

GOVERNMENT OF PAKISTAN
CABINET SECRETARIAT, CABINET DIVISION
NATIONAL TELECOM & INFORMATION TECHNOLOGY SECURITY BOARD
(NTISB-II)

No. 1-5/2003 (NTISB-II)

Islamabad 20 July, 2018

Subject: Advisory - Prevention Against "Vega Stealer" (Advisory No 138)

1. **Introduction.** Security researchers have discovered a new malware named "Vega Stealer" developed to steal saved login and credit card credentials from Chrome and Firefox browsers. Apart from credential stealing capability, the malware also steals sensitive documents from the targeted device.

2. **Affected Products.**

- a. Mozilla Firefox browser.
- b. Chrome browser.

3. **Technical Analysis.**

- a. **Vega Stealer** is distributed through a spam email campaign with different subject lines including "Online store developer required".
- b. The email is propagated with a document attachment called "brief.doc" containing malicious macros which once enabled downloads the Vega Stealer payload.
- c. **Vega Stealer** after infecting a targeted system starts stealing data and searches the victim's desktop and sub-directories for files in different formats including ".doc, .docx, .txt, .rtf, .xls, .xlsx, .pdf." This is done for exfiltration after which the malware sends the stolen data to a remote command and control (C&C) server.

4. **Mitigation Measures.** Following mitigation measures are suggested as under:-

- a. Avoid clicking unknown links and downloading attachments sent by anonymous users.
- b. Always scan suspicious files on Virus Total and keep your system up to date.
- c. Install an Anti-Phishing toolbar e.g "PANDA SAFE WEB" to run quick checks on websites visited and compare them to lists of known phishing sites.
- d. Security patches are continuously released in response to the identified vulnerabilities, it is advised to update the browser on regular basis
- e. Deploy a spam filter e.g. SpamSieve that detects viruses, blank ends, etc.
- f. Be aware of pop-ups and ensure following steps:-

23 JUL 2018

M(A)

M(I T)

A.S (Rev. Div.)

CCIT

30/07/18

CEO PRAL

29085-R

FBR eDOX Dy. Ho.

Received in Ch. Sect.

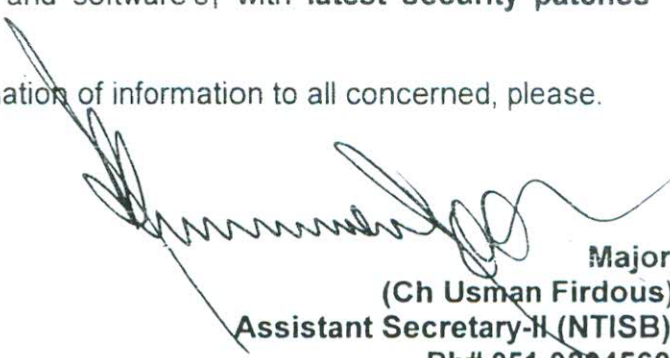
23 JUL 2018

sent to CEO PRAL
31/7/18

- (1) Never enter **personal information** in a pop-up screen.
 - (2) Do not click on **URL. and web links in a pop-up** screen. If clicked then change all the passwords immediately.
 - (3) **Do not dopy web addresses** into your browsers from pop-ups.
- g. Check your **online accounts and bank statements** regularly to ensure that no unauti.orized transactions have been made.

5. **Recommendations.**

- a. Regularly check the vendor website for updates and release of security patches.
 - b. Strictly follow all mitigation measures vide para 4.
 - c. Educate the employees, about **phishing attacks, social engineering** and counter measures
 - d. **Install and update well reputed antiviruses** such as Kaspersky Avira, Avast etc and **monitor** the antivirus status on all equipment.
 - e. Keep all operating systems and software's, with **latest security patches and updates.**
6. Forwarded for perusal and dissemination of information to all concerned, please.



Major
(Ch Usman Firdous)
Assistant Secretary-II (NTISB)
Ph# 051-9204560

All Secretaries of Ministries / Divisions of Federal Government and Chief Secretaries of Provincial Governments