Twitter Thread by _MG_

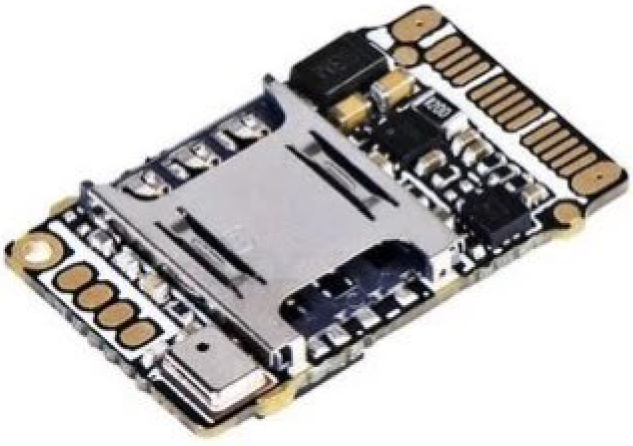
_MG_
@_MG_

Woke up to like 100 tags on this iPhone implant. Which is found in this video here: https://t.co/9khbpmUQEH

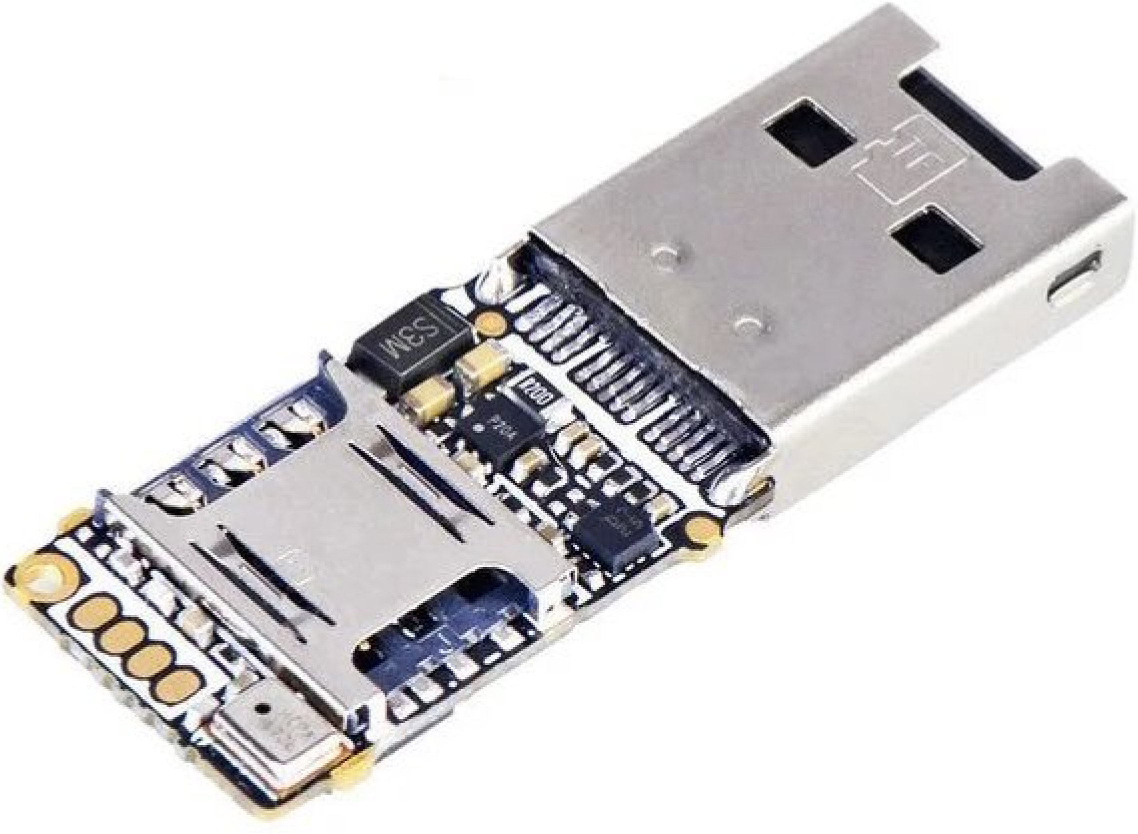
I don’t speak Russian, but I do have a first grade language fluency in hardware. So lets take a look!
Thread 1/n

So a lot of people have correctly identified it as this GPS & Wifi based location tracker with microphone.
A very common type of device, similar to what is found in those extremely suspicious looking USB cables:
https://t.co/uBhi7tRhiW

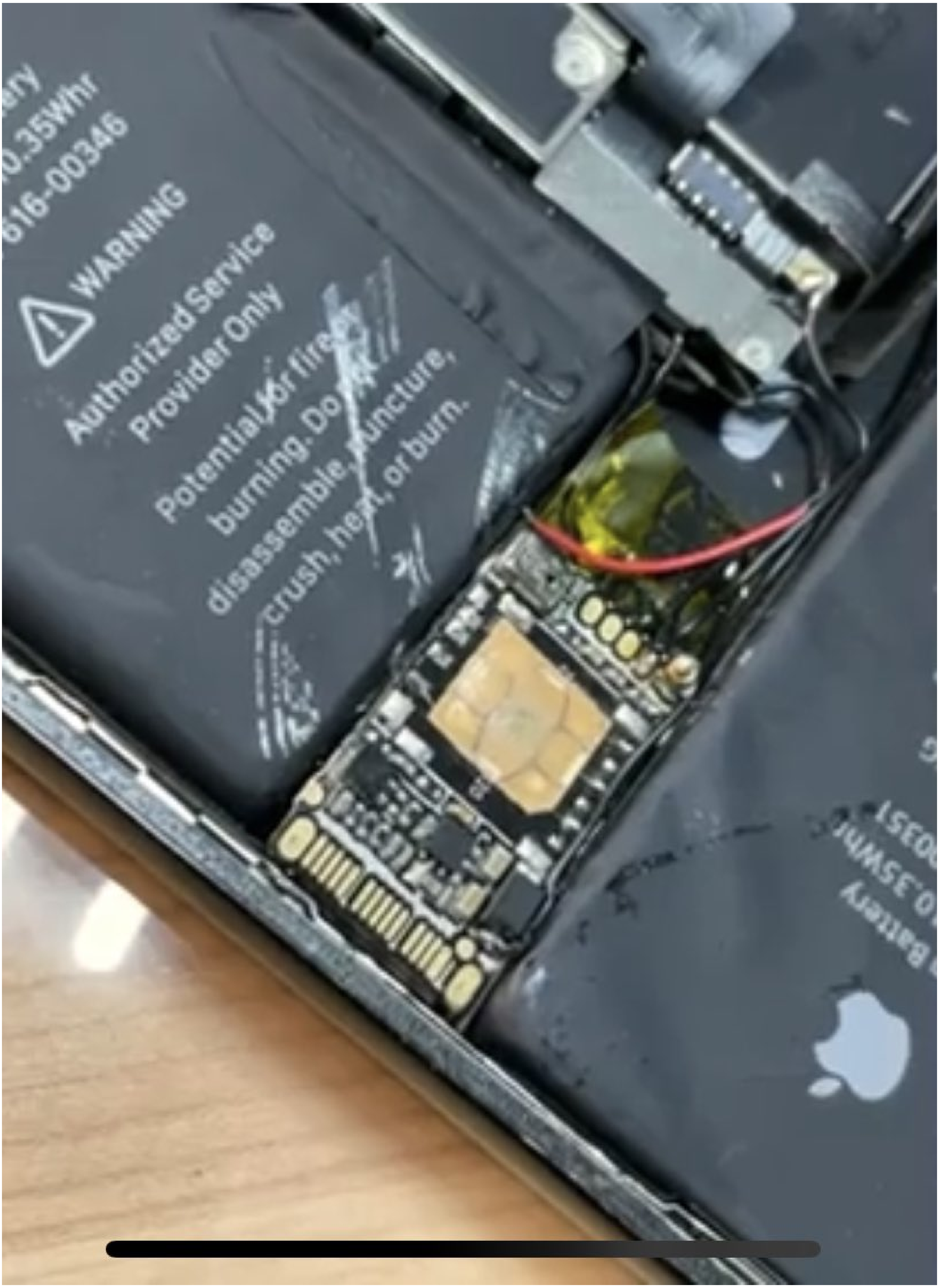
2/n



The headers are designed to attach a specific USB connector that fits a micro SD card in the tip.
3/n



A repurposed board is very “hobby implant” but... we see the SIM card was removed, which would make this a wifi-only implant. Yet an external GSM antenna is attached and only the ground for power? Cant see the other side though...
4/n


ery
10.35Whr
616-00346
WARNING
Authorized Service
Provider Only
Potential for fire or
burning. Do not
disassemble, puncture,
crush, heat, or burn.
Battery
10.35Whr
00351

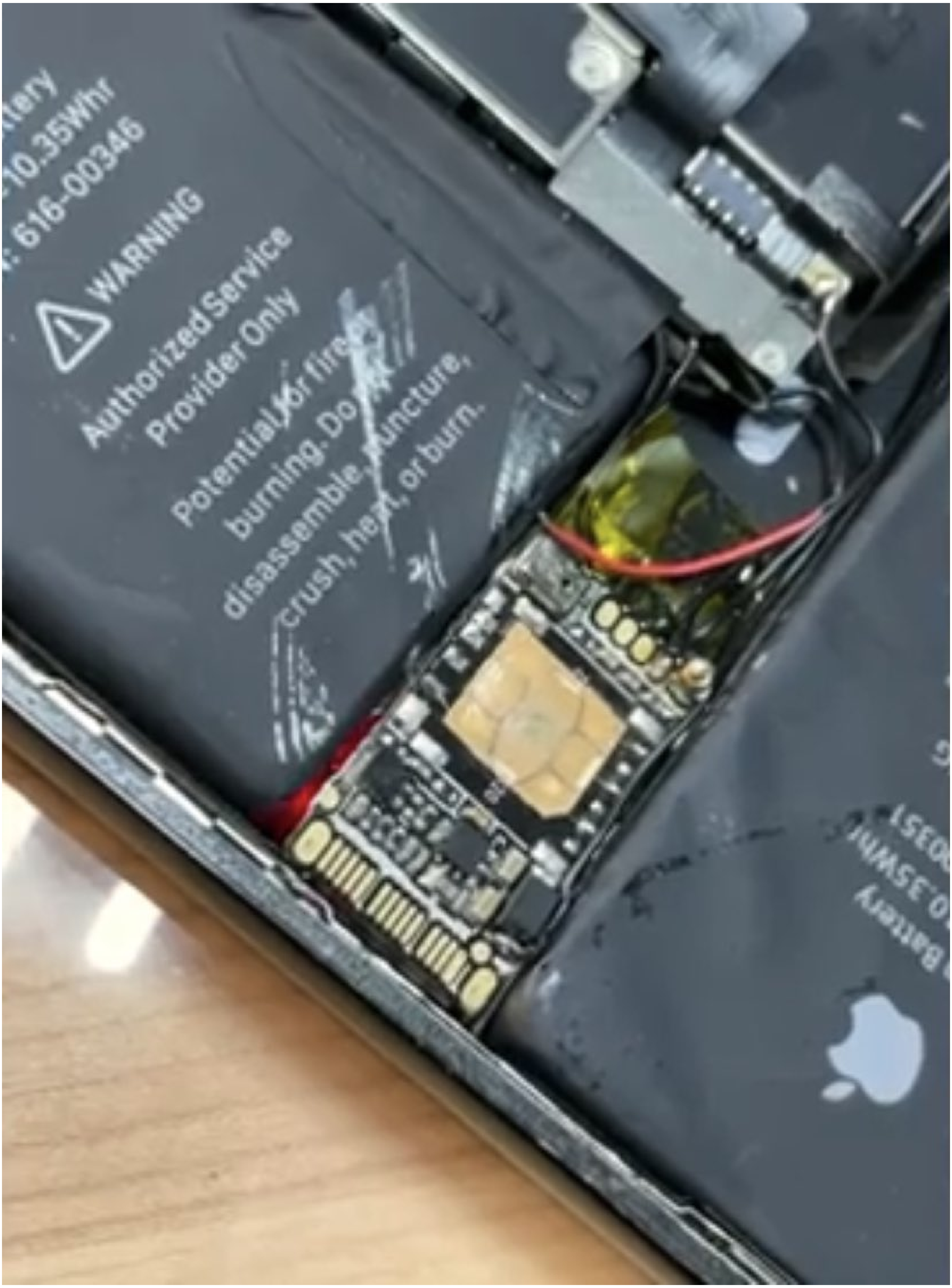
Upon closer inspection, they removed the SIM slot housing and soldered a SIM card directly to the pads. That gains a little more space.

Thanks @dcuthbert

5/n https://t.co/Sq9X6yByPV

> They've cut the simcard and attached it that way, so removed the housing.
>
> — Daniel Cuthbert (@dcuthbert) January 14, 2021

You can see an antenna in the upper right. Right on a metal shield which will hurt the range.
There is normally not a convenient place for an implant, but they swapped the battery for a smaller one.
6/n


ttery
10.35Whr
616-00346
WARNING
Authorized Service Provider Only
Potential for fire or burning. Do not disassemble, puncture, crush, heat, or burn.

This feels like a proof of concept done for the video, or a fairly low grade implant done with a tiny budget. It could be done way smaller by not repurposing an existing thumb drive module.

7/n

For many adversaries that want location & mic, I suspect they generally don’t need a hardware implant. But there are always exceptions. That’s not really my area though.
8/n

Looks like @Requiem_fr has a nice visual comparison showing the battery reduction for clearing space.

This is a technique I have also used in power supplies when needing a little extra space for... activities ■

9/n https://t.co/KjgfREmhZt

> Unlike what is explained in the video, the lower part of the battery has been replaced by a same module than used for the the upper part. Allowing them to get enough space. pic.twitter.com/0LpUOpSrRC
>
> — Requiem (@Requiem_fr) January 14, 2021

If true, this seems almost like it was intended to be found. The work is really primitive for gov work, not to mention the other ways they can pull location & mic.

10/n https://t.co/AwNiFpIE2V

> After being released from detention, Olga Kerimova, election campaign chief for opposition candidate & @navalny associate @SobolLubov, got her iPhone back. It came with an upgrade: a crudely onboarded bugging and tracking device.
> These nitwits can't do anything subtle. pic.twitter.com/bMHfVVlrCc
>
> — Christo Grozev (@christogrozev) January 14, 2021

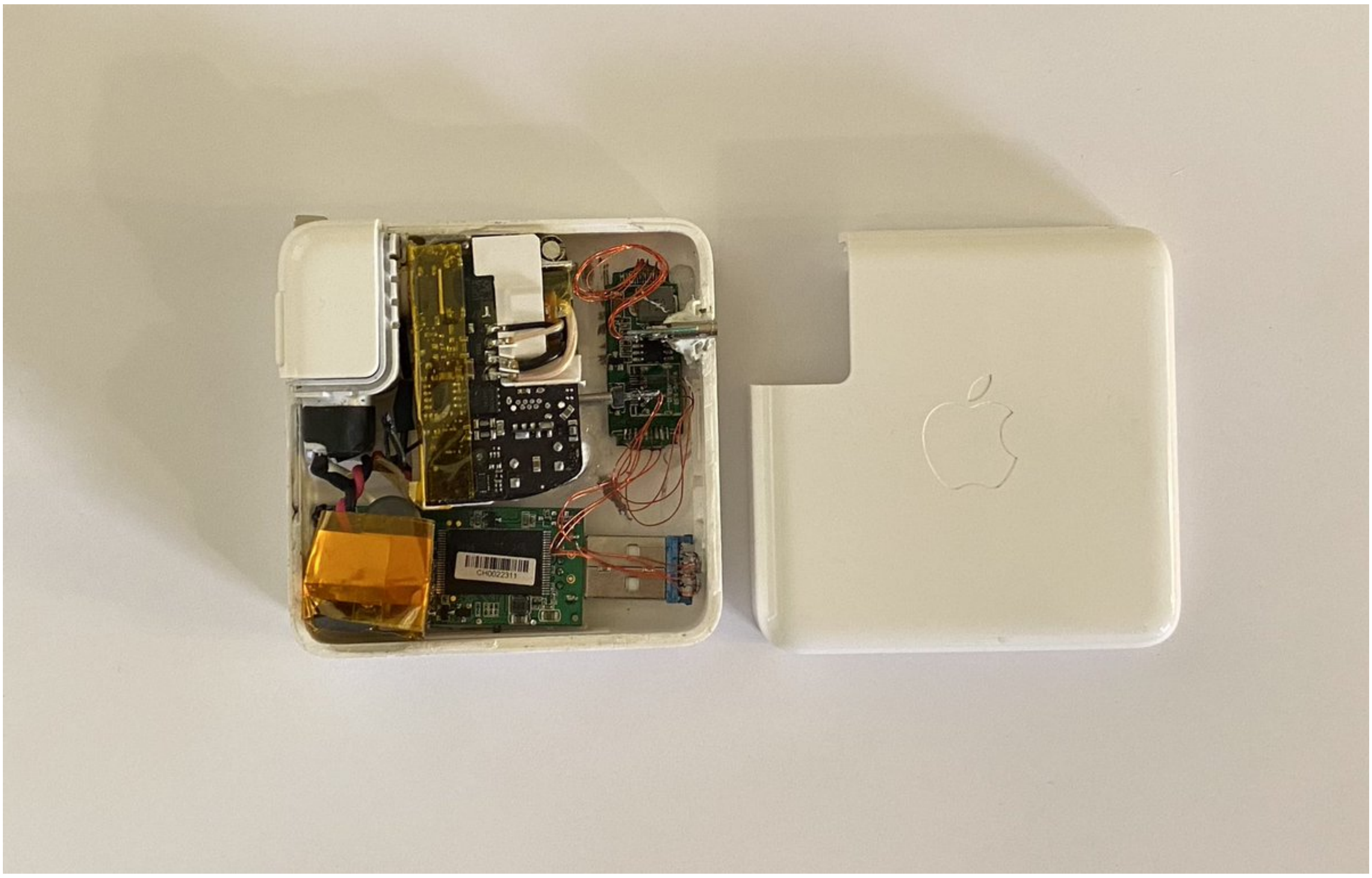
The “shrink the power source” approach was what I used for this project:

11/n https://t.co/gz3cuKC6jb

> Demo of a work in progress. I\u2019m looking for help with writing payloads. Come chat with me at @defcon if you\u2019d like to collaborate.
>
> Power adapter. Silent infection. Cross platform. Not just Apple hardware.
>
> Project page with info: https://t.co/b62N5cWVSG
> 1/n pic.twitter.com/pxwrb9o9HU
>
> — _MG_ (@_MG_) August 3, 2018

Here is a previously unpublished picture of the internals. It’s all cannibalized COTS hardware.
This was before I got into hardware design. Not very good, but enough for a proof of concept.

12/n



One plausible idea: this only needed to last long enough to see where the phone went before it was torn open. That would give some valuable info.

13/n https://t.co/M77sGjOmcW

> Maybe they may know that they turn off the phones and just want to know gps location... for that when they turn off the phone the implant is still running on the battery ... it's desperate but smart to come later and stop the whole world
>
> — UniCOrN \U0001f984 (@UniC0rN_2021) January 14, 2021

Anyway. I’m just going off a few pictures as I haven’t had the time to properly research it. For all I know, this was created as a stand-in for video demo purposes.
14/n