# Hacker group draws increased scrutiny from feds

September 11 2011, By PAUL ELIAS , Associated Press

(AP) -- Anonymous is not so anonymous anymore. The computer hackers, chat room denizens and young people who comprise the loosely affiliated Internet collective have increasingly turned to questionable tactics, drawing the attention of the FBI, the Department of Homeland Security and other federal investigators.

What was once a small group of pranksters has become a potential national security threat, federal officials say.

The FBI has carried out more than 75 raids and arrested 16 people this year in connection with illegal hacking jobs claimed by Anonymous.

Since June, the Department of Homeland Security has issued three "bulletins" warning cyber-security professionals of hacking successes and future threats by Anonymous and related groups, including a call to physically occupy Manhattan's Wall Street on Sept. 17 in protest of various U.S. government policies.

San Francisco police arrested more than 40 protesters last month during a rowdy demonstration organized by Anonymous that disrupted the evening commute. The group called for the demonstration after the Bay Area Rapid Transit system shut off it cell service in San Francisco stations to quell a planned protest over police shooting on a subway platform.

"Anonymous' activities increased throughout 2011 with a number of

high-profile attacks targeting both public and private sector entities," one of the bulletins issued last month said.

Some members of the group have also called for shutting down Facebook in November over privacy issues, although other Anonymous followers are disavowing such an attack - underscoring just how loosely organized the group is and how problematic it is to police.

"Anonymous insist they have no centralized operational leadership, which has been a significant hurdle for government and law enforcement entities attempting to curb their actions," an Aug. 1 Homeland Security bulletin noted. "With that being said, we assess with high confidence that Anonymous and associated groups will continue to exploit vulnerable publicly available Web servers, websites, computer networks, and other digital information mediums for the foreseeable future."

Followers posting to Twitter and chatting in Internet Relay Channels insist there are no defined leaders of Anonymous and that it's more of a philosophy than a formal club, though a small group of members do the most organizing online.

"Anonymous is not a group, it does not have leaders, people can do ANYTHING under the flag of their country," wrote one of the more vocal members who asked not to be identified.

"Anything can be a threat to National Security, really," the member said in an email interview. "Any hacker group can be."

The member said that the group as a whole wasn't a national security threat, but conceded some individuals acting as Anonynous may be considered dangerous.

DHS' latest bulletin, issued Sept. 3, warned the group has been using

social media networks to urge followers working in the financial industry to sabotage their employers' computer systems.

The DHS warning comes on the heels of several Anonymous-led protests of the Bay Area's transit agency that led to FBI raids of 35 homes and dozens of arrests, as well as to the indictment of 14 followers in July on felony computer hacking charges in connection with a coordinated "denial of service attack" against Paypal's website last year.

Security officials said the "DDoS" attacks occur when a website is overwhelmed by malicious messages carried out by thousands of followers, usually with easily downloadable software.

"Anonymous has shown through recently reported incidents that it has members who have relatively more advanced technical capabilities who can also marshal large numbers of willing, but less technical, participants for DDoS activities," the August DHS bulletin said.

Anonymous orchestrated the crashing of Paypal late last year after the online financial service suspended Wikileaks' account after the website published confidential diplomatic cables and other sensitive U.S. government intelligence. The group also targeted Visa, Mastercard and others for the same reason and has carried out several other hacks during the year. Last month, for example, the group claimed responsibility for hacking a website belonging to the Bay Area Rapid Transit agency and releasing personal information of 2,000 passengers.

"Anonymous is incredibly active," said Josh Shaul, chief technology officer of Application Security, Inc., a New York-based provider of database security software. It's rare to have a hacking group willing to work outside of the shadows. These guys are quite brazen."

Anonymous emerged in 2003 from an Internet chat channel where

members organized random Web incidents for their own amusement. By 2008, the prankster nature of Anonymous morphed into "hacktivism," where members sabotaged websites and leaked confidential information for political purposes.

Investigators suspect a splinter Anonymous group known as LulzSec was responsible for a June 15 denial of service attack on the CIA's public website.

This summer, Anonymous claimed credit for hacking into a Booz Allen Hamilton website and leaking email addresses of 90,000 U.S. military personnel and hacking a Monsanto Co. website and releasing personal data of 2,500 employees.

Until July, law enforcement officials around the world had arrested just a handful of suspected hackers thought to be affiliated with Anonymous. But on July 19, the FBI fanned out across the United States and raided more than 35 homes, seizing dozens of computers and arrested 16 on charges that they participated in the Paypal attack.

In response, Anonymous said it hacked a website on Sept. 1 belonging to police chiefs in Texas. The group posted personal information such as emails about internal investigations before the site was shut down.

FBI investigators in court filings said that the raids and arrests were made from a list of 1,000 computer users that Paypal cyber-security workers identified as the most active attackers. The fourteen appearing in San Jose federal court have pleaded not guilty and were released on bail after promising not to access Twitter, Facebook and other social media sites.

Most of the defendants were younger than 30. Security experts and the Department of Homeland Security say most of Anonymous followers are

so-called "script kiddies," young people who carry out the attacks and who are "less skilled hackers" than the vocal group members who call for the protests and attacks.

The DHS defines script kiddies as: "Unskilled individuals who use scripts or programs developed by others to attack computer systems and networks and deface websites."