Broadcasters blame zombie hack on easy passwords

Jim Finkle, Reuters

(Reuters) - Poor password security allowed hackers to broadcast a bogus warning on TV networks that the United States was under attack by zombies, broadcasters said, and one expert in the technology said the emergency channel they broke into remained vulnerable.

The attacks on Monday on a handful of stations prompted the government to order broadcasters to change passwords for the equipment that authorities use to instantly push out emergency broadcasts through what is known as the Emergency Alert System, or EAS.

The FCC would not comment on the attacks, but in an urgent advisory sent to television stations on Tuesday the agency said: "All EAS participants are required to take immediate action."

It instructed them to change passwords on equipment from all manufacturers that forces emergency broadcasts on to television networks, interrupting regular programming. It instructed them to make sure that gear was secured behind firewalls and to also inspect systems to ensure that hackers had not queued "unauthorized alerts" for future transmission.

The attacks came at a time when officials and outside security experts are warning the United States is at risk of a cyber attack that could cause major physical damage or even cost lives. President Barack Obama [1] has told Congress that some hackers are looking for ways to attack the U.S. power grid, banks [2] and air traffic control systems.

While the zombie hoax appeared to be somewhat innocuous, the fact that hackers could easily broadcast an emergency message showed that they might be able to wreak havoc with more alarming communications.

"It isn't what they said. It is the fact that they got into the system. They could have caused some real damage," said Karole White, president of the Michigan Association of Broadcasters.

White and her equivalent in Montana, Greg MacDonald, said they believed the hackers were able to get in because stations had not changed the default passwords they used when they shipped from the manufacturer.

The "zombie" hackers targeted two stations in Michigan, and several in California, Montana and New Mexico [3], White said.

A male voice addressed viewers in a video posted on the Internet of the bogus warning broadcast from KRTV in Great Falls, Montana, a CBS affiliate: "Civil authorities in your area have reported that the bodies of the dead are rising from the grave and attacking the living."

The voice warned not "to approach or apprehend these bodies as they are extremely dangerous."

STILL VULNERABLE

Larry Estlack, chairman of the Michigan Emergency Alert System, told Reuters that passwords sometimes do not get changed because the EAS uses equipment that is not easy to set up.

"Some people have trouble getting through the setup procedure. It is fairly complex," he said.

But Mike Davis, a hardware security expert with a firm known as IOActive Labs, said there were other ways to remotely access the systems that would allow hackers to bypass password checks even if they were changed.

Davis said he had submitted a report to the Department of Homeland Security's U.S. Computer Emergency Readiness Team, or US-CERT, about a month ago that detailed security flaws in EAS equipment that he warned make it vulnerable to attacks.

"Changing passwords is insufficient to prevent unauthorized remote login. There are still multiple undisclosed authentication bypasses," he told Reuters via email. "I would recommend disconnecting them from the network until a fix is available."

Davis also said he was able to use Google [4] Inc's search engine to identify some 30 systems that he believed were vulnerable to attack as of Wednesday morning.

Officials with US-CERT could not be reached.

Bill Robertson, vice president of privately held electronics [5] manufacturer Monroe Electronics of Lyndonville, New York, told Reuters that equipment from his company had been compromised in at least some of the attacks after hackers gained access to their default passwords.

Monroe publishes the default passwords for its equipment in user manuals that can be accessed on its public website.

Robertson said that he believed attackers had been able to access the devices over the Internet because television stations had not properly secured the equipment behind fire walls, which is what Monroe recommends.

"The devices were not really locked down right. They were exposed," he said.

He said that the company is working to beef up security on the equipment and may update its software [6] so that it forces customers to change default passwords.

"They were compromised because the front door was left open. It was just like saying 'Walk in the front door,'" he said.

Federal Emergency Management Agency spokesman Dan Watson said the breach did not have any impact on the government's ability to activate the Emergency Alert System.

(The story is corrected to change "his" to "her" in the eighth paragraph)

(Reporting by Jim Finkle; Editing by Lisa Shumaker and Patrick Graham)

Source URL (retrieved on *12/19/2013 - 11:46am*):
http://www.ecnmag.com/news/2013/02/broadcasters-blame-zombie-hack-easy-passwords?qt-most_popular=0&qt-recent_content=0

Links:
[1] http://www.reuters.com/people/barack-obama?lc=int_mb_1001
[2] http://www.reuters.com/sectors/industries/overview?industryCode=128&lc=int_mb_1001
[3] http://www.reuters.com/places/mexico?lc=int_mb_1001
[4] http://www.reuters.com/finance/stocks/overview?symbol=GOOG.O&lc=int_mb_1001
[5] http://www.reuters.com/sectors/industries/overview?industryCode=104&lc=int_mb_1001
[6] http://www.reuters.com/sectors/industries/overview?industryCode=174&lc=int_mb_1001