Hijacking the Outdoor Digital Billboard

Tottenkoph ~ Rev ~ Philosopher

Who are we?

Tottenkoph
tottenkoph@gmail.com
Member; Hackers for Charities

Rev
Host; Denver, CO 2600

Philosopher
Member; Denver, CO 2600

What do we cover?

- Tools and Information Needed
  In case you wanted to try hacking the billboard, here's some information and tools that will come in handy.
  <Obligatory Disclaimer> We are not suggesting, teaching, or condoning the hacking of The Company's Outdoor Digital Billboard Network. </Obligatory Disclaimer>
- Physical and Network Vulnerabilities
  Yes, they exist and yes, there are many of them

What do we cover?

- What *NOT* to Do
  A few things that you would want to avoid if you were going to attempt hacking the billboard. (See previous slide for Obligatory Disclaimer)
- The Purpose a Hacked Digital Billboard Serves
  Who would want to do this? Why?

Why did we do it?

- Was told, “I bet you can’t hack *that*.”
- No one had done it yet
- Saw it as a possible target for future lulz
- We were drunk and it sounded like a good idea at the time

Who are they?

- International telecommunications company
- Boasts that they have the only digital billboard network in the country

  This is quickly changing as other companies are realizing they can save and make money by doing this as well as get the environmentalists off their back (can claim they're being "green" by not building more billboards). By the time that this presentation is given, they will also have added billboards in various parts of Europe.

The Company (Cont.)

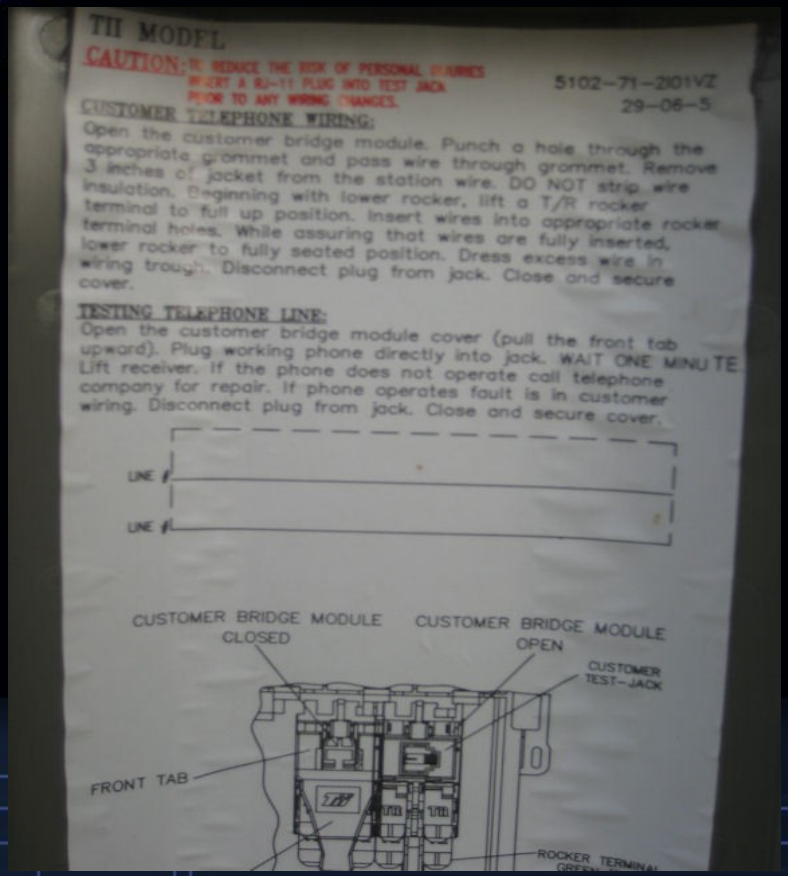
- VERY litigation happy
  They have a super big team of lawyers (we assume) and we have… none. So we're not going to specify which company it is and maintain that this is for informational purposes only. </ass covering>
- Appears as the blurry thing in all of our pictures
  Blurred out because, again, they're very litigation happy.
- Utilizes different manufacturers for their boards
  This provides various ways to get into their network.

Billboard

To our knowledge, three primary types of billboards exist:

- The first type contains a Verizon Telephone Network Interface with clearly marked ADSL POTS splitter and half-ringer.
- Instructions as to the testing and wiring of the telephone line accessible from an exposed phone jack suggest the performance of a basic GO-NO-GO continuity test from the site of said billboard; further use and/or potential vulnerabilities of this line for remote access are unknown.
- Self-actuated data connections for update purposes are presumed.

Billboard with Verizon Telephone Network Interface



Wireless/Satelite

- The second type of billboard site noted contains a nondescript box with a satellite dish.
- It is known that the only three methods of billboard access and maintenance are satellite, POTS and wireless.
- The existence of POTS in addition to potentially unencrypted wireless traffic at the sites of digital billboards presents a theoretical security risk in the instance of the presence of potential intruders on the intranet.

The billboard (Cont.)

Plug in

- An unlabeled box similar to the one present at the second classification also exists at the site of the third, secured with a standard commercial Master brand lock.
- The medium of external communication from this billboard is unknown at present, although the presence of POTS is conjectured.
- An E-Clips surge suppressor is also visible at the site of the third billboard.

The billboard

Physical Vulnerabilities

- Social Engineering

  -- Sales people are really cool people because they'll answer any question you have if they think they're going to get a sale. We were able to find out image specs, uploading information, and some security procedures.

  Sooper Seekrit Passphrase: Money is no option.

  -- "I work for IT" or "I'm a college student majoring in marketing". Yeah, they still fall for that.

Physical Vulns (cont.)

- The Billboard

  --One security camera, pointing at the images on the billboard

  --Nothing surrounding the area around the billboard on the ground (gate, fence, etc.)

  --Located off the side of a road, most of which don't experience heavy traffic between 2:30 and 4:00 in the morning.

Physical Vulnerabilities (cont.)

- The Billboard (cont.)
  --Usually within walking distance of a parking lot that's almost empty during the same hours
  --The only thing between you and the console at the bottom of a billboard is a:
  Commercial
  Masterlock
  (LOL!)
  NOTE: Sometimes there isn't a lock at all.

Network Vulnerabilities

- They are vulnerable to:
  --People connecting wirelessly (that's right folks, to connect, you don't have to worry about passwords or encryption)
  --Packet sniffing (able to see where they're broadcasting to, could spoof the address, and voila)
  --War dialing (depends on the location, but we were told by a sales associate that this is one of their concerns)

Network Vulns. (cont.)

- They are guilty of:
  --Not closing unused ports
  --Using default usernames/passwords (admin, password, etc.)
  --Using global usernames/passwords (A newly found friend of ours that works for them told us this)

Information

- Image requirements
  From The Company's web site:
  DIGITAL BULLETINs
  200 h x 704 w pixel resolution or
  2.778" h x 9.778" w (No Bleed)
  RGB / 72 DPI / JPG format
- Which billboard you're going to go to
  It helps to plan ahead when and where you're going.
- Cover story
  This is useful for when you're questioned by authority figures (police, parents, etc).

Tools

- A laptop
  Depending on which billboard you approach, you may need a laptop with all of the spiffy wireless and packet sniffing tools that are out there nowadays.
- Lock pick kit
  +1 “Ninja” point. +1 Style
- Bolt Cutters (in lieu of lock pick kit)
  -1 “Ninja” point. +1 “brute forcing” point.
- Misc. tools dependent upon the type of billboard.

What Not to Do

- Try this during the day or peak hours of the evening
  As a rule of thumb, wait about half an hour after last call to ensure that the drunks are well on their way home and the cops are busy with them, not you.
- Do it during the holidays and/or weekend
- Forget to use gloves
- Mess with the box with the bright orange sticker


WARNING
Potential
Arc Flash
Hazard
Can shock, burn, or cause death.
PANDUIT PPS050707W2100

What not to do (cont.)

- Hack a billboard near your house
- Leave any sort of evidence that you were there (besides the image)
- Pay for the advert and claim it was a hack.

SKULL PHONE

YOU'RE DOING IT WRONG.

Who would do this?

- (Graffiti) Artists
  It's a new medium that is in a public place that gets lots of exposure.
- Young people
  Hormones + Destruction of someone else's property = lulz
- Hackers
  It's something new to exploit and take advantage of.

Who would want to do this? (Cont.)

- Extremists
  Digital billboards would be a great way for them to spread their message to a large audience quickly and with little or no cost to them.
- Governments
  See above.

Why would they want to?

- Vandalism
  There will always be someone who wants to destroy someone else's property (for example, adding a word bubble next to [insert name here]'s face that says "LOLDONGS").
- Digital Graffiti
  Again, it's a new medium and they can either slightly alter pre-existing adverts to convey something else or the images can be taken offline and the graffiti artists could use the then-blank billboard as a clean canvas.

Why would they want to do this? (cont.)

- Guerilla Advertising
  Sort of became a buzz word that doesn't hold any true meaning to the listener. It usually alludes to aggressive, unconventional marketing methods that is done on the cheap, uses psychology and focuses more on creativity and generating more referrals and bigger transactions.
- Spreading propaganda
  Why just settle for the news, tv commercials, emails, and posters? By posting your message on the billboard network, it'll appear for eight seconds on every billboard in that particular network repeatedly for an undetermined amount of time.
- The Lulz
  Note: This defense will only be useful in Internet court.

EOF

- For more information contact Tottenkoph: tottenkoph@gmail.com
- Website with pictures, information and video coming soon!