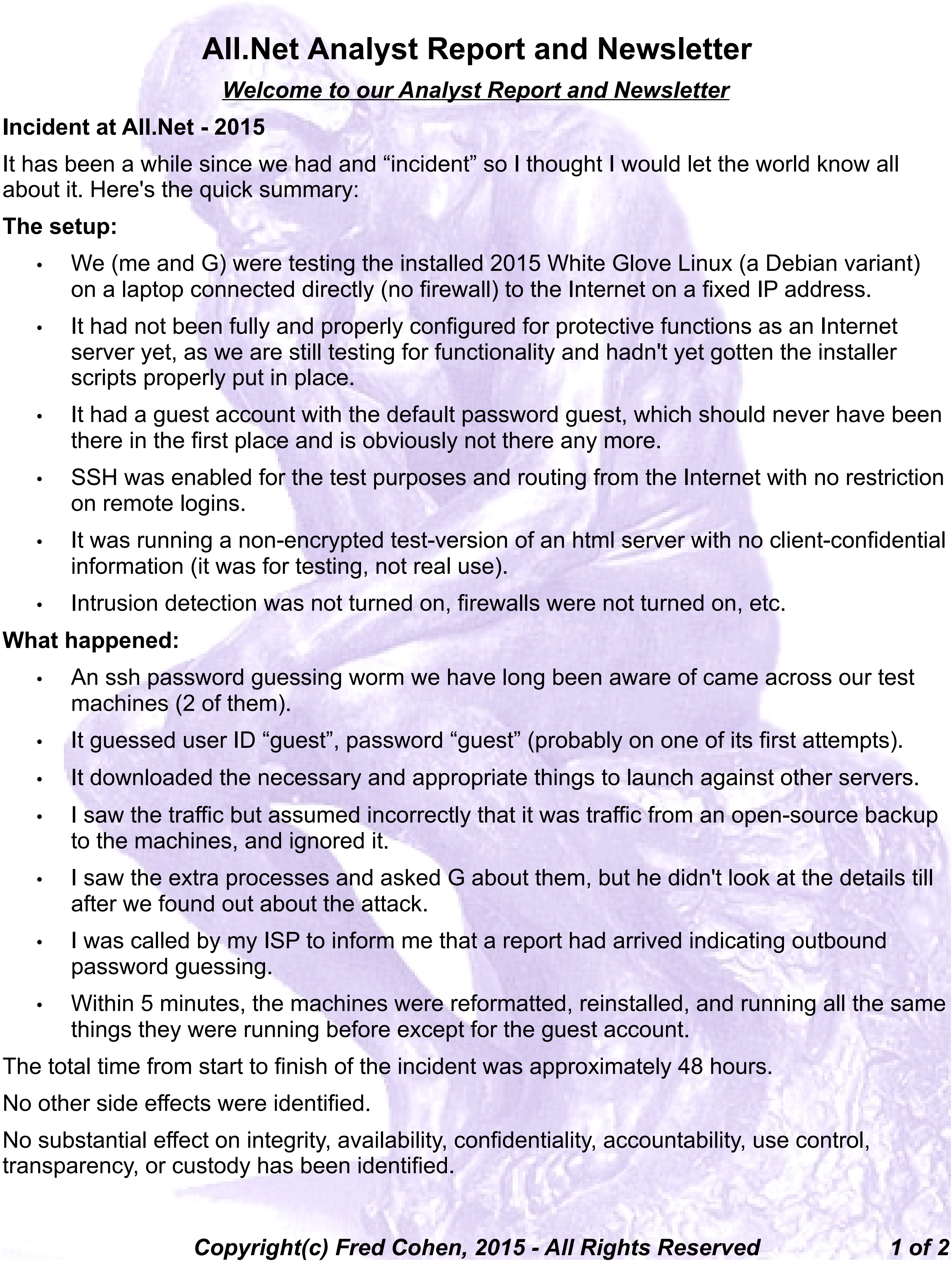

# All.Net Analyst Report and Newsletter

***Welcome to our Analyst Report and Newsletter***

## Incident at All.Net - 2015

It has been a while since we had and "incident" so I thought I would let the world know all about it. Here's the quick summary:

### The setup:

- We (me and G) were testing the installed 2015 White Glove Linux (a Debian variant) on a laptop connected directly (no firewall) to the Internet on a fixed IP address.
- It had not been fully and properly configured for protective functions as an Internet server yet, as we are still testing for functionality and hadn't yet gotten the installer scripts properly put in place.
- It had a guest account with the default password guest, which should never have been there in the first place and is obviously not there any more.
- SSH was enabled for the test purposes and routing from the Internet with no restriction on remote logins.
- It was running a non-encrypted test-version of an html server with no client-confidential information (it was for testing, not real use).
- Intrusion detection was not turned on, firewalls were not turned on, etc.

### What happened:

- An ssh password guessing worm we have long been aware of came across our test machines (2 of them).
- It guessed user ID "guest", password "guest" (probably on one of its first attempts).
- It downloaded the necessary and appropriate things to launch against other servers.
- I saw the traffic but assumed incorrectly that it was traffic from an open-source backup to the machines, and ignored it.
- I saw the extra processes and asked G about them, but he didn't look at the details till after we found out about the attack.
- I was called by my ISP to inform me that a report had arrived indicating outbound password guessing.
- Within 5 minutes, the machines were reformatted, reinstalled, and running all the same things they were running before except for the guest account.

The total time from start to finish of the incident was approximately 48 hours.

No other side effects were identified.

No substantial effect on integrity, availability, confidentiality, accountability, use control, transparency, or custody has been identified.

## How we screwed up so badly

While the incident had no averse effects, we screwed up badly in many ways. While I don't believe these sorts of screw-ups would be present in any of our production systems, I hate to do things wrong, even in testing new systems and developments. It reminds me, every 10 years or so, that I am getting lazy about protection, and so lessons must be learned including this public mia culpa. Hopefully you won't make any of these mistakes.

- **We left a guest account:** I didn't know it was present but had indicators (e.g., the initial user ID added got UID 1001 instead of 1000, a definite hint). Fixed.
- **We didn't turn on the internal firewalls:** No sensitive information, test purposes, etc. all excuses, but in the end, we didn't have them automated yet and didn't take the time.
- **I ignored my responsibility to look into the traffic details:** Flashing lights flash for a reason. I failed to thoroughly check it out in detail after I identified it to G and found that a transfer was indeed underway.
- **I ignored my responsibility to know what all the processes were:** This is the worst of it. I should always know what every process on a server is there for and that it should be there. Again, we have automation for this but haven't gotten it wrung out on WG2015 yet.

In short, I got lazy, we got lazy, and that is how we screwed up.

## Things we didn't screw up

I imagine that my readers will want to tell me there are lots of other things screwed up from my description above, and I welcome your comments. As I get them, I will note new and/or interesting ones by adding them to this short piece. But to give you a hint, here are things we didn't screw up:

- WG is intended to be able to safely run directly connected to the Internet without intrusion detection required or a firewall in front of it. If we do our job right, it will be safe for the intended purposes under this condition.
- HTML without encryption is perfectly fine for our test purposes. We don't care if you or the NSA or anyone else watches our HTML exchanges and the content included in them. We don't even care if they alter them en route. Have at it...
- Yes – we reinstalled the same operating environment with only that change (guest account off) and a few updates unrelated to that change. It's intended to run safely on the open Internet in these conditions. We will be turning on the “server” firewall rules and other related process limitation and so forth over time, but in fact, none of these are necessary to run safely and we do need to continue our testing as we update.

## Summary

We hate to screw up, and don't want to do it again. The best way to assure this is by telling everyone what we did and what happened. Then they can avoid it, we will feel ashamed of ourselves, and hopefully, we will not repeat these mistakes for another 10 years.