Subject: **Prevention Against Cyber Espionage - Advisory No 03 January, 2018**

1. Introduction. A malicious url **"blocked.win"** is getting popular in WhatsApp groups and social media. The website claims that after installation of the (fake) application it can show you the contacts who blocked you on WhatsApp. The website asks the user to share its link with **14 users** or **7 WhatsApp groups** for downloading of malicious android executable, which will ultimately hack user's phone.

2. **Summary of Malicious Link**

a. **URL address.** blocked.win.

b. **Malicious File Name.** 9Apps_best.apk.

c. **Size of File.** 3.40 MB.

d. **Malware Type.** File Stealer Trojan.

e. **Spreading Mechanism.** WhatsApp Message Sharing.

3. **C&C (Command & Control) Servers**

Se	C&C URL	IP address	Hosting Country
a.	go.oclserver.com	-	-
b.	xns5.com/mac003.html	-	USA
c.	go.pushnative.com/ntfc.php	188.42.162.211 188.42.162.146 188.42.162.170 188.42.162.246	Holland
d.	free.promotrkon.com	99.198.108.194	USA
e.	**blocked.win**	**216.58.201.208**	**USA**

4. **Mode of Operation**

a. When a user clicks on the above mentioned link, it gets the users location upon visiting the website.

b. The link prompts the user to share this link with WhatsApp groups and friends.

c. The malicious link then traps the user into downloading a malicious apk file.

5. Recommendations

a. **Install and UPDATE well reputed antiviruses for android** Such as Avast, AVG etc.

b. Block ,C&C Servers at para 3 in firewalls of own networks.

c. Don't click on the link to restrict the advisory from getting the location.

d. Regularly update the android OS and its applications.