

Forum:[Hack Forums](#)

Thread: [Fastflux network system](#)

push eax - April 1, 2013, 11:54 am

First of all I'm posting this on behalf of a friend, DO NOT PM ME HERE REGARDING THIS PRODUCT ONLY THROUGH THE CONTACT DETAILS SPECIFIED BELOW

I'm here to represent my latest product

"Stealth core" which is a fastflux system for your botnet, phishing sites, or what ever you need it for

Don't know what is fast flux? Short explanation here quoted from wiki:

Spoiler ([Click to View](#))

Fast flux is a DNS technique used by botnets to hide phishing and malware delivery sites behind an ever-changing network of compromised hosts acting as proxies

The simplest type of fast flux, referred to itself as "single-flux", is characterized by multiple individual nodes within the network registering and de-registering their addresses as part of the DNS A (address) record list for a single DNS name.

This combines round robin DNS with very short—usually less than five minutes (300s)[2] -- TTL (time to live) values to create a constantly changing list of destination addresses for that single DNS name. The list can be hundreds or thousands of entries long.

Within a malware attack, the DNS records will normally point to a compromised system that will act as a proxy server. This method prevents some of the traditionally best defense mechanisms from working — e.g., IP-based access control lists (ACLs). The method can also mask the systems of attackers, which will exploit the network through a series of proxies and make it much more difficult to identify the attackers' network.

Features (Panel):

- Interface in EN/RU
- Block any node from being used
- Close registration of nodes:

After you close the registration no new nodes will be able to register, this is a good way of keeping researchers and such away from acting as nodes

- Enable registration for specific guid:

Incase you want to install directly from a botnet and disregard the closed registration you can make exception for this guid

- Core functionality like adding domains, setting TTL and so on.
- Jabber notification if active nodes are becoming too low to have a functional network *

Features (Core):

- Paranoid criterias for installation

prevent from executing and jailed enviroments such as vmware, sandboxes, as so on, fool researchers by connecting to a fake c&c

- Port mapping

working with mostly all routers i have tested with that supports UPNP, which is a good % not lame like locust version.

- Checker if nodes are suitable for the job, if they are not it will permanantly delete itself.

- Custom made lightweight nameserver that is optimized just for this purpose, it will only process A-record requests and nothing else

* = in progress / todo / idea / likely to implement

If you have suggestions about more functionality let me know

Price starts from \$800 which includes 5 nameserver changes and additional updates

Please chatters and wastetimers don't add it

Serious speculants I can show how the system performs under virtual machines, maybe will prepare a video too.

Jabber: synthetic@exploit.im