Pakistan Telecom Authority, Islamabad

PTA Cyber Security Advisory No: 075 **20-April-2020**

Name: New info-stealing Malware in the name of COVID-19

Threat Classification: Information Stealing Malware

Summary:

Cyber criminals have been reportedly probing the internet for vulnerable routers to compromise them and changing their DNS IP settings. Once the DNS IP addresses are changed to **109.234.35.230 and 94.103.82.249** as reported, then the user's browser requests are redirected to malicious webpages, offering users to install latest COVID-19 application, claiming to be from World Health Organization (WHO). The application is an info-stealing malware which, when installed, steals sensitive information like browser credentials, cookies, saved login credentials, Crypto-currency wallet passwords etc. and sends to the command and control (C&C) server.

Following are the reported IP addresses used in malicious COVID-19 themed webpages:

i. **176.113.81.159**
ii. **193.178.169.148**
iii. **95.216.164.181**

Indicators of Compromise:

Sr. No.	C&C Server	Repository URL
1.	whoer-vpn.net	https[:]//bitbucket[.]org/softup23/self/downloads/setup_who.exe
2.	emailonlinechase.com	https[:]//bitbucket.org/verify19/update19/downloads/setup_pr.exe
3.	emailonlinechase.com	https[:]//bitbucket.org/whoupd/s1/downloads/setup_who.exe
4.	emailonlinechase.com	https[:]//bitbucket.org/whoupd/s1/downloads/setup_who.exe

5.	whoer-vpn.net	https[:]//bitbucket[.]org/softup23/self/downloads/setup_who.exe
6.	whoer-vpn.net	https://bitbucket.org/softcov3/v1/downloads/file_signed.exe

Recommendations:

- Block following IP addresses at the Gateway level or network perimeter:
  i. **109.234.35.230**
  ii. **94.103.82.249**
  iii. **176.113.81.159**
  iv. **193.178.169.148**
  v. **95.216.164.181**
- Change the default credentials of your Router's control panel and disable the router's remote administration.
- Change the cloud account credentials (like Linksys etc.), or any remote management account of the router in order to mitigate brute-forcing or credential-stuffing attacks.
- Configure the router to receive DNS servers from your concerned ISP.
- Ensure to update the router to latest and stable firmware to prevent attackers from exploiting the unpatched vulnerabilities.
- Use licensed antivirus and regularly obtain its latest updates with its real-time scanning capabilities enabled.
- Only use licensed software and avoid download/use of cracked and pirated software.
- In case of any incident, please report to this office.