How to Stop Political Attacks
By Tim Wilson
Dark Reading, May 30, 2007
http://www.darkreading.com/document.asp?doc_id=125231&WT.svl=news1_1

Not all hackers are motivated by money. In fact, there is a growing number of politically-motivated attacks on businesses and government agencies, and the methods they use are different -- and potentially harder to stop -- than their cash-hungry counterparts, experts say.

Is your company ready to stop them?

The cyber battle between Russia and Estonia is just one example of the current trend toward the use of computers for political gain, industry observers say. Whether they are cyberterrorists trying to coopt or disable a nation's leading business, "hacktivists" mining the sensitive data of a target company, or ticked-off customers trying to deface your Website, many cyber criminals are using hacking to make their point. (See DOS Gets Political in Estonia and Estonian Attacks Raise Fears of Cyber 'Nuclear Winter'.)

"I suspect I could start a Website called 'Death to Western Civilization.com' and get a couple thousand paid subscribers in a very short time," says Andrew Colarik, an IT security consultant and co-author of Cyber Warfare and Cyber Terrorism, a book published earlier this month. "There are a lot of people on the Web who are influenced to join these movements."

But defending your company against politically motivated attackers is a different challenge than defending it against financially motivated criminals, experts say. You can't just follow the money.

"Attackers will scour Websites associated with a country's government and find flaws in them -- even in some of the most out-of-the-way portions of their Web presences -- and deface them with political messages," notes Joze Nazario, senior security researcher at Arbor Networks, which tracks security incidents.

In its study of Estonia, Arbor Networks recorded 128 unique denial-of-service attacks on Estonian-based URLs. Most lasted less than one hour, with the longest lasting 10 hours and 30 minutes. At its peak on May 9, the attack shut down up to 58 sites at once.

Are businesses at risk from this sort of all-out attack? "In some cases, they could be," Colarik says. "Unless they have a personal grudge against a particular company, most politically motivated attackers will go after high-value, prominent companies -- the IBMs, the Yahoos, the Amazon.coms. It's all about exerting power, so in most cases, they'll go after the companies that have the most money or power."

"It's a pretty tricky [question], but I think it comes down to companies that are extremely intertwined -- and visibly so -- with the government," says Nazario. Key defense contractors fall into this category, but most attackers who want to make a statement about government will usually target the government systems themselves, he says.

So far, DOS attacks, such as the ones seen in Estonia, are the most frequent vector used by political hackers, experts say. Web defacement is another popular political statement, particularly among hacktivists, who are generally trying to make their voices heard by the target company as well as the viewing public.

But those are not the only exploits used by political attackers. "We've seen hacktivists tap into, say, a Congressman's Outlook folders to steal his schedule," Colarik says. "Or they might put spyware on the machine of an administrative staffer -- someone who's not tech-savvy -- so that they can collect data and pass it over to a political opponent."

In some cases, an insider may play a role in the hack. "In banks, for example, an employee might collect data and sell it, and it may end up in the hands of a [politically-motivated] interest."

So what should companies do if they fall into the realm of potential political target? The IT organization should do its best to keep a low profile and decentralize as much as possible, Colarik advises. "If your organization is decentralized but your IT operations are not, you aren't decentralized," he says. "Most of these attackers work in small, local cells, so spread out your systems to give yourself some protection.

"If you're in the AT&T computer operations center, you don't put a big sign up on the building that says 'AT&T Computer Operations Center.' " This principle applies to the logical side of security as well, and IT organizations in high-profile companies should take advantage of Internet service providers' abilities to anonymize IP addresses and email server addresses so that they can't be readily identified with the company.

Nazario agrees that the best strategy is for the company to keep a low political profile. "Protect the brand, keep it out of the negative press, and don't become associated with activities that would give rise to the kinds of nationalist 'retaliation' attacks we see," he advises.

Both Nazario and Colarik say companies should develop a close relationship with their ISPs. "Work with the providers to ensure that if a DOS attack comes your way that you have adequate response measures in place to thwart the attack and repel the traffic," Nazario says, adding that companies should continually audit all Websites under the brand name to ensure that flaws don't allow attackers to penetrate an out-of-the-way server.