Fire in the Skype

Skype powered botnets...

Cédric BLANCHER

cedric.blancher@eads.net  
EADS Corporate Research Center  
DCR/STI/C IT Security lab

sid@rstack.org  
Rstack Team  
http://sid.rstack.org/

Hack.lu - Luxembourg  
19-21 October 2006  
http://hack.lu/
The biggest botnet ever?
Key factors for a good botnet

Want a good botnet? Need two things:
- Massive number of bots
- Resilience

Definition from Wikipedia
Resilience generally means the ability to recover from (or to resist being affected by) some shock, insult, or disturbance. However, it is used quite differently in different fields.

In fact, it’s all about resilience...
Why use Skype?
Where popularity hurts...

Skype is an interesting piece of software

- Very popular, 100M+ users, average 5M+ connected
- Very good firewall ”punching” capabilities
- Obfuscated and persistent network flow

Heavy fuel for kiddies...
And... It kindly provides network API so we can use all this transparently
So we have the numbers. We now need resilience…

- Skype provides network connectivity and obfuscation
- Skype is resilient by design ;)
- Just need nickname(s) for communications

Cool isn’t it ? Can we make better?
Keeping your botnet up is somehow keeping master(s) connected and reachable

- Credentials caching roughly means your login last for ages\(^1\)
- Multiple login from different places is possible this way
- Skype handles everything else for us

Why does it make us stronger?

- Will be able to reconnect anytime using cached credentials
- Won’t get disconnected until last instance dies
- Network ensures connectivity and proper routing

0.02€ ideas: steal credentials to create more masters with different nicknames, create multiples bots with same nickname, etc.

\(^1\)Like yesterday’s jam!
Finding bots
Building the big thing

Just exploit supernodes privileges!
- List of supernodes
- List of clients and version
- Looks perfect for a potential targets list!

Just need a flaw, say a ”non-exploitable” heap overflow...

Then, things are easy...
- Exploit Skype
- Install bot as Skype plugin
- Generate plugin authorization token and execute

One can also think social engineering, XSS, DNS cache poisoning, etc. so people actually install your stuff.
The biggest botnet ever?

No!
The BEST botnet ever...

BTW, functionalities misusage is not specific to Skype and any alike P2P based communication system can be used

Think of...

- Teredo IPv6 over IPv4 P2P network
- Hamachi P2P network tunneling
- Many others to come in the future
Greetings...
And questions?

Thanks to Serpi, Recca, Philippe and Newsoft

DCR/STI/C team
at EADS CRC France

Rstack.org team
http://www.rstack.org/

MISC Magazine
http://www.miscmag.com/

French Honeynet Project
http://www.frenchhoneynet.org/

Download theses slides from http://sid.rstack.org/