How Hacktivism Affects Us All

Caught up in protests, young social activists are committing online crime.

By Robert Vamosi Sep 6, 2011 6:30 PM

Illustration by Edel Rodriguez

In December 2010, a group of nearly 3000 activists under the name “Operation Payback” launched online attacksagainst PayPal, MasterCard, and Visa, briefly knocking the three financial services’ sites offline and attempting to prevent consumers from accessing their online banking services. The activists retaliated against the three companies for severing ties with WikiLeaks, an online repository for whistleblower data that had recently included thousands of secret communications from the U.S. State Department and other world governmental agencies. Nine months later more than a dozen people--most between the ages of 19 and 24--were arrested in connection with these denial-of-service (DoS) attacks, even as new attacks were hitting corporate, military, and government sites worldwide.

A combination of hacking and social activism, *hacktivism* is defined as the use of digital tools in pursuit of political ends. The earliest example dates back to 1999, when the loose network known as Cult of the Dead Cow created “Hacktivismo,” an organization espousing that freedom of information was a basic human right. The group designed software to circumvent censorship controls on the Internet that some governments used to prevent citizens from seeing certain content.

Lately, however, the hacktivism term has been applied to protests against multinational organizations, governments, and even rural law enforcement agencies, and the tactics now include DoS attacks on sites, as well as leaks of confidential documents to the public. And although hacktivists typically go after nonretail organizations, the fallout from these attacks can still affect millions of people.

“The generation that grew up with the Internet seems to think it’s as natural to show their opinion by launching online attacks as for us it would have been to go out on the streets and do a demonstration,” says Mikko Hypponen, chief research officer for F-Secure. “The difference is, online attacks are illegal while public demonstrations are not. But these kids don’t seem to care.”

Online Vigilantes

“If you have a public presence, you are susceptible to attack--whether from a hacktivist or from legitimate cybercrime,” says Alex Eckelberry, vice president and general manager of security software for GFI Software. “It is something that every organization, especially ones with a high level of potential public scrutiny, must be concerned with,” Eckelberry says. For example, following the airing of a TV special critical of WikiLeaks, PBS saw its website defaced--and private documents breached and posted publicly--in May.

“Hacktivism has shown just how fragile an underbelly most enterprises and governments have, as well as much of the security industry,” says Dave Marcus, director of security research and communications for McAfee. Many of the attacked organizations had some security in place, but not enough to withstand the protests. “Hacktivism has revealed how poorly many companies handle the process of securing data, much of which is consumer,” Marcus notes. “I think consumers should be asking the companies that hold their data, ‘How well are you really protecting my info?’”

Collateral Damage

Today’s hacktivism creates a high level of embarrassment that goes beyond corporate press releases about data breaches, or identity theft. “This stuff gets out there and can be very public and quite dangerous, not only to the institution being hacked, but, by collateral damage, to innocents,” Eckelberry says.

In protesting recent police actions on the Bay Area Rapid Transit system in San Francisco, someone posted the names, addresses, and mobile phone numbers of more than 2000 MyBART subscribers online--ordinary riders. A week later, online attackers posted the names and addresses of 102 BART police officers online. Both disclosures were complemented by real-world protests at BART stations.

Sony is another prime example of the ripple effect that hacktivism can cause. In 2010, teenage researcher George Hotz

reverse-engineered the Sony private key and published it online, thereby allowing almost anyone the opportunity to rewrite the firmware and, by declaring themselves a developer on the Sony network, gain free access to any of Sony's online games. This action fits the hacker philosophy that all information--even proprietary information--should be free.

Sony subsequently sued Hotz, and as a result attracted the attention of hacktivists. The company then suffered many embarrassing DoS attacks and a data breach, including the exposure of 12 million customer credit card numbers. Sony Pictures had 75,000 "music codes" and 3.5 million "music coupons" exposed. Sony has estimated its total losses to be $173 million, including increased customer support, incentives to welcome customers back, legal costs, loss of sales--and better security.

Political Impact

Some politically motivated data breaches have inspired full-blown revolutions. In the spring of 2011, protestors, often young, took to the streets in the Middle East, rallying against their governments, some of which had been in power for decades. They were emboldened by, among other things, technology. For some, WikiLeaks and a decentralized online organization known as Anonymous created the environment that gave rise to the "Arab Spring" by posting secret government documents online.

About the same time, Anonymous split and formed a smaller group called Lulz Security, or LulzSec. That group allegedly attacked an affiliate of the FBI because it was investigating Anonymous, and later it attacked the Arizona Department of Public Safety because the group disagreed with Arizona's immigration policy. After 50 days, LulzSec rejoined with Anonymous, although in mid-July the group split off once again with the express purpose of attacking Rupert Murdoch's News International, ostensibly protesting that organization's alleged celebrity cell phone hacks by posting Murdoch's email online.

No Upside to Hacktivism?

None of the security experts interviewed condoned the recent actions of the hacktivists. Random disclosures could endanger lives--a high price to pay for increased security awareness. Throughout the spring and summer of 2011, thousands of pages of confidential documents and personnel information from targeted companies have appeared on public sites such as Pastebin. Law enforcement appears to be slowly catching up with the parties responsible.

Already one former member of Anonymous regrets his involvement. In an interview with Cisco Security, "SparkyBlaze" said he was "fed up with [Anonymous] putting people's data online and then claiming to be the big heroes." He goes on to say: "Getting files and giving them to WikiLeaks, that sort of thing, that does hurt governments. But putting user names and passwords on a pastebin doesn't [affect governments], and posting the info of the people you fight for is just wrong."