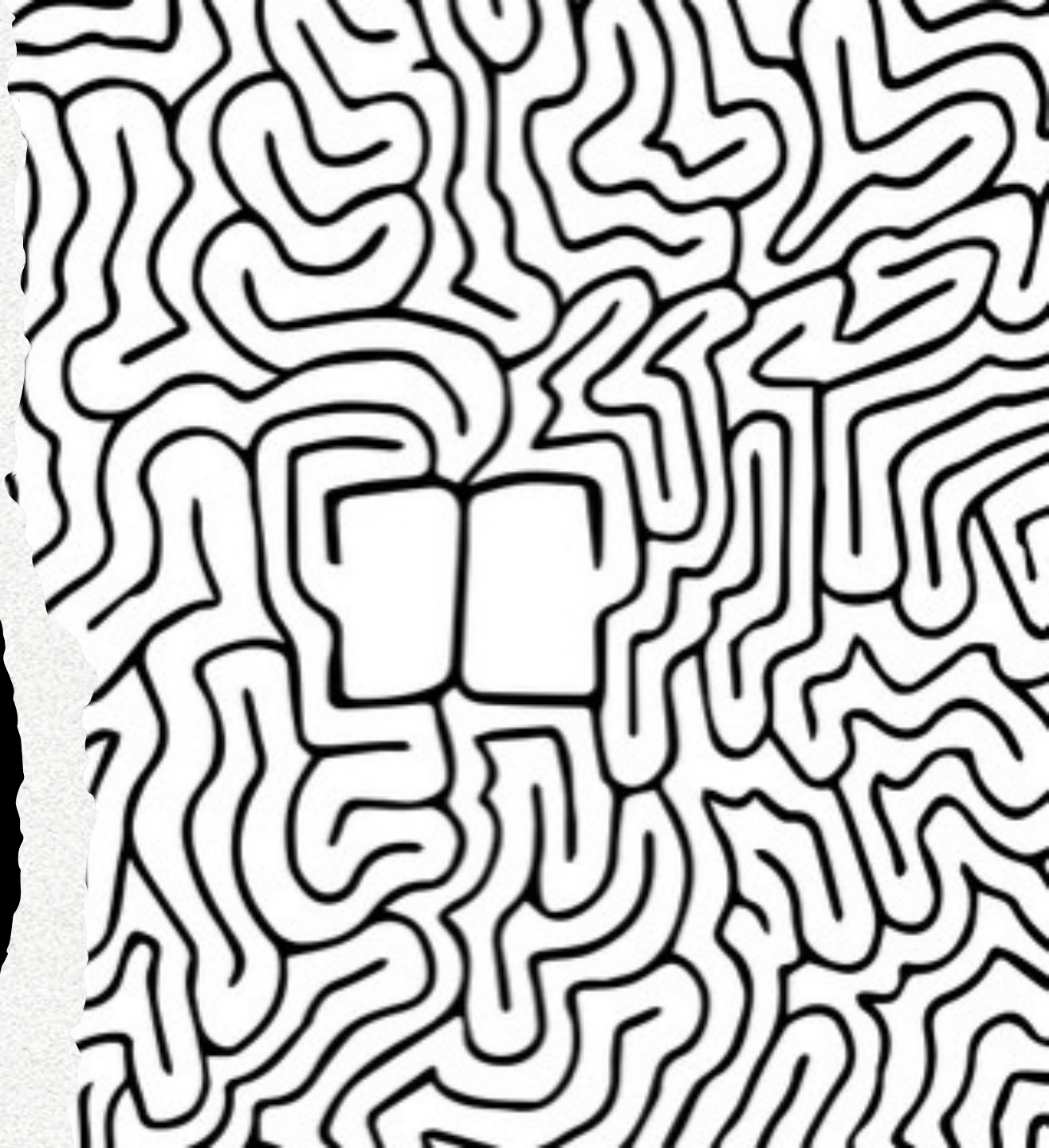
Dysfunctional Unity

the Road to Nowhere



whoami/whatami

- michael aguilar (v3ga | @v3ga_hax)principal consultant – secureworks adversary group
- specialties:
  - physical security
  - social engineering
  - adversary simulations
  - binary exploitation
  - web exploitation
  - making medical devices play doom

agenda

- free time activities
  - exploit development and offensive coding
  - reading about exploit development and offensive coding
  - running/cycling/swimming
  - tattoos
  - grindcore / powerviolence / thrash
    - cr0ws - Side Project

agenda

- what is dysfunction
  - how it applies to the realm medical things
- wars won through attrition
  - my life in the medical device testing realm and lessons learned from recent CVE releases
- lurking dangers in the interconnected space
  - low defenses, high gains, little detections
- my vision for a brighter future
  - roadmaps for success
  - enrichments to the federal workforce



what is dysfunction?

- According to merriam-webster.com, dysfunction is described as “abnormal or unhealthy interpersonal behavior or interaction within a group”
- The groups that I am viewing is security researchers / manufacturers / rule makers. These are three separated entities two of normally (I believe) work cordially together

- Occasionally, the talks netween manufacturer and researcher turn to separated ideas. Ideological vs. proven and utilized logic that has been battle tested, time and time again within the confines of system and network exploitation and study.
  - FDA guidelines are just that, recommendations.
    - There are some hard laws, but HOW stringent are they?
- When there is an impasse between a researcher and manufacturer, WHO is the neutral, LOGICAL third part that can both comprehend the details being explained technologically and how it fits into the larger picture?
  - MY feeling is that the reporting telemetry that I have turned in REGARDING adversarial medical devices are not fully comprehended to the best of abilities.
  - Reading about a threat is one thing, understanding the full scope of what can possibly occur due full comprehension of the attack pattern is another.
- I mean, wea are just talking a single device…

what is dysfunction?



what is dysfunction?

- When companies I have spoken with are talking about “their devices” and the exploits conducted, we are speaking in the singular.
- There are two issues incorrect with this view:

- One – These systems many times, are interconnected to a Hospital or Healthcare Organization network
  - Yes it may **SAY** not to do so but why is there an ethernet port/wifi on the device TO do this?
    - Do Hospitals end up connecting them anyways?
  - Active Directory networks (Hospital networks) have NTLM credentials and other items floating around if not on the exploited Medical Device
    - These are PRIME candidates for easy NTLM credential theft leading to lateral movement in the hospital.
    - Furthermore, even IF the system does NOT use AD tied credentials BUT is networked, it’s a free proxy INTO the healthcare organization.
    - I have taken down major organizations, including healthcare, from credentials with extremely limited access through abusing various Active Directory flaws.

what is dysfunction?

- Two – When the findings or data for a report showing that a threat actor CAN get onto a system using offensive manners, and the flaw was unpatched for the 510K submission, HOW is the device still then cleared for 510K acceptances by the FDA?
  - This one I am still waiting on a clear answer. (Maybe someone can fill me in)
    - Many times, I have heard as a rebuttal, that the device is in a “protected” medical facility, ie the kind with guards…badge readers and people in hospital scrubs…
  - This is why I feel a need for additional support from offensive security experts is needed to be integrated into places such as the FDA/CISA that are responsible for ingesting and comprehending this type of data.
    - People that have conducted offensive operations, that understand the tooling, tactics and procedures used by threat actors as well as the possible weak spots of things like physical security.

what is dysfunction?



a lil b&e (authorized)

- As mentioned previously, I also lead physical security assessments.
- In 2022, I broke into 4 buildings successfully with no detections, no notices and little stopping from authority figures.
- My team was successful in achieving all goals set forth to enter these highly protected areas.
- I was able to gain trust and thusly inside people working on our behalf via in person social engineering efforts.
- If you want to say I cannot get in front of one of these devices to be able to exploit it in a timely manner, I will take that Pepsi challenge (with proper authority).
  - My record for opening and exploiting a closed medical devices system (aka Time on Door) was less than two minutes to open the case, expose a hidden Windows IOT system, establish networking and gain a shell.

hacker tricks

- Adding onto a layer of dysfunction is, again, placing a “connected” device ONTO a Healthcare network.
  - If it is not meant to be connected can it not be devised to be designed without these ports available?
- These hospital network themselves have a plethora of already existing issues including lack of staffing, budgetary issues, politics and other.
- Key Point:
  - On NUMEROUS Adversarial Assessments on medical infrastructure and networks, there is seemingly ALWAYS an OU marked as “Windows Defender/XYZ Protection Disabled”.
  - This is an excellent place to start once you have bloodhound data gathered while conducting network based assessments in healthcare.
- These are large moving gears of war that are slow to react.


WE, UH, WE FIXED THE GLITCH.

fixing the glitch

- GOOD, goal based offensive testing can help to fix many of these issues experienced in both the device manufacturing as well as the hospital system networks.
- It's hard, sticker shock is sometimes truly difficult for these companies and networks to take, but I will tell you this with utmost certainty
  - Which is cheaper? Buying an extremely thorough and goal-based assessment that will help to correct flaws experienced in response technology, staff reactions, playbooks and others OR millions of dollars to a ransomware operator.
  - Plus work with the vendor to use goals like we do to keep scope manageable.
- I GUARANTEE you the report you get from my one my Adversarial Simulations will increase YOUR security budget.
  - I like to view myself as an Adversary AND Budget Force Multiplier ☺

wars won through attrition

- I love having open discussions
  - I love to learn, from other people, other ideas and have a fairly open mind
- Some things; however, needs a dose of reality
- Someone told me something recently that stuck like glue. STOP BEING POSITIVE. BE REAL.
  - A lot of my HOPES were based on the POSITIVE feeling that things will change, you just need to keep proving it.
  - I think that it is time for everyone to be real with themselves and determine this: What is your end game?
    - Actually, make devices with better development methods free of flaws?
    - Do what you can to try to shove a project through and hope the test doesn't see anything?
    - Do we want to enforce things vs. set "you should"?
      - IE – Device was part of a ransomware scenario as the origin – Here's your ransom bill? And a fine of the same amount? I'm not sure, I do not work in massive law scenarios.

wars won through attrition

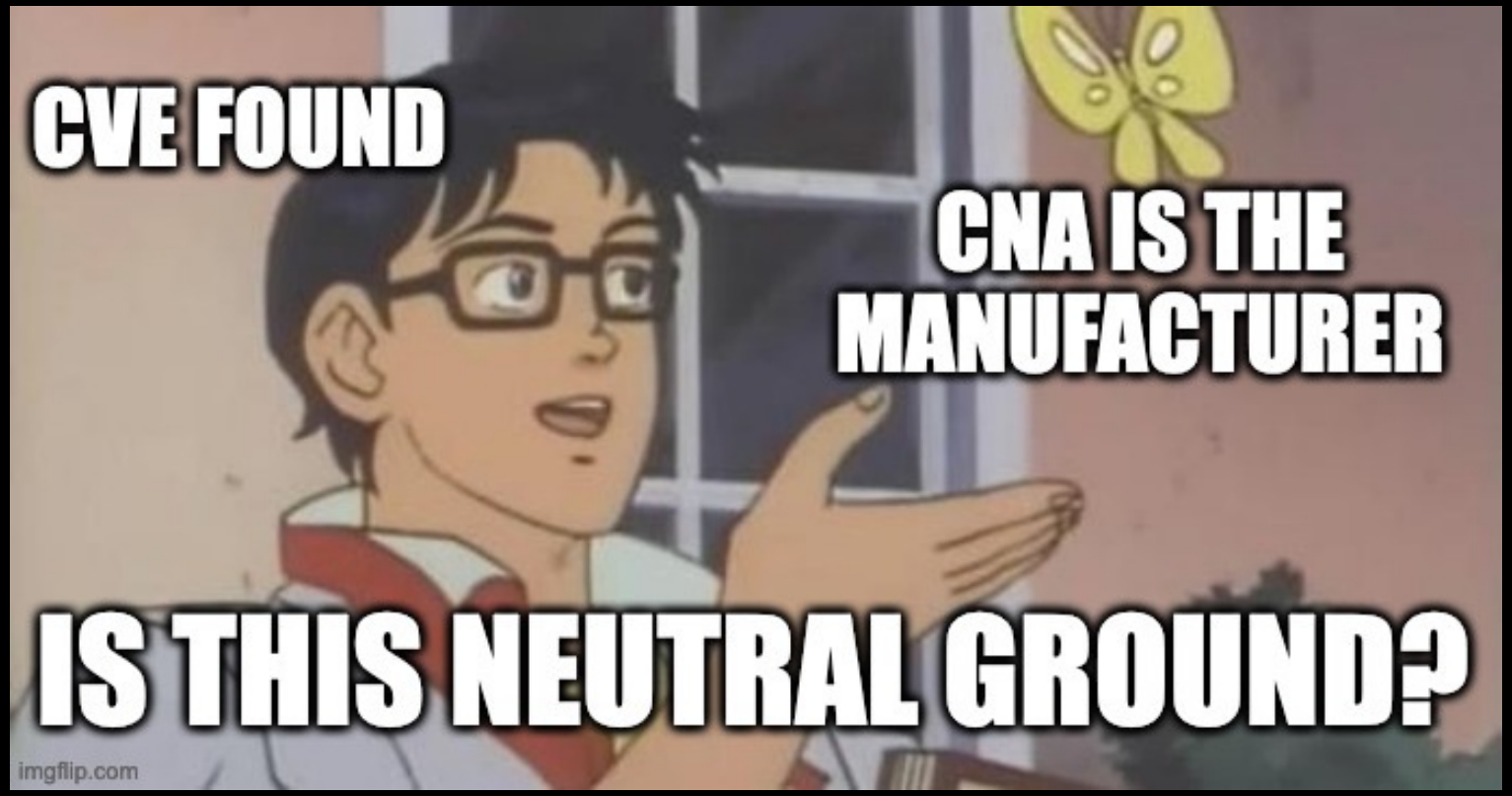
- Working with companies to release vulnerabilities within their systems has shown me two types of groups.
  - Group A: Very Receptive
  - Group B: We talk. They do not get the primitives. We talk more. They add more engineers that start to get angry on the phone. We talk more. They then ask if there is any of their data on my testing system that exists from that company it must be deleted henceforth with conformation (legal sounding). We end up releasing vulnerabilities.
    - Legal words “affirm, in writing”
- Group B – Does that sound like a great “working relationship”
  - Where is the goodwill?
  - Where is the technical understanding?
  - Why is there no admission that these interconnected systems could wreak havoc on the attached Active Directory environment?

wars won through attrition

- A word on neutrality. And this is my opinion (open for discussion).
  - XYZ company has a flaw, they agree to go through their disclosure process. (this is good).
  - XYZ company is also a CNA – They can release the vulnerability with severity and description.
  - XYZ company is also the party responsible for ingesting the vuln, understanding the impact, and potentially…arguing it down…



wars won through attrition



lurking dangers in the interconnected space

- I touched in this previously how healthcare systems and device manufactures need to enhance defensive posture
  - And how offensive testing helps
- The main issue is the high gain these facilities and networks offer
  - The risk of loss of life and loss of patient care abilities is great
    - Multiple ransomware attacks bringing healthcare to paper and pen statuses have caused facilities to shut their doors
  - Multiple health systems are routinely breached, losing massive quantities of patient health records and other personal telemetry
    - Some of this data may include genomic data
      - Its easy to change a Drivers License number, not so much your genome

lurking dangers in the interconnected space

- When I get access to medical devices with networking, all of this can be achieved using offensive operations from that one starting point.
- We must not adhere to the “status quo” but look to do better.
  - This cannot be positive thinking; it must be action.
  - We need better development “principles”. Start with ethos.
- The things I can do teams of people on state sponsored teams can and will do if needed.

lurking dangers in the interconnected space - Example

- Research to weaponization
  - DICOM research came out 5 years ago warning about PE files able to be included in the DICOM header space and the potential ramifications of this.
    - https://github.com/d00rt/pedicom
  - Since then, the research has seemingly been latent with no POC other than their message box and a PDF of the research describing the payload creation in broad terms.

lurking dangers in the interconnected space - Example

- DICOM PAYLOAD EXECUTION

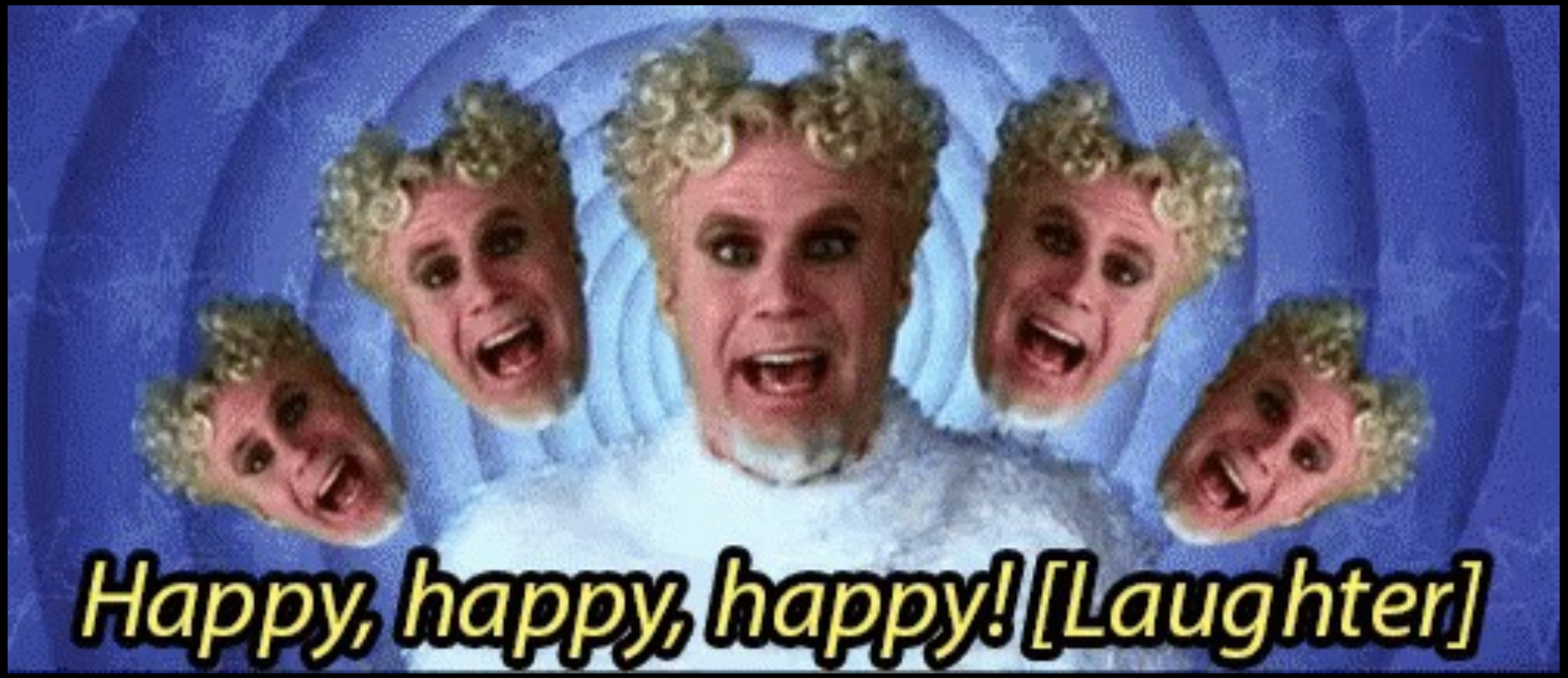
lurking dangers in the interconnected space - Example



lurking dangers in the interconnected space - Example

- From an x86 binary analysis point of view, it was easy to understand and add my malicious payload to in the appropriate spaces.
  - If the original research d00rt (thanks d00rt for researching this) did not release a payload creation script, there was probably a reason.
  - More work needs to be done with evasion.
  - The method can/is/was easily scripted, though I am hesitant about adding this to a public repo due to people then using this in offensive operations. (Tool tentatively called *Asmodeus*).
  - It allows for the file to be executed via command line while also imported into various DICOM projects while keeping the file integrity intact as the research paper teaches.

The road to a brighter future



The road to a brighter future

- we need better actual cohesion between all parties.
  - we need neutral third parties to work through some disagreements regarding severities and outcomes
  - we need to look to bring more offensive minded engineers onto positions that ingest and comprehend these data points so someone can say, “oh shit that’s really bad” if it actually is.
  - we honestly need better cohesion. Here is the thing, for ALL of the CVE’s released (and a few were good to work with/some kinda meh)… I have received the following:
    - Fuckall. There are no bounties, there is no grand anything. No coins, no points, no letter of thanks. This was time taken out of my day, conference and life to make a difference, the least we can do is try to work … patiently together.
      - We don’t need loud voices on the phones.

The road to a brighter future

- we also need to come to a consensus on how to enforce a “guideline”
  - Is there like a three strike rule?
  - Do we even have any kind of anything for repeat offenders?
  - Was the test even a test or was it just a Nessus scan?
  - What IS considered a valid cybersecurity artifact for a 510k or any other FDA ingested consumer product?
    - Is there any internal literature of what a thorough artifact is?
- Again, I see having like minded, offensive security hackery kind of folks (with proven track records) being able to help solve these things somewhat easily from working in the “field”
  - We have all seen GOOD reports of tests and WTF is this kind of reports.
    - Lets aim for better, we all will benefit from it.