SIGNAL DIRECTIVE:	***Svc Directive NR***: OG3-131-16
ISSUING OFFICE: Regiment G3	***DATE ISSUED***: 15 Feb 16
TASKED UNIT: AUC	***DATE REQUIRED***: 27 Feb 2016

1. References:

a. Radio Message from CG, PA with Cnr 6/CMB 1002-41-2016 dtd 10 February 2016

b. Command Guidance, and

c. VAPT and PANET Monitoring Result

2. Per above references, forwarded is the Cybersecurity Bulletin Number 046 with topic regarding 5 Tips to Detect, Contain and Control Cyber Threats.

3. ITR, all concerned 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

8. For information and widest dissemination.

REFERENCE OF AUTHORITY:	***AUTHENTICATION***:
Regiment Commander, ASR	BY ORDER OF COL SANCHEZ
COORDINATING AUTHORITY: G3	LTC DEVEZA

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:
10 February 2016

SECURITY CLASSIFICATION:
CONFIDENTIAL

ORIGINATOR:
6/CMB 1002-41-2016

1. References:

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

2. As per above references, forwarded is the Cybersecurity Bulletin Number 046 with topic regarding **5 Tips to Detect, Contain and Control Cyber Threats.**

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 Chief, CMB, OG6, PA	6630
RELEASER'S NAME AND TITLE	
COL VENER ODILON D MARIANO GSC (SC) PA 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

10 February 2016

CYBERSECURITY BULLETIN

Cybersecurity Bulletin: #46

Five (5) Tips to Detect, Contain and Control Cyber Threats

As we move to reduce cyber dwell time, there are several fundamental concepts that should be considered. Listed below are five (5) practices that would help us decrease dwell time by detecting, containing and controlling cyber threats:

1. **Fundamental Security Controls.** The first step to protecting our network is ensuring our basic security controls are in place. By enacting **fundamental security controls** – such as **regular patching, restrictive administrative access, two-factor authentication, and network segmentation** where appropriate – the attacker is forced to invest greater resources in finding a way in. In the process of implementing best practice security controls, a core step should be to identify high-value targets – systems

and people vital to our success. These are the targets that adversaries most frequently want to exploit for financial or intellectual gain. Security monitoring should be elevated on these assets. Such an approach enables our cybersecurity teams to dedicate operational time to prioritize alerts while easing the process to apply focused controls on endpoints, network devices, or the high-value targets themselves.

2. **Granular Visibility and Correlated Intelligence.** A breach will occur regardless of the fundamental security measures in place. However, enterprises can withstand breaches by ensuring both have granular visibility of their network and enterprise communications. Enterprises should implement network monitoring functionality such as **Netflow** and collect logs from any device that records indemnity usage. This enables us to create red flags related to identity theft, data loss, and abnormal activity on a day-to-day basis. While these alerts are important, a critical capability lies in correlating actions to every machine or user, whether on or off the network. Detailed information relating to all incoming emails, such as full headers and even content, will allow cybersecurity teams to cycle back to the origin of the incident.

Forensic visibility is imperative when attackers breach the perimeter and internal security controls. With forensic data, we have an increased ability to trace threats back to their origin and to calculate dwell time. Dwell time is a new metric for incident responders and incidentally is the only one Forcepoint uses to measure its security posture.

3. **Continuous Endpoint Monitoring.** With continuous endpoint monitoring, we are able to cultivate a keen perception of people, processes, and machines – translating user activity on the end point to policies and vice versa in near real-time. When done right, the resulting contextual awareness allows security teams to stitch together the framework of an incident and correlate seemingly unrelated events. This means faster response times and less time spent doing traditional forensic work trying to understand attacker movements and intentions.

The majority of attacks start with the host or employee, so continuous end point monitoring is a major evolution in security posture, and critical for expedited incident response. This heightened insight into the end point allows for quicker detection of malware and abnormal behaviors of users. By not only looking for malware and paying attention to odd user activity, we will be able to reduce dwell time. This reduction in dwell time and forensics evidence will provide the ability to apply context and protect more than single systems.

4. **Actionable Prediction of Human Behavior.** Predicting attack profiles based upon an adversary's likely plan, a science within the broader topic of incident response, allows us to anticipate movements an attacker might take to access high-value targets. More specifically, by understanding the previous path of an attacker – where he/she previously traveled – security professionals can start to predict his/her future path.

This matters because the ability to predict future movement is critical to containing lateral movement and reducing dwell time. The cybersecurity team is better able to anticipate the next steps of an attack and isolate it. This is much like the game of chess, in that the adversary has multiple pieces on the board and has taken multiple moves. The attacker also has many more planned moves to create a checkmate scenario. Security professionals can determine steps they should take, such as taking certain resources off-line or notifying users to be on the lookout for odd behavior, to ensure that checkmate does not happen.

5. **User Awareness.** It is imperative that we educate personnel not only on policies and government mandates, but also on the growing risk that advanced threats pose to the organization. By launching formal educational programs, security professionals gain greater buy-in from end users, increasing the likelihood of changing risky behavior. Additionally, the security team must also be able to educate personnel in one-off situations such as when users become targets of threat actors.

When an attack is identified, successful or not, it is important to provide the targeted users with information about the attack so they can be aware of what future attacks may look like. If an attack is successful, security professionals should not punish the users, but realize that mistakes are going to occur. This is an opportunity to steer future actions in the right direction. In effect, users become human "Intrusion Detection Systems" and provide information that might otherwise be missed within the cybersecurity framework. No product on the market is going to find all malware or all bad user behaviors. With that said, if you combine good technology and processes with great people, enterprises amplify the ability to combat advanced threats, reduce dwell time, and detect lateral movements.

The longer attackers remain in the enterprise (longer dwell time), the more damage they can cause, and the more intellectual property they can steal. We should not focus solely on keeping attackers out, but on ensuring that the attacker stays in the network for as little time as possible — constantly striving to further reduce dwell time. Attackers may come back, but they will realize that their efforts are too costly and have

little return on investment. When attackers experience an enterprise attuned to dwell time, they quickly realize that even if they found an open door the enterprise would immediately detect them, and boot them out. They will then go somewhere else, in search of a less-protected enterprise.

References:

This was cross-posted from:

http://www.scmagazine.com/five-tips-to-detect-contain-and-control-cyber-threats/article/467856/

http://www.raytheon.com/capabilities/rtnwcm/groups/cyber/documents/content/rtn_269210.pdf

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. Email: tacadenamdm@army.mil.ph.