PTA CERT for Telecom Sector

Security Advisory-No: Ext:166/59-30

04, Jan 2019

Threat Classification: Malware

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

Summary of Malicious 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 Invoice.xlsx	10%

d) Malware Type. Exploit-based Trojan

e) C&C Server

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

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

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 above.

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

Recommendations:

a) Install and update licensed and well-reputed antivirus software.

b) Block C&C Servers mentioned above in firewalls of own networks

c) In case indicators of compromise found in the system, please disconnect the computer from the Internet and reinstall windows.

d) Maintain and update OS and all software periodically.

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

f) Forwarded for perusal and dissemination of information to all concerned

g) In case of any incident, please report to this office.