NetworkWorld
THE CONNECTED ENTERPRISE

INSIDER

Hacktivism

HACKTIVISTS VS THE WORLD

Anonymous wreaks havoc on Web

Credit: Rob Sheridan

INSIDE

Anonymous attack on HBGary Federal didn't ruin company

HBGary's Greg Hoglund discusses impact of Anonymous attack

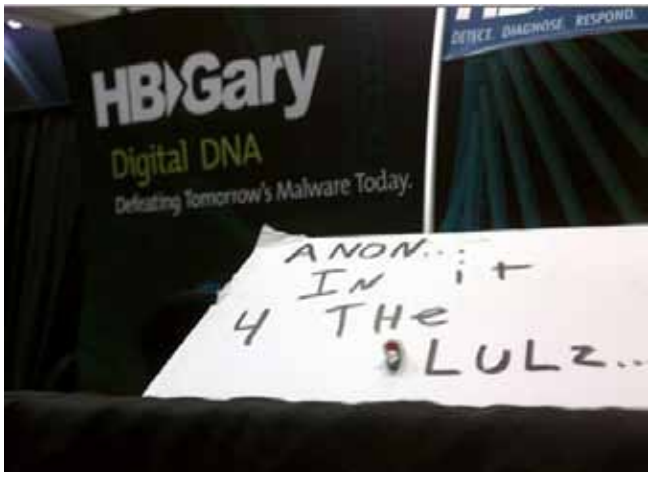
BY ELLEN MESSMER, NETWORK WORLD , DEC. 9, 2011

When HBGary Federal, had its website hacked and sensitive e-mail exposed by hacktivist group Anonymous last February, it became a question of how Sacramento, Calif.-based security firm HBGary could survive the damage to its reputation.

But in spite of the bruising, HBGary not only didn't lose business customers in the course of the past year, but "we ended up getting additional business," says Greg Hoglund, founder and CEO of HBGary. Calling it an unexpected and even "weird side effect," Hoglund said the widely-publicized attack by Anonymous on HBGary Federal, a separate company set up by HBGary in 2009 to market to the federal government, appears to have elicited a sense of identification from many other companies. "They saw us go through things they were experiencing," he says.

Last February, members of Anonymous, apparently furious that then-CEO of HBGary Federal, Aaron Barr, had publicly alluded to his effort to infiltrate the hacktivist group to expose its leaders, lashed out by breaking into the HBGary Federal website. Anonymous then seized tens of thousands of the firm's e-mail to post them online. The dark episode even had HBGary President Penny Leavy, Hoglund's wife, going onto an Anonymous IRC channel to basically beg for the attack to end.

Some of that e-mail included e-mail from Barr to a Bank of America law firm proposing a way to marginalize WikiLeaks, the group that in the past has published confidential corporate and government documents it secretly obtains, by hacking into it and feeding it fake documents.



However, the bigger scandal in the hacked e-mail bundle was associated with comments made about possibly "disrupting" Glenn Greenwald, a Salon columnist who has been sympathetic to WikiLeaks, as well as a proposal to undermine US Chamber Watch, a critic of the U.S. Chamber of Commerce. The scandal forced Barr to resign from HBGary Federal and when Barr wanted to discuss his experiences chasing after Anonymous in a session scheduled at the Defcon Conference in July this year, HBGary Federal said it would seek an injunction against him if he did.

"Anonymous never came within in two to three network layers of us."

Greg Hoglund

HBGary was reluctant to say much about HBGary Federal. Ted Vera, COO of HBGary Federal, did not respond to a Network World inquiry to discuss its current situation either. A very long trail of inter-office e-mail correspondence between executives of HBGary and HBGary Federal even now litters the Internet, laying bare their thoughts up until that moment in February when the attack began. But today, Hoglund barely seems to want to acknowledge HBGary Federal anymore, even after having licensed his company name to it.

Hoglund waves off references to HBGary Federal and the e-mail as not consequential to HBGary itself in terms of being attacked. "We shared an e-mail service, Google, with HBGary Federal," Hoglund says. "Anonymous never came within 2 to 3 network layers of us."

The devastating attack on HBGary Federal, Hoglund says, has convinced him that "you must use multi-factor authentication in every portal in your enterprise."

Directly after the Anonymous attack on HBGary Federal, vandals tore up HBGary's booth at the RSA Conference 2011 last February, and Barr also cancelled a presentation he was scheduled to give at another conference at that time running adjacent to RSA, saying he was getting death threats.

The investigation by law enforcement into the HBGary Federal incident is said to be ongoing. But Hoglund says he'll be at the RSA Conference 2012 in February, speaking on the topic "Modern Cyberthreats: The Changing Face Behind the Keyboard." He says his talk will be about advanced persistent threats, which are stealthy attacks to seize important data, and "all the things I learned about APT threats this year." ■

Anonymous' Robin Hood campaign could hurt more than banks

Anonymous and TeaMp0isoN launch credit card fraud campaign in an attempt to hurt banks

BY LUCIAN CONSTANTIN, IDG NEWS SERVICE, NOV. 30, 2011

Hacktivist groups Anonymous and TeaMp0isoN have joined together in a new campaign that involves compromising credit card details and using them to donate money to charities, homeless people and anti-government protesters around the world.

The two hacker outfits, who call their alliance p0isAnon, have named the new credit card fraud campaign "Operation Robin Hood" in reference to the famous English outlaw who, according to folklore, stole money from the rich and gave it to the poor.

"Operation Robin Hood is going to return the money to those who have been cheated by our system and most importantly to those hurt by our banks," p0isAnon said in a statement released on Monday. "Operation Robin Hood will take credit cards and donate to the 99% as well as various charities around the globe," it added.

> **"Operation Robin Hood is going to return the money to those who have been cheated by our system.**
> **POISANON SAID IN A STATEMENT**

Anonymous and TeaMp0isoN claim that they've already started their campaign. "We have already taken Chase, Bank of America, and CitiBank credit cards with big breaches across the map. We have returned it to the poor (the TRUE 99%) who deserve it," the hacktivist groups said in their joint statement.

According to Amy Kornbluth, Citi's head of consumer communications for Europe, Middle East, and Africa (EMEA), the company is currently looking into these claims, but doesn't have an official statement yet. Visa Europe did not respond to a request for comment.

The politically motivated hackers implied that their actions won't hurt cardholders because credit card fraud victims are generally reimbursed by banks. However, this might not be true in all cases, because the laws regulating fraud liability vary around the world.

"After 60 to 120 days of the transaction date, depending on the association and the country, both the customer and Citi do not have rights any longer to initiate a dispute," Kornbluth said. "Upon noticing a suspected fraudulent transaction the customer should report it immediately to the respective Citiphone customer service unit who will act swiftly to investigate the issue," she added.

Even if in most circumstances card holders might not be liable for costs resulting from fraudulent transactions, merchants can be. "Ultimately the money is lost by either the issuer bank or the acquirer/merchant depending on the chargeback rules and processes followed/not followed," Kornbluth said.

For example, if p0isAnon members use the stolen credit card information to buy blankets for Occupy Wall Street protesters, the affected banks could initiate chargebacks to recover the money from merchants, who could be left to cover their losses if they didn't follow all the procedures correctly.

Kornbluth confirmed that chargebacks can also be initiated for fraudulent donations. There are multiple online reports from organizations and independent software developers who received fraudulent donations and were later forced to pay chargeback fees in addition to returning the donated amounts.

PayPal offers a donation service for nonprofits, but its user agreement states that sellers don't benefit from protection if the sold item is not a physical, tangible good that can be shipped. Since a donation doesn't meet this criteria, a successful chargeback for a fraudulent transaction could end up costing a nonprofit a fee of US$20 in addition to the donated amount.

Anonymous and TeaMp0isoN are defiant when it comes to possible law enforcement actions against them resulting from this campaign. "We are not afraid of the Police, Secret Service, or the FBI," they said.

The groups also pointed out that "Operation Robin Hood" is an extension of the older "Operation Cash Back," which encouraged people to empty their bank accounts and put their money into credit unions. ■

Anonymous threatens to expose Mexican drug cartel

BY JOHN RIBEIRO, IDG NEWS SERVICE , OCT. 31, 2011

Anonymous advised its members to protect their online identities, and not to wear the traditional Anonymous mask in public, or even purchase them online, as a core group decides if it should take on a Mexican drug cartel that is said to have kidnapped a member of the group.

The hacker group had earlier threatened to expose the identity of members and supporters of a Mexican drug cartel by Nov. 5, in retaliation for the kidnapping of a group member, and hacked the web site of a former state official, alleging that he has associations with the dreaded Zetas cartel.

But there are fissures showing among the leaders as fear of handling the drug cartel builds up, with some expressing concern that new, inexperienced members could get quickly exposed and compromised.

The action has been cancelled, Sm0k34n0n wrote in a Twitter message in Spanish on Monday. High-profile colleague anonymouSabu described sm0k34n0n as one of the campaign's promoters in another Twitter message. But other groups from Latin America are said to be considering a core action group, and warning other members to stay away. AnonymouSabu was all for the action late Sunday.

A video in Spanish posted on YouTube on Oct. 6 by a person calling himself "MrAnonymousguyfawkes", threatened that Anonymous will publish the names, photos, and addresses of police officials, journalists, and taxi drivers that collaborate with the drug cartel, hoping the government will arrest them.

"You made a huge mistake by taking one of us. Release him. And if anything happens to him, you (expletive) will always remember this upcoming November 5th," said a masked person in the video, according to a translation provided by another user of YouTube.

Nov. 5 is known in the U.K. as Guy Fawkes day after his Nov. 5, 1605, conspiracy to attempt to blow up the British Parliament. The Guy Fawkes mask, popularized by the movie V for Vendetta, has been adopted by Anonymous.

Anonymous claimed on Sunday to have defaced the website of a former official in the Mexican state of Tabasco. On Monday, the website bore a message in Spanish by Anonymous Mexico stating that he was a part of Zetas.

"We all know who they are and where they are," said the speaker in the video. Anonymous did not however claim that its hacking skills gave it special access to information on the cartel. Nor are its traditional tactics such as DDoS (distributed denial-of-service) attacks on websites likely to be of use against armed gangs, according to various analysts.

The drug cartel has killed people who have criticized them on blogs and other social media, according to reports. The Committee to Protect Journalists in New York reported in September the murder of a journalist in direct retaliation for information posted on social media.

As newspapers are censored by fear, Mexican citizens, and many journalists, are turning to social media and online forums to share news and inform each other, said Sara Rafsky, a research associate in CPJ's Americas program. "So it should be no shock that drug cartels are turning their attention to the Internet." ■

Lulzlover hacked coalition of law enforcement, data dumped for 2,400 cops and feds

There's been no shortage of OWS video footage and some of the outrageous stunts the cops have pulled, but it caused another Anonymous hacker to lock and load on the police. From a land of cracked hashes, located somewhere over the rainbow tables, comes an AntiSec dump of the "entire member database" from C.L.E.A.R. Coalition of Law Enforcement and Retail. The hacker, Exphin1ty, claimed to be a part of Anonymous and AntiSec when addressing "lulzlovers around the world" on Pastebin. The leak contains personal data for over 2,400 law enforcement, federal agents, loss prevention professionals, and big corporations like Microsoft. While this would seem painfully obvious, @exphin1ty pointed out, "Governments of the world, '123456' is never a secure pass phrase, even when hashed. Sigh. #antisec."

"The American law enforcement's inhumane treatments of occupiers has caught our attention. You have shown through these actions that you are nothing more than puppets in the hands of your government. We have seen our fellow brothers & sisters being teargassed for exercising their fundamental liberal rights, the exact ones that were bestowed upon them by their Constitution," Exphin1ty wrote in Pastebin announcing the dump. Here's the rest of his statement:

"This fun little database dump includes hashed passwords, physical and email addresses, phone numbers etc. of many military, law enforcement officers, large corporations such as Microsoft, federal agents & security companies. Many of the users reuse their passwords elsewhere, so we encourage all of our lulz loving friends to deface & leak their twitters, facebooks and private email accounts as well as spreading their d0xes far and wide across the internet ocean. The website requires new members to be approved by an administrator, meaning the validity of this information is relatively high."

— Ms. Smith

Security researcher feels the wrath of Anonymous

BY TIM GREENE, NETWORK WORLD, FEB. 7, 2011

Wikileaks defenders Anonymous are firing both barrels at a security researcher who promised to name people in the group. Aaron Barr vowed he'd expose organizers of the online activist group Anonymous next week, but in response Anonymous hacked his Twitter account, broke into his company network and posted more than 44,000 of the company's e-mails.They also posted his home address, phone number and Social Security number on his Twitter page.

Barr, the CEO of HBGary Federal, said in an interview with the Financial Times that he'd expose the leaders of the hacktivist group Anonymous next week at a conference in San Francisco, where he is scheduled to speak at the Security B-Sides event.

Since that story ran, Anonymous has broken into HBGary Federal's network where it says it found Barr's research on the group, and declared it to be "woefully inaccurate."

"Aaron Barr missed a great deal of information that has been available online, and in fact failed to identify some of those whose identities were never intended to be hidden," the group says in the release.

Anonymous has also posted an e-mail exchange between the hacked e-mail account of Greg Hoglund (the founder of HBGary Federal's parent company, HBGary) and an HBGary Federal employee in which Anonymous convinces the employee to open up a firewall port through which the hackers gained access to the company network.

In addition to exposing personal details about Barr on his Twitter page, it doctored his photo with a Special K logo on his forehead and a piece of white tape over his mouth.

A post said, "Okay Anons, we're giving Aaron back his account in T-Minus 60 minutes. If he doesn't admit defeat in his first Tweet, we're taking it back."

An hour later the most recent post read: "Today Anonymous has shown its fury. We will destroy those who we feel need to be destroyed. Everyone learned their lesson? Back to normal." His photo had been distorted to a caricature with the words "Forever Barrlone" written on it.

A later Tweet that subsequently disappeared read, "Account control is now switching to the real Aaron Barr; Mr. Barr, you should know that we're still watching. Place nice or we won't."

After 45 minutes or so Barr hadn't Tweeted. Reached by phone, he referred questions about his battle with Anonymous to a spokesperson for HBGary Federal because he was busy dealing with problems spawned by Anonymous. "Right now I'm trying to make sure I don't lose my money or anything else," Barr said.

Later a post on his Twitter page read, "ok. So Anon has done a number on me. Probably going to take a bit to piece things together, probably more to come."

Anonymous, a loose confederation of international hackers, gained notoriety last year when it defended Wikileaks founder Julian Assange who was under siege for posting thousands of U.S. diplomatic cables online. Anonymous' tactics were to launch denial of service attacks against sites that were undermining Wikileaks' sites. ■

Anonymous supporters claim NBC News Twitter hack

BY ROBERT MCMILLAN, IDG NEWS SERVICE, SEPT. 9, 2011

Hackers calling themselves the Script Kiddies took control of the NBC News Twitter account on Friday afternoon and used it to send out a series of hoax Twitter messages claiming there was a repeat terrorist attack on New York's Ground Zero.

The Script Kiddies had control of the account, which has more than 120,000 followers, for about 10 minutes before it was suspended. During that time they sent three messages stating that hijackers had crashed two airplanes on the site of the Sept. 11, 2001, terrorist attacks. "This is not a joke, Ground Zero has just been attacked. We're attempting to get reporters on the scene. #groundzeroattacked." said one of the messages.

Then, a minute later, perhaps sensing that the jig was up, they wrote. "NBCNEWS hacked by The Script Kiddies. Follow them at @s_kiddies!"

That s_kiddies Twitter account was immediately suspended, but according to a cached version of the page, the group describes themselves as "Anonymous Supporters :: Hackers :: Exploiting simplistic methods with hilarious results :: Occasionally doing it for teh lulz :: We are The Script Kiddies."

This type of account compromise is a regular occurrence on Twitter, although it is typically celebrities, and not trusted news organizations, that fall victim. Often the accounts are taken over following a phishing attack. Script Kiddies did not respond to an email asking them how they managed to take over the NBC News account.

Script kiddies is a hacking term, referring to technically unsophisticated hackers who rely on automated scripts rather than hacking wiles to conduct their online attacks.

Friday wasn't exactly a gold star day for accuracy on Twitter. Earlier in the day, an account associated with CBS News show "What's Trending" erroneously posted a Twitter message citing rumors that Apple founder Steve Jobs had died. That message was quickly deleted and "What's Trending" apologized. ■

Anonymous breaches SF's public transport site

BY JEREMY KIRK, IDG NEWS SERVICE, AUG. 15, 2011

Anonymous released personal data on Sunday belonging to more than 2,000 public transport customers in the San Francisco area in retaliation for the Bay Area Rapid Transit (BART) system's shutdown of mobile phone service.

The data came from myBART.org and consists of user names, last names, addresses and telephone numbers for riders who used the website to manage their accounts. On Monday, the site was a blank white page with the message that it was unavailable for "renovation."

The attack comes after BART shut off mobile-phone service to hundreds of thousands of commuters on Thursday night. The agency claimed that riders planned a disturbance that threatened the safety of other passengers. The shutdown meant passengers could not dial emergency services.

BART, which has its own police force, has been criticized for the fatal shootings of two men over the last two years by its officers. Charles Hill, a 45-year-old homeless man, was fatally shot after he confronted police with a knife. In 2009, Oscar Grant was shot in the back during a scuffle with police.

In a statement, BART said personal information for 2,400 of its 55,000 users of the myBART.org website were affected. The website has been shutdown, and law enforcement has been notified, BART said. No financial information was stored on the site, it said.

But BART warned that people should be alert they could be targeted by scammers because of the breach. BART also provided information for how users can request a free credit report.

"We are sorry this intrusion into the myBART data occurred, and we notified those affectedright away in case anyone tries to exploit the information," the agency said. "We will provide an update as soon as we have additional information."

Anonymous publicly posted the data. The domain for that website, which uses the country code top-level domain for Austria, was blank except for a message in German that read "Back soon, do not worry." ■

Credit: Lauren Crabbe - PC World

myBART hack could have been worse

The disclosure of 2,000 usernames and passwords by Anonymous against a San Francisco transportation website could have been more damaging, according to a doctoral candidate at the University of Cambridge.

Joseph Bonneau, who is working on a thesis on password security, analyzed the disclosed passwords and found that more than 1,300 were randomly generated when users signed up for accounts at myBART, a marketing site for BART.

Between 2001 until 2006, myBART did not allow users to change passwords, which consisted of two digits plus up to eight lowercase characters, Bonneau said in an interview. That was good, since users were unlikely to reuse the randomly generated passwords on other accounts, such as e-mail or social networking services.

It's not uncommon for people to use the same password across a range of websites. Security experts generally advise against it, since if the password is compromised, a variety of data could be obtained by hackers by trying out the password on other sites.

In the case of myBART, which was a marketing site, the accounts that were compromised aren't valuable.

"There's no interest for criminals or even people who want to do vandalism in the myBART account, but if you can try those passwords and e-mail addresses elsewhere, you can get interesting accounts," Bonneau said.

It's rare for websites to mandate randomly generated passwords. Bonneau and a colleague, Sren Preibusch, conducted a survey in 2010 of password practices across some 150 popular websites. Only one issued a randomly generated passwords. — Jeremy Kirk

Anonymous at it again

Group says it posted e-mail addresses, passwords of 90,000 military members

BY NANCY GOHRING, IDG NEWS SERVICE, JULY 11, 2011

The Anonymous hacking group said Monday it had broken into military contractor Booz Allen Hamilton's network and posted 90,000 military e-mail addresses and passwords online.

Booz Allen isn't commenting. "As part of @BoozAllen security policy, we generally do not comment on specific threats or actions taken against our systems," the company said via its Twitter feed.

In addition to the e-mail addresses, which Anonymous suggests expose members of the intelligence community, the group also posted other data it said could potentially offer access to other government agencies and contractors.

"We infiltrated a server on [Booz Allen's] network that basically had no security measures in place,"

Anonymous said in a statement, posted to the torrent site where it uploaded the data.

The group warned on Sunday that it planned new activity. Via the @anonymouSabu Twitter account, it wrote: "ATTN Intelligence community: Your contractors have failed you. Tomorrow is the beginning."

It also said there would be two releases of information on Monday.

Anonymous and another hacking group, LulzSec, have been attacking government and law enforcement targets for a couple of months as part of a campaign they call "Antisec." Anonymous broke into an Arizona police system and released e-mails from there. It also attacked Turkish government websites. Authorities in several countries, including Spain, the U.K. and Turkey, have arrested people they say are affiliated with Anonymous.

LulzSec has disbanded following member arrests. It had attacked networks of the U.S. Central Intelligence Agency, the U.S. Senate and the U.K.'s Serious Organized Crime Agency. ■

Exxon Mobil, ConocoPhillips and Canadian Oil Sands targeted

BY TIM GREENE, NETWORK WORLD, JULY 13, 2011

Anonymous has posted names, addresses, phone numbers and email addresses of Monsanto employees, and is promising action against Exxon Mobil, ConocoPhillips, Canadian Oil Sands Ltd., Imperial Oil, the Royal Bank of Scotland and others.

In the case of Monsanto, the hacker group has posted information about 2,500 employees and affiliates of Monsanto and claim to have taken down corporate Web sites and mail servers, according to the Sophos Naked Security blogger.

Anonymous didn't indicate how it broke into the network, but mentioned that port 6666 - used for IRC chat - was opened. The port can be used for introducing Trojans and worms that can infect IRC servers and clients.

The group says it is setting up a Wiki where the data it stole from Monsanto can be posted, Sophos says.

Monsanto could not be reached immediately for comment.

Meanwhile, Anonymous has posted its intent to protest against Exxon Mobil, ConocoPhillips, Canadian Oil Sands Ltd., Imperial Oil and the Royal Bank of Scotland for their role in extracting petroleum products from tar sands in Alberta, Canada.

In what it calls Operation Green Rights, the group throws its support behind protesters in Montana who view the extraction as an environmental threat. "We will, over the course of the next few days, use the powers we posses to spread news about this scenario and the corporations involved. We are actively seeking leaks to expose the corruption that we all KNOW is beneath this," Anonymous says in a press release on its Web site.

News of the Monsanto attack came about the time when one Anonymous Twitter account said that July 12 would be the biggest day in Anonymous history, but the Monsanto incident doesn't seem to fit the bill. In the past, for example, the group has taken down MasterCard's Web site and exposed volatile emails stolen from HBGary Federal. ■

The lesson of Anonymous? Corporate security sucks

Experts say top execs pay attention to Anonymous for the wrong reasons

BY TIM GREENE, NETWORK WORLD, AUG. 8, 2011

LAS VEGAS -- Anonymous has run up quite a score against corporations, governments and law enforcement agencies, but for all these warnings corporate executives are turning their heads from the real problem -- their network security is terrible, a panel of experts concluded at Defcon.

The particularly high profile attack against security firm HBGary by the hacker collective earlier this year caught the attention of C-level executives for a few weeks, but then they relaxed, says krypt3ia, a panel member, a security blogger and longtime infosec practitioner.

The executives could have redoubled efforts to better defend their networks, but that's not what's happening. Rather than invest in better security, they're looking to hedge the economic impact if they do get hacked, he says.

"It's no coincidence that hack insurance is up," he says. He said he'd heard at the conference that a major corporation laid off security staff and bought hack insurance instead. He wouldn't name the corporation.

In doing so, executives have taken their eye off the main goal, which is protecting corporate intellectual property. By and large the Anonymous hacks and attacks have not scored valuable business intelligence, says Josh Corman, director of security research for Akamai, but it's just a matter of time until they do.

"Your executives are distracted by DDoS attacks, a new noisy thing that distracts us from the actual mission," Corman says.

Meanwhile the panel had a low assessment of Anonymous in whose name many high-profile defacements, data thefts and posting of stolen information have been made.

"Build a better Anonymous," says Jericho, another panel member and security blogger. Stealing documents and posting them all with few or none of them revealing wrongdoing doesn't make a point about whey the victim was attacked in the first place, he says.

"Releasing 250,000 documents is cool, but it hurts the cause," he says. "It's noise."

Krypt3ia says stealing and posting information from random police agencies in response to police in the United Kingdom arresting a teenager purported to be a key member of Anonymous spinoff LulzSec is irresponsible.

He cited the case of data about Phoenix police being posted in protest of the Arizona immigration laws they enforce. "Cops are bound to carry out the laws," he says. Protests about the laws should be aimed at the legislators who create them, he says, but releasing personal information about police and other law-enforcement workers is reckless. "There could be people in danger now," he says.

Corman says that Anonymous was by design decentralized, but that loose structure has enabled just about anyone to carry out attacks and attribute them to Anonymous. In some cases -- like the assistance groups using the name Anonymous gave to support uprisings in the Middle East -- the actions may coincide with what the groups founders intended.

But a change has occurred and now Anonymous attacks have less clear motivations, Corman says. "It's a franchise. Some people took the name and did Arab Spring and used it locally," he says. "Then it was hijacked by smaller groups and now it's become something of a public nuisance."

Krypt3ia gives them less credit. "I think they just wanted to smash things, and if they get caught, we say, 'We believe this ...'" he says. "You want to out people for doing bad things, do it right. ... Stop taking down stuff that's unimportant."

He says Anonymous should do its homework better and use other methods than network attacks and infiltration. "Learn your target," he says. "Know what they're doing. The only real dirt comes from insiders, people in the know who have access to very dirty things." ■

Three tips for a better Anonymous

Has the Anonymous movement reached a midlife crisis?

There's no question that the loosely confederated collective has gained members and attention over the past year, for computer attacks on PayPal, Sony, and government contractor HB Gary Federal, and for the erratic cyber-rampage carried out by its sister group, LulzSec. But maybe the group needs to grow up a bit in order to get its message across.

At the Defcon hacking conference in Las Vegas Saturday, cyber experts had some tips for building a better Anonymous.

1. Look out for your new members.

Following a December, 2010, denial of service attack on the PayPal website, the company handed the U.S. Federal Bureau of Investigation about 1,000 IP addresses linked to the attack. Those people may have thought they were downloading software -- Anonymous uses a program called

FBI warns hacktivists: You're breaking the law

BY MERIDITH LEVINSON, CIO, DEC. 19, 2011

Last July, the FBI executed what is arguably its most public campaign against hacktivists--individuals who breach computer systems to make a political or ideological statement. On Tuesday, July 19, the G-men cuffed 12 men and two women allegedly associated with hacktivist group Anonymous for their supposed involvement in a dedicated denial of service (DDoS) attack against PayPal's website in December 2010.

The July raid appeared to be the largest public indication that the FBI was finally making headway in its investigation of hacktivist activity during a year when groups including Anonymous and LulzSec made a mockery of public- and private-sector computer systems. Between December 2010 and August 2011 alone, they broke into dozens of corporate and government networks with outrage, defiance and glee.

In fact, hacktivist activity had long been on the FBI's radar, according to Shawn Henry, executive assistant director of the FBI's Criminal, Cyber, Response and Services Branch. He first noticed it in the late 1990s, when he was working as a supervisory special agent at FBI headquarters on computer intrusion cases. At the time, hacktivism consisted mostly of website defacements, he says. Today, it's more menacing. Consider the outcomes of just three data breaches launched in the name of hacktivism:

LulzSec's hack into Sony's PlayStation network in April 2011 is reportedly expected to cost Sony $171 million by the end of the entertainment company's 2012 fiscal year.

When Former HBGary Federal CEO Aaron Barr threatened to expose top members of Anonymous, the hacktivist group retaliated by breaking into the security company's systems and exposing controversial and confidential emails. Barr subsequently received death threats and was forced to step down from his job.

After Anonymous broke into the member database for Bill O'Reilly's website, a woman who's name, email address, physical address and password were exposed during the breach suffered $400 in fraudulent credit card charges and huge amounts of embarrassment after hackers posted pornographic pictures to her Facebook page and sent pornographic emails via her AOL account, the LOIC, (Low Orbit Ion Cannon) in its attacks -- and joining a movement, not committing a federal crime.

"Anonymous has this idea moving forward that anyone can join us and take up arms, but they're not educating the people who are using these tools," said Jericho, the pseudonymous security expert who founded Attrition.org, a Web site that compiles information on the computer security industry. "Anonymous needs to educate their people as much as the public on their goals."

According to Gregg Housh, an Anonymous spokesman, he was overwhelmed with emails during the December attacks from neophytes looking to join in. "The emails were all, 'I don't know what you guys are doing, but I'd like to help'," he said Saturday. "I was getting anywhere from 100 to 150 of those an hour for a week-and-a-half period." He couldn't respond to the emails, he said, because that would have meant participating in criminal activity.

Housh noted that there is an IRC (Internet relay chat) room channel called "New Blood" where Anonymous members will help.

2. Vet what you release.

Anonymous exposed HB Gary Federal's proposed disinformation campaigns against organizations such as Wikileaks, but the disgraced security firm is far from the only company involved in such operations, according to Krypt3ia, anonther pseudonymous security blogger. "It's been going on for a very long time in the private sector," he said. "It's nothing new. It's just somebody got... caught."

That means that there's a pretty good chance that Anonymous could be the target of such a campaign. There's nothing to stop any hacker from leaving a file with Anonymous's tagline, "We are legion" on a hacked computer to direct blame toward the group.

"How do you know that you're getting the real dirt? How do you know you're not getting disinformation?" Krypt3ia said.

3. Look out for collateral damage.

When LulzSec published thousands of usernames and passwords two months ago, it didn't take long for some innocent bystanders to get hurt. People had their Web mail accounts compromised and fraudulent Amazon orders placed from their accounts. Anonymous says it wants to take on hypocritical corporations and corrupt governments. Exposing the personal information of regular people doesn't help that cause.

Anonymous brought the HB Gary emails to light, but historically the best information has come from insiders such as Watergate's Deep Throat (FBI agent Mark Felt) and a member of the military, Bradley Manning, who supplied documents to Wikileaks -- not hackers, Krypt3ia said. "The real dirt has only come from insiders."

Jericho and Krypt3ia were speaking at a Defcon discussion that was supposed to include the former Federal CEO of HB Gary, Aaron Barr, but legal threats from Barr's former employer kept him offstage, hidden somewhere in the audience. HB Gary has tried to distance itself from Barr, but moving to prevent him from speaking about this experience is probably not going to sit well with the hackers who support Anonymous, said Joshua Corman, a security researcher who was also on the panel.

according to Ars Technica.

Henry maintains that the FBI isn't motivated by hacktivist groups' ideological agendas. What matters most to the FBI, he says, is that these groups are breaking the law.

"When anybody breaches a network and steals data and then publicizes it--whether they're from a foreign country and they're using the data to help their country's industry, they sell it as an organized crime group, or they just display it because they think the company they stole it from is acting inappropriately--the fact that the data is stolen is a violation of federal law," he says, his voice rising with conviction. "Hacktivism is no different from organized crime groups or foreign governments. It's the exact same activity, perhaps done for a different reason or purpose, and it's all still illegal."

In this exclusive interview with CIO.com, Henry speaks for the first time with the media specifically about hacktivism. Though Department of Justice guidelines prevented him from discussing specific hacktivist groups and open cases, he describes the threat hacktivists pose, the challenges associated with investigating them, and the FBI's success disrupting these groups. He also has a special message for hacktivists.

CIO.com: What threat do hacktivists pose? Is there some threat that their ideology poses, in addition to breaking into computer systems?

Shawn Henry: I look at three different threats to our critical infrastructure in the United States: [The first is] organized crime groups that primarily access the networks of the financial services sector. They steal data and monetize it to the tune of hundreds of millions of dollars a year. There are foreign governments breaking into computer networks and stealing data from .mil, .gov and .com domain names. They steal data to help their governments compete with the U.S., to help their industry. That's being done to the tune of billions of dollars a year.

Then there are individual hackers breaking into networks for other reasons. It may be for personal interest--hacking computers to test their skills. They may be hacking into computers to make some type of a statement.

All of those groups--regardless of whether they're organized crime operating out of Eastern Europe, a foreign government, or a 16-year-old kid down the block--once they're in, they have gained control of that network. They have the ability to do a lot more than steal data. They have the ability to change data. So data integrity is at risk. They have the ability to turn off data. They can shut the network down if they gain administrative access. If I'm the owner of a network, it doesn't matter who's in my "house": If each and every one of those groups has the ability to do the exact same thing, I'm at significant risk. Anybody who has that administrative access to that network has the ability to steal data, change data and deny us access to our own data.

"We have arrested people ... who have been responsible for tens of millions or hundreds of millions of dollars in damages".

SHAWN HENRY, executive assistant director of the FBI's Criminal, Cyber, Response and Services Branch.

What makes investigating these organizations and individuals so difficult?

Henry: One of the most significant challenges is attribution: How do you identify who committed the crime? In the physical world, if someone robs a bank, we have video cameras and maybe eye witnesses. We may have evidence, fingerprints. We have clues right away. The pool of subjects who may have robbed that bank is limited to the number of people in the vicinity of the bank at the time of the robbery. In the cyber world, the pool of candidates is limited to anybody who has access to an Internet connection at any time in the world, regardless of where they're sitting. That increases the pool of candidates. [Moreover,] the evidence we have is digital. It's fragile. It's transient.

Regardless of who the actor is, intrusion investigations by nature are complex. They're most often international in nature--they have some international nexus--whether beginning or ending overseas.

There are advantages to working these cases. The biggest advantage for us is the partnerships we've developed internationally. Many countries around the world recognize that this is a worldwide problem. We've had a lot of success working with our partners internationally.

How can you say the FBI has been successful when a hacker claiming to be affiliated with Anonymousrecently launched an attack on CLEAR that resulted in the exposure of the names, phone numbers, email and home addresses, and passwords of more than 2,400 law-enforcement, federal, military, loss-prevention and corporate professionals? .

Henry: We've had success in the U.S. against cancer, but thousands of people die from cancer every year. We've had success in organized crime. There's still organized crime in this country, but we've arrested thousands of people involved in organized crime over the years and put heads of organized crime in prison.

To say we haven't been successful because we see activity, you have to look at the totality. We have been successful in this area. There are some statistics that have been published on the number of arrests we've made. It's not near the totality of our success in this year. We've identified people. We've arrested people in intrusion cases--in many cases, people who have impacted major networks, people who have stolen millions of pieces of data, people who have been responsible for tens of millions or hundreds of millions of dollars in damages in the U.S. A lot of our successes aren't publicized&for operational purposes.

Final Thoughts From Henry to Hacktivists

My organization is a believer in civil rights and civil liberties, and the first amendment is something I hold very dear. I have no problem with people picketing and protesting in the street. But the freedom for me to swing my arm ends where your nose begins. If you are impinging on others' rights, that's illegal.

"I encourage people to promote and express their views. We in this country have probably the most robust system to enable that. We have laws that allow people to express their views. We have so many freedoms in that area that people who violate the law are way outside their lane. There are so many opportunities for people to do it lawfully that it's irresponsible for them to do it otherwise." ■

Hire hackers vs. 20 years jail time

BY MS. SMITH, NETWORK WORLD, SEPT. 16 2011

I've always thought hackers could save the world if they chose to, so a post on MSDN blogs my eye. I stopped on Terry Zink's Cyber Security Blog and watched the TED video, Hire the hackers!

Misha Glenny is, among other things, a journalist and "underworld investigator." This TED talk, Hire the hackers! opens with a clip from Anonymous. His presentation is described as "Despite multibillion-dollar investments in cybersecurity, one of its root problems has been largely ignored: who are the people who write malicious code?"

After talking about Anonymous, Glenny said, "We are at the beginning of a mighty struggle for control of the Internet. The Web links everything, and very soon it will mediate most human activity. Because the Internet has fashioned a new and complicated environment for an old-age dilemma that pits the demands of security with the desire for freedom." He then profiles several convicted coders from around the world and concluded with:

Now I think we're missing a trick here, because I don't think people like Max Vision should be in jail. And let me be blunt about this. In China, in Russia and in loads of other countries that are developing cyber-offensive capabilities, this is exactly what they are doing. They are recruiting hackers both before and after they become involved in criminal and industrial espionage activities -- are mobilizing them on behalf of the state. We need to engage and find ways of offering guidance to these young people, because they are a remarkable breed. And if we rely, as we do at the moment, solely on the criminal justice system and the threat of punitive sentences, we will be nurturing a monster we cannot tame.

Although the idea of hiring hackers is not a new one, I enjoyed Glenny's talk. So much so, that if you have a spare 18 minutes, I'd recommend watching it. He covers a great deal of territory in a relatively short time, including the moral compass of hackers and Asperger syndrome which is a common card played in defense after hackers are caught. If you don't watch, then maybe you can browse the interactive transcript and jump right to the parts that interest you?

A few of the comments on Glenny's talk caught my eye. Toby Dillon wrote, "Hackers are problem solvers and the only question is: do you want us working for you or against you? The moral thing to do is to hire them, work with them, and integrate them, not force them into a lifetime of serving criminal organizations."

Most security professionals are also hackers. Shaya Nerad pointed out that hacking is a skill set; it's what hackers choose do with those skills that sets them apart. "Anonymous is a pack of happy canines running under a full moon. There are a few really clever wolves and a bunch of dogs pretending they are wolves who are really on leashes in their parents basements, and a few coyotes who wish that they were wolves but don't have the class." As Nerad said, it will be the "script kiddies" who will be busted.

Meanwhile, as if sending a loud message to Anonymous hackers, or a threat to keep people from joining and participating in the hacking collective, the Obama administration is cracking down on cyber attacks. The White House is pushing for the Computer Fraud and Abuse Act (CFAA) to be updated so that hacking or other digital crimes can be investigated and prosecuted as organized crime. PressTV reported, "Under the proposed law, hackers who endanger national security would be put in prison for up to 20 years. The proposal would also double current prison times and increase fines in each category of computer crimes." Holy wowza! 20 years?

CDT, the ACLU, the EFF and a coalition of other groups asked Congress to be cautious with the language in CFAA. "Violations of terms of service or computer use policies are not computer crimes," said the group. "Our primary concern -- that this will lead to overbroad application of the law -- is far from hypothetical. Three federal circuit courts have agreed that an employee who exceeds an employer's network acceptable use policies can be prosecuted under the CFAA. At least one federal prosecutor has brought criminal charges against a user of a social network who signed up under a pseudonym in violation of terms of service."

Yet at the hearing about updating CFAA, James A. Baker, associate deputy attorney general, disagreed. According to InformationWeek, Baker said the Obama administration "will resist any attempts to restrict the CFAA's use of 'exceeds authorized access' as a benchmark for determining when a crime had been committed, especially when malicious insiders were involved."

Cybersecurity experts from the Secret Service, the FBI and DHS work together to combat cybercrime. This week, during Congressional testimony, witnesses from the three organizations warned of continuing attacks and evolving cyber-threats against the financial sector. The FBI reported that it is currently investigating 400 wire transfer cases. Assistant director of the Secret Service, A.T. Smith, said cybercrooks are taking advantage of the growing amount of personal information online as well as the ability to share attack tools and strategies over the Internet. "The Secret Service has observed a marked increase in the quality, quantity and complexity of cybercrimes targeting private industry and critical infrastructure."

While I believe hackers could save the world if they chose to, do you see a clear-cut right or wrong in these opposing viewpoints about hiring hackers or sending them to prison for 20 years? I'm not talking about crackers, cybercriminals stealing for financial gain, those who are taking advantage of innocent bystanders who have had their personal information dumped online, but instead asking about some of the hackers involved in Anonymous. Like Glenny suggested, how about hiring those with skills for cyber-warfare?

Both the NSA and FBI were looking to hire cyberguns at DefCon. Homeland Security was headhunting cyber-warriors even before that. Although some hackers would never go over to what they consider "the dark side," surely working for the government would beat prison? I might know a couple brilliant but excessively curious dudes who dabbled in this or that, and then were swept up into G-man life faced with such options. It didn't kill them. ■