

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

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

Islamabad 21 May, 2018

Subject: Prevention Against Cyber Espionage (Advisory No 125)

1. **Introduction.** Chrome extension is a built-in feature of chrome browser to install feature based applications like Calculator, Adblock, and VPN etc. Recently, popular chrome extensions are found to be infected with malware which are being used by approximately 20-million users. Downloading and enabling these extensions in chrome can steal sensitive information from the browser.

2. **Affected Extensions.** Following is the list of compromised Chrome browser extensions along with the number of people that have installed it:-

- a. AdRemover for Google Chrome™ (10 million+ users).
- b. uBlock Plus (8 million+ users).
- c. [Fake] Adblock Pro (2 million+ users).
- d. HD for YouTube™ (400,000+ users).
- e. Webutation (30,000+ users).

3. **Technical Details**

- a. The above mentioned malicious browser extensions can access all online activities of user, incl passwords, web history and credit card details.
- b. These malicious extension can receive commands from the remote server, which are executed in the extension 'background page' and can manipulate browser's behavior in any way.

4. **Recommendations**

- a. Install extension from trusted sources only.
 - b. Install and update well reputed antiviruses such as Kaspersky, Avira, Avast etc.
 - c. Update all softwares including Windows OS, Windows Browser, Microsoft Office regularly.
 - d. Remove any unwanted extension from Google Chrome by going to **Customize and Control > More Tools > Extensions**
 - e. Don't download attachments from emails unless you are sure about the source.
5. Forwarded for perusal; and dissemination of information to all concerned, please.

Q

M(A)

M(I.T)

A.S (Rev. Div)

1029-55 (BOS-IT)
28.5.18

66213-R
2018

[Signature]

[Signature] 28/05/18
Chief (BOS-IT)

[Signature] 28/05/18

[Signature]
Major
(Ifikhar Ali)
Assistant Secretary (NTISB-II)
Ph# 051-9204560

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

[Signature]

[Signature] 29/05/18
Secy (I.T)

P1, P4
sptdt

[Signature]
30.5.18

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

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

Islamabad 21 May, 2018

Subject: Prevention Against Cyber Espionage (Advisory No 124)

1. **Introduction.** Recently, a critical vulnerability regarding Microsoft Outlook has been disclosed by the security researchers that could allow attackers to steal sensitive information including login credentials from windows system.

2. **Technical Details**

- a. This vulnerability resides in Microsoft Outlook that it automatically initiates an SMB connection whenever remotely hosted RTF based email message is previewed.
- b. A remote attacker can exploit this vulnerability by sending an RTF email to a target.
- c. Microsoft Outlook will automatically execute the attacker's malicious content handling over the victim's credentials and allowing the hackers to take control of the victim's system.

3. **Affected Products.** All outdated versions of windows that utilize Microsoft Outlook are compromised.

4. **Recommendations**

- a. Update windows immediately.
- b. Block specific ports 445, 127 and 139 used for incoming and outgoing SMB connections.
- c. Make use of complex passwords.
- d. Block NT LAN Manager (NTLM) Single Sign-on (SSO) authentication.
- e. Don't click on links from un-trusted sources.

5. Forwarded for perusal and dissemination of information to all concerned, please.

[Handwritten signature]
25/5

[Handwritten signature]

[Handwritten signature]
22/05/18

[Handwritten signature]
Chief (BOT-IT)

[Handwritten signature]
Dobun

[Handwritten signature]
28/05/18
Major (Iftikhar Ali)
Assistant Secretary (NTISB-II)
Ph# 051-9204560

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

[Handwritten signature]
Dobun

[Handwritten signature]
29/05/18
Secy (IT)

[Handwritten signature]
Pr. putup
SP
30.5

[Handwritten signature]
SS (BOT-IT)

662/2-A

[Handwritten signature]

M(A)

M(IT) ✓

A.S (Rev. Div.)



Pakistan Revenue Automation (Pvt) Ltd.

Plot #: 156, Software Technology Park
Service Road (North), Sector: I-9/3,
Islamabad
Ph. 051-9259435, Fax: 051-9259356

No. PRAL/CEO/ 732

Date: 21-05-2018

Mr. Farooq Ahmad
Secretary (IT)
Federal Board of Revenue
Islamabad

Subject: ADVISORY – PREVENTION AGAINST 7-ZIP VULNERABILITY

Please refer to the subject cited above;

As per announcement from M/s Kaspersky via their website link
<https://threats.kaspersky.com/en/vulnerability/KLA11240/>, all employees of FBR should
be informed regarding the serious risk pose by 7-Zip file achiever software.

Enclosed please find Advisory Notice, which may be circulated within FBR with the
purpose of creating precaution and data safeguard awareness among FBR officials.

Additionally, as we are receiving frequent advisories from various security agencies/firms,
therefore it is suggested that these advisory notices may be posted online at FBR's
website as well, in order to keep FBR personnel aware of the latest cyber security threats.

M. Imran Amjad
Mohammad Imran Amjad
Chief Executive Officer

Encl: As above.

Asst. Secy
24/5

66728-11

