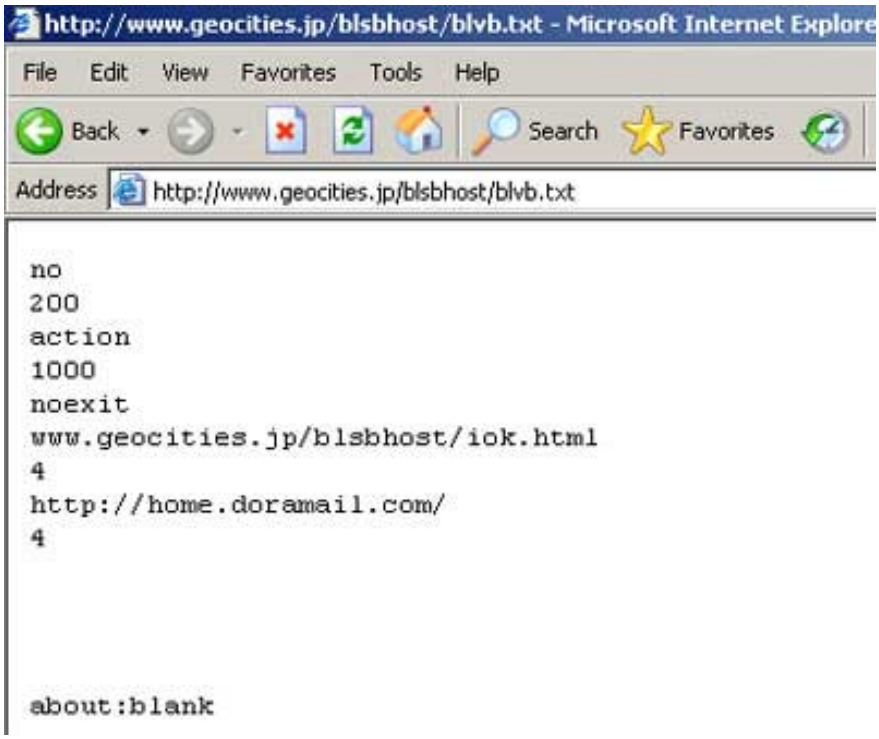
The DDoS attack culprit website Vietco shows up!

Subjects conducting attacks to deny distributed services (DDoS) on the e-commerce website Vietco recently were investigated by the investigating agency on April 28, 2006. The audience has initially embraced DDoS behaviors

Subjects conducting attacks to deny distributed services (DDoS) on the e-commerce website Vietco recently were investigated by the investigating agency on April 28, 2006. The object has initially claimed these DDoS behaviors. This person was identified as Nguyen Thanh C. (Dac Lac), a member of the hacker group "Baby", known by his nick name DantruongX .



Just change the link information above the "victim" website, all computers on the BOTNET network will attack simultaneously!

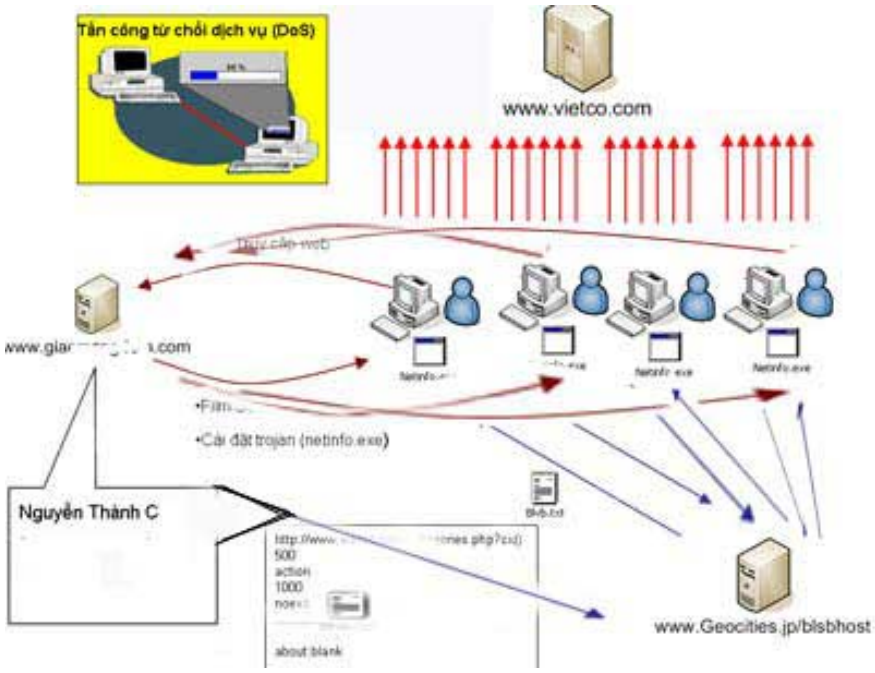
According to information from the BKIS network security center, the subject who attacked DDoS e-commerce website Vietco.com on April 28, 2006 was detained by police in Dak Lak. Initially, C. admitted that acts of intentionally denying services to vietco.com website in the past time as VietNamNet reported. The direct agency investigates the case of C15 - Ministry of Public Security. After more than a month of monitoring, C15

proceeded to arrest Nguyen Thanh C. on April 28 morning. In the evening of the same day, the family sponsored C. and was released on bail.

After VietNamNet published an article about the risk of bankruptcy of Viet Co company website, many network security units actively contacted VietnamNet to help this business solve the problem. Notably, VSEC Network Security Center - free help with system security, server upgrade and DDoS protection. The BKIS Network Security Center also contacted for information to conduct the analysis and then transferred it to the police department to support the investigation process.

Mr. Nguyen Tu Quang, director of BKIS said: " *According to the information we have, it is likely that this hacker has successfully built a quite strong BOTNET network in Vietnam.* "

Viet Co DDoS attack is conducted in the following order: Hacker uses a trojan installed on the porn website www.giac . .com . This Trojan takes advantage of an IE vulnerability - any computer that has not updated this IE error, when accessing www.giac . com will immediately be installed by the Trojan, becoming zoombie (*zoombie - live zombies - only compromised computers and can be remotely controlled for attack purposes.*)



System diagram of DDoS attack deployment on Vietco.com

At a specified time, the zoombie computers when online will automatically access the website http:///www.geocities./blsbhost/ hosted by DantruongX. On this site, hacker has set a file Blvb.txt to order machines zoombie to access with a huge number of times to vietco.com. Each time the attack is launched, the author only needs to change the information pointing to the "victim" web. In fact, the last time "victims" of DOS attacks originating from here are not only Vietco.com but also some other sites in education and e-commerce industry.

Information from the investigation agency said, even after VietNamNet reported that Viet Co asked to rescue bankruptcy due to DDoS attack, the attacks of DantruongX still took place 1 week later. This coincides with the

information that VSEC Network Security Center recorded when helping free Viet Co to upgrade the server and fight DDoS attacks. VSEC said, although after upgrading the website and having some measures to counteract, vietco.com was resurrected, but still suffered from continuous attacks lasting weeks later.

According to information from the unit coordinating the investigation: Nguyen Thanh C. also related to counterfeiting ATM card. However, this incident is currently being clarified by the investigation agency and has not yet reached an official conclusion. The source also said that in the process of building the BOTNET network and carrying out the attack, Nguyen Thanh C. also has the coordination and assistance of another object who is also a member of the hacker group. VietNamNet will continue to update the next information to readers.

According to Phung Minh Bao - director of Viet Co Company (the managing unit of Vietco.com TMT website), the first time the investigating agency found out and has sufficient evidence of the person conducting DDoS attack has High level online, is a great meaningful success. It affirms the strictness of the law on a network and encourages many units that are "heaving" to do e-commerce. " *This has a great deterrent to misconduct on the internet, which is considered difficult to detect and handle* ."

Talking about Viet Co DDoS engine, Mr. Bao said that before a while, Viet Co had invited C. to do web design for a while, but due to the work was not suitable, C. had moved to work. " *However before and after these things happened, we still kept a very good relationship* " - Mr. Bao said and said that during Vietco's DDoS he still had contact with C. and he was Give some . tips to fight DDoS.

Mr. Bao stressed, he was very surprised that the final investigation results of C15 showed that C. was the culprit. He said if this was a DDoSer case that was exploited or "hired" for others, he would try to ask the police to clarify to complain if he was eligible. In the case of personal purpose of C. to create a reputation, he will not complain and expect that the matter will only be handled as an example for other hackers, not too badly dealt with, making photos enjoy his future.

The Phong