

Forum:[Hack Forums](#)

Thread: [Random infections...](#)

yosefebesh - November 20, 2015, 9:32 pm

I have never used my RAT for malicious purposes, and I have never infected anybody. I sent my RAT over skype to my friend, for testing purposes. I keep getting random infections, but weird PC's. Running windows, they have nothing in them. Nothing in the desktop, no downloaded programs. I can't access their desktops, and they have no mic/camera. Keylogged, no activity. They are classified weird, like placehol-69969 and pc/admin and stuff. What is this?

BahNahNah - November 20, 2015, 9:33 pm

Skype uploads to VT. They are hunnypots.

Armada - November 20, 2015, 9:40 pm

(Nov 20, 2015 10:32 PM)yosefebesh Wrote: [\[CITE\]](#) I have never used my RAT for malicious purposes, and I have never infected anybody. I sent my RAT over skype to my friend, for testing purposes. I keep getting random infections, but weird PC's. Running windows, they have nothing in them. Nothing in the desktop, no downloaded programs. I can't access their desktops, and they have no mic/camera. Keylogged, no activity. They are classified weird, like placehol-69969 and pc/admin and stuff. What is this?

The likely correct answer to this is the fact, your subject/friend/whoever, sent it to a site, or ran an anti virus which distributes samples.

- As stated these are likely honeypots, they will rather information but are unlikely to remain within the network. ?

yosefebesh - November 20, 2015, 10:23 pm

(Nov 20, 2015 10:40 PM)??mªDa Wrote: [\[CITE\]](#) The likely correct answer to this is the fact, your subject/friend/whoever, sent it to a site, or ran an anti virus which distributes samples.Oh, He's right in front of me, irl.

Root - November 20, 2015, 10:46 pm

Don't Use skype to send servers.

yosefebesh - November 20, 2015, 10:47 pm

(Nov 20, 2015 11:46 PM)Cyber Army Wrote: [\[CITE\]](#) Don't Use skype to send servers. was an unencrypted test stub. Thanks for the tip though.

Root - November 20, 2015, 10:49 pm

Even if its crypted just don't use it :)

yosefebesh - November 20, 2015, 10:55 pm

(Nov 20, 2015 11:49 PM)Cyber Army Wrote: [\[CITE\]](#) Even if its crypted just don't use it :) Yeah thanks for the tip man. I got a question about a certain spreading method (PM'ing!!) that I'm going to have to modify...

Armada - November 20, 2015, 11:10 pm

(Nov 20, 2015 11:55 PM)yosefebesh Wrote: [\[CITE\]](#) Yeah thanks for the tip man. I got a question

about a certain spreading method (PM'ing!!) that I'm going to have to modify...
If you have PHYSICAL access to the terminal at ANY point why not utilize that vector?

Throw your "attack" on the usb and plug and play

yosefebesh - November 20, 2015, 11:44 pm

(Nov 21, 2015 12:10 AM)??m^aDa Wrote: [\[CITE\]](#) If you have PHYSICAL access to the terminal at ANY point why not utilize that vector?

Throw your "attack" on the usb and plug and playThe problem is I was only willing to project a stub test on my friends computer, not a complete-fledged attack.

Armada - November 20, 2015, 11:57 pm

(Nov 21, 2015 12:44 AM)yosefebesh Wrote: [\[CITE\]](#) The problem is I was only willing to project a stub test on my friends computer, not a complete-fledged attack.

IMO you have no concept of a targeted attack, but ok, t each their own ?

dinplei1 - November 22, 2015, 8:20 am

There are more simple and effective ways to send Skype .