GAWKER

Inside Anonymous' Secret War Room

John Cook and Adrian Chen
03/18/11 01:00PM Filed to: EXCLUSIVE

130.63K

Dissident members of the internet hacktivist group Anonymous, tired of what they call the mob's "unpatriotic" ways, have provided law enforcement with chat logs of the group's leadership planning crimes, as well as what they say are key members' identities. They also gave them to us.

The chat logs, which cover several days in February immediately after the group hacked into internet security firm HBGary's e-mail accounts, offer a fascinating look inside the hivemind's organization and culture.

They demonstrate that, contrary to the repeated claims of Anonymous members, the group does have ad hoc leaders, with certain members doling out tasks, selecting targets, and even dressing down members who get out of line. They prove that, contrary to their claims, at least one of the hackers responsible for releasing the publishing the e-mail addresses of thousands of Gawker users last December is in fact a key member of Anonymous. They show a collective of ecstatic and arrogant activists driven to a frenzy by a sense of their own power—they congratulated one another when Hosni Mubarak resigned, as though Anonymous was responsible—and contain bald admissions of criminal behavior that could serve as powerful evidence in criminal proceedings if the internet handles are ever linked to actual people.

The logs are from an invite-only IRC chat channel called #HQ, populated by people calling themselves Sabu, Kayla, Laurelai, Avunit, Entropy, Topiary, Tflow, and Marduk.

They were supplied by two individuals who go by the names Metric and A5h3r4 and describe themselves as former Anonymous supporters who became increasingly disenchanted with the movement's tactics, particularly the extent to which the group's more sophisticated members tolerate children and teens

participating in risky operations (British authorities arrested a 15-year-old and a 16-year-old in January, and Dutch police arrested a 16-year-old in December). They recently launched a firm they call Backtrace Security.

"The bastards are becoming arrogant sociopaths," said A5h3r4 via chat. "Acting first, not thinking of the consequences. They're recruiting children. I am a pretty far left person—I believe in privacy and free expression, but Anonymous is a vigilante group now. A mob without conscience. And I worry they will radicalize even more. In short, I believe they're on their way to becoming a genuine threat."

The logs show a collective of ecstatic and arrogant activists driven to a frenzy by a sense of their own power.

While Anonymous describes itself as a leaderless collective, the #HQ channel had a clear head honcho, a hacker who goes by the name of Sabu who claims credit for conducting the HBary hack. In plotting his next attack, on Hunton and Williams, a law firm that discussed hiring HBGary to conduct dirty tricks campaigns against Wikileaks supporters on behalf of its client Bank of America, Sabu threatens to "rape these niggers":

17:46 <&Sabu> hunton.com will be a nice fucking hit
17:46 <&marduk> hm see potential vulns [vulnerabilities]?
17:48 <&Sabu> yeah
17:48 <&Sabu> I see some potential openings
17:48 <&marduk> :]
17:49 <&Sabu> we could rape these niggers

Here is Sabu directing the other channel members to come up with a target list for their next hack, including potential media outlets and so-called "whitehat"

internet security firms, and ordering Kayla to get working:

> 17:52 <&Sabu> can you guys put together a private pad containing a list of whitehat targets, lawyers, reporters, any media that requires counter-intelligence attack
>
> [snip]
>
> 18:31 <&Sabu> guys im going offline I will be back online toorrow
> 18:31 <&Sabu> tomorrow I should have a new laptop
> 18:31 <&Sabu> muah
> 18:31 <&Sabu> and kayla
> 18:31 <&Sabu> please work on whitehat targets
> 18:34 <&marduk> will request
> 18:34 <@kayla> Sabu ofc <3 :)

"I rooted their boxes, cracked their hashes, owned their emails and social engineered their admins in hours."

And here he is excoriating Laurelai, an HQ member who had created a set of instructions for how to carry out an Anonymous attack. Sabu derided it as a stupid move that would help federal investigators make a conspiracy case if leaked and generally make Anonymous look as devious as HBGary. In the same breath that he insists Anonymous is disorganized and leaderless, Sabu plays the role of a leader, enforcing unit discipline while the other members stand by. Laurelei fights back by criticizing Sabu for quickly going public with the HBGary hack, rather than secretly listening in on their e-mails for weeks, and Sabu responds by openly admitting to his involvement: "I'm the one that did the op, I rooted their boxes, cracked their hashes, owned their emails and social engineered their admins in hours."

04:44 <&Sabu> who the fuck wrote that doc
04:45 <&Sabu> remove that shit from existence
04:45 <&Sabu> first off there is no hierachy or leadership, and thus an operations manual is not needed

[snip]

04:46 <&Sabu> shit like this is where the feds will get american anons on rico act abuse and other organized crime laws
04:47 <@Laurelai> yeah well you could have done 100 times more effective shit with HBgary
04:47 <@Laurelai> gratted what we got was good
04:47 <&Sabu> if you're so fucking talented why didn't you root them yourselves?
04:47 <@Laurelai> but it could have been done alot better
04:47 <&Sabu> also we had a time restraint
04:48 <&Sabu> and as far as I know, considering I'm the one that did the op, I rooted their boxes, cracked their hashes, owned their emails and social engineered their admins in hours
04:48 <&Sabu> your manual is irrelevent.

[snip]

04:51 <&Sabu> ok who authored this ridiculous "OPERATIONS" doc?
04:51 <@Laurelai> look the guideline isnt for you
04:51 <&Sabu> because I'm about to start owning nigg3rs
04:51 <&marduk> authorized???
04:52 <@Laurelai> its just an idea to kick around
04:52 <@Laurelai> start talking
04:52 <&Sabu> for who? the feds?
04:52 <&marduk> its not any official doc, it is something that Laurelai wrote up.. and it is for.. others

04:52 <&marduk> on anonops
04:52 <&Sabu> rofl
04:52 <@Laurelai> just idea
04:52 <@Laurelai> ideas
04:52 <&Sabu> man
04:52 <&marduk> at least that is how i understand it
04:52 <@Laurelai> to talk over
04:53 <&Sabu> le sigh
04:53 <&marduk> mmmm why are we so in a bad mood?
04:53 <&Sabu> my nigga look at that doc
04:53 <&Sabu> and how ridiculous it is

[snip]

04:54 <&marduk> look, i think it was made with good intentions. and it is nothing you need to follow, if you dont like it, it is your good right
04:55 <&Sabu> no fuck that. its docs like this that WHEN LEAKED makes us look like an ORGANIZED CRIME ORGANIZATION

Members of the HQ chat were, understandably, obsessed with security. But they seemed to believe that they were safe in that chat room, candidly discussing their own efforts to distance themselves from any illegal activity. Here is Topiary, who has given a number of media interviews, discussing plans to stop speaking for Anonymous in the first person in order to "avoid being raped by Feds":

15:13 <@Topiary> also I'm going to start saying, with future press, that I'm an observer/associate of Anon that agrees with Anonymous actions, rather than say I'm Anon
15:13 <@Topiary> kind of like Barrett/Housh [Anonymous spokesmen Barrett Brown and Gregg Housh]
15:13 <@Topiary> to avoid being raped by Feds

15:14 <@tflow> aw
15:14 <@tflow> why

[snip]

15:15 <@Topiary> all I have to do is stop saying "we" and start saying "they" when referring to Anon
15:15 <@tflow> it will decrease the lulz in interviews
15:15 <@Topiary> hm, valid point

And here, in the same vein, they discuss how to interact with the press without being seen as an actual member of the group, including references to Sabu, Kayla, and Tflow's efforts to maintain plausible deniability about their roles in the HBGary hack.

23:12 <&marduk> i would refrein from using "rep" ever
23:12 <&marduk> simply because.. that makes you/us directly tiable/responsible for what happens
23:12 <&marduk> no need to
23:12 <&marduk> example: the penny lock
23:12 <&marduk> yeah sabu/kayla/tflow obviously were involved in the hack. but they never admitted to
23:13 <&marduk> from the logs, you can only deduct that they knew about the operation

Sabu didn't feel the need to be as discreet in the HQ chat. Here he is taking responsibility for the HBGary hack, which involved tricking a Nokia network security specialist named Jussi into handing over passwords:

02:39 <&Sabu> "Greatest social hack of all time: http://is.gd/duaZcG - Anonymous vs. hbgary.com."

02:39 <&Sabu> rofl
02:39 <&Sabu> people are really enjoying the socialing of jussi
02:39 <&Sabu> man I was talking to my little brother who witnessed the whole shit
02:39 <&Sabu> I think he and I were as excited as people are about it now
02:39 <&Sabu> we were fitdgeting and giggling and shit
02:40 <&Sabu> as jussi dropped firewall
02:40 <&Sabu> then reset the pw
02:40 <&Sabu> then gave us the username

The logs also seem to prove that members of Anonymous were involved in hacking into Gawker's servers last December. Gnosis, the group that claimed credit for the hack, claimed in interviews to have no affiliation with Anonymous. But Kayla, a member of the HQ chat who was intimately involved with the HBGary attack, implicitly takes credit at one point for the Gawker attacks after someone mentions a Gawker article:

18:26 * kayla h8's gawker :D
18:26 <@kayla> Nick Denton especially h8's me :D

Kayla claims to be a 16-year-old girl, and has publicly admitted involvement with the HBGary infiltration (some, including Metric and A5h3r4, doubt Kayla's claims and suspect her to be in reality Corey Barnhill, a New Jersey hacker in his late 20s who also goes by the name Xyrix). Whoever Kayla is, she was definitely involved in the attack on Gawker. The HQ chats show that Anonymous made use of a the domain internetfeds.mil.nf in preparing HBGary e-mails for release. According to Matt Keys, a journalist who infiltrated the group, the Internet Feds (and not Gnosis), were the real Gawker attackers. And Kayla was one of them. "Kayla was one of two hackers who broke into the Gawker database," Keys told Gawker. "It was her idea. She coordinated the attack. She carried it out with another hacker. A third was involved in the

distribution of the torrent, but the brainchild of the Gawker hack attack was Kayla." Keys provided Gawker with screengrabs from the Internet Feds IRC chat as evidence.

Ever since Anonymous began taking down the websites of PayPal, Mastercard, and other firms that refused to do business with Julian Assange, Wikileaks has insisted that it has no connection with Anonymous. But the logs seem to show that Laurelai, one of the HQ chat members, is a Wikileaks volunteer. When Sabu asks fellow chat members who she is, they respond that she's affiliated with the group:

04:51 <&Sabu> who the fuck is laurelai and why is he/she/it questioning our owning of hbgary
04:51 <&marduk> uhm.. she is with wl
04:51 <&Sabu> and?
04:51 <&marduk> and kayla knows her.
04:51 <&Sabu> bleh

Laurelai is also involved in Crowdleaks, a site devoted to translating and disseminating Wikleaks' material. According to Metric and A5h3r4, Laurelei has claimed in chats to be affiliated with the group. They caution that it could be puffery, though, as not everything she's claimed has been reliable.

Speaking of puffery, the HQ chat's reaction to Mubarak stepping down in Egypt serves as a handy indicator of just how seriously Anonymous takes itself, and it's power:

18:13 <~Avunit> and mubarak is gone
18:13 <~Avunit> for if you dont watch the news
18:15 <&Sabu> oh wow i didnt know fuck yes

18:15 <&Sabu> congrats all
18:15 * Avunit bows to sabu.

The logs show an obsession with media coverage, and HQ members take delight in interacting with reporters, whether it's a genuine attempt to get the word out or a chance to fuck with gullible reporters. Here they are doing the latter to a *Guardian* reporter:

11:59 <@Topiary> Goddamnit this Guardian bitch is requesting access to "secret" inner-circle channels so she can tell everyone about how hard Anon works and to have first-hand experience at our inner workings
11:59 <@Topiary> I say we fake a secret channel and discuss in BATSHIT CODE
11:59 <@Topiary> and then invite her
11:59 <@tflow> lol

[snip]

12:01 <@Topiary> fuck niggahs, do you wanna make one on anonops called #over9000 or something?
12:01 <@Topiary> then we invite her and just, I don't know
12:01 <@Topiary> we just go to town in hackers on steroids talk
12:02 <&marduk> mhh not sure but i could utter some cryptic stuff
12:02 <~Avunit> bitch: create it

[snip]

12:03 <@tflow> Topiary: so she's not actually believing that anonymous isn't secretive?
12:03 <@tflow> if so, epic troll the guardian and teach them a lesson
12:03 <@Topiary> epic troll time
12:03 <~Avunit> speak like cryptic, only to eachother and be blunt to her

12:03 <~Avunit> god yeah
12:03 <~Avunit> lets roll
12:03 <@Topiary> she wants to delve into the secret underbelly, we'll give her a trolling hellstorm

The obsession with secrecy and security in HQ led naturally to paranoia, as seen in this account from Entropy, who became convinced when his boss called him into the office unexpectedly—earlier in the logs he referred to talking the "CCIE security written test," suggesting he's an internet security specialist—that it was some sort of sting.

14:50 <@entropy> my boss called me
14:50 <@entropy> ans asked me if i can come into work
14:50 <@entropy> they couldnt have got anythign this fast right
14:51 <@entropy> my hands are fuckign shaking
14:51 <@entropy> should i go there
14:51 <@tflow> gahh..
14:51 <@entropy> its way to fats right
14:52 <@entropy> fast
14:52 <@kayla> for what?
14:53 <@entropy> for the police to do anything?
14:53 <@kayla> i'd say so
14:53 <@entropy> thats what i think
14:53 <@kayla> why would they go to your work and not your house?
14:53 <@entropy> i have no idea
14:53 <@kayla> i think you're being paranoid :D
14:53 <&marduk> yah that makes no sense, rly
14:53 <@entropy> ok fuck
14:54 <@entropy> too many wierd things now im fuckign paranoid as shit
14:54 <@entropy> i need to calm the fuck down
15:10 <@entropy> theres two people with my boss in my conf room

15:10 <@entropy> two guys
15:10 <@entropy> i have no fucking idea whats goign on
15:10 <@entropy> should i call a layer before i go in there or ?
15:10 <@entropy> just to be safe?
15:16 <~Avunit> djklgadklgjdlgjak
15:16 <~Avunit> sdgmldgjklal
15:17 <~Avunit> dgjdklagjldgjkladjgkladg
15:18 <~Avunit> we're getting bullshitted badly rite?
15:18 <~Avunit> entropy
15:18 <@entropy> i fucking wish i was bullshitting
15:18 <@entropy> im goign to fucking throw up
15:19 <~Avunit> jesus shitting fuck

Turns out it was nothing!

Metric and A5h3r4 also provided us with what they say are the actual identities of Sabu, Kayla, Laurelai, Avunit, Topiary, and other members of the chat. We couldn't connect the handles to the names provided with any certainty, so we're not publishing them.

But they say they provided the same information to the FBI. When we called the special agent they gave it to, he replied, "as an agent on that case, I'm not going to discuss ongoing investigative matters" and referred us to a spokesman, who had no immediate comment. Metric and A5h3r4 also say they've handed the material to the Department of Defense, but declined to identify to whom.

Barrett Brown, who is generally regarded by Anonymous members as a spokesman for the group, said he has known about the "security breach" for some time: "We're aware of the security breach as other logs from 'HQ' have been posted before (and I should note that HQ is not really HQ anyway — you will note that the actual coordination of performed hacks will not appear in those logs). I can tell you that those who were responsible for pulling off

HBGary ... no longer use that room due not only to this security breach, but other factors as well." When we repeated Metric and A5h3r4's claims that Anonymous had become megalomaniacal and vindictive, Brown replied: "I can also confirm that we have become vindicative megalomaniacs."