The 10 Most Mysterious Cyber Crimes
Corinne Iozzo
http://www.pcmag.com/article2/0,2817,2331225,00.asp

The most nefarious and crafty criminals are the ones who operate completely under the radar. In the computing world security breaches happen all the time, and in the best cases the offenders get tracked down by the FBI or some other law enforcement agency.

But it's the ones who go uncaught and unidentified (those who we didn't highlight in our Cyber Crime Hall Fame that are actually the best. Attempting to cover your tracks is Law-Breaking 101; being able to effectively do so, that's another story altogether.

When a major cyber crime remains unsolved, though, it probably also means that those of us outside the world of tech crime solving may never even know the crime occurred.

These are some of the top headline-worthy highlights in the world of unsolved computing crime—cases in which the only information available is the ruin left in their wake.

**The WANK Worm (October 1989)**
Possibly the first "hacktivist" (hacking activist) attack, the WANK worm hit NASA offices in Greenbelt, Maryland. WANK (Worms Against Nuclear Killers) ran a banner (pictured) across system computers as part of a protest to stop the launch of the plutonium-fueled, Jupiter-bound Galileo probe. Cleaning up after the crack has been said to have cost NASA up to a half of a million dollars in time and resources. To this day, no one is quite sure where the attack originated, though many fingers have pointed to Melbourne, Australia-based hackers.

**Ministry of Defense Satellite Hacked (February 1999)**
A small group of hackers traced to southern England gained control of a MoD Skynet military satellite and signaled a security intrusion characterized by officials as "information warfare," in which an enemy attacks by disrupting military communications. In the end, the hackers managed to reprogram the control system before being discovered. Though Scotland Yard's Computer Crimes Unit and the U.S. Air Force worked together to investigate the case, no arrests have been made.

**CD Universe Credit Card Breach (January 2000)**
A blackmail scheme gone wrong, the posting of over 300,000 credit card numbers by hacker Maxim on a Web site entitled "The Maxus Credit Card Pipeline" has remained unsolved since early 2000. Maxim stole the credit card information by breaching CDUniverse.com; he or she then demanded $100,000 from the Web site in exchange for destroying the data. While Maxim is believed to be from Eastern Europe, the case remains as of yet unsolved.

**Military Source Code Stolen (December 2000)**
If there's one thing you don't want in the wrong hands, it's the source code that can control missile-guidance systems. In winter of 2000, a hacker broke into government-contracted Exigent Software Technology and nabbed two-thirds of the code for Exigent's OS/COMET software, which is responsible for both missile and satellite guidance, from the Naval Research Lab in Washington, D.C. Officials were able to follow the trail of the intruder "Leaf" to the University of Kaiserslautern in Germany, but that's where the trail appears to end.
Anti-DRM Hack (October 2001)
In our eyes, not all hackers are bad guys (as evidenced by our list of the Ten Greatest Hacks of All Time); often they're just trying to right a wrong or make life generally easier for the tech-consuming public. Such is the case of the hacker known as Beale Screamer, whose FreeMe program allowed Windows Media users to strip digital-rights-management security from music and video files. While Microsoft tried to hunt down Beale, other anti-DRM activists heralded him as a crusader.

Dennis Kucinich on CBSNews.com (October 2003)
As Representative Kucinich's presidential campaign struggled in the fall of 2003, a hacker did what he could to give it a boost. Early one Friday morning the CBSNews.com homepage was replaced by the campaign's logo. The page then automatically redirected to a 30-minute video called "This is the Moment," in which the candidate laid out his political philosophy. The Kucinich campaign denied any involvement with the hack, and whoever was responsible was not identified.

Hacking Your MBA App (March 2006)
Waiting on a college or graduate school decision is a nail-biting experience, so when one hacker found out how to break into the automated ApplyYourself application system in 2006, it was only natural that he wanted to share the wealth. Dozens of top business schools, including Harvard and Stanford, saw applicants exploiting the hack in order to track their application statuses. The still-unknown hacker posted the ApplyYourself login process on Business Week's online forums; the information was promptly removed and those who used it were warned by schools that they should expect rejection letters in the mail.

The 26,000 Site Hack Attack (Winter 2008)
MSNBC.com was among the largest of the thousands of sites used by a group of unknown hackers earlier this year to redirect traffic to their own JavaScript code hosted by servers known for malware. The malicious code was embedded in areas of the sites where users could not see it, but where hackers could activate it.

Supermarket Security Breach (February 2008)
Overshadowed only by a T.J Maxx breach in 2005, the theft of at least 1,800 credit and debit card numbers (and the exposure of about 4.2 million others) at supermarket chains Hannaford and Sweetbay (both owned by the Belgium-based Delhaize Group) in the Northeast United States and Florida remains unsolved more than six months later. Chain reps and security experts are still unclear as to how the criminals gained access to the system; the 2005 T.J.Maxx breach took advantage of a vulnerability in the chain's wireless credit transfer system, but Hannaford and Sweetbay do not use wireless transfers of any sort. Without more information, the difficulty in tracking down those responsible grows exponentially.

Comcast.net Gets a Redirect (May 2008)
A devious hack doesn't always mean finding a back door or particularly crafty way into a secure network or server; sometimes it just means that account information was compromised. Such was the case earlier this year when a member of the hacker group Kryogeniks gained unauthorized access to Comcast.net's registrar, Network Solutions. The domain name system (DNS) hack altered Comcast.net's homepage to redirect those attempting to access webmail to the hackers' own page (pictured). Spokespeople for Comcast and Network Solutions are still unclear as to how the hackers got the username and password.