

Full-Disclosure: RE: [Full-Disclosure] RE: [Fwd: [TH-research] OT: Israeli Post Of fice break-in]

RE: [Full-Disclosure] RE: [Fwd: [TH-research] OT: Israeli Post Of fice break-in]

Source: <http://www.derkeiler.com/Mailing-Lists/Full-Disclosure/2004-01/0423.html>

From: Evgeny Pinchuk (*EvgenyP_at_Radware.com*)

Date: 01/13/04

To: "'John.Airey@rnib.org.uk'" <John.Airey@rnib.org.uk>, ge@egotistical.reprehensible.net, bugtra

Date: Tue, 13 Jan 2004 13:51:55 +0200

AFAIK Post Office branches in Israel have 1 to 3 hubs (I think) that manage the whole branch network.

So the intruder doesn't have to know the whole topology of the PO network.

Getting access to these hubs is a different story, but I still think that with some social engineering you could get to them.

Hiding a small AP in very messy place is not a problem.

Post offices are very unorganized and no one really controls what's going on in there from the aspect of networking. (Although POs branches have CCTV)

By sniffing the branch network they could have gathered CC numbers and account numbers.

The rest is just stealing the money. Also AFAIK, Western Union is connected to the same network :).

All the information above is collected from my personal observations and it's not very reliable.

Good Day,

Evgeny Pinchuk.

-----Original Message-----

From: John.Airey@rnib.org.uk [mailto:John.Airey@rnib.org.uk]

Sent: Tuesday, January 13, 2004 11:10 AM

To: ge@egotistical.reprehensible.net; bugtraq@securityfocus.com

Cc: full-disclosure@lists.netsys.com

Subject: [Full-Disclosure] RE: [Fwd: [TH-research] OT: Israeli Post Office break-in]

I can't resist any longer. I have to ask a few questions.

1. How did they know which switch to connect to? Wouldn't this require some knowledge of network topology.
2. If it is indeed a switch and not a hub, how did they obtain access to set this port to monitor traffic?
3. How did they get access to the switch. Shouldn't it have been locked away.
4. How did they convert electrons to money? Was this by raiding bank

RE: [Full-Disclosure] RE: [Fwd: [TH-research] OT: Israeli Post Of fice break-in]

Full-Disclosure: RE: [Full-Disclosure] RE: [Fwd: [TH-research] OT: Israeli Post Of fice break-in]

accounts or collecting credit card numbers?

5. How could they be unable to hide a WAP in a rack (assuming the switch was in a rack)? I can think of several ways to hide one without it being visible.

Seems like a bit of an inside job to me, but I'm no Dick Tracy...

—

John Airey, BSc (Jt Hons), CNA, RHCE
Internet systems support officer, ITCSD, Royal National Institute of the Blind,
Bakewell Road, Peterborough PE2 6XU,
Tel.: +44 (0) 1733 375299 Fax: +44 (0) 1733 370848 John.Airey@rnib.org.uk

Even if you win the rat race, that will still only make you a rat.

—

DISCLAIMER:

NOTICE: The information contained in this email and any attachments is confidential and may be privileged. If you are not the intended recipient you should not use, disclose, distribute or copy any of the content of it or of any attachment; you are requested to notify the sender immediately of your receipt of the email and then to delete it and any attachments from your system.

RNIB endeavours to ensure that emails and any attachments generated by its staff are free from viruses or other contaminants. However, it cannot accept any responsibility for any such which are transmitted. We therefore recommend you scan all attachments.

Please note that the statements and views expressed in this email and any attachments are those of the author and do not necessarily represent those of RNIB.

RNIB Registered Charity Number: 226227

Website: <http://www.rnib.org.uk>

Full-Disclosure – We believe in it.

Charter: <http://lists.netsys.com/full-disclosure-charter.html>

Full-Disclosure – We believe in it.

Charter: <http://lists.netsys.com/full-disclosure-charter.html>

RE: [Full-Disclosure] RE: [Fwd: [TH-research] OT: Israeli Post Of fice break-in]