

-----Original Message-----

From: CuvIELlo, Peter M LTG DISC4
Sent: Thursday, August 23, 2001 11:08 AM
To: DISC4 Army CIO Executive Board; DISC4 MACOM IAPMs
Cc: Dmuchowski, Thaddeus A LTC(P) DISC4; Boutelle, Steven W MG DISC4; Borland, David SES DISC4; Hylton, James C BG(P) HQASC; Alexander, Keith B BG HQ INSCOM; Noonan, Robert W LTG ODCSINT; Chiarelli, Peter W. BG ODCSOPS; Sohm, Richard W Mr DISC4
Subject: Reverse Proxy Server Policy
Importance: Low

Reference SecArmy/Chief of Staff Army (CSA) Memorandum dated 8 August 2001, Subject: Army Knowledge Management (AKM) Guidance Memorandum Number 1.

1. Attacks on our computer networks are becoming increasingly more sophisticated. The recent Code Red worm is no exception. The automated attack features of the Code Red worm both confirm and warn us that we can expect more sophisticated and malicious payloads in the future. For Code Red, the Defense Information Systems Agency (DISA) was forced to shut down most access to DoD web pages (Inbound Port 80 traffic) from outside the NIPRNET in order to prevent an overload of our unclassified networks. As a result, many important functions, such as E-business, that requires INTERNET access were disrupted. While INTERNET access to Army web pages is now partially restored, in the future we can expect more disruptions unless protective measures are implemented.

2. To immediately increase our protective posture, this message directs that all mission essential, publicly accessible, Army web sites (e.g., sites that must be accessed from the INTERNET that can be affected by another Port 80 shut down) will be protected behind a currently operational, Army Computer Emergency Response Team (ACERT) certified Army "reverse web proxy server." The following instructions will be supplemented by more detailed implementing instructions issued by the ACERT/Army Network Operations and Security Center (ANOSC).

A. By 28 August 2001 MACOM and PEO/PM IAPMs will provide the ACERT with a prioritized list of all mission-essential web servers that must be accessed from the INTERNET. The list will identify which web sites are not protected as well as those already protected behind a "reverse web proxy server." Any web server that for technical reasons cannot be put behind a proxy server will be evaluated by the ACERT and ANOSC. The ACERT will recommend to the web site owner alternative security procedures necessary to protect the web server that must be implemented before INTERNET access to the web server will be allowed.

B. After 7 September 2001 the ANOSC/ACERT will begin shutting down INTERNET (Inbound Port 80 traffic) access at all Army security routers. As a result, Army web sites not behind proxy servers or otherwise protected with an approved alternative security solution, will not be available to personnel outside

the NIPRNET (the “.mil” domain).

C. Before a web server is put behind a proxy server or is allowed to be accessed from the INTERNET utilizing an alternative security solution, the following actions must be accomplished:

(1) MACOMs and PEOs/PMs must install all (not just Code Red) IAVA fixes for their server(s) before submitting them to the ACERT for connection behind a “reverse web proxy server.” The ACERT will scan the system(s) to verify that all fixes are in place. Systems that are not IAVA compliant for all IAVAs will not be put behind the proxy server and INTERNET access will not be allowed until compliance is verified.

(2) The web site must be registered in accordance with Army and DoD web policy on the Government Information Locator Service (GILS) web page, <http://sites.defenselink.mil>. MACOM and PEO/PM IA Program Managers must state that that GILS registration (registration takes 5-10 days to complete) has been initiated when the web site is submitted to the ACERT.

(3) Joint Task Force Computer Network Operations (JTF -CNO) requires all technical points of contact (system administrators) for all web sites be identified to the ACERT. To accomplish this, web site system administrators must register to the IAVA Compliance Reporting Database before a web site is put behind a proxy server or otherwise protected (see paragraph 4 and <https://information.assurance.us.army.mil> for further information).

3. Beyond the immediate fixes outlined above, this message directs development, not later than 30 August 2001, of an Army enterprise-wide, centrally managed, reverse web proxy server acquisition and consolidation plan to protect all Army publicly accessible web sites. The plan will be developed in accordance with (IAW) and to support goals 1,3, and 4 of reference above. The HQDA, ODISC4, IA Office will contact selected MACOMs and PEOs/PMs to assist in developing and funding the centrally managed, web proxy server enterprise consolidation strategy. The POCs for this action are LTC John Quigg, phone (703) 604-8377 (DSN 664), email: <mailto:john.quigg@hqda.army.mil> and Roy Lundgren, phone (703) 604-7579 (DSN 664), email: <mailto:leroy.lundgren@hqda.army.mil>.

4. Finally, we must fix what we know is broken and that is compliance with ACERT issued Information Assurance Vulnerability Alert (IAVA) messages. IAVA requires the personal involvement of commanders at all levels in taking charge of how well their commands implement the Army's IAVA process. The Army currently has the highest rate of Code Red infections. Much of this is a “self-inflicted wound.” On 21 June 2001 the ACERT identified the vulnerability that Code Red exploits and published an IAVA message that mandated the fix that all MACOM and PEO/PM system administrators were required to complete.

This did not happen and now we are attempting to recover from damage and disruption caused by organizations that failed to comply with the IAVA process. I ask commanders at all levels direct their IA Program Managers/Officers to brief them on their command's IAVA compliance status. By 14 September 2001, I will send an Army CIO message directing the use of a consolidated, enterprise-wide IAVA compliance and critical infostructure reporting database. This database will not only assist commanders in achieving greater accountability in reporting IAVA compliance, but will provide the Army, its MACOMs, and PEOs/PMs with a more accurate assessment of critical infostructure assets and training, e.g., types of servers and the training status of our information technology (IT) professionals. The Army POCs for the IAVA/critical infostructure asset reporting database are Ron Sturmer, phone (703) 604-6870 (DSN 664), email: <mailto:ronald.sturmer@hqda.army.mil> and Ralph Lowenthal, phone 607-5886 (DSN 327), email: <mailto:ralph.lowenthal@hqda.army.mil>.

5. Some commands “may” have obtained unauthorized commercial INTERNET access as “field expedient” workarounds. These unprotected “backdoors” into the NIPRNET violate DoD policy, compromise the overall security of the Army’s and DoD’s networks and systems, and will be identified and terminated. If your command has an unauthorized connection(s), take action to immediately terminate that access capability. The Army POC for alternative connections resolution is Mr. Bill Buzinski, phone (703) 607-5888 (DSN 327), email: <mailto:william.buzinski@hqda.army.mil>.

6. The VCSA, in his 160453Z January 2001 message, again stated the Chief of Staff, Army’s position that keeping Army systems and networks secure and operational is “a force protection issue and compliance with the IAVA process is mandatory.” Your system administrators and network managers are fighting a cyber war daily. In the cyber battle space it truly takes only a very few who do not do their jobs to put us all at risk. Take for action.

PMC

Pete Cuvillo
LTG USA
DISC4/CIO