Subject: **Advisory - Prevention Against Cyber Espionage (Advisory No. 59)**

Introduction. A malicious email; named as "**Overdue Invoice**" has been reported by various users. The email contains malicious. XLSX file that can **lure targets to provide bank details for payments**. Downloading and running he file executes malware in background, thus infecting the system.

2. Summary of Malicous Emails

a. **Name of Attachments.** Overdue Invoice.xlsx

b. **CV Index.** CVE-2017-11882

c. **Antivirus Detection Rate of Extracted files**

Ser	Files extracted	Detection percentage
1.	gave1.exe	12%
2.	vbc.exe	14%
3.	overdue Invocie.xlsx	10%

d. **Malware Type**. Exploit based Trojan

e. **C&C Servers**

Ser	URL	IP Address	IP Location
1.	pokhnaljank.com	194.36.173.171	USA
2.	ns1.jaobhaenrasam.com		
3.	ns2.jaobhaezrasam.com		
4.	jaobhaezrasam.com		
5.	atharabnday.com		

3. **Indicators of Compromise.** The malware makes following files on the infected system:-

a. C:\User\<admin>\Appdata\Roaming**vbc.exe**

b. C:\User\<admin>\Appdata\Local\Temp\Setup000009a4**OSETUP.DLL**

4. **Capabilities of Malware**

a. The malware is capable of getting system IP, user location, network configuration details, computer configurations and it can upload these details on its C&C server mentioned in para 2(e).

b. The malware has the ability to act as a key logger and steal the usernames and passwords of infected systems.

5. **Recommendations.**

a. **Install and update licensed and well reputed antivirus softwares.**

b. Block C&C Servers at para 2(e) in firewalls of own networks

c. In case indicators of compromise (para 3) are found in the system, please disconnect the computer from internet and reinstall windows.

d. Maintain and update OS and all softwares periodically.

e. Don’t download attachments from emails unless you are sure about the source.