[Full-Disclosure] IRC spying on EEYE!

rap1st rap1st at darksaber.org
Thu Oct 14 21:25:25 BST 2004

- Previous message: [Full-Disclosure] [OpenPKG-SA-2004.043] OpenPKG Security Advisory (tiff)
- Next message: [Full-Disclosure] IRC spying on EEYE!
- **Messages sorted by:** [date] [thread] [subject] [author]

```
Hello!

Since the government is increasing it spying on irc, I too have increased
my irc spying. Ive recently intercepted some communication between EEYE's
own Marc Maiffret aka the chameleon, and RLoxley of Team Hackphreak!

<RLoxley> hey
<RLoxley> waykee
<chame|eon> hey man!
<chame|eon> long time
<RLoxley> hey man
<RLoxley> tried to call you a bit ago today
<chame|eon> hows it goin??
<chame|eon> get my message service?
<RLoxley> looking for work, so i can start getting pussy again
<RLoxley> no, called your office, and left it with your asst
<chame|eon> oh cool
<chame|eon> im not in today
<RLoxley> i havent had your cellie# in ages
<RLoxley> how you doing man?
<chame|eon> im ok
<chame|eon> I came up with a great security concept the other day
<chame|eon> care if I run it by you?
<RLoxley> sure
<chame|eon> i was sleeping the other night
<chame|eon> and it hit me
<chame|eon> you know how good tripwire does to catch file mods right?
<RLoxley> yep, sure do
<chame|eon> but what if a hacker disbales tripwire
<RLoxley> then it is useless
<chame|eon> how can we stop them though?
<RLoxley> you have to have an external means of making tripwire always
on, cant disable it
<chame|eon> ok
<chame|eon> well, here is my soultion
<chame|eon> run multiple instances of tripwire
<chame|eon> at first I thought 2 instances would suffice
<RLoxley> so one is watching the other
<chame|eon> but after hours of pondering, I came to the conclusion that
3 instances makes the most sense
<RLoxley> 2 should work, as they watch each other
<chame|eon> here is the deal.. if a hacker suspects you are running
```

```
multiple instances.. he might disbale a 2nd one, but leave the third
<RLoxley> highly unlikely that someone could disable both, at the same
time
<chame|eon> RLoxley Ive seen it happen
<chame|eon> a hacker can disbale two instances simultaneously!
<RLoxley> yeah, the hackers sure have more time than we do
<chame|eon> yes, sometimes I think the hackers might be close to as
smart as us! LOL
<RLoxley> or smarter
<chame|eon> gotta stay three steps ahead of them
<chame|eon> with 3 instances of tripwire!
<chame|eon> now, here is my big idea
<chame|eon> team Hackphreak markets this with Eeye
<chame|eon> what do you think?
<chame|eon> you had mentioned you needed a job
<RLoxley> yep, i do
<chame|eon> is this something you might be interested in?
<RLoxley> if there is money in it, i would be interested in damn near
anything
<chame|eon> ok great
<RLoxley> you need to do something for me though, give me a number, i
need to hear your voice, and see if this is really you
<RLoxley> i know your voice
<chame|eon> im at starbucks
<chame|eon> no phone right now
<RLoxley> and as you can imagine, i must be careful
<chame|eon> call my office tomorrow morning
<chame|eon> ok?
<RLoxley> saturday?
<chame|eon> yeah
<chame|eon> Ill be there
<RLoxley> whgat time
<chame|eon> working on installing tripwire
<chame|eon> have you ever installed multiple instances?
<RLoxley> i never have
<chame|eon> uhm.. around 10am PST
<RLoxley> i run snort, and sentaurus
<chame|eon> hmm.. that can leave you pretty insecure
<chame|eon> imho
<RLoxley> hehe, that is not ALL i run
<chame|eon> you need to be running tripwire
<RLoxley> that is just what i run in relation to this stuff
<chame|eon> and at least 2 instances of it
<chame|eon> how many firewalls do you run?
<RLoxley> 3
<chame|eon> hmm.. I run 6
<chame|eon> Ive found that most hackers cant get past 6 firewalls
<RLoxley> wow, you are worse than me
```

- Previous message: [Full-Disclosure] [OpenPKG-SA-2004.043] OpenPKG Security Advisory (tiff)
- Next message: [Full-Disclosure] IRC spying on EEYE!
- **Messages sorted by:** [date] [thread] [subject] [author]