

Forum:[Hack Forums](#)

Thread: [Botnet using smtp and pop3 protocols](#)

WinterSnow - January 3, 2014, 11:51 am

Hello guys,

I'm a c++ coder that recently got curios about the virus world and started coding these , to expand my expertise.

My latest project relies on a botnet without the use of irc:

Once the machine is infected , it awaits emails from a predetermined gmail account , the object of the emails determines the ID of the machine which needs to read it , and in the text-box are writed precise characters which the botnet acknowledges as comands.

It then sends an email to another gmail account confirming infection etc.

It has many functions implemented in it , one of them is a keylogger , which sends the victims logs via email attachment.

Now , since I'm very ignorant in security and "tracking down":
What are the chances that someone can track back to me ?

Ps: This is my first post , so I feel kind of disrespectful asking an advise on it , sorry for that. Thank you all

Sajuuk - January 3, 2014, 12:15 pm

If they're experienced at backtracing malware, the chances are fairly good.

Doisti74 - January 3, 2014, 4:32 pm

as proof of concept, the idea is ok. but in real life, it demands creating gmail accounts by hand or capturing user's credentials, and this is a lot of work.

WinterSnow - January 3, 2014, 4:43 pm

Thanks for your quick answers.

Thing is , its 1 gmail account , created by hand - "stolen from somebody" , where the bots read from (i adapted a mesure to not make the mail overflow).

And another one , from where i send mail-commands to the bot , and recieve the logs etc.

I use gmail cause its the only online email which doesnt complain about multiple accesses from different locations , nor about software accessing it via smtp.

I leave no trace when creating the gmail account , since I can do it from wherever I want.

I've already tested it on my machines and it seems to work fine , no av detected it.

How could someone get back to me ?

Thanks again for your answers guys , I really appreciate it.

tux1 - January 3, 2014, 6:59 pm

This sounds a pretty dumb idea for a variety of reasons.

Quote:Once the machine is infected , it awaits emails from a predetermined gmail account , the object of the emails determines the ID of the machine which needs to read it , and in the text-box are writed precise characters which the botnet acknowledges as comands.

The problem is that the bot would need to have the the email credentials hardcoded in the binary so it could login and read the emails that contains the commands.

The other problem is how are you going to know the ids of the bots? The trojan would need to send an email notifying the person of a new infection and an id.

In terms of traceability it's pretty simple. because as I said if you were using gmail the email and password would have to be hardcoded in the file so anyone could find them and login to the account and seee all the information. So really that chance is very high.

WinterSnow - January 3, 2014, 10:56 pm

(Jan 3, 2014 07:59 PM)tux1 Wrote: [\[CITE\]](#) The problem is that the bot would need to have the the email credentials hardcoded in the binary so it could login and read the emails that contains the commands.

The other problem is how are you going to know the ids of the bots? The trojan would need to send an email notifying the person of a new infection and an id.

And thats exactly what it does Hah.

(The logs and info were crypted before emailing etc , but your damn right on the hardcoding)

Thank you for your time on explaining me why it was a dumb idea. I was searching an alternate way to send comands and interact indirectly with the bot , my bad search :)

Ps: was pretty damn fun to code at least