THE HOMELAND SECURITY *NEWS CLIPS*

PREPARED FOR THE DEPARTMENT OF HOMELAND SECURITY BY BULLETIN NEWS WWW.BULLETINNEWS.COM/DHS

TO: THE SECRETARY AND SENIOR STAFF

DATE: THURSDAY, JUNE 16, 2011 7:15 AM EDT

TODAY'S EDITION

[redacted]

[redacted]

CIA Web Site Hacked; Group LulzSec Takes Credit (WP)

By Ellen Nakashima

Washington Post, June 16, 2011

The hacker group LulzSec claimed credit Wednesday for taking down the CIA's Web site for a couple of hours, the latest in a string of embarrassing Web site disruptions the group has pulled off — apparently more to poke fun and highlight vulnerabilities than to cause real damage.

At 5:48 p.m., LulzSec, which dubs itself "the world's leaders in high-quality entertainment at your expense," posted an alert on Twitter: "Tango down — cia.gov — for the lulz."

The site was back up by 8 p.m.

But the fact that the group could penetrate Web sites and harvest system administrators' credentials underscores the risks of failing to secure sites, experts said.

"Web sites are the low-hanging fruit," said Richard Stiennon, a cyber expert and author of "Surviving Cyberwar." "But the Web sites are running on a server. Once you completely own the server that the Web site is on, you can watch the insiders log in and record their activity, and that can be a front door into the organization."

In recent weeks, LulzSec has claimed credit for hacking or bringing down Web sites belonging to PBS, Sony, the U.S. Senate and the Atlanta chapter of InfraGard, a public-private partnership between the FBI and the private sector dedicated to sharing information and intelligence to prevent hostile acts against the United States.

In the case of InfraGard, LulzSec stole and published 180 user names, passwords and e-mail addresses of members. When it hacked the Senate site, it published the user names and passwords of system administrators — enough to show that the group had done it.

LulzSec, Stiennon said, spun off from Anonymous, another hacker group that has claimed responsibility for

Web site attacks against organizations that it perceived as hostile to WikiLeaks, an anti-secrecy Web site that has published massive amounts of leaked U.S. government documents.

Anonymous, in turn, he said, spun off from users of 4chan, a collection of uncensored online message boards — a site "for hackers and geeks to hang out."

"LulzSec's motivation appears to be to doing it for grins and giggles," he said. "This is a very old hacker mentality, which is if you're vulnerable, you're stupid and deserve to be embarrassed and taken out."

LulzSec, which also calls itself "The Lulz Boat," has a somewhat "anarchistic" agenda, he said. "They're against government control of information, much as they're against media control of music and movies."

Last month, after PBS's "Frontline" ran a documentary on WikiLeaks that LulzSec perceived as unfair, the group hacked into PBS's site and posted a fake article claiming that rapper Tupac Shakur was alive and living in New Zealand.

The assault on the CIA was by denial of service, or overloading the site's server with requests for access.

CIA spokeswoman Marie Harf said the agency is "looking into these reports."

Similar denial-of-service attacks were carried out against Sony gaming sites last week. LulzSec claims to have 1 million user names and passwords for subscribers to these sites, Stiennon said.

As opposed to being "uber hackers working for a foreign agency," LulzSec basically publishes its findings for entertainment, he said. One sign it might be working, he said, is that the group has more than 158,000 followers on Twitter.

Just this week, it posted a hotline number on its Twitter feed to take suggestions for what sites to hack next.

[redacted]

Hackers Claim Hit On CIA Website (AFP)

By Glenn Chapman

AFP, June 16, 2011

SAN FRANCISCO (AFP) – A hacker group was brazenly ramping up its antics as waves of cyberattacks targeting even the US spy agency expose how poorly defended many networks are against Internet marauders.

"It's becoming a big problem, because at the end of the day these guys are doing whatever they want," said Panda computer security labs technical director Luis Corrons. "This is showing us that we have a long way to go to protect our systems and our information."

The public website of the US Central Intelligence Agency (CIA) on Wednesday joined a growing list of hacker targets that has included Sony, The International Monetary Fund, and Citibank.

The CIA told AFP it was looking into reports that cia.gov was knocked offline temporarily by a hacker group calling itself Lulz Security.

Lulz has claimed in recent weeks to have cracked into Sony, Nintendo, the US Senate, the Public Broadcasting System news organization, and an Infragard company that works with the FBI.

The group is flaunting its notoriety with a telephone hotline for people to call and suggest targets for cyberattacks.

"Our number literally has anywhere between five and 20 people ringing it every single second," members of the group said in a message on their @LulzSec Twitter account.

Setting up a telephone hotline was "kind of eccentric" given that the hackers could have easily created an online forum asking for targets, according to Corrons.

"These guys are upsetting a lot of people," Corrons said. "They think they will never be caught, and that could be their biggest mistake."

Lulz has seized the spotlight amid unrelenting reports of cyberattacks with apparent motivations ranging from spying and profit to glory and activism.

"As we get more connected more of the time, the number of potential attackers is growing because anyone can do it from anywhere in the world," Corrons said. "As the number of potential attackers grows, the number of successful attacks grows."

Hacker group Anonymous, from which Lulz is believed to have formed, gained notoriety with cyberattacks in support of controversial website WikiLeaks.

Unlike cyber criminals who amass armies of "zombie" computers by stealthily infecting machines with viruses, people volunteered to install software in support of Anonymous campaigns, according to Corrons.

"Anonymous has been out there for years," Corrons said, noting the group had launched attacks on music or movie firms taking people to task for pirated songs or films.

"When the WikiLeaks case came, they reacted fast and gained a lot of popularity," he said.

Anonymous used a tried and true distributed-denial-of-service (DDoS) attack that overwhelms websites with simultaneous requests for pages or other bits of content.

At times about 5,000 computers, each firing off about 10 requests per second, took aim at websites for Anonymous, according to Spain-based PandaLabs.

"There are not so many people now as there were a few months ago; I see fewer people connected," Corrons said of Anonymous. "Maybe people are realizing that you can protest, but this is not the best way."

Lulz may be related to Anonymous, but its tactics are more sophisticated.

Lulz cracks computer system defenses instead of simply flooding websites with page requests.

"In the Lulz group, they know what they are doing when it comes to breaking into places," Corrons said.

"It's their way to say the security here sucks and we are going to show you why," he continued. "Based on the way they act, I would say they are young people."

Other attacks reported in recent months, such as those on the IMF, weapons maker Lockheed Martin, and Gmail accounts connected to Chinese activists, bore signs of being the work of spies with political or financial objectives.

"This is showing us that we have a long way to go to protect our systems and our infrastructure," Corrons said. "This is a failure from private companies and even security companies -- there is a lot of room to improve."