Lessons from Estonia

The first example of cyberwar?

The bad news: it was really cheap, and it forced an entire country to break off from the Internet.

The good news: nobody died, and this is a wake-up call for the rest of us.

What should you do? Firewalls, alternate hosts, etc.

What should WE do? More effort on public education, ISPs that quarantine abusive users, and security enforcement.

What happened in Estonia?

April 26-27, 2007: the Estonian government moved a statue, the “Bronze soldier” from the central square of Talinn to a cemetery on the outskirts of the capital.

Riots broke out, and one person was killed.

And a denial-of-service attack on all government computers and many businesses followed.

E-stonia

Estonia prides itself on the use of modern technology.

Broadband access rates (16.2%) are comparable to the US (19%) or Italy (14%).

The Estonian Parliament has declared Internet access a “fundamental human right”.

They claim to be the “first paperless government”.

80% of banking transactions are online.

You can vote for Parliament over the Internet.

What was the attack?

A fairly normal “denial of service” attack: lots of pings.

(A colleague at Stanford once was subjected to something like this for daring to testify in Congress against something that Internet pornographers wanted).

The maximum data rate was estimated at 90 Mbps. This is not actually very much data, but Estonia is a small country.

By contrast, Blue Security was forced offline by an attack involving more than 2 Gbps in 2006.

Who did it?

The Estonians blamed the Russian government.

Most of the attacks could be traced to IP addresses in Moscow, and they stopped on May 10 (the day after May 9, which is V-E day in Russia).

Mikko Hypponen (from F-secure) suggested in the newspapers that if the government had done it, the attack would have been more successful.

Or it could have been bought and paid for.

But in reality: it seems to have been started by one disgruntled ethnic Russian living in Estonia, Dmitri Galushkevich. He's been fined 17,500 kroons ($1600).

Another example

Jay Echouafni (CEO of Orbit Communications) paid three botnet owners to attack other websites, with nets of 3,000-10,000 computers. One of these operators (Richard Roby) admitted the attacks in a plea bargain.

That is, botnets are now commercial: you can buy and sell services, in an increasingly overseas market.

Estimate: there are five million zombie computers in the world.

And renting them costs about 25 cents/bot!

Other political examples

In 1998 Tamil groups sent 800 emails a day to Sri Lankan embassies (today this sounds laughable)

In 2000 Israeli and Palestinian groups attacked the websites of Hezbollah and the Israeli Foreign Ministry.

In 1999 Chinese hackers overwrote the website of the U embassy in Beijing.

Also in 1999, Chinese and Taiwanese websites were attacked.

And in 2001 perhaps 1,000 US and Chinese websites were overwritten after a mid-air collision between US and Chinese military aircraft.

What might a DDOS attack cost?

The Estonian attack, if bought commercially, might have cost perhaps $100,000. Each attack might have been $2,000 and adding them all up (a few dozen), perhaps $100,000.

So cyberwar is available to the middle class.

And Estonia cut its links to the Internet as a result.

Now most of the people doing these attacks are fairly childish. (The commercial spammers seem more interested in pump-and-dump stock schemes and the like). But business blackmail is real: Internet bookmakers, for example, have been victimized.

Online blackmail

“Ivan Maksakov, Alexander Petrov, and Denis Stepanov were each sentenced to 8 years in prison and a $3,700 fine.

Victims of the online blackmail gang included Canbet Sports Bookmakers, who refused to pay a $10,000 ransom demand and found their website had been taken out of action by the hackers during the Breeders' Cup Races, losing them more than $200,000 in lost business for every day of downtime.

According to prosecutors, the gang made over 50 similar blackmail attacks in 30 different countries during their six months of activity.”

(from *sophos.com,* 2006).

And another

“Blackmailers target $1m website

Alex Tew, 21, hit the headlines at the start of the year when he revealed his Million Dollar Homepage had made him a million dollars in four months.

But the publicity brought the unwanted attention of extortionists who knocked the site over with a massive denial-of-service attack

Mr Tew's encounter with the net criminals began on 7 January when he received an e-mail threatening to bombard the site with data unless he paid a ransom of $5,000 (£2,800).”

BBC, 2006.

What's to do?

Individual websites:

Traffic throttling.

Rejecting high hop-count packets (many redirects suggest packets are concealing their source)

Smarter routers.

Alternate hosts.

Cooperative defense

Quarantining bad sites/networks.

ISPs that keep track of deceptive packet addresses.

More research.

US CyberSecurity Divison budget: $93M

FBI bank robbery budget: $2B.

Also, as users upgrade their home computers, they become less vulnerable to being taken over.

Responsible ISPs

Some combination of spam, piracy and blackmail is going to force the ISP industry to be better at cutting off service to abusers.

(For example, my university is regularly pressured by its ISP to find and stop students who are running zombie computers involved in spam).

This may take some international escalation: many of the evil sites are in foreign countries. But it is coming.

Conclusion

Things are getting better: standard software is more resistant, the ISPs are more attuned to the problem, and the routers are getting smarter.

My hope is that the crooks will move on to something else, as the Internet gets smarter about stopping them.

Estonia may well have had the benefit of alerting a great many more governments to the dangers, and increasing the chance that they'll cooperate.