Nguyen Thanh Cong's Confidence (DanTruongX) And Some Methods to Prevent Denial of Service from xFlash

Before doing this article, I wanted to send my apology to Viet Co and its customers. I am very regretful of the things I have done, just because of my superficial, aggressive actions that have adversely affected me.

Before doing this article, I wanted to send my apology to Viet Co and its customers. I am very regretful of the things I have done, just because of my superficial and aggressive actions, which have adversely affected the Vietnamese e-commerce environment. I hope to have a forgiveness from everyone, so that I can start over, start a new, better, more useful life. And I hope that you will have a chance to improve and contribute a part to the development of information technology in Vietnam.

And then I want to give you some methods, prevent and limit the harmful effects caused by xFlash DDoS.

In my study too. First in about 2002 in the process of researching information technology, our group of love kids discovered security holes of IE and Flash, applications from Action Script programming code in Macromedia Flash. From those errors, we were quickly applied by the group of children with the purpose of children who are passionate and like to express themselves.

And from the agile actions that helped us quickly gain popularity in the "Network of the Lake" without knowing

that it was a misconduct that endangered the situation of E-commerce in Vietnam later. and now I really regret it.

However, since our baby group discovered it and expressed itself, we still have a purpose of honoring that we should never hack or hack into government networks, domains or servers that are set. in Vietnam.

And realize your wrongdoings. now I want to bring some knowledge about preventing from the harm caused by xFlash DDoS:

- If you use a Linux Server that uses CPanel when it detects that DDoS is available if you have root access right away, Suppend Site is being hacked and temporary password is installed after completing the password settings for the folder or site. Under attack, you can Unsuppend to continue watching.

Create a .htaccess file placed in the directory or site that is being flooded as follows:

.htaccess
****
AuthUserFile /forum/.htpasswd
AuthGroupFile / dev / null
AuthName "Password Protected Area"
AuthType Basic
****
and create a .htpasswd file
****
@domain :: @ dGdK8ZQg / FjU
****
The above user and pass are: @domain:

The above is just an example where you can go to http://google.com and Search with the keyword .htaccess Generator to create your own password at will.

You should leave the password with the @ symbol in front and the sign: behind because WinXP has fixed the URL entry password: http:/// user: pass@domain.com/, if there is @ and: then the Attacker will not be able to pass By entering User and Pass directly by URL.

Then your job is to create an appropriate Firewall configuration for your site.

.htaccess
********** **********
RewriteEngine on
RewriteCond% {HTTP_REFERER}! ^ Http (s)?: // (www.)? Tenmienbitancong.com [NC]
RewriteRule. (Php | html | asp) $ http://sitefirewall.com [NC, R, L]
********** **********

With Mod Rewrite on you can fight up to 95% of DDoS damage caused by xFlash, it prevents you from harming xFlash's automatic access to your site.

Explanation: on your server, run the programming code of PHP, ASP, HTML when an Attacker attacks the site you specifically have, such as attacking http://tenmienbitancong.com/ it will read the index.php file at This Mod

Rewrite will work and Foward will go to http://sitefirewall.com then from http://sitefirewall.com you place a code like this:
Go to Web Site

If you are a real visitor, they will Click "Go to Web SIte" to gain access to the site. if you enter "hiden xFlash" and it will not be accessible. You can study a number of ModRewrite types. Combine with the source code on your site to better configure your site against xFlash.

With these two ways you can rest assured that your site will pass xFlash. As for the room method, there is only one method: access to the address http://macromedia.com/shockwave/download/download.cgi?P1_Prod_Version=ShockwaveFlash&promoid=BIOW and upgrade to the latest version "FLASH PLAYER" you will be assured that you will no longer be a hidden Client for XFlash DDoS. And this upgrade is completely free.

And by the way, I want to give advice to those who are currently Attacker and who are intending to be Attacker, so think more carefully not because of personal conflicts or because of the reputation of being lacking in action. Thinking like me that your honor and future might be lost, I hope that hackers in Vietnam should take actions to improve their lives to have a good and useful future for life. Do useful things to contribute to the development of Vietnamese informatics and in your work, focus on working and earning money from your own effort and wisdom.

If you need support or questions regarding xFlash DDoS prevention, I would like to answer and support you. Wishing to help you, businesses that are suffering from DDoS by xFlash and more than ever, it's a desire, an action, a sincere apology to everyone of a person who really recognizes. Mistake, really regret, to help me start over.

In addition, I would like to thank the brothers at security365.org, and the friends who encouraged, advised and guided me to follow the true path.

The email questions or questions, please send to tbcong911@yahoo.com

Nguyen Thanh Cong