

Brazen, publicity-seeking hackers on attack spree

June 24 2011, By RAPHAEL G. SATTER and PETER SVENSSON ,
Associated Press



In this Monday, May 31 2011 file frame grab of the PBS website, as PBS officials confirmed its official Twitter account that the website had been hacked. Lulz Security has stolen mountains of personal data in about a dozen different hacks, embarrassing law enforcement on both sides of the Atlantic while boasting about the stunts online.(AP Photo, File)

(AP) -- Can you be famous if no one knows your name? A new band of hackers is giving it its best shot, trumpeting its cyber-capers in an all-sirens-flashing publicity campaign.

Lulz Security has stolen mountains of personal data in a dozen different hacks, embarrassing [law enforcement](#) on both sides of the Atlantic while boasting about the stunts online.

The group, whose name draws on Internetspeak for "laughs," has about

270,000 followers on the messaging site [Twitter](#). Although LulzSec has declined interview requests, it has laid out its prankster philosophy in "tweets" and press releases.

"Vigilantes? Nope. Cyber terrorists? Nope. We have no political motives - we do it for the lulz," the group said in a message sent shortly after it emerged in early May.

LulzSec's Twitter mascot is a black-and-white cartoon dandy that looks like a cross between Mr. Peanut and The New Yorker magazine's monocle man. Its rambling messages are peppered with references to YouTube sensation Rebecca Black, the Dungeons and Dragons role playing game and tongue-in-cheek conspiracy theory.

One of LulzSec's victims says the group sets itself apart from the rest of the hacker underground with its posturing and bragging on Twitter.

"Most of the hacker groups that are pretty well known out there ... don't really like to flaunt their findings. They'll do it among their peers, but not typically the public," said Karim Hijazi, a security expert whose emails were ransacked by the [hacking group](#) last month.

LulzSec made its name by defacing the site of the U.S. Public Broadcasting Service, or PBS, with an article claiming that rapper Tupac Shakur was still alive. It has since claimed hacks on major entertainment companies, FBI partner organizations, a pornography website and the Arizona Department of Public Safety, whose documents were leaked to the Web late Thursday.

Many attacks have yielded sensitive information including usernames and passwords - nearly 38,000 of them, in the case of Sony Pictures. Others appear to have been just for kicks. In a stunt last week, LulzSec directed hundreds of telephone calls to the customer service line of

Magnets.com, a New Jersey-based manufacturer of custom refrigerator magnets.

LulzSec uses a similar technique to temporarily bring down websites, flooding them with bogus Internet traffic. This is an old hacker standby that doesn't require much sophistication. Members also break in to sites to steal data. That requires more skill and often involves duping employees into revealing passwords.

LulzSec's actions against government and corporate websites are reminiscent of those taken by the much larger, more amorphous group known as Anonymous. That group has launched Internet campaigns against the music industry, the Church of Scientology, and Middle Eastern dictatorships, among others.

Both are fiercely protective of the secret-busting site WikiLeaks. The hacking groups' supporters share the same brand of offbeat humor inspired by Internet catchphrases and viral videos.

LulzSec has repeatedly insisted on its independence.

"We're not AnonOps, Anonymous, a splinter group of Anonymous, or even an affiliate of Anonymous," the group has said. "We're LulzSec."

An Anonymous member told The Associated Press that he believed LulzSec was formed by people from Anonymous who got tired of the time it took to reach consensus and launch hacking projects. He said that they also wanted to go beyond the ethical boundaries of Anonymous.

"They wanted to go on more adventurous, brazen hacking adventures and really get their names out there," he said. He spoke on condition that his name is withheld given the pressure being put on Anonymous members by law enforcement.

Judging by the timing of its [tweets](#) and other communications, he believes that LulzSec is based mainly in the eastern half of the U.S., but a few members are European. The number of members is not known, but there appears to be no more than a handful, perhaps a dozen.

Anonymous also uses Twitter as a soapbox, but more as a way of recruiting helpers than publicizing its exploits. It's also been more selective about its targets. It attacked the Egyptian Ministry of Information's website during the revolution in the country, but has shied away from leaks of ordinary user information, for example.

There's every sign authorities are paying attention to the new group, although it isn't clear how much progress they've made in tracking the hackers down. On Tuesday, 19-year-old Ryan Cleary was arrested as part of a joint FBI-Scotland Yard investigation into hackings linked to both LulzSec and Anonymous.

British Police Commissioner Paul Stephenson described Cleary's arrest as "very significant," although LulzSec has shrugged off the development - and promised more spectacular hacks.

The Anonymous member believes law enforcement has little chance of finding LulzSec. He told the AP that LulzSec likely used such methods as logging on only from public Wi-Fi hotspots. Police could possibly trace the attacks to the hotspot, but by the time they get there, any hacker would be long gone.

Hijazi believes LulzSec harassed him because his firm, Unveillance, tracks "botnets" - clusters of computers that can be controlled remotely because they've been infected with malicious software. The botnets, each of which can have more than a million computers, are usually controlled by cybercrime gangs.

He speculates that LulzSec wants botnets because it would boost its power to bring down websites. But the group would be stepping on the toes of some very dangerous people if members started taking over botnets, he said.

"It's going to make everyone really mad, both the good guys and some really big bad guys," he said. "I hope law enforcement finds them first."

©2011 The Associated Press. All rights reserved. This material may not be published, broadcast, rewritten or redistributed.

Citation: Brazen, publicity-seeking hackers on attack spree (2011, June 24) retrieved 23 April 2024 from <https://phys.org/news/2011-06-brazen-publicity-seeking-hackers-spreec.html>

<p>This document is subject to copyright. Apart from any fair dealing for the purpose of private study or research, no part may be reproduced without the written permission. The content is provided for information purposes only.</p>
--