Apology about my malware!

Dec 26, 2015

Hello everyone, especially the guys from “Malwaremustdie”.

My name is Jerry Xu, a junior student of Shanghai Jiao Tong University. I think you must know me deeply through my github page.

I feel so sorry about the malware I made these day. A very sincere apology.

[http://blog.malwaremustdie.org/2015/12/mmd-0047-2015-sshv-ssh-bruter-elf]

The malware is a project of Operating System. The only requirement of the project is to write a program suit the definition of the virus, spreading, hiding and executing (To tell the truth I do not know the difintion as well). There are many team in my class and they try to spread the virus by portable device or something else.

Addition Explaination about the project

The professor want us to write a virus in order to let us understand more about Linux. (For example, writing the hidden-process-module let me know the syscall and syscall table.) So the spreading part is not a important part. When I and my partner thinking how to spread, We found a library called libssh and it is very easy to use. We have had a presentation on the Christmas Day and the professor have warned us about the harmful of the virus. He said he will warn the next set of student not to make this kind. I believe the academic atmosphere and the attitude to information security in Chinese University is good and healthy. :)

I promise the malware I made is for academic use only, and it won’t be runned forever. I have never had any thought about truly using it. The IPs I set are all the server I own. (Enumerating the similar IP is to act as cracking) When we test, because of the poor wordlist, none of other server had been cracked. And I have never send my code to others, expect my TA because the malware is my project. I have delete my repository of this malware.

I have handed in my project on Christmas. And no more touch I will have with this malware from now on.

I feel shocked that a very tiny program I wrote will cause such big effect. The malware I wrote has been run only for one week and only dozens of IP are tried. How powerful your ognizaiton are! Can I ask whether it is possible for you guys to hack my Linux server without the root password? I feel it to powerful for your expunging.

My major is Computer Science and the researching area of me is Machine Learning. I don't know much about the malware. I even do not understand many terminology in your analyzing article. All the knowledge are found from Internet.

Thanks for reading my code and analyzing it. And thanks for telling me the seriousness. The server you guys expunged on 101..* is only a virtual machine and it is easy to reinstall. But can you tell me what you guys have done on my 178..* server? I cannot login in it through SSH and Digital Ocean website. And I do not know how to solve it except format it. Have you expunge it too?

I do not want to be a hacker in future and I hate malware a lot of course. I don't want to hide myself and I will take responsibility. The fully expose of myself makes me feel very unsafety. I regret to put so much on my github page. Can you delete the picture and the link to my github page from your website? Thanks!

Malware must die! Ha! I agree with it!

My e-mail is fei960922@163.com. I am glad to contact with you guys.

Personal Blog of Jerry Xu
fei960922@gmail.com
(mailto:fei960922@gmail.com)

fei960922 Hello World!
(https://github.com/fei960922)
fei960922
(http://www.renren.com/725686138)