solutions.

Mitigation Measures:

- Network connections made by the compromised machines with other machines on the same network needs to be isolated from the network and further analysis is required.
- Set remote access restrictions.
- Encrypt all sensitive organizational information.
- Convert HTML email into text only email messages or disable HTML email messages.

Prevention Measures:

- Make sure Antivirus is updated with latest signature in all systems.
- 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.
- Restrict users' abilities (permissions) to install and run unwanted software applications.
- 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, CEPT,
Mysore- 570010