Subject: **Advisory – Prevention Against Multi – Vector Targeted Malware Campaign (Advisory No. 18)**

1. **Introduction.** A **spear phished email campaign** has been launched **against defense and government organizations of Pakistan** to gain access to their sensitive data. The email contains an **intelligently crafted legitimate** looking **fake / malicious link** (gov-pk.org) for downloading a **malicious document file**. Additionally, the domain also hosts a phishing link to hack email accounts of PAEC employees.

2. **Summary of Malicious Email Campaign**

   a. **Subject.** Cyber Policy 2019

   b. **Malware Download Link.** http.//pakcert.gov-pk.org/CNS Guidelines 2019.zip

   c. **Phishing Link.** http://mail.paec.gov-pk.org

   d. **Malware type.** HTA driven Powershell Infection

   e. **Antivirus Detection Rate.** Very low

   f. **Threat Level.** Critical

   g. **File Name.** Cyber_Security.docx.lnk

   h. **C & C Services**

Ser	C & C server URL	C & C IP address	IP Location
(1)	pakcert.gov-pk.org **(C&C server)**	185.208.209.162	Netherlands
(2)	mail.paec.gov-pk.org **(phishing link)**	185.183.99.201	Romania
(3)	gov-pk.org **(hosting domain)**	162.255.119.101	USA

3. **Capabilities of Malware**

   a. The malware downloaded from the link upon extraction and execution, invokes powershell and shows the victim a fake page in foreground and executes malware in background.

   b. If powershell executes successfully, it drops additional payload to infect the endpoint and exfiltrate data from it.

   c. Malware has the capability to steal documents from endpoint system.

4. **Recommendations.** In order to safeguard from this threat following is recommended: -

a. Blacklist / Block C & C servers mentioned in para-2(h) in firewalls of own network.

b. **Use limited privileges user on the computer** to deter malware infection from gaining administrative access or **allow administrative access only to system / network administrators**.

c. Make sure that both **endpoint based firewall and network based firewall are operational** in the organizational environment.

d. **Strict implementation of Software Restriction Policies (SRP) to block binaries executing from %APPDATA% and %TEMP% locations as most malware runs from these paths.**

e. Execution of Powershell / WSCRIPT in organizational environment should be strictly monitored. Ensure installation and utilization of the latest version of PowerShell and enable logging of it. For reference guide follow the instructions mentioned in link.

https://www.fireeye.com/blog/threatresearch/

2016/02/greater visibility.html.