AGENCE FRANCE-PRESSE

Supporters of Wikileaks founder Julian Assange wear Guy Fawkes masks as they demonstrate against his arrest in Amsterdam in December 2010. The "Hacktivist" group "Anonymous" has adopted the Guy Fawkes image as its public face.

"Hacktivists" Strike Back

Cyber attacks on financial institutions serve as a warning sign

In December 2010, the websites of international financial services giants Visa, MasterCard and PayPal were temporarily shut down, victims of a coordinated cyber attack dubbed Operation Payback by its perpetrators. "Hacktivists" who support Wikileaks and its founder Julian Assange attacked after the companies terminated service and disabled donations to the website. The economic impact of the attack remains unclear and the targeted companies denied suffering consequential losses. But the attackers, using the names "Anon" and "Anonymous," demonstrated the ability of cyber attacks to infiltrate and damage businesses and government agencies.

A modern form of protest

Anonymous didn't protest by chanting slogans or waving signs — it struck against Wikileaks' perceived enemies in the spirit of the virtual world they share. Wikileaks, whose *raison d'être* is exposing classified or confidential government or corporate information, is under pressure from the United States and other governments after leaking more than 250,000 U.S. State Department diplomatic cables in November 2010. The U.S. accuses Wikileaks of endangering lives by revealing unlawfully obtained secret government information and requested that companies cut ties with the website, as reported in *The Independent*.

Amazon, the online retailer that hosted Wikileaks on its servers, was the first to pull out. Visa, MasterCard and PayPal soon followed, essentially crippling Wikileaks' ability to accept donations that support publishing efforts. The cyber attacks started soon after.

When Anonymous staged its attack in the virtual world, it used a favorite weapon of the cyber warrior — distributed denial of service attacks. DOS attacks work by flooding a targeted computer system with incoming messages, denying service to legitimate users. A typical DOS attack uses thousands of "compromised" computers, usually surreptitiously infected with malicious programs, or malware, allowing a master con-

troller to direct the computers remotely. These networks, or botnets, are widely used by organized crime. Cyber gangsters have used DDOS to extort "protection" money from businesses in the same way traditional gangsters extort businesses in person.

Operation Payback hacktivists created a voluntary botnet. They recruited people from within their network and asked them to download malware, avoiding the need to infect strangers' computers, Noa Bar Yossef, a security strategist at data security company Imperva, told *PC World*. Hacktivists used sites such as Twitter to plan attacks and communicate and coordinate their efforts, according to technology magazine *Fast Company*.

Ironically, Wikileaks itself was hit with a DDOS attack. "The Jester," who calls himself a "hacktivist for good," attacked Wikileaks in November 2010, shutting the site down briefly before hundreds of thousands of classified diplomatic cables were posted. According to a CNN story, "The Jester" has attacked websites involved in "online incitement to cause young Muslims to carry out acts of violent Jihad." He told CNN he is against Wikileaks "for attempting to endanger the lives of our troops, other assets and foreign relations."

> "CONSUMERS AND TAXPAYERS MAY NOT REALIZE IT, BUT BENEATH THE SURFACE, THE RISING THREAT OF CYBER ATTACKS, COMPUTER VIRUSES AND IDENTITY FRAUD IS COSTING THEM BILLIONS."
>
> — Henry Truc, personal finance writer for GoBankingRates.com

How effective were hacktivists?

According to the BBC, the websites targeted by Anonymous experienced service disruptions, but the attacks on credit card companies left transaction processing capabilities unaffected. MasterCard acknowledged it experienced a "service interruption" in some Web-based services, but neither its core processing capabilities nor its cardholder account data were compromised. Ted Carr, spokesman for Visa, told the BBC that the network handling cardholder transactions continued normal operations. Anonymous originally announced an attack on Amazon, but later shifted its target to PayPal. The online money transfer service reported that its blog went offline, but that transactions continued, though more slowly than usual.

Other attacks were more successful. News reports indicated that Swiss bank PostFinance suffered disruptions for 10 hours and the website of the Swedish prosecutors handling Assange's sexual assault case was taken down for several hours.

Anonymous aimed high with its attacks on Visa, MasterCard, PayPal and Amazon. Visa and MasterCard are the two largest consumer payment systems in the world, reporting 2010 revenues of $8 billion and $5.5 billion, respectively. PayPal, a subsidiary of online auctioneer eBay, announced revenue of almost $2.8 billion in 2010. There is nothing to indicate that the DDOS attacks caused significant financial damage to the targeted companies, amounting to little more than virtual graffiti on the online bank "lobbies."

The aftermath

After the attacks by Wikileaks supporters, law enforcement officials arrested several people. Five hacktivists from Anonymous were arrested in England in January 2011, although police there declined to confirm their involvement. Additionally, two teenage hackers were arrested in the Netherlands in December 2010. As of early 2011, police in Europe and North America continued to issue arrest warrants for suspects associated with the unlawful cyber attacks.

Though these recent attacks were largely unsucessful, they focused attention on the potential for criminals and terrorists to create large-scale financial havoc and expose confidential credit data to the world. British officials estimate that Internet attacks and viruses cost the world economy about $86 billion annually, a cost ultimately borne by consumers and taxpayers. Securing financial institutions and other critical civilian infrastructure will clearly remain a costly challenge. □