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

No. 1-5/2003 (NTISB-II) Islamabad 03 Dec, 2020

Subject: **Advisory - Prevention Against Cyber Espionage (Advisory No. 24)**

1. A malware is being spread through **social engineering tactics** targeting military and intelligence organizations including DAs abroad in a well-planned targeted manner. For this purpose, attackers have crafted a malicious MS-Word file that looks like a legitimate document being title **"Here_s what to expect from Biden on top nuclear weapons issues".** Downloading and clicking on the fake MS-Word document executes a malware in the background on the target system / computer, eventually, the victim machine is compromised and becomes prone to data exfiltration. The crafted MS-Word document mimics as a verified Microsoft software thus rendering it undetectable through anti-virus.

2. **Summary of Malicious Email**

a. **Subject.** Biden attitude on dealing with nuclear weapons.

b. **Downloaded File.** Here_s what to expect from Biden on top nuclear weapons issues.docx

b. **MD5 Hash.** b56c98106376f4704d5c45ba8c427c1b

e. **Malware APT Group.** SideWinder

f. **Vulnerability ID.** CVE-2017-11882

9. **Antivirus Detection Rate.** Low

h. **File Size.** 747 Kbs
File Extension. .docx

j. **C&C Servers**

Ser	URL address	IP Address	Country
(1)	recent.wordupdate.com	46.17.175.27	-
(2)	-	23.57.85.167	Italy
(3)	-	104.27.184.80	US
(4)	-	23.82.140.14	US
(5)	wordupdate.com	172.67.142.252	US

3. **Indicators of Compromise**

a. Files downloaded or rewritten from another process

(1) C:\intel\new.exe (self-copies)
(2) C:\users\appdata\temp\ellonak.xml executed through pkgmgr.exe
(3) Trojan:Win32/CryptInject named as dismcore.dll

b. Startup entry as **new.lnk** and C:\intel\new.exe

c. Creates Startup entry for persistence

(1) Key **new-lnk** with description as **JacaRg.dll** and value as **C:\intehnew.exe**

(2) Key **programs.bat** with value as **C:\users\pc\appdata\roaming\microsoft\windows\startmenu\lprogram\startup\program.bat**

(3) Key **windll** with value as **C:\users\pc\appdat\roaming\windll.exe**

4. **Capabilities of Malware**

a. The RTF based malware is specially designed for targeted attacks and can steal files and keystrokes (along with stored usernames / passwords) from windows system and browsers.

b. The adversary resists in system by creating several copies and several execution points of original sample.

c. The attacker can gain remote access of the system and can execute additional payload from it and run Microsoft certified files to evade antivirus detection.

d. The attacker ran malware through Equation Editor that read other registry keys for execution and transferred information through temporary files.

e. The malicious files are customized libraries is categorized as Ave_Maria stealer which executes through dll hijacking.

5. **Recommendations**

a. **Regularly update well reputed antiviruses** such as Kaspersky, Avira, Avast etc. and scan system regularly.

b. Update all software including Windows OS, Microsoft Office and all other on regular basis.

c. Uninstall all not in use applications and software from system and personal phone.

d. **Do not download attachments from emails unless you are sure about the source.**

e. Window Defender and Firewall of system to be kept on as recommended settings.

6. Forwarded for perusal and dissemination of information to all concerned and under command, please.

Major
(Ch Usman Firdous)
Assistant Secretary (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. Additional Secretary-II, Cabinet Division, Islamabad
5. Secretary, NTISB, Cabinet Division, Islamabad
6. Deputy Secretary, NTISB, Cabinet Division, Islamabad
7. Director (IT), Cabinet Division, Islamabad