

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

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

Islamabad 22 Jul 2020

Subject: Prevention Against Indian APT Attack Group Sidewinder (Advisory No.12)

24 JUL 2020
M(A)

M(IT)

A.S (Rev. Div.)

Chief (IT)
Asst. Secy (IT-I)

1. Introduction. Since Jan 2019, a suspected **APT attack organization (Sidewinder / Rattlesnake) from India** is employing modern payloads through spoofed emails to target defense / government departments of Pakistan. Such emails portray topics as per the interest of target audience (ref NTISB Advisory No.22, 5 and 12) and contain a **malicious word attachment**. Downloading and opening email, displays a legitimate document in foreground but simultaneously executes a malicious code in the background providing unauthorized access of sensitive data / information to hacker.

2. Summary of Recent Attack

- a. Attack Vector. Phishing Emails, SMS, Social Media platforms & WhatsApp
- b. Email Subject. BGI 43 or can be any purporting to be related to work.
- c. Email attachment. Can be a word document.
- d. Antivirus Detection Rate. Nil
- e. File Size. 744 KB
- f. File Extension. .doc (Document File)
- g. Classification. Sidewinder APT Malware
- h. Detailed Info
 - (i) <https://s.tencent.com/research/report/479.html>
 - (ii) <https://mp.weixin.qq.com/s/CZrdsIzEs4iwlzEs4iwlzTzJH7Ubg>
 - (iii) <http://it.rising.com.cn/dontai/19658.html>
- i. Vulnerable Software. All versions of Microsoft Office Word (2007, 2010, 2013, 2016) till update.

3. C & C Servers

Ser	IP Address	Protocol	Country
a.	185.99.133.106	https (443)	New Zealand

FOR FAX Dy.No. 127799-R
 Received in Chairman's Sect.
 on 24 JUL 2020

4. Indicators of Compromise

- a. HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\atlas2.0
(Persistence Registry Key)
- b. C:\ProgramData\AtlasFiles2.0\Duser.dll
(MD5sum = 137e7200b0f0a24dcd1ec696302b286f)
- c. C:\ProgramData\AtlasFiles2.0\Atlas2.0
- d. C:\ProgramData\AtlasFiles2.0\rekeywiz.exe
- e. C:\ProgramData\AtlasFiles2.0\rekeywiz.exe.config

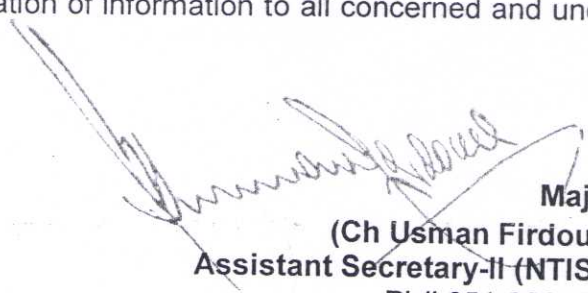
5. Capabilities of Malware

- a. Malware has capability to **bypass antivirus and windows** whitelisting.
- b. The Malware is specially designed for targeted attacks and can **steal backup files, stored usernames, passwords and present files (including word, excel, ppts and text documents etc.)**.
- c. It can **automatically executes** itself on **windows restart** and every instance of this malware has **extremely low detection rate**.

6. Recommendations

- a. All emails / messages must be scrutinized before opening attachments to avoid trap of social engineering.
- b. Execution of **mshta.exe, cscript.exe** and **wscript.exe** must be blocked on every system running in enterprise environment.
- c. **Execution of powershell and malformed commands or windows powershell altogether** must be blocked if not required.
- d. Implement strict **Software Restriction Policies / Application Whitelisting** to **block unsigned executables** running from %AppData%, *StartMenu\Programs\Startup* and %TEMP% paths.
- e. **Execution of unsigned executables** from sensitive web servers and endpoints must be blocked.
- f. **It is mandatory to enable 2 factor authentication on all your email accounts (Gmail, Yahoo, Hotmail etc) and social media accounts (Facebook, Whatsapp etc) especially interment banking** to prevent any sort of unauthorized access and financial loss.
- g. **Regular maintenance and updation of well reputed antivirus sol.**
- h. Mission critical systems should have genuine windows and updated Microsoft office products along with licensed Anti-virus.

- i. Any phishing / social engineering attempt must be reported on below email address for analysis and suggesting mitigation measures: -
asntisb2@cabinet.gov.pk
7. Forwarded for perusal and dissemination of information to all concerned and under command, 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

Copy to: -

1. Secretary to the Prime Minister, Prime Minister Secretariat, Islamabad
2. Secretary to the President, Aiwan-e-Sadar, Islamabad
3. Cabinet Secretary, Cabinet Division, Islamabad
4. Special Secretary, Cabinet Division, Islamabad
5. Secretary, NTISB, Cabinet Division, Islamabad
6. Deputy Secretary, NTISB, Cabinet Division, Islamabad
7. Director (IT), Cabinet Division, Islamabad