War on Anonymous: British Spies Attacked Hackers, Snowden Docs Show

COLLAPSE STORY

BY MARK SCHONE, RICHARD ESPOSITO, MATTHEW COLE AND GLENN GREENWALD, SPECIAL CONTRIBUTOR

's enemies has
ling to
Snowden and

obtained by NBC News.

The blunt instrument the spy unit used to target hackers, however, also interrupted the web communications of political dissidents who did not engage in any illegal hacking. It may also have shut down websites with no connection to Anonymous.

According to the documents, a division of Government Communications Headquarters (GCHQ), the British counterpart of the NSA, shut down communications among Anonymous hacktivists by launching a "denial of service" (DDOS) attack – the same technique hackers use to take down bank, retail and government websites – making the British government the first Western government known to have conducted such an attack.

The documents, from a PowerPoint presentation prepared for a 2012 NSA conference called SIGDEV, show that the unit known as the Joint Threat Research Intelligence Group, or JTRIG, boasted of using the DDOS attack – which it dubbed Rolling Thunder -- and other techniques to scare away 80 percent of the users of Anonymous internet chat rooms.

The existence of JTRIG has never been previously disclosed publicly.

The documents also show that JTRIG infiltrated chat rooms known as IRCs and identified individual hackers who had taken confidential information from websites. In one case JTRIG helped send a hacktivist to prison for stealing data from PayPal, and in another it helped identify hacktivists who attacked government websites.

In connection with this report, NBC is publishing documents that Edward Snowden took from the NSA before fleeing the U.S. The documents are being published with minimal redactions.

Intelligence sources familiar with the operation say that the British directed the DDOS attack against IRC chat rooms where they believed criminal hackers were concentrated. Other intelligence sources also noted that in 2011, authorities were alarmed by a rash of attacks on government and corporate websites and were scrambling for means to respond.

"While there must of course be limitations," said Michael Leiter, the former head of the U.S. government's National Counterterrorism Center and now an NBC News analyst, "law enforcement and intelligence officials must be able to pursue individuals who are going far beyond speech and into the realm of breaking the law: defacing and stealing private property that happens to be online."

"No one should be targeted for speech or thoughts, but there is no reason law

▶ PLAY VIDEO (0:00)

British Spies Can Snoop on Social Media, Documents Reveal

NIGHTLY NEWS

“Targeting Anonymous and hacktivists amounts to targeting citizens for expressing their political beliefs,” said Gabriella Coleman, an anthropology professor at McGill University and author of an upcoming book about Anonymous. “Some have rallied around the name to engage in digital civil disobedience, but nothing remotely resembling terrorism. The majority of those embrace the idea primarily for ordinary political expression.” Coleman estimated that the number of “Anons” engaged in illegal activity was in the dozens, out of a community of thousands.

"Targeting Anonymous and hacktivists amounts to targeting citizens for expressing their political beliefs."

In addition, according to cyber experts, a DDOS attack against the servers hosting Anonymous chat rooms would also have shut down any other websites hosted by the same servers, and any other servers operated by the same Internet Service Provider (ISP), whether or not they had any connection to Anonymous. It is not known whether any of the servers attacked also hosted other websites, or whether other servers were operated by the same ISPs.

In 2011, members of the loose global collective called Anonymous organized an online campaign called “Operation Payback” targeting the pay service PayPal and several credit card companies. Some hacktivists also targeted U.S. and British government websites, including the FBI, CIA and GCHQ sites. The hacktivists were protesting the prosecution of Chelsea Manning, who took thousands of classified documents from U.S. government computers, and punishing companies that refused to process donations to WikiLeaks, the website that published the Manning documents.

The division of GCHQ known as JTRIG responded to the surge in hacktivism. In another document taken from the NSA by Snowden and obtained by NBC News, a JTRIG official said the unit’s mission included computer network attacks, disruption, “Active Covert Internet Operations,” and “Covert Technical Operations.” Among the methods listed in the document were jamming phones, computers and email accounts and masquerading as an enemy in a "false flag" operation. The same document said GCHQ was increasing its emphasis on using cyber tools to attack adversaries.

In the presentation on hacktivism that was prepared for the 2012 SIGDEV conference, one official working for JTRIG described the techniques the unit used to disrupt the communications of Anonymous and identify individual hacktivists, including some

involved in Operation Payback. Called “Pushing the Boundaries and Action Against Hacktivism,” the presentation lists Anonymous, Lulzsec and the Syrian Cyber Army among “Hacktivist Groups,” says the hacktivists’ targets include corporations and governments, and says their techniques include DDOS and data theft.

Under “Hacktivism: Online Covert Action,” the presentation refers to “Effects Operations.” According to other Snowden documents obtained by NBC News, “Effects” campaigns are offensive operations intended to “destroy” and “disrupt” adversaries.

"Anyone here have access to a website with at least 10,000+ unique traffic per day?"

The presentation gives detailed examples of “humint” (human intelligence) collection from hacktivists known by the on-line names G-Zero, Topiary and p0ke, as well as a fourth whose name NBC News has redacted to protect the hacker's identity. The hacktivists were contacted by GCHQ agents posing as fellow hackers in internet chat rooms. The presentation includes transcripts of instant message conversations between the agents and the hackers in 2011.

“Anyone here have access to a website with at least 10,000+ unique traffic per day?” asks one hacktivist in a transcript taken from a conversation that began in an Operation Payback chat room. An agent responds and claims to have access to a porn website with 27,000 users per day. “Love it,” answers the hacktivist. The hackers ask for access to sites with traffic so they can identify users of the site, secretly take over their computers with malware and then use those computers to mount a DDOS attack against a government or commercial website.

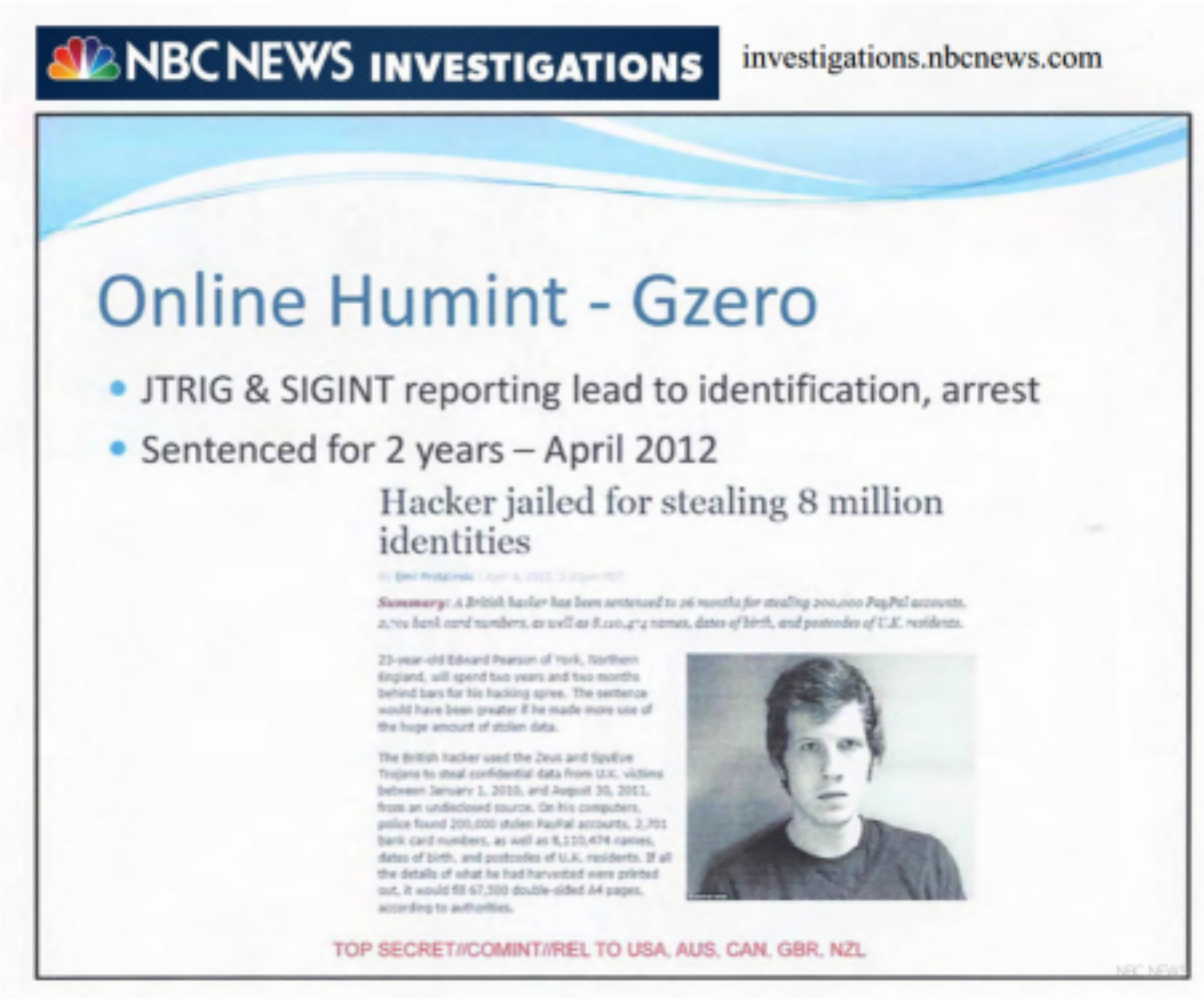
A GCHQ agent then has a second conversation with a hacker known as GZero who claims to “work with” the first hacktivist. GZero sends the agent a series of lines of code that are meant to harvest visitors to the agent’s site and make their computers part of a “botnet” operation that will attack other computers.

The “outcome,” says the presentation, was “charges, arrest, conviction.” GZero is revealed to be a British hacker in his early 20s named Edward Pearson, who was prosecuted and sentenced to 26 months in prison for stealing 8 million identities and information from 200,000 PayPal accounts between Jan. 1, 2010 and Aug. 30, 2011. He and his girlfriend were convicted of using stolen credit card identities to purchase

take-out food and hotel stays.

In a transcript taken from a second conversation in an Operation Payback chat room, a hacktivist using the name "p0ke" tells another named "Topiary" that he has a list of emails, phone numbers and names of "700 FBI tards."

An agent then begins a conversation with p0ke, asking him about what sites he's accessed. The hacktivist responds that he was able to defeat the security on a U.S. government website, and pulled up credit card information that's attached to congressional and military email addresses.



Screen shot of Power Point

The agent then asks whether p0ke has looked at a BBC News web article called "Who loves the hacktivists?" and sends him a link to the story.

"Cool huh?" asks the agent, and pOke responds, "ya."

When p0ke clicked on the link, however, JTRIG was able to pull up the IP address of

the VPN (virtual private network) the hacktivist was using. The VPN was supposed to protect his identity, but GCHQ either hacked into the network, asked the VPN for the hacker's personal information, or asked law enforcement in the host nation to request the information.

A representative of the VPN told NBC News the company had not provided GCHQ with the hacker's information, but indicated that in past instances it has cooperated with local law enforcement.

In whatever manner the information was retrieved, GCHQ was able to establish p0ke's real name and address, as shown in the presentation slides. (NBC News has redacted the information).

P0ke was never arrested for accessing the government databases, but Topiary, actually an 18-year-old member of Anonymous and LulzSec spokesman from Scotland named Jake Davis, was arrested in July 2011. Davis was arrested soon after LulzSec mounted hack attacks against Congress, the CIA and British law enforcement.

Two weeks before his arrest, the Guardian published an interview with Davis in which he described himself as "an internet denizen with a passion for change." Davis later pled guilty to two DDOS attacks and was sentenced to 24 months in a youth detention center, but was released in June 2013 after five weeks because he had worn an electronic ankle tag and been confined to his home without computer access for 21 months after his arrest. Davis declined comment to NBC News.

In the concluding portion of the JTRIG presentation, the presenters sum up the unit's "Effects on Hacktivism" as part of "Op[eration] Wealth" in the summer of 2011 and apparently emphasize the unit's success against Anonymous, including the DDOS attack. The listed effects include identifying top targets for law enforcement and "Denial of Service on Key Communications outlets."

A slide headlined "DDOS" refers to "initial trial info" from the operation known as "Rolling Thunder." It then quotes from a transcript of a chat room conversation between hacktivists. "Was there any problem with the IRC [chat room] network?" asks one. "I wasn't able to connect the past 30 hours."

"Yeah," responds another. "We're being hit by a syn flood. I didn't know whether to quit last night, because of the DDOS."

The next slide is titled "Information Operations," and says JTRIG uses Facebook, Twitter, email, instant messenger, and Skype to dissuade hacktivists with the message, "DDOS and hacking is illegal, please cease and desist."

The following slide lists the outcome of the operation as “80% of those messaged where (sic) not in the IRC channels 1 month later.”

Gabriella Coleman, the author and expert on Anonymous, said she believed the U.K. government had punished a large number of people for the actions of a few. “It is hard to put a number on Anonymous,” she said, “but at the time of those events, there were thousands of supporters and probably a dozen or two individuals who were breaking the law.”

Said Coleman, “Punishing thousands of people, who are engaging in their democratic right to protest, because a couple people committed vandalism is … an appalling example of overreacting in order to squash dissent.”

Jason Healey, a former top White House cyber security official under George W. Bush, called the British government’s DDOS attack on Anonymous “silly,” and said it was a tactic that should only be used against another nation-state.

Jason Healey, a former top White House cyber security official under George W. Bush, called the British government’s DDOS attack on Anonymous “silly."

He also questioned the time and energy spent chasing teenage hackers.

“This is a slippery slope,” said Healey. “It’s not what you should be doing. It justifies [Anonymous]. Giving them this much attention justifies them and is demeaning to our side.”

In a statement, a GCHQ spokesperson emphasized that the agency operated within the law.

“All of GCHQ's work is carried out in accordance with a strict legal and policy framework,” said the statement, “which ensure[s] that our activities are authorized, necessary and proportionate, and that there is rigorous oversight, including from the Secretary of State, the Interception and Intelligence Services Commissioners and the Parliamentary Intelligence and Security Committee. All of our operational processes rigorously support this position.”

Told by NBC News that his on-line alias appeared in the JTRIG presentation, the hacker

known as p0ke, a college student in Scandinavia, said he was confused about why he hadn't been confronted by authorities. (NBC News is withholding his name, age and country of residence.)

But p0ke said he had stopped hacking because he'd grown bored with it, and was too busy with his studies. He was never a "hacktivist" anyway, he said. "Politics aren't mah thang," he said in an online interview. "Seriously tho, I had no motive for doing it."

He said that hacking had only satisfied an urge to show off. "Fancy the details for a while," he wrote, "then publish em to enlarge my e-penis."

A British hacktivist known as T-Flow, who was prosecuted for hacking alongside Topiary, told NBC News he had long suspected that the U.K.'s intelligence agencies had used hacker techniques to catch him, since no evidence of how his identity was discovered ever appeared in court documents. T-Flow, whose real name is Mustafa Al-Bassam, pleaded guilty but did not serve time in an adult facility because he was 16 when he was arrested.

"When I was going through the legal process," explained Al-Bassam, "I genuinely felt bad for all those attacks on government organizations I was involved in. But now that I know they partake in the exact same activities, I have no idea what's right and wrong anymore."

Journalist Glenn Greenwald was formerly a columnist at Salon and the Guardian. In late 2012 he was contacted by NSA contractor Edward Snowden, who later provided him with thousands of sensitive documents, and he was the first to report on Snowden's documents in June 2013 while on the staff of the Guardian. Greenwald has since reported on the documents with multiple media outlets around the world, and has won several journalism awards for his NSA reporting both in the U.S. and abroad. He is now helping launch, and will write for, a new, non-profit media outlet known as First Look Media that will "encourage, support and empower ... independent, adversarial journalists."

First published February 5th 2014, 12:26 am

MARK SCHONE

Mark Schone is a digital editor with the investigative unit at NBC News. He is also an adjunct professor at New York University's graduate journalism school. Previously, he