# 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:
**26 April 2016**

SECURITY CLASSIFICATION:
**CONFIDENTIAL**

ORIGINATOR:
**6/CMB 2604-55-2016**

1. References:

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

2. As per above references, forwarded is the Cybersecurity Bulletin Number 056 with topic regarding **HOW TO DETECT MONITORING SOFTWARE ON YOUR COMPUTER.**

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:** |
|---|---|
| LTC JOEY T FONTIVEROS (INF) PA<br>Chief, CMB, OG6, PA | 6630 |
| **RreleaseR'S NAME AND TITLE**<br>COL VENER ODILON D MARIANO GSC (SC) PA<br>AC OF S FOR CEIS, G6, PA | |

HEADQUARTERS
PHILIPPINE ARMY
***OFFICE OF THE ASSISTANT CHIEF OF STAFF FOR COMMUNICATIONS, ELECTRONICS AND INFORMATION SYSTEMS, G6***
Fort Andres Bonifacio, Metro Manila

6/CMB

26 April 2016

## CYBERSECURITY BULLETIN

**Cybersecurity Bulletin: #56**

### HOW TO DETECT MONITORING SOFTWARE ON YOUR COMPUTER

The advancement of technology into everyday life means that spying software is no longer confined to the domain of professional snoopers, as is evident in the raft of commercial spying and monitoring software now widely available for use on home computers. And with this surge into the home market a hard sell is taking place, usually based on fear and suspicion of a cheating spouse, unregulated internet surfing of children etc. If you think someone is spying on you there are some simple steps you can take to find out.

#### Third-party software

This is usually known as remote control software or **virtual network computing (VNC)** software and it allows someone to see what you are doing on your computer. However, it needs to be installed on your computer in the first place.

By checking in the start menu you can see which programs are running. Go to All Programs and look to see if something like **VNC, RealVNC, TightVNC, UltraVNC, LogMeIn, GoToMyPC** and so on are installed. If any of these programs are installed, then someone can connect to your computer without you knowing it as long as the program is running in the background as a Windows service.

It might seem a bit sloppy to furtively install this type of software on someone's computer but many people assume that most people are ignorant about software on their computer and wouldn't understand what it is.

Usually, if one of the above listed programs is installed, there will be an icon for it in the task bar because it needs to be constantly running to work. Check all of your icons and see what is running. If you find something you're not familiar with, do a quick internet search to see what pops up.

That's said it's easy for monitoring software to hide the taskbar icon, so if you don't see anything unusual there, it doesn't mean you don't have monitoring software installed.

## Checking the ports

The above tasks are easy to carry out even for people without technical knowledge. If you've checked the installed programs and you're still reasonably suspicious that someone is monitoring you (and it's not the TV telling you so) then as a next step you can check the computer's ports.

There's no need to recoil in horror, running the rule over ports is reasonably straightforward. Ports are a virtual data connection in which computers share information directly, so if you've got spy software on your system, a port could be open to enable the data transfer.

You can check all the open ports by going to **Start, Control Panel, and Windows Firewall**. Then **click** on **'Allow a program or feature through Windows Firewall'** on the left hand side of the box. This will open another box and you'll see a list of programs with check boxes next to them.

The ones that are checked are 'open' and the unchecked or unlisted ones are 'closed'. Go through the list and see if there is a program you're not familiar with or one that matches VNC, remote control, and so on suggesting a spying program. If you do discover one, you can simply halt it in its tracks by **unchecking the box**; putting paid to the snooping misdeeds.

## TCP connections

However, if blocking spies was a simple as this, the spied upon would be rolling in clover and the spies would be scuttling off gnashing their teeth.

Unfortunately, it can be rather more complicated. Checking the ports is a necessary step and it may help identify and stop snoopware. However, in some cases the spying software may only have an out bound connection to a server.

In Windows, all out bound connections are allowed, which means nothing is blocked. If all the spying software does is record data and send it to a server, then it only uses an outbound connection and won't show up in the ports list mentioned above.

One way to check this is to analyse something called the **Transmission Control Protocol (TCP)** which will show you all the connections from your computer to other computers. It's not as technical as it sounds; it just requires a few careful steps.

Luckily you can download a **TCPView** program which shows all the TCP connections. You'll see a box which lists several columns. On the left side is the process name, which will be the programs running. You'll see things like Mozilla Firefox (or the browser of your choice), BullGuard and other programs. Look at the **'State'** column and you'll see processes listed under Established. This means there is currently an open connection.

What you need to do is filter out of the list the processes you don't recognize. BullGuard and Mozilla Firefox are to be expected but if there's something you don't understand you need to figure out what it is. This is made easy by simply doing an internet search for the process name. The search results will tell you whether the process is safe or not.

You can also check the Sent Packets and Sent Bytes columns, which instantly identifies which process is sending the most data from your computer. If someone is monitoring your computer, they have to be sending the data somewhere and you should see it here.

**Further help**

These are the basic techniques to establish whether you are being spied on via monitoring software that has been stealthily installed on your computer. And unless you're being snooped upon by an intelligence agency or someone with deep technical expertise, you should be able to 'out' the snoop software. If after carrying these steps you do still have suspicions then perhaps you ought to seek help from ASR (P) or OG6, PA .

**References:**

**This was cross posted from:**
http://www.bullguard.com/blog/2016/02/how-to-detect-monitoring-software-on-your-computer.html

**DO YOU WANT TO KNOW MORE? TALK TO US.**

**POCs:**

**a. LTC JOEY T FONTIVEROS (INF) PA** – Chief, Cyberspace Management Branch, OG6, PA at Landline Telephone Nr: 02-845-9555 Local 6630 and Mobile Telephone Nr: 0917-628-1057. Email: fontiverosjt@army.mil.ph.

**b. Sgt Mark Dave M Tacadena (SC) PA** – Branch NCO, Cyberspace Management Branch, OG6, PA at Landline Telephone Nr: 02-845-9555 Local 6630 and Mobile Telephone Nr: 0998-534-2877.