USA TODAY.com

Cybercrime, Inc. -- Malicious-software spreaders get sneakier, more prevalent

So-called bot herders team with organized crime to steal identities, account info
[FINAL Edition]

USA TODAY - McLean, Va.

Author:	Byron Acohido and Jon Swartz
Date:	Apr 24, 2006
Start Page:	B.1
Section:	MONEY
Document Types:	News
Text Word Count:	2715

Document Text

SEATTLE -- At the height of his powers, Jeanson James Ancheta felt unstoppable.

From his home in Downey, Calif., the then-19-year-old high school dropout controlled thousands of compromised PCs, or "bots," that helped him earn enough cash in 2004 and 2005 to drive a souped-up 1993 BMW and spend $600 a week on new clothes and car parts.

He once bragged to a protege that hacking Internet-connected PCs was "easy, like slicing cheese," court records show.

But Ancheta got caught. In the first case of its kind, he pleaded guilty in January to federal charges of hijacking hundreds of thousands of computers and selling access to others to spread spam and launch Web attacks.

In separate cases, federal authorities last August also assisted in the arrest of Farid Essebar, 18, of Morocco, and last month indicted Christopher Maxwell, 19, of Vacaville, Calif., on suspicion of similar activities.

The arrests underscore an ominous shift in the struggle to keep the Internet secure: Cybercrime undergirded by networks of bots -- PCs infected with malicious software that allows them to be controlled by an attacker -- is soaring.

Without you realizing it, attackers are secretly trying to penetrate your PC to tap small bits of computing power to do evil things. They've already compromised some 47 million PC's sitting in living rooms, in your kids' bedrooms, even on the desk in your office.

Bot networks have become so ubiquitous that they've also given rise to a new breed of low-level bot masters, typified by Ancheta, Essebar and Maxwell.

Tim Cranton, director of Microsoft's Internet Safety Enforcement Team, calls bot networks "the tool of choice for those intent on using the Internet to carry out crimes."

Budding cyberthieves use basic programs and generally stick to quick-cash schemes. Brazen and inexperienced, they can inadvertently cause chaos: Essebar is facing prosecution in Morocco on charges of releasing the Zotob worm that crippled systems in banks and media companies around the world; Maxwell awaits a May 15 trial for allegedly spreading bots that disrupted operations at Seattle's Northwest Hospital.

More elite bot herders, who partner with crime groups to supply computer power for data theft and other cyberfraud, have proved to be highly elusive. But the neophytes tend to be sloppy about hiding their tracks. The investigations leading to the arrests of Ancheta, Essebar and Maxwell have given authorities their most detailed look yet at how bots enable cybercrime.

Estimating the number of bots is difficult, but top researchers who participate in meetings of high-tech's Messaging Anti-Abuse Working Group often use a 7% infection rate as a discussion point. That means as many as 47 million of the 681 million PCs connected to the Internet worldwide may be under the control of a bot network.

Security giant McAfee detected 28,000 distinct bot networks active last year, more than triple the amount in 2004. And a February survey of 123 tech executives, conducted by security firm nCircle, pegged annual losses to U.S. businesses because of computer- related crimes at $197 billion.

Law enforcement officials say the ground floor is populated by perhaps hundreds of bot herders, most of them young men. Mostly, they assemble networks of compromised PCs to make quick cash by spreading adware -- those pop-up advertisements for banking, dating, porn and gambling websites that clutter the Internet. They get paid for installing adware on each PC they infect.

"The low-level guys ... can inflict a lot of collateral damage," says Steve Martinez, deputy assistant director of the FBI's Cyber Division.

Ancheta and his attorney declined to be interviewed, and efforts to reach Essebar with help from the FBI were unsuccessful. Steven Bauer, Maxwell's attorney, said his client was a "fairly small player" who began spreading bots "almost as a youthful prank."

The stories of these three young men, pieced together from court records and interviews with regulators, security experts and independent investigators, illustrate the mind-set of the growing fraternity of hackers and cyberthieves born after 1985. They also provide a glimpse of Cybercrime Inc.'s most versatile and profitable tool.

Ancheta: Trading candy

School records show that Ancheta transferred out of Downey High School, in a suburb near Los Angeles, in December 2001 and later attended an alternative program for students with academic or behavioral problems. Eventually, he earned a high school equivalency certificate. Ancheta worked at an Internet cafe and expressed an interest in joining the military reserves, his aunt, Sharon Gregorio, told the Associated Press.

Instead, in June 2004, court records show, he discovered rxbot, a potent -- but quite common -- computer worm, malicious computer code designed to spread widely across the Internet.

Ancheta likely gravitated to it because it is easy to customize, says Nicholas Albright, founder of Shadowserver.org, a watchdog group. Novices often start by tweaking worms and trading bots. "I see high school kids doing it all the time," says Albright. "They trade bot nets like candy."

Ancheta proved more enterprising than most. He infected thousands of PCs and started a business -- #botz4sale -- on a private Internet chat area. From June to September 2004, he made about $3,000 on more than 30 sales of up to 10,000 bots at a time, according to court records.

By late 2004, he started a new venture, court records show. He signed up with two Internet marketing companies, LoudCash of Bellevue, Wash., and GammaCash Entertainment of Montreal, to distribute ads on commission.

But instead of setting up a website and asking visitors for permission to install ads -- a common, legal practice -- he used his bots to install adware on vulnerable Internet-connected PCs, court records show. Typically, payment for each piece of adware installed ranges from 20 cents to 70 cents.

Working at home, Ancheta nurtured his growing bot empire during a workday that usually began shortly after 1 p.m. and stretched non- stop until 5 a.m., a source with direct knowledge of the case says. He hired an assistant, an admiring juvenile from Boca Raton, Fla., nicknamed SoBe, court records show. Chatting via AOL's free instant- messaging service, Ancheta taught him how to spread PC infections and manage adware installations.

Checks ranging as high as $7,996 began rolling in from the two marketing firms. In six months, Ancheta and his helper pulled in nearly $60,000, court records show.

During one online chat with SoBe about installing adware, Ancheta, who awaits sentencing May 1, advised his helper: "It's immoral, but the money makes it right."

Sean Sundwall, a spokesman for Bellevue, Wash.-based 180solutions, LoudCash's parent company, said Ancheta distributed its adware in only a small number of incidents listed in the indictment. GammaCash had no comment.

Maxwell: Infecting a hospital

At about the same time -- in early 2005 -- Christopher Maxwell and two co-conspirators were allegedly hitting their stride running a similar operation. From his parents' home in Vacaville, Calif., Maxwell, then an 18-year-old community college student, conspired with two minors in other states to spread bots and install adware, earning $100,000 from July 2004 to July 2005, according to a federal indictment.

They ran into a problem in January 2005 when a copy of the bot they were using inadvertently found its way onto a vulnerable PC at Seattle's Northwest Hospital. Once inside the hospital's network, it swiftly infected 150 of the hospital's 1,100 PCs and would have compromised many more. But the simultaneous scanning of 150 PCs looking for other machines to infect overwhelmed the local network, according to an account in court records.

Computers in the intensive care unit shut down. Lab tests and administrative tasks were interrupted, forcing the hospital into manual procedures.

Over the next few months, special agent David Farquhar, a member of the FBI's Northwest Cyber Crime Task Force, traced the infection to a NetZero Internet account using a phone number at Maxwell's parents' home, leading to Maxwell's indictment on Feb. 9. He pleaded not guilty.

Essebar: Birth of a worm

As authorities closed in on Ancheta and Maxwell last summer, 18- year-old Farid Essebar was allegedly just getting started in the bots marketplace. The FBI says the skinny, Russian-born resident of Morocco operated under the nickname Diabl0 (pronounced Diablo but spelled with a zero). Diabl0 began attracting notice as one of many copycat hackers tweaking the ubiquitous Mytob e-mail worm. E-mail worms compromise a PC in much the same way as a bot, but the victim must help, by clicking on an e-mail attachment to start the infection.

Diabl0 created a very distinctive version of Mytob designed to lower the security settings on infected PCs, install adware and report back to Diabl0 for more instructions. Last June, David Taylor, an information security specialist at the University of Pennsylvania, spotted Diabl0 on the Internet as he was about to issue such instructions. Taylor engaged the hacker in a text chat.

Diabl0 boasted about using Mytob to get paid for installing adware. "I really thought that he was immature," Taylor recalls. "He was asking me what did I think about his new bot, with all these smiley faces. Maybe he didn't realize what he was doing was so bad."

In early August, Diabl0 capitalized on a golden opportunity when Microsoft issued its monthly set of patches for newly discovered security holes in Windows. As usual, independent researchers immediately began to analyze the patches as part of a process to develop better security tools. Cybercrooks closely monitor the public websites where results of this kind of research get posted.

Diabl0 latched onto one of the test tools and turned it into a self-propagating worm, dubbed Zotob, says Charles Renert, director of research at security firm Determina. Much like Mytob, Zotob prepared the infected PC to receive adware. But Zotob did one better: It could sweep across the Internet, infecting PCs with no user action required.

Diabl0 designed Zotob to quietly seek out certain Windows computer servers equipped with the latest compilation of upgrades, called a service pack. But he failed to account for thousands of Windows servers still running outdated service packs, says Peter Allor, director of intelligence at Internet Security Systems.

By the start of the next workweek, Zotob variants began snaking into older servers at the Canadian bank CIBC, and at ABC News, The New York Times and CNN. The servers began rebooting repeatedly, disrupting business and drawing serious attention to the new worm. "Zotob had a quality-assurance problem," says Allor. Diabl0 had neglected to ensure Zotob would run smoothly on servers running the earlier service packs, he says.

Within two weeks, Microsoft's Internet Safety Enforcement Team, a group of 65 investigators, paralegals and lawyers, identified Essebar as Diabl0 and pinpointed his base of operations. Microsoft's team also flushed out a suspected accomplice, Atilla Ekici, 21, nicknamed Coder.

Microsoft alerted the FBI, which led to the Aug. 25 arrests by local authorities of Essebar in Morocco and Ekici in Turkey.

The FBI holds evidence that Ekici paid Essebar with stolen credit card numbers to create the Mytob variants and Zotob, Louis Reigel, assistant director of the FBI's Cyber Division told reporters.

While Ancheta operated as a sole proprietor, and Maxwell was part of a three-man shop, Essebar and Ekici functioned more like freelancers, says Allor. They appeared to be part of a loose "confederation of folks who have unique abilities," says Allor.

"They come together with others who have unique abilities, and from time to time they switch off who they work with."

Despite their notoriety, Essebar, Ancheta and Maxwell represent mere flickers in the Internet underworld. More elite hackers collaborating with organized crime groups take pains to cover their tracks -- and rarely get caught.

"Those toward the lower levels of this strata are the ones that tend to get noticed and arrested pretty quickly," says Martin Overton, a security specialist at IBM.

Acohido reported from Seattle, Swartz from San Francisco.

*Spamming. Bots deliver 70% of nuisance e-mail ad

*Phishing. Bots push out e-mail scams that lure victims into divulging log-ons and passwords.

Parson was the only hacker arrested in connection with MSBlaster, which infected more than 20 million PCs.

Swartz reported from San Francisco, Acohido from Seattle.

[Illustration]
GRAPHIC, Color, Sam Ward, USA TODAY (illustratrion); PHOTO, B/W, Downey, Calif., Police; GRAPHIC, B/W, Alejandro Gonzalez (BAR GRAPH)

Abstract (Document Summary)

As authorities closed in on [James Ancheta] and [Christopher Maxwell] last summer, 18- year-old Farid Essebar was allegedly just getting started in the bots marketplace. The FBI says the skinny, Russian-born resident of Morocco operated under the nickname Diabl0 (pronounced Diablo but spelled with a zero). Diabl0 began attracting notice as one of many copycat hackers tweaking the ubiquitous Mytob e-mail worm. E-mail worms compromise a PC in much the same way as a bot, but the victim must help, by clicking on an e-mail attachment to start the infection.

Diabl0 latched onto one of the test tools and turned it into a self-propagating worm, dubbed Zotob, says Charles Renert, director of research at security firm Determina. Much like Mytob, Zotob prepared the infected PC to receive adware. But Zotob did one better: It could sweep across the Internet, infecting PCs with no user action required.

By the start of the next workweek, Zotob variants began snaking into older servers at the Canadian bank CIBC, and at ABC News, The New York Times and CNN. The servers began rebooting repeatedly, disrupting business and drawing serious attention to the new worm. "Zotob had a quality-assurance problem," says [Peter Allor]. Diabl0 had neglected to ensure Zotob would run smoothly on servers running the earlier service packs, he says.