Pakistan Telecom Authority Headquarters, Islamabad

PTA Cyber Security Advisory No.:120 **11-12-2020**

Name: FireEye’s Red Team assessment tools recently Hacked

Summary:

It has been recently reported that a leading cybersecurity company “FireEye” has hacked by a sophisticated state-sponsored hacking group using novel techniques, as per their initial analysis of the attack. The attackers specifically targeted FireEye's assets and used tactics designed to counter both forensic examination and security tools that detect malicious activity.

For more details, please visit following links:

- https://www.fireeye.com/blog/products-and-services/2020/12/fireeye-shares-details-of-recent-cyber-attack-actions-to-protect-community.html
- https://www.fireeye.com/blog/threat-research/2020/12/unauthorized-access-of-fireeye-red-team-tools.html

Recommendations:

- FireEye has released many of countermeasures against reported malicious Red Team tools for publicly available technologies like OpenIOC, Yara, Snort, and ClamAV. These are available at following FireEye GitHub repository link: https://github.com/fireeye/red_team_tool_countermeasures
- It is highly recommended to utilized the FireEye’s GitHub repository which contains a list of Snort and Yara rules that can be used by the organizations and security professionals to detect FireEye's stolen Red Team tools when used in the attacks.

- It is also recommended to engage directly with FireEye’s partners for additional countermeasures of the aforementioned tools.

- Update all software including Operating Systems, Servers, web browsers etc. to the latest and stable versions with appropriate patches.

- Whenever required, access the system with minimal access rights and privileges.

- Maintain and implement a strong password policy throughout the infrastructure.

- Install, regularly maintain and update Antivirus solution from a well reputed vendor.

- Regularly provide Cyber security awareness trainings to the employees.

- Do not download attachments from emails unless they are from the trusted source.

- Avoid download/use of cracked and pirated software.

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