GENERAL HEADQUARTERS
ARMED FORCES OF THE PHILIPPINES
OFFICE OF THE DEPUTY CHIEF OF STAFF FOR COMMAND AND CONTROL, COMMUNICATIONS, CYBER INTELLIGENCE, SURVEILLANCE, TARGET ACQUISITION AND RECONNAISSANCE SYSTEMS, J6
Camp General Emilio Aguinaldo, Quezon City

CD-2202-045 25 Feb 2022

SUBJECT: **AFP Cybersecurity Bulletin 2022-02 "Wiper Malware"**

TO: **See Distribution**

1. References:

a. Cybersecurity & Infrastructure Security Agency (CISA) latest article dated 16 February 2022 regarding "Russian State-Sponsored Cyber Actors Target Cleared Defense Contractor Networks to Obtain Sensitive U.S Defense Information and Technology",
b. Harvard Business Review (HBR) latest article dated 24 February 2022 regarding "The Cybersecurity Risk of an Escalating Russia-Ukraine Conflict",
c. Microsoft latest article dated 15 January 2022 regarding "Destructive Malware Targeting Ukrainian Organizations".

2. Above references pertain to the report about the Ukraine's parliament and other government and banking websites being hit with another punishing wave of distributed-denial-of-service attacks. Based on the cybersecurity researchers, said unidentified attackers had also infected hundreds of computers with destructive malware. Relatedly, Symantec Threat Intelligence detected three (3) organizations hit by the Wiper malware. All three (3) targets had close affiliation with the government of Ukraine. In addition, the U.S Cybersecurity Infrastructure Security Agency (CISA) recently issued a warning of the risk of Russian cyberattacks spilling over onto U.S networks, which follows previous CISA warning on the risks posed by Russian cyber-attacks for U.S critical infrastructure.

3. ITR, be advised that all AFP offices/units are warned and reminded to be vigilant in monitoring and securing their respective ICT infrastructure, information systems, and personnel against the cyber-related activities in relation to the Russia-Ukraine conflict. Also, be vigilant against fake news and disinformation in social media.

4. Further, the AFP cyber units should BPT conduct accounting of readiness of cybersecurity incident response team (CSIRT), network administration monitoring and cybersecurity incident response to AFP networks and systems.

5. Moreover, be prepared on imminent cyber-attacks which might be exploited by cyber criminals which may result to internet outage, and other COTS services, and possible connectivity issues on GPS/SATCOM services if things will escalate relative to Russia-Ukraine conflict.

6. Likewise, the following cybersecurity best practices are recommended to strengthen the security of your respective ICT infrastructure and information systems and also to mitigate the risks of being attacked by the said malicious malware:

a. Ensure the conduct of patching on respective workstations and security systems to scan for the critical and high vulnerabilities that allow remote code execution or denial-of-service, especially the externally facing equipment.

b. Enhance the monitoring of network traffic, emails, and endpoint systems. This is to review the network signatures and indicators for focused activities, monitor for new phishing trends, and adjust the email rules in a timely manner.

c. Ensure that anti-malware software is installed and implemented in respective workstations to detect and prevent malicious files from executing and performing commands on workstations.

d. Be reminded on the use of official AFP email services and combat net radios in transferring and communicating classified information. Further, Secured Video Teleconferencing is advised to be used in conducting conferences.

e. Avoid clicking suspicious emails and downloading attachments from unknown websites and emails. This is to prevent malware infection which might compromise your devices.

f. Avoid downloading suspicious applications from unknown sources. These applications may be attached with malware that can compromise your devices.

7. Furthermore, all concerned Information Systems Officers/NCOs are reminded to include this information as part of the Troops Information and Education (TI &E) on all its subordinate units for enhancing the cybersecurity awareness of the AFP.

8. For information and reference.