September 23, 2011 9:25 pm

They're watching. And they can bring you down

By Joseph Menn

Why the world is scared of hacktivists

An Anonymous member wearing a Guy Fawkes mask demonstrates at a station in San Francisco after the restriction of mobile phone services on platforms

It took more than being arrested at his home in the Netherlands by a swarm of police officers to shake 19-year-old Martijn Gonlag's faith in Anonymous, an amorphous cyber-collective that has terrorised law enforcement and leading companies on five continents.

Gonlag, who lives in Hoogezand-Sappemeer, 100 miles north-east of Amsterdam, was interrogated for two days last year before being released pending a trial that could send him to jail for six years. But the college student stood by his decision to download attack software and participate in 2010's electronic assaults on the websites of Visa, MasterCard and others that had stopped processing donations to WikiLeaks as it published secret diplomatic cables. "WikiLeaks hasn't been charged, but they were being worked against by governments and companies. That wasn't right," Gonlag told the Financial Times.

More

The state of technology security overall is so weak that intelligence officials see hacking as one of the

Editor's Choice

TECHNOLOGY SPECIAL

Billion dollar brains: meet the next generation of Silicon Valley stars

LIFE & ARTS

HBO has turned watching television into the ultimate in cultural immersion

Most popular in Life & Arts

1. They're watching. And they can bring you down
2. The Wellcome at 75
3. At home with Heston
4. Billion dollar brains
5. New life for forgotten fuel

ON THIS STORY
Billion dollar brains
Sailing away with the Nobel
Birth of the global mind

largest threats to western powers. While their top concern is nation-backed attacks, the lines between protesters, criminals and spies can be hard to discern. Gonlag is one of thousands who have joined an unprecedented wave of what has been dubbed "hacktivism", referring to the combination of computer hacking with political activism. The largest and best known of these groups is Anonymous, a virtual mob that makes it easy for people with little technological aptitude to participate in protests, many of them illegal.

The increasingly likely threat of apprehension isn't enough to dissuade many Anonymous supporters from what they compare with "sit-ins" – conscious acts of trespassing that inconvenience their targets while bringing the underlying issues to wider attention. Yet though such dedication persists even after dozens of recent arrests in the UK, US, Italy and elsewhere, there are signs that Anonymous is being torn apart from the inside. Internal feuds thus might finish the job that law enforcement – infuriated by attacks on the CIA, FBI and US defence contractors – has barely begun.

The most important split is between the leadership and the rank and file. Gonlag underwent his own change of heart when he watched an administrator in an Anonymous chat channel encourage a minor to download the same software that had led to his weekend behind bars. The old hand told the teenager that he wasn't in danger because the attack tool would mask his internet address.

"LOL," Gonlag typed in the chat channel, for "laughing out loud". He meant it as a warning born of hard-won experience. But the administrator immediately shot him a private message: "Shut the f*** up." "That showed to me they are trying to use kids to do their dirty work," Gonlag recalled. "That's when the tide turned and I left Anonymous."

To admirers, the hacktivism trend reflects the increased importance of technology in more and more aspects of life. The net is now democratising both legitimate political expression and hacking in the same way it once democratised media, allowing anyone to blog or publish an electronic book.

But others, including the companies that have lost business due to web outages or been robbed of customer information by hacktivists, believe Anonymous sets a dangerous precedent. "Motivation-wise, I think these guys are on a massive power trip. There is definitely some criminal element," says Karim Hijazi, founder of tech security start-up Unveillance, which had its internal e-mails published by hackers with Lulz Security (commonly known as LulzSec), an Anonymous offshoot.

Even some supporters worry that if the group continues on its current path, it could trigger a legislative backlash that would bring heightened monitoring at the expense of the privacy that Anonymous prizes.

Steven Chabinsky, FBI deputy assistant director, says the bureau is placing "a lot of emphasis and focus on Anonymous and other groups that would be like them. These organisations have managed to use new technologies to connect to otherwise disenfranchised hackers to gather force and momentum in a way we have not seen before." Since July, the FBI's most useful ally has been Scotland Yard and its beefed-up e-Crime unit, which says it has arrested three of the

Multimedia
Video
Blogs
Podcasts
Interactive graphics
Audio slideshows

Tools
Portfolio
FT Lexicon
FT clippings
Currency converter
MBA rankings
Today's newspaper
FT press cuttings
FT ePaper

Updates
Alerts Hub
Daily briefings
FT on your mobile
Share prices on your phone
Twitter feeds
RSS feeds

Quick links
Mergermarket
How to spend it
SchemeXpert.com
Social Media hub
The Banker
fDi Intelligence
Professional Wealth Management
This is Africa
Investors Chronicle

Services
Subscriptions
Corporate subscriptions
Syndication
Conferences
Annual reports
Jobs
Non-Executive Directors' Club
Businesses for sale
Contracts & tenders
Analyst research
Company announcements

four founders of LulzSec.

. . .

Martijn Gonlag, former Anonymous supporter, who faces jail for hacking

Anonymous began as a small group protesting internet censorship, using novel ways designed to grab press attention. As idealists swelled the ranks, though, its unusually open and officially leaderless structure allowed it to be penetrated by cyber criminals and career hackers, who launched direct attacks on law enforcement. This was a long way from the chatter on teen-oriented message boards inside the 4chan website, which was founded in 2003. (The name “Anonymous” comes from the identity given by default to anyone posting comments there.)

These message boards were all about ephemera, with pictures or other material disappearing automatically after a short period. But some items caught the imaginations of enough people in the nameless crowd that they spread to the rest of the web world. The boards were the take-off point for the annotated cat pictures known as LOLcats and for the prank that tricked people into clicking on links to singer Rick Astley’s 1987 song “Never Gonna Give You Up” – the infamous “rickrolling”.

Little on 4chan was political and anyone trying to do something positive risked being tagged as a self-righteous “moral fag”, as the lingo had it. Still, given the off-colour taste of many of the 4chan items posted, internet censorship naturally hit a nerve.

It was the Church of Scientology, which had a history of using copyright laws to go after critics and suppress internal documents, that was the catalyst for transforming Anonymous from online hangout to activist power. The process took less than a fortnight.

In January 2008, 4chan visitors and others passed around a YouTube video of Tom Cruise talking about Scientology. Ignoring the maxim that, on the internet, squashing something makes it bigger, the church served YouTube with a copyright warning and got the video taken down. This offended 4chan

regulars such as Gregg Housh, an anti-establishment website programmer.

A debate began over what to do. One suggestion was that since YouTube videos are often downloaded and reposted, the group should look out for a repost and grab a copy for distribution to other sites. It did just that, adding text naming another internet chat that viewers could join to plot next steps. More than 50 people signed in. Some suggested an answering video, with a digitised voice reading a press release where “Anonymous” declared “war” on Scientology. As Housh and his online peers put the finishing touches to the press release, someone suggested the ominous tagline: “Expect Us”. Housh loved it. “You win!” he shouted.

Housh, who is now 34, thought the video would last for a week or so before new people stopped watching. “This is the internet,” he shrugs. But the online tech tabloid The Register found the fresh imagery and tone irresistible, embedding the video on its front page. High-traffic gossip site Gawker followed and then came cable channel CNN.

The chat channel grew so crowded with new participants that communication was close to impossible – the messages scrolled too quickly up the screen. Housh dispersed the flock to new channels for every big city and set up a secret one for core organisers to thrash through plans to keep the movement going.

The group held real-world demonstrations in front of Scientology churches. In keeping with the nameless spirit of their movement and to guard against lawsuits, they picked a uniform disguise – Guy Fawkes masks like those used in the movie V for Vendetta. Thousands appeared at the appointed hour and Anonymous took on new life as an outward-facing social force. And the more its members intersected with other activists, the more they thought about where internet freedom was imperilled on the world stage.

Anonymous’s attention on Scientology flagged but participants put up a website, WhyWeProtest, to explain their reasoning on net censorship and related issues.

After the suspect Iranian elections in 2009, local activists appeared and asked how to organise online without being caught by the government’s surveillance techniques. Housh and his colleagues coached them with the best research they could find. At one point he was speaking to five activists inside Iran. Then came days of silence before one got back in touch using the code word. The other four were dead, he said, and he wouldn’t be in contact again.

Housh was shattered. So much for the fun and games. “I'm done,” he said. Anonymous would play a role in the Arab uprisings that began in December 2010, but he and others merely provided resources instead of trying to shape events.

Anonymous has received nowhere near the press coverage for its Middle East activities as it has for its web attacks. To some, though, the former were a high-water mark, showing that the large and haphazard collective could unite to do good.

WikiLeaks founder Julian Assange

“They have done some spectacularly stupid things, but they should be commended for what they did during the Arab Spring,” says a technology activist from Canada, who uses the name Oxblood Ruffin. Now 60, Ruffin has worked on monitoring-circumvention tools for people in repressive countries since 1996, and his group is sometimes credited with coining the term “hacktivism”. “There were a lot of Anons involved in keeping servers running [during the Arab Spring], in telling people how to use the net and mobile phones safely. That’s 10,000 per cent hacktivism.”

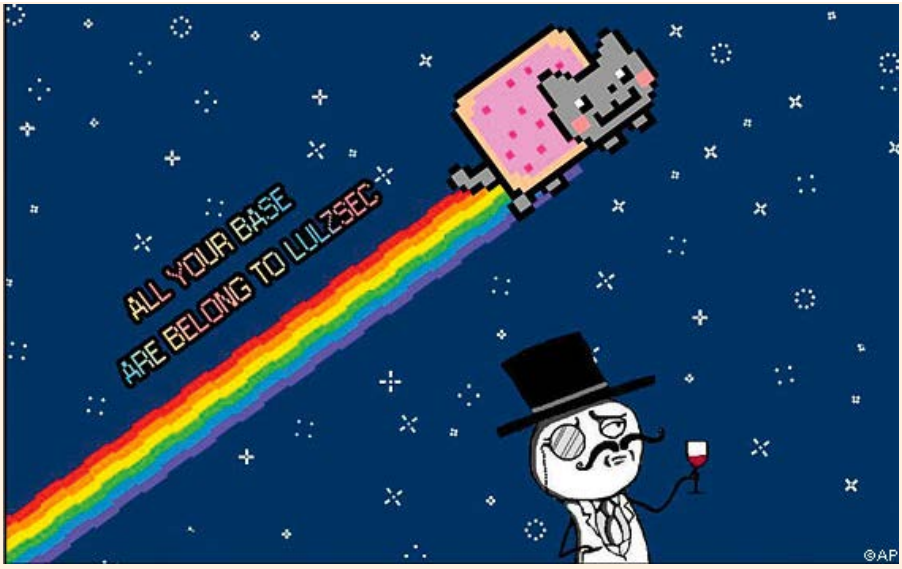
But like the topics on the message boards where Anonymous originated, an infinite number of “operations” can be presented in the quest for sufficient support. The next natural winner on the chat channels was WikiLeaks. Interest surged as it began to expose government secrets, and even more so when MasterCard, PayPal and other companies refused to process donations.

Anonymous could have taken any number of avenues to express itself, but the main one favoured by members was denial-of-service attacks that overwhelmed financial websites and temporarily knocked them offline.

With help from the press, Anonymous’s attacks on behalf of WikiLeaks brought it to its widest ever audience, attracting thousands of people like Martijn Gonlag: college students, slackers and office workers who were rooting for WikiLeaks founder Julian Assange, himself a hacker of some repute 15 years previously.

It was both easier and more effective than traditional forms of protest. Sign into a chat channel, download the software and afflict the comfortably off while spreading the word. “Going on the street with a flag is not going to get you any media attention. It won’t help any more in a digital world,” Gonlag reasoned. “We need to do other things.”

. . .



Screen grab of the hacked Public Broadcasting System website after it aired an unflattering report on WikiLeaks and its founder Julian Assange. Anonymous also targeted financial websites that refused to process donations to WikiLeaks

At a psychological level, firing away at corporate or government websites echoes a shift in media habits that is rewiring people who grew up with the internet, the so-called digital natives. Global revenue from gaming has overtaken movies as active participation replaces passive consumption of video.

Like many other hacktivists, Gonlag was an avid player of “first-person shooter” games, the protagonist in his own adventures. Digitally attacking MasterCard and Visa elevated that engagement to the real world, a literal dream come true.

As Anonymous grew during the WikiLeaks period, it expanded its pioneering use of social networks and other technology. Leaders of various operations coordinated via chat channels and Facebook groups, reaching out to the masses through YouTube and multiple Twitter accounts.

The electronic equivalent of a paper trail, though, also attracted security researchers. This posed a potential threat to the biggest players within Anonymous – those whose computers ran the group’s chats or controlled the botnets, or networks of compromised machines, that were being used in some of the assaults and that could also be used for sending spam or stealing data.

Law enforcement has a dismal record on cybercrime, arresting fewer than 1 per cent of the perpetrators, according to technology research firm Gartner. The limited expertise typically can’t overcome the difficulty in proving who was at which keyboard at what time and the logistical challenge of chasing cases across national borders.

Most of the best cyber crime sleuths work for private security companies, where they can make a name for themselves by exposing new problems or major hackers. In February of this year, I wrote an article in the FT citing chief executive Aaron Barr of security concern HBGary Federal. He told me he had uncovered the true names of many Anonymous leaders and planned to explain his techniques at an imminent security conference.

The article set off a panic. A small group of Anonymous leaders and their associates set out to determine what Barr knew – by any means necessary. Taking charge was “Sabu”, a hacker whose first political acts online had come a

decade earlier, when he disrupted communications during US Navy bombing exercises in Puerto Rico. He was joined by “Kayla”, “Tflow” and “Topiary”, later the spokesperson for LulzSec.

It took them less than a weekend to gain access to HBGary Federal’s e-mails. When the hacktivists subsequently discovered that many of Barr’s identifications were off-base, they published them, devastating the security company and forcing Barr’s resignation on February 28.

If the Arab Spring had been the zenith for Anonymous in politics, the HBGary hack marked a peak in industry impact. Sabu, Topiary and some of the others didn’t stop there. They formed LulzSec and went on a 50-day rampage, largely against western law enforcement agencies and security companies. With fewer people, they could move faster than Anonymous and communicate more effectively, soon amassing more than 300,000 followers on Twitter.

LulzSec briefly took down the public sites of the CIA and the UK’s Serious Organised Crime Agency. Such stunts ensured more media coverage and redoubled a police effort, eventually forcing LulzSec to merge back into the safety of Anonymous.

In a break from Anonymous tradition, LulzSec also published what it rooted out from hacked companies, including the phone numbers of police officers and thousands of credit card numbers belonging to Sony customers, among others. Sony said the spate of attacks on its networks, which shuttered the PlayStation online system for more than a month, will cost it in excess of $170m.

In theory, the dumps of private data were designed to keep the news reports coming and thereby embarrass companies into improving their defences, as well as to expose any security contractor complicity in internet surveillance or other repression.

Indeed some security professionals say that Sony’s massive brand damage and LulzSec’s antics, which included announcing details of the security holes it had crawled through, have prompted executives to take a harder look at their practices. Warnings by officials and experts about the state of technology security had long gone unheeded, in part because costly breaches often aren’t disclosed and public embarrassment is rare.

Ironically, the criminal hackers within Anonymous and LulzSec therefore might have done more to advance corporate security than any initiative from White House officials or the burgeoning private security industry.

“It is a great classroom to illustrate all the concerns that security people have had for decades,” says Jeff Moss, founder of the DefCon hacking convention and a US administration adviser.

Chris Wysopal, a co-founder of the security firm Veracode, who in 1998 testified before a Senate committee about internet vulnerabilities, agreed that in some ways LulzSec was fulfilling a mission that at times seems impossible to complete through legitimate channels.

“I struggle with trying to figure out a way to raise awareness that there are a lot of systems out there that are insecure,” says Wysopal. “There is a benefit to the community hearing this information. When doctors tell patients they have a given illness, they can take action. What LulzSec is doing is pointing it out in

a more sensational way.”

. . .

Yet many of the Anonymous members who supported the denial of service attacks didn’t like the antisecurity operations that were generating so much new press. Others choked at the wanton dissemination of financial data and passwords of random citizens.

“Anonymous does have a leadership and they don’t give a **** about us,” one member known as SparkyBlaze wrote in a self-published list of parting complaints. “Does Anon have the right to remove the anonymity of innocent people? They are always talking about people’s right to remain anonymous, so why are they removing that right?”

Some followers came to believe that the leaders sought only personal aggrandisement or were effectively in cahoots with the organised criminals who may have raided Sony’s credit-card hoard after Anonymous knocked down the door. Even stalwarts such as Housh are unhappy that much of Anonymous’s infrastructure is now housed on computers used by Russian criminals. “It’s not like the Russians wanted us to get HBGary, but I want to know personally why they are doing this,” he says of the chat hosts. “Where is the money coming from?”

Gonlag began actively working against Anonymous after the HBGary hack, as did other ex-followers. Private security experts, including Aaron Barr, bent on professional redemption, joined PayPal and other victims in gathering documents pointing to real identities. Gonlag has passed on tips to the FBI. “I don’t like being a snitch, but what they are doing is wrong.”

In July, Scotland Yard’s e-Crime unit arrested young British men it accused of being Topiary and Tflow; Kayla’s arrest was claimed in early September. Once irrepressible on Twitter, Sabu, too, has gone quiet. Suspicions about who is ratting out whom abound, hindering collaboration on new projects.

The annual DefCon hacking convention in Las Vegas this August drew many current and former members and sympathisers of Anonymous. The latter included a surprising number whose day jobs involve warding off such threats but who welcome the increased scrutiny Anonymous has brought to cyber-defence.

Opinion was divided. At one panel, professional analysts suggested ways the mob might improve on itself, such as by setting criteria for responsible behaviour for security firms that wish to avoid being attacked. At another meeting, former Anonymous member Jennifer Emick railed against what the organisation had become and fended off hecklers, including one in a Guy Fawkes mask.

Speaking to me outside the convention, Barr agreed that Anonymous has brought internet activism to a level that will be maintained or exceeded regardless of whether the group itself survives.

Less clear is whether the anarchic hacking carried out against security companies like his own former employer will continue. Although he says it may depend on who is arrested and convicted, Barr guesses that it will go on regardless. “I think it’s reached a critical mass.”

Joseph Menn is an FT technology correspondent in San Francisco

.....

Technology special

Billion dollar brains

Sailing away with the Nobel

Birth of the global mind

Post your own comment

Comments

Sorted by newest first | Sort by oldest first

Fred Chores | September 25 9:41am | Permalink Report

Great work.

Ferd Turgeson | September 25 1:08am | Permalink Report

Can you get rid of the masked guy on your opening page.

Realpolitech | September 24 10:54am | Permalink Report

From an earlier posting:

This has really been a great week for Cyber and Psychological warfare professionals. In one week we have seen riots in the UK and flash mob issues in the US. The US and UK need to monitor both these situations carefully because social networking can be used by foreign governments to cause mayhem in targeted countries. Forget HAARP hardware; this is real, a very clear and present danger to democracies and dictatorships with advanced communications systems. The neutron bombs of Bank deregulation (repeal of Glass-Stegall) and the housing bubble has created stagnate economies unable to keep technologically advanced youth employed. Security concerns and welfare/Medicaid/retirement programs have created a wealth transfer BLITZKRIEG! Whole neighborhoods have been laid to waste as both home and home owner become TARP-financial liabilities. As the jobless rate approaches 10% in some Western countries the feeling of hopelessness has increased. College tuition has more than doubled and most students graduate only to move back home with debt exceeding $120,000 USD. To prevent foreign governments from taking advantage of the American people via propaganda campaigns, psychological warfare cyber terrorism and destructive social networking (misinformation warfare) operations like we have witnessed this week, our government created the Patriot Act. We owe the current and past administrations a debt of gratitude we can never repay. Our leaders and institutions will continue to protect the American people from this new and terrifying form of modern warfare.

http://online.wsj....SJ_hp_mostpop_read