Subject **Prevention Against Cyber Espionage -Advisory No 12 March, 2018**

1. **Introduction.** Recently, malware writers are utilizing hacked websites for the generation of crypto-currencies to earn money. Hackers, embed malicious scripts into the compromised website so that they can make use of visiting user's CPU resources to mine crypto currency.

2. **Technical analysis**

   a. Malicious crypto mining scripts are embedded into the websites.

   b. The JavaScript code written into the function is designed mostly to mine **Monero** crypto-currency.

   c. Attackers mostly utilize **CoinHive online services** to embed JavaScript miner into compromised websites.

   d. Then the script can run directly from the browser to mine crypto-currency on the computers of the users who visit the website.

   e. When the user visits the website then his CPU's resources are utilized to the full potential at the time of browsing.

   f. Due to 100% utilization of CPU at the time of browsing via Android or windows system, this mining technique can damage the user's hardware including slow performance and reduced battery power.

3. **Reported Websites.** Following websites are reported to be infected by mining scripts. Shortly after the incident was reported, the developers of the said websites removed the malicious scripts:-

   a. COMSATS Institute of Information Technology (https://www.comsats.edu.pk/).

   b. PIA (http://www.piac.com.pk).

4. **Mitigation Measures.** Crypto-currency mining malware are rising in popularity at an exponential rate. Following best practices are suggested in this regard:-

   a. Continuously monitor CPU utilization if you are having problems with system performance while browsing websites, if CPU usage goes to 100% while surfing the Internet then close the browser and clear the browser cache to remove all traces of executing script.

   b. Use **"No Coin"** chrome extension and **"NoMinern** add on for FireFox to 'stop crypto mining.

   c. Make use of Adblook in both chrome and FireFox.

   d. Keep all the softwares, browsers, anti-malware solution and operating system up-to-date.