MESSAGE FORM

(INSTRUCTION: FILL-UP BOXES INSIDE DOUBLE LINES ONLY)

FOR COMCEN/SIG USE

PRECEDENCE ACTION/PRECEDENCE INFO
"PRIORITY"

FM: CG, PA

TO: All Unit Commanders
Attn: G6/Signal Officer/IS Officer

INTERNAL: All G-Staff, Personal, Special & Tech Staff, C, AOC/SAGS/XA

INFO: CSAFP
Attn: J6

GROUP:
11 April 2017

SECURITY CLASSIFICATION:
CONFIDENTIAL

ORIGINATOR:
6/CMB 1104-99-2017

1. References:

   a. Command Guidance, and;
   b. VAPT and PANET Monitoring Result.

2. As per above references, forwarded is the Cybersecurity Bulletin Number **17-14** with topic regarding **How Can I Tell If I Have Malware and What Can I Do About It?**

3. ITR, all concerned G6/Signal Officers/Information System Officer/NCOs are reminded to include this information as part of TI & E on all of its subordinate units as part of enhancing the Cybersecurity Awareness of the Philippine Army.

4. For information and widest dissemination.

DRAFTER'S NAME AND TITLE	**PHONE NR:**
MAJ RENATO A LABIS (SC) PA Acting Chief, CMB, OG6, PA	6630
RreleaseR'S NAME AND TITLE COL VENER ODILON D MARIANO GSC (SC) PA AC of S for C4S, G6, PA	

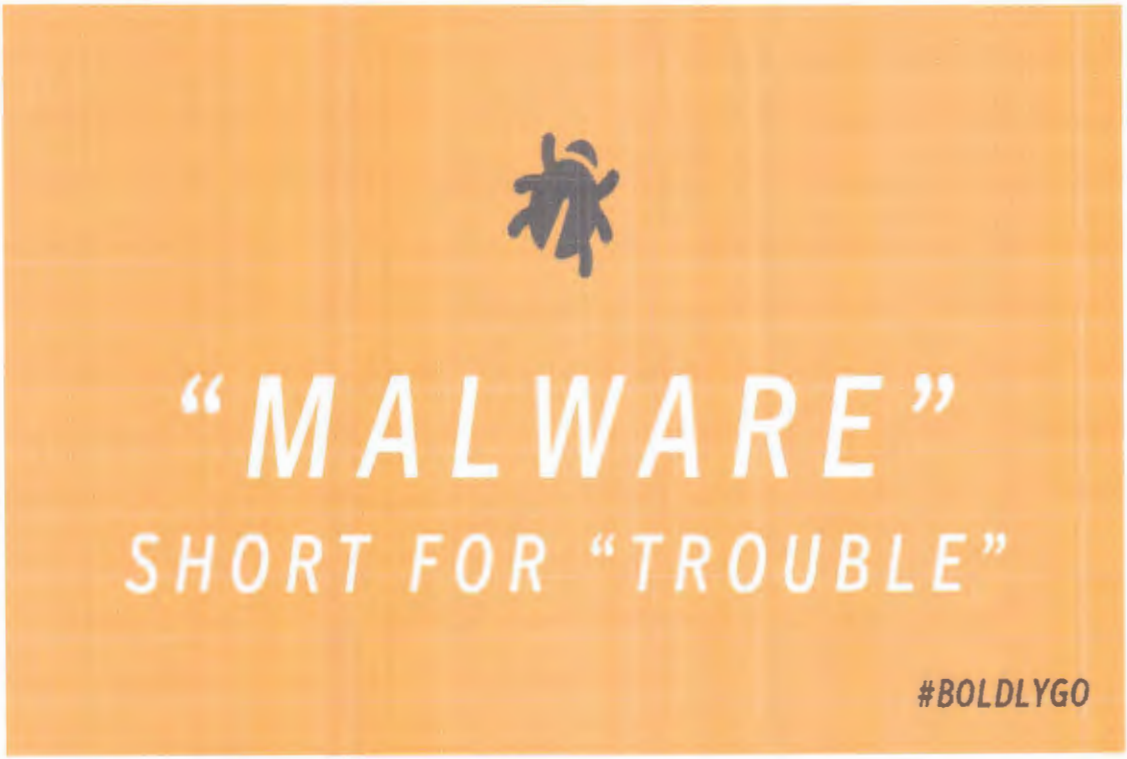
HEADQUARTERS
PHILIPPINE ARMY
OFFICE OF THE ASSISTANT CHIEF OF STAFF FOR
COMMAND AND CONTROL COMMUNICATIONS, AND CYBER SYSTEMS, G6
Fort Andres Bonifacio, Metro Manila

6/CMB 11 April 2017

CYBERSECURITY BULLETIN

Cybersecurity Bulletin: #17-14

How Can I Tell If I Have Malware and What Can I Do About It?



Malware has become a catchall term for various types of cybersecurity risks, such as viruses, Trojan horses, worms, adware, ransomware and spyware. Many of us use these terms interchangeably to describe strange symptoms or behaviors encountered on a computer. However, all of them share a common goal, which is to compromise the safety of your devices. Symptoms of malware may appear obvious or discrete; knowing how to detect these dangerous intrusions will help you determine how to go about fixing the problem should it ever occur.

Malware is short for malicious software and refers to programs specifically engineered to compromise the security features on a computer, allowing people to comb through your personal data and, in some cases, commit identify theft. If this sounds like something you want to avoid, join the club! Nobody wants malware on their computer. Learning to be proactive about your computer's security features is

the best way to avoid a malware intrusion. But first, let's take a look at a few red flags that can indicate a malware problem:

Signs of Malware

Most of the time, the presence of malware will be obvious even though you might not know how it got on your device. In fact, most people have no idea that malware has been installed until their computers start acting funny. You might notice a few changes on your computer including strange ads or pop-up windows—even when you're not surfing the web. You may also experience unwanted changes to your browser and a slower experience on your computer.

Specifically, watch out for ads that pop up a few seconds after a webpage is done loading. These ads will often contain inappropriate content, are difficult to close, and display flashing colors while blocking what you're trying to view. Take all of these signs seriously. If you suspect your computer has malware installed, turn it off immediately and disconnect it from the Internet.

How Did I Get Malware?

Malware is usually installed unintentionally as a result a few missteps taken by the user. Malware can be installed accidently by clicking on a link and hidden or masked by another software. This often happens when users download content from unknown or untrustworthy sources. Seemingly harmless downloads, like screen savers, toolbars, and torrents, are likely suspects.

Another reason you might find malware on your computer is because you neglected to update your anti-virus/malware software, operating system or other programs on your computer. Updating your security features is just as important as having them in the first place. If you don't have quality anti-virus or anti-spyware installed on your computer, you're at a higher risk of malware intrusion.

Malware, like a virus, can agitate problems exponentially. In other words, once you get malware on your computer, it may trigger more intrusions, which trigger more malware installs. The best thing to do is nip the problem in the bud as soon as you see any signs of malware.

How to Avoid Malware

- Computer security almost always begins with anti-virus/malware software. While this advice may be obvious to some, many computers don't have proper security software installed. Make this a priority on your computer; it's the best thing you can to do to avoid malware.

- Run periodic diagnostic scans with your anti-virus/malware software. You can set it up so the program runs scans automatically during regular intervals. Run a malware detection scan at least once a week, preferably at night so you won't need to use the computer.