PHYS.ORG

Most home computers, including yours, are vulnerable to attack

April 12 2013, by Peter Reiher

North Korea recently launched a cyber attack on South Korean TV stations and banks. Iran carried out a cyber campaign against U.S. banking sites. The U.S. and Israel released malware that disabled Iranian nuclear centrifuges. Or did they?

There's no doubt someone did all these things, and there are reasons to believe that those suspected are responsible. But because of the way the Internet is designed and the poor general state of computer security, it is extremely difficult to pinpoint an attack's origin. Attackers are far ahead of our ability to track them.

While a cyber attack can't reduce a city to rubble in the way bombs can, it is certainly possible to damage a nation through cyberspace. Many critical systems that modern nations depend on - power grids, military intelligence and air traffic control - rely on computers and networks. One good way to discourage cyber mayhem is ensuring that anyone who perpetrates it suffers consequences, so being able to place blame properly is important.

But that's not so easy. Although it's often possible to determine which messages are part of an attack and even which specific machines sent the damaging message, that's not the same as identifying the person or nation that is the source of an attack. Attackers often use compromised machines that belong to ordinary users throughout the world.

A vast number of computers on the Internet have been compromised by attackers. Even estimating how many is hard, but it is at least in the hundreds of millions. You may have one sitting on your desk at home. A 2007 study suggested that one in four home computers is compromised.

These machines, scattered throughout the world, can be used to launch attacks from any country the attacker chooses. The attack could even be launched exclusively from machines within the target country. In a series of attacks in South Korea during 2011, for example, the majority of the attacking machines were located within that country.

So, even when a cyber trail seems to lead back to a certain country, that evidence may mean nothing. Any form of action taken against the apparent source of the attack might be unjust and ineffective.

Part of the problem is the very nature of the Internet, which was designed to allow any user to easily reach out and touch any other user. But that touch can be a caress or a punch. Most machines on the Internet are susceptible to attack from the outside, and when it happens, there are usually few fingerprints to identify the source.

A complete solution is likely to be beyond our technical capabilities at this point, and the "fingerprint" problem makes it difficult to establish treaties mandating proper behavior in cyber warfare. But we should nevertheless seek ways of establishing better cooperation between nations, including protocols for handling known compromised machines.

Last year's joint work by groups in the U.S. and Russia to take down the Grum botnet, which was responsible for sending vast quantities of commercial spam to email addresses worldwide, is an example of the kind of international cooperation required. By jointly locating the computers and sub-networks used to issue commands to this botnet and disconnecting them from the Internet, groups in the U.S., Russia and other countries rendered it ineffective. Only cooperation between law enforcement agencies and computer network operators across borders makes such remedies possible.

If it were more difficult to compromise users' machines and harder to launch attacks against critical sites, opportunity and benefit would be reduced and the problem would be less serious. Perfectly securing a machine or network is very hard, but improving security significantly is relatively easy.

For example, a recent report from the Center for Strategic and International Studies discussed Australia's Defence Signals Directorate's approach of using four basic measures to improve computer security. By only running applications from an approved list of safe programs, by aggressively applying patches to those applications as they become available, by being equally aggressive in applying patches to the underlying operating system (such as Windows or Linux), and by limiting the number of users permitted to change vital system configuration values, the directorate demonstrated an 85% reduction in risk of compromise.

Such general improvement in the security of everyone's computers would not only help protect the computers of individual users, it would benefit the Internet as a whole and everyone who uses it.

More information: Peter Reiher, an adjunct professor of computer science at the UCLA Henry Samueli School of Engineering and Applied Science for more than 20 years, has done extensive research on denial-of-service attacks and other Internet security issues. He wrote this for the Los Angeles Times.

Citation: Most home computers, including yours, are vulnerable to attack (2013, April 12) retrieved 25 April 2024 from https://phys.org/news/2013-04-home-vulnerable.html