BRIAN MCWILLIAMS CULTURE AUG 13, 2002 2:00 AM

White-Hat Hate Crimes on the Rise

A group of black-hat hackers, in a campaign called "Project Mayhem," have declared war on white-hat hackers who've gone to work for security firms. By Brian McWilliams.

WHEN HACKERS BROKE into Ryan Russell's server and plastered his private e-mails and other personal files on the Internet last week, Russell tried to shrug it off as a harmless prank.

But Russell, editor of Hack Proofing Your Network and an analyst with SecurityFocus.com, also seemed shaken by the incident.

"There's a group out there whose goal in life is to show they're smarter than you and they have the tools to do it," said Russell, a "white-hat" hacker who goes by the nickname "BlueBoar."

The break-in at Russell's Thieveco.com site, which is hosted by a Canadian ISP, appears to be the latest in a series of attacks against white hats and prominent figures in the information security profession.

Claiming responsibility for the attacks is a shadowy group named el8. Earlier this year, members launched Project Mayhem, a campaign designed to "cause worldwide physical destruction to the security industry infrastructure," according to an article published last month in el8's online magazine.

While the authors of el8's e-zine have an obvious penchant for tongue-in-cheek hyperbole and black humor ("Going to Defcon or Blackhat? Initiate a napalm strike," urges one recent article), most victims of Project Mayhem are not amused.

OpenBSD co-founder Theo de Raadt, cited as a top el8 target, angrily refused to discuss the compromise in late July of a file server maintained by the open-source, Unix-based operating-system project. On Aug. 1, a dangerous Trojan horse program was discovered amid the code for OpenBSD, which is used by thousands of organizations and renowned for its security.

While de Raadt wouldn't comment on whether there were any suspects in the case, the lead article in the latest el8 newsletter, published in early July, contains an obvious smoking gun. The article begins with several lines of screen-display from what appears to be an OpenBSD.org system. The "w-command" output suggests that attackers had access to one of de Raadt's accounts.

According to Steve "Hellnbak" Manzuik, co-moderator of the VulnWatch security mailing list, hacker feuds are nothing new, and Project Mayhem isn't the first time that security professionals have been attacked by "script kiddies," or inexperienced hackers.

"The only real difference is that the el8 guys are not script kiddies. Nothing has changed, other than the bar has been raised," Manzuik said.

Much of Project Mayhem's modus operandi appears borrowed from Hollywood. The group's newsletter cribs heavily from the 1999 movie *Fight Club*, starring Brad Pitt and Edward Norton, which depicts disaffected young males who find release in punching each other out and contemplating the complete and total destruction of society.

"They are referencing it constantly. They're like a copycat of the movie, only moved to the hacker scene," said Thor "Jumper" Larholm, a white-hat security researcher with Pivx Solutions.

Indeed, some of Project Mayhem's recent victims appear to be honoring a recurring line in *Fight Club*: "The first rule of Project Mayhem is you do not ask questions."

Shane "K2" Macaulay, a member of a hacking counter-attack think tank called the Honeynet Project, had several recent e-mail conversations with Honeynet founder Lance Spitzer, as well as other colleagues, intercepted by hackers and mockingly reproduced in the latest el8 zine. Macaulay declined interview requests.

Other Honeynet members refused to comment on el8's published threats against their project, although one Honeynet participant conceded that "there are people in the movement that may be able to make some of their claims come true."

Why so much venom against white hats, the hackers who ostensibly break software in order to help make the Internet safer? The el8 zines don't clearly spell out the group's motivations, but Project Mayhem appears to be a violent incarnation of the "anti-sec" movement, a campaign to persuade hackers not to publish information about the security bugs they uncover.

"Why be targeted by us when you can join us? Why post info, codes, or bugs when the end result is your entire system, family, and friends being owned? Doesn't it look like more fun to be a black hat than a white hat?" asks el8 in its latest newsletter.

According to Eric "Loki" Hines, founder of Fate Research Labs, el8 members are frustrated by white hats who spill the beans about security vulnerabilities, thereby enabling vendors to create patches and protect users.

"You've got to realize that these people are walking around with exploits that vendors haven't even heard of yet. They're pissed and they've got this almost God-like power that enables them to break into any network that they want," Hines said. He reported that FateLabs.com was knocked offline last week by a denial-of-service attack immediately after the security firm published an advisory about a security bug.

Mark "Simple Nomad" Loveless, a senior security analyst with Bindview Corporation, said el8's stance is just an extreme version of that shared by many disillusioned hackers.

"The commercial security industry is feeding off of white-hat hackers, and with the amount of fear, uncertainty and doubt being slung in the industry, I am not surprised by this feeling from el8," Loveless said.

One recent Project Mayhem victim says being attacked by el8 "made me realize the errors of my ways." Christopher "Ambient Empire" Abad, a security expert with Qualys, confirmed that excerpts of e-mails and other files stolen from his

directory on a server were published in el8's latest zine. A message in the newsletter announced that a CD-ROM of his files would be available for purchase at the Defcon hacker convention.

"Not all that glitters is white hat," said Abad, whose new website includes a message that says "Support Hacker Reform ... The rights of the people come

before the rights of the corporation and the government."

Other hackers said they are sympathetic toward Project Mayhem, although they were quick to distance themselves from the recent attacks on white hats.

Members of one group, which has recently taken over an Internet relay chat channel named #phrack, last week co-authored a mission statement saying that white hats will be "hunted down" if they continue to publicize information about security bugs.

"If they do not change they will continue to be targeted, and it sucks to get owned, fired, physically beaten," said the #phrack manifesto, which was posted, along with the contents of Russell's home directory, at the website of one of the #phrack channel's operators, a 16-year-old who uses the nickname "gayh1tler."

But Hines said the constant threats he receives from angry black hats will not frighten Fate Research Labs into sitting on vulnerabilities it discovers.

"One of these days, these kids are going to have to pay a mortgage and get a job. And they're not going to become lawyers or doctors -- they're going to do what they're good at. And that means getting a career in the security industry," Hines said.