

GOVERNMENT OF PAKISTAN  
CABINET SECRETARIAT, CABINET DIVISION  
NATIONAL TELECOM & INFORMATION TECHNOLOGY SECURITY BOARD  
(NTISB)

No. 1-5/2003 (NTISB-II)

Islamabad 25<sup>th</sup> June 2019

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

*M(A)*  
*M(I-T)*  
*A.S (Rev. Div.)*

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.

Summary of Malicious Email Campaign

- a. Subject. Cyber Policy 2019
- b. Malware Download Link. [http://pakcert.gov-pk.org/CNS Guidelines 2019.zip](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

*Send to PAEC*  
*As per practice*  
*upload*  
*on*  
*website*  
*1.7.2019*  
*2-7-19*  
*SS-11*  
*Send to file*  
*copy*  
*1857017*  
*2-7-19*

Ser	C & C server URL	C & C IP address	IP Location
(1)	<a href="http://pakcert.gov-pk.org">pakcert.gov-pk.org</a> (C&C server)	185.208.209.162	Netherlands
(2)	<a href="http://mail.paec.gov-pk.org">mail.paec.gov-pk.org</a> (phishing link)	185.183.99.201	Romania
(3)	<a href="http://gov-pk.org">gov-pk.org</a> (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.

FBR eDOX By No. 2098  
Received in Chairman's Sectt.  
on 28 JUN 2019

*chup 17/18/19*

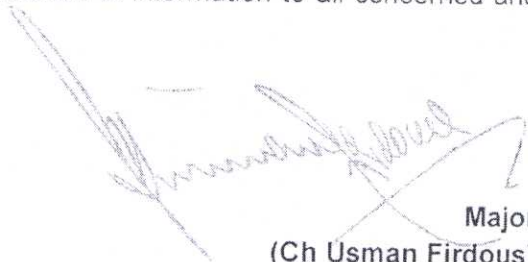
4. **Recommendations.** In order to safeguard from this threat following is recommended: -

- 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.

6. Forwarded for perusal and dissemination of information to all concerned and under command, please.



Major  
(Ch Usman Firdous)  
Assistant Secretary-II (NTISB)  
Tel#051-9204560

**All Secretaries of Ministries / Divisions of Federal Government and Chief Secretaries of Provincial Government.**

1. SPS to Cabinet Secretary, Cabinet Division Islamabad
2. PS to AS-III, Cabinet Division Islamabad
3. APS to Secretary, NTISB, Cabinet Division Islamabad
4. APS to Deputy Secretary, NTISB, Cabinet Division Islamabad