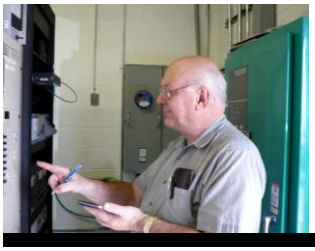


The
Broadcasters' Desktop Resource
www.theBDR.net ... edited by Barry Mishkind – the Eclectic Engineer

EAS Q&A

Secure EAS Codecs Prevent Zombie Attacks

With Barry Mishkind and Ed Czarnecki

[June 2013] As of June 11th it will have been four months since the "Zombie EAS Alert." Perhaps you are wondering the status of the investigation and what has been done to prevent a re-occurrence.

We asked Ed Czarnecki from Monroe Electronics about what is known and what has been done.

BDR: Could you recap for us what happened during that "Zombie" alert?

Ed C.: From what we know, this particular incident was made possible by two combined issues (1) leaving factory default passwords in place, and (2) leaving the devices connected directly to the public Internet – without firewalls or any other network security protections.

These two factors together left several systems open to someone simply logging into the devices and issuing the infamous "zombie" messages.

BDR: Is there any way this attack could have been avoided?

Ed C.: If there had been a firewall and a non-default password, it would not have happened.

BDR: Was this an example of a problem with the CAP Server?

Ed C.: No. The IPAWS CAP service was not involved. This was an attack on the end points of the system at a few individual stations.

BDR: What steps do you recommend broadcasters should take to protect their systems?

Ed C.: By and large, the broadcasting community has already taken efforts to protect themselves, but attacks and exploitations are going to be ongoing reality.

Two important preventive actions are to get the latest version of software installed on the CAP EAS device, and get the device behind a firewall. Broadcasters should check in periodically with the manufacturer to see if there have been any additional software updates.

BDR: So, was all that buzz and warnings from the FCC and FEMA about changing passwords not enough?

Ed C.: The advisory to change passwords back in February was important, but it is really part of a larger security discussion.

Anyone who is familiar with the constant flow of software updates to patch vulnerabilities in operating systems, browsers, etc. will understand why CAP EAS devices need to be behind a firewall, and running the latest version of software. Changing passwords had to do with a specific type of unauthorized access that happened during the "zombie attack."

The advisory to change your default passwords was valid - it still is - and was in response to a specific situation a few months ago. But making sure your software is updated and your network connections are secured remains critical.

BDR: So, what has Monroe Electronics done to prevent a repetition of February's attack?

A: For our part, our latest periodic software release for the DASDEC includes a cumulative security update.

We have also been contacting those users that left their equipment connected directly to the public Internet, to urge them to both get their equipment secured behind firewalls, and apply the software update. These are simple but critical matters of IT security.

We have been reaching out all of our customers to impress upon them the importance of applying our latest version 2.0-2 update, as well as keeping their CAP EAS gear and network connections behind a firewall. We have also changed the method of distributing our software. This has been ongoing for some time now.

BDR: You mentioned your software version 2.0-2, released this spring. Could you talk a bit more about how it addresses the potential for unauthorized access?

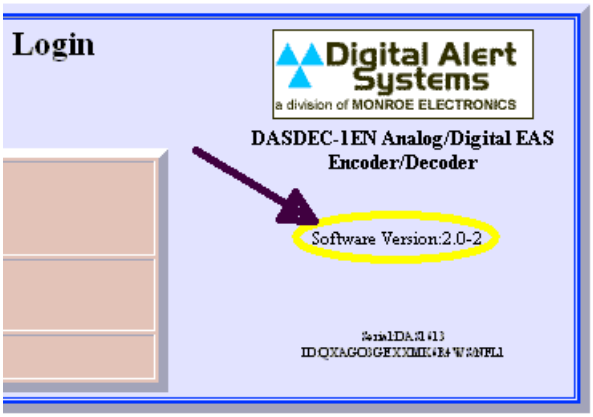
Ed C.: We periodically release software updates, which is why it is generally important for customers to check with us periodically to be sure they have the most current release.

Our current release was issued on April 24th, and it in-cludes a number of very good feature enhancements, a cumulative security update, and a few adjustments to en-hance the connection to the IPAWS system.

Version 2.0-2 also removes several areas of possible risk. We are just working proactively to head off any potential issues.

BDR: How does as station know if they have the current update and are protected?

Ed C.: The DASDEC log in screen will display the installed version 2.0-2 on the right hand side of the interface.



If an earlier version is running, the customer should immediately contact our tech support team at support@digitalalertsystems.com for instructtions on how to access the software and release notes.

BDR: Let go back to the February "Zombie Alert." What are the chances this could happen again?

Ed C: The simple answer is that unless everyone continues to do their part, eventually something could happen somewhere, even if not a Zombie-like attack.

Leaving CAP EAS equipment exposed on the public Internet is inappropriate, as most broadcasters understand already. We have advised that this equipment and all other station network connections should at least be behind a firewall.

The FCC and FEMA have both have issued similar guidance. The FCC issued an advisory soon after the Zombie incident stressing the importance of firewalls, password discipline, and other basics.

Recently, the FEMA also reminded the EAS community of the importance of applying the

manufacturers' most recent software updates, and generally use good operational and IT security practices.

And to repeat, the users need to ensure that the latest software is on their CAP EAS equipment, as the FEMA suggests. These systems are periodically updated for feature enhancements, "bug fixes" and security patches.

In this regard, CAP EAS manufacturers are no different than any other software-based appliance providers.

BDR: Can you tell us about any government investigation into the attacks? Has there been any news?

Ed C: I am sorry to say I do not really have any information that I can share.

These past few months have been an interesting experience. We have been proactive in giving detailed briefings and working to coordinate with several Federal agencies, including the FCC, the FEMA, the DHS cyber-security group, as well as CERT. We have also been in contact with Federal Law Enforcement. The FCC and FEMA have been great to work with so far.

BDR: Back in 2011, your company issued a white paper on network security for broadcasters. What is in it and is it still available?

Ed C: It takes more than software updates to protect a company. There should be a security policy in place that aims at minimizing risks to each organization's internal network. Because CAP EAS appliances are connected to the Internet, additional security measures are strongly suggested to ensure the safety of both the device and your network.

Stations should also employ additional tools to defend the device and the internal network, such as firewalls, antivirus, proxy servers, intrusion protection and detection, and so on. Our white paper – available here – discusses this in terms of the idea of a boundary or perimeter defense. The security conversation, including policies for software, access, and control, is something that needs more attention in the broadcast sector.

BDR: In your opinion, what is the next step?

Ed C: Training is important so people can learn what is critical. And not just for the engineers. It is just a fact or life, not just for CAP EAS, but for all business operations in general.

Management needs to understand and buy into the need for security – *and support their engineering and IT departments.* There is more to it than buying a firewall or antivirus. Entities like the NAB and SBE should be in the forefront of increasing education and support. The end result needs to be an improved culture of operational and cyber security in the industry, including among manufacturers.

- - -

Ed Czarnecki Ph.D. is the Senior Director for Strategy, Development & Regulatory Affairs for Monroe Electronics/Digital Alert Systems in Lyndonville, NY. You can contact Ed at: ed.czarnecki@monroe-electronics.com

- - -

Return to The BDR Menu