THE ACCURACY OF

MR ROBOT

TOM WEBSTER IS NOT MR ROBOT

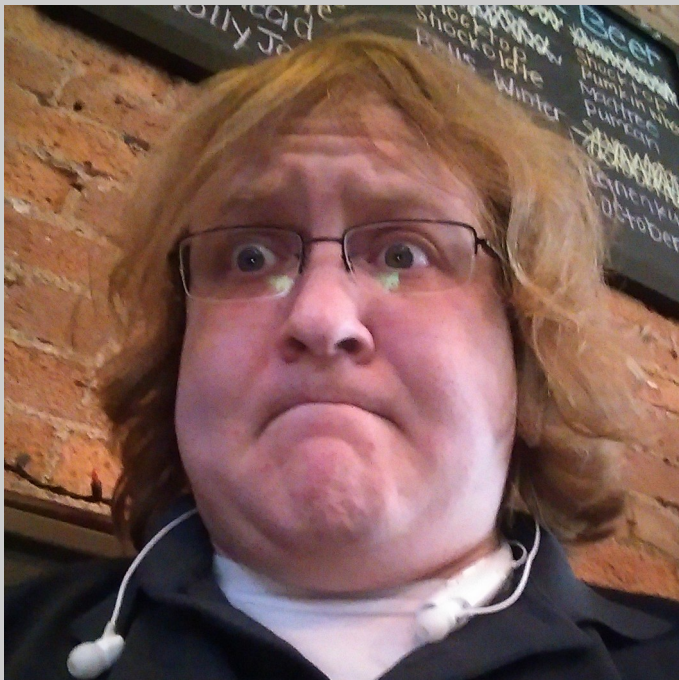
“SamuraiLink3”

SamuraiLink3.com

SamuraiLink3@gmail.com

Plus.google.com/+tomwebster

@SamuraiLink3

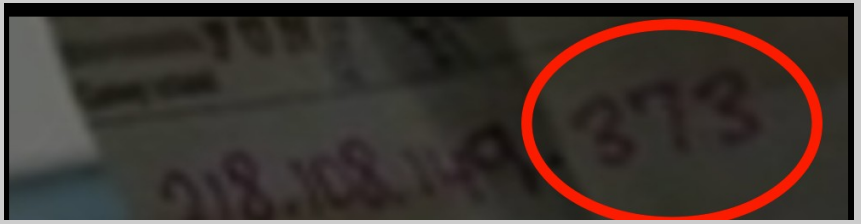


INFOSEC IN TV/FILM

It usually goes something like this:

FAILS

We all fail sometimes



- Invalid IP address
  - Interesting story here, the show's legal department simply wouldn't allow showing a real IP address, as it posed too much of a liability risk to the show, so they had to use an invalid IP.
- Time is sped up on many of the hacks
  - Not even infosec people want to wait for John the Ripper to finish, Mr. Robot took the liberty of cutting time out of time-intensive hacks.
- A payload was supposed to open port 22 (ssh), but the target was a Windows machine. Sure, you can run ssh on Windows, but it's an unlikely connection type, also a reverse shell is much much more likely in this scenario.

SCRIPT KIDDIE

Easy, fundamental

- Watching people on open wifi
- Dictionary attacks against weak passwords
  - Many passwords or dictionary basis words are discovered through observation or social engineering.

HACKTIVIST

Someone was paying attention

- Dropping USB keys with autorun malware
- Remotely accessible Raspberry Pi with Kali
  - Technical advisors worked in a cell connection so the Pi was "always accessible", even behind NAT on it's ethernet connection.
  - The command was netcat with a listening shell: `nc -l -p6996 -e /bin/sh`
- Phishing calls used to get personal information.
  - This is your bank's fraud department calling...

RED TEAM

True professionalism

- HID/RFID Cloning
  - Whoops! Sorry! Didn't even see you there!
- Social Engineering with SET (The Social Engineering Toolkit by Dave Kennedy)
  - Really cool, SET got screen time on national television.

APT

(this is for those of you playing the at-home infosec drinking game)

- One person entered a space before each command. Why?
  - export HISTCONTROL=ignorespace
    - This allows you to enter a command, prefixed by space, and it will NOT be added to the history file. This is the default behavior in most *nix environments.
- Android Malware Install
  - Uses Framaroot to force-root the device through one of several security holes in older Android builds.
  - Then installs Flexispy, which watches many IM programs and other device details. This is a real spy application in use today. The install is shot-for-shot what happens to a real device.

CREDITS

Where to go for more details

samurailink3.com/talks/mr-robot/