



# Recita: La storia di un nerd – Mario che riprogrammò il pacemaker del presidente

Original Published on January 12, 2016

**By Alessandro Mazzarisi**

Senior Technician at National Research Council Institute of Clinical Physiology

## **Quante cose non avevano funzionato in quei giorni perché ciò potesse accadere...**

*Serve un racconto di fantasia per alzare l'attenzione su un tema scottante. Per adattarsi alle normative che si evolvono, i nuovi Medical-Device invece di essere certificati ex-novo, usano sempre le certificazioni ricevute per prodotti di precedente generazione, aggiungendo solamente strati di sicurezza. È quello che accade anche per i canali trasmissivi così detti sicuri, costruiti su tecnologie vecchie e ben conosciute. È noto a tutti che è utile che di sicurezza ne parli, e sia verificata da chi di sicurezza ne fa il suo mestiere. Quando in gioco ci sono grandi interessi come sui pacemaker e i defibrillatori impiantabili, fatti pagare a caro prezzo alla collettività, servono competenze indipendenti per dare le dovute autorizzazioni, a partire dagli Ingegneri Biomedici e Clinici.*

***Quante cose non avevano funzionato in quei giorni perché ciò potesse accadere***

Mario era arrabbiato con il mondo, e Mario era un nerd, uno che con la tecnologia ci sapeva fare.

Odiava il suo ex-presidente perché improvvisamente lo aveva licenziato ed era rimasto solo e senza soldi da parte, perché aveva dedicato tutta la sua vita al lavoro.

Non vedeva il suo ex-presidente da due anni.

L'azienda che offriva servizi di Ingegneria Clinica era stata completamente de-localizzata all'estero.

Regolarmente il suo ex-presidente tornava nella città di Mario, dove continuava a vivere con la sua famiglia.

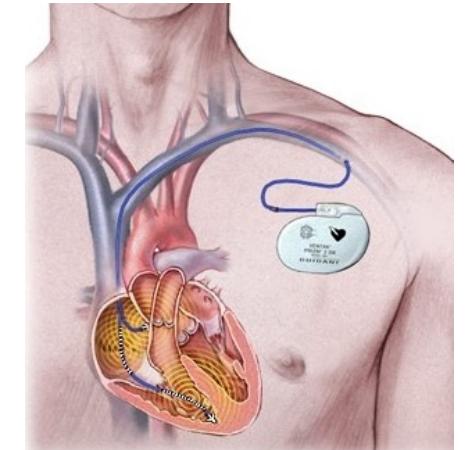
Una mattina, lo vide entrare in Ospedale, e Mario sapeva bene perché il suo ex-presidente era lì.

Aveva lavorato in quell'ospedale come esperto della sicurezza ambientale e conosceva personalmente il presidente.

Il presidente era un cardiopatico.

Aveva un cuore aritmico compromesso da anni.

Portava un pacemaker con defibrillatore impiantabile.



Mario, in preda alla depressione autodistruttiva che lo assillava da tempo, iniziò a convogliare la sua energia negativa su chi lo aveva ridotto in quello stato.

Conosceva tutto sulle tecnologie di comunicazione digitali, ed era un esperto di telecomunicazioni e apparati radio ricetrasmettenti.

Quel giorno rivedendo il suo ex-presidente, fu rapito da un'idea distruttiva a cui più pensava e più provava un senso di sollievo, un tarlo che gli suggeriva incessantemente:

***"E se provassi a riprogrammare il pacemaker del presidente?"***

Era una sfida intellettuale allettante per una mente che aveva perso la bussola, il sacro confine tra un atto lecito e uno illegale.

Si ricordò che quando faceva bonifiche di sicurezza ambientale, usava un registratore digitale di segnali radio auto costruito, che ancora conservava.

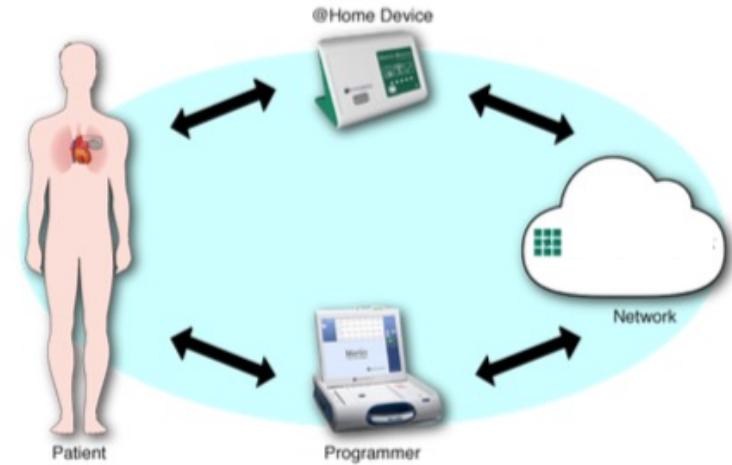
Una scatola nera che nel raggio di pochi metri era in grado di registrare le comunicazioni digitali via radio di qualsiasi dispositivo elettronico.



Per poterci riuscire era necessario conoscere la frequenza trasmissiva e il tipo di modulazione con cui il pacemaker parlava con la rete di monitoraggio, oppure avere tempo e la certezza che stesse trasmettendo solo una coppia di dispositivi alla volta.

Con un po' di lavoro poteva adattarsi perfettamente a qualsiasi tipo di dispositivo wireless, anche un pacemaker.

## Era proprio il suo caso



Quel giorno non aveva con sé quel giocattolo da spia di altri tempi; era nella soffitta di casa sua, ed era venuto il momento di farlo lavorare di nuovo.

Rimandò la vendetta e tornato a casa, tirò fuori tutto il necessario per riprendere a fare il suo lavoro di un tempo:

**dopo due anni, il ricevitore passivo e il software che analizzava le comunicazioni, incredibilmente, funzionavano ancora.**

Aveva un paio di dubbi – 1) come avrebbe potuto avvicinassi al suo ex-presidente, e 2) non sapeva quando sarebbe tornato di nuovo in città.

Per riprogrammare il pacemaker, la vicinanza fisica era un requisito indispensabile.

Mario si mise a spiare le comunicazioni del presidente: la posta elettronica, il cellulare e i social network a cui era registrato.

Senza troppe difficoltà scoprì il prossimo appuntamento del presidente nell'ospedale della sua città; purtroppo aveva solo una settimana di tempo per organizzare la sua azione.

Doveva trovare il modo di avvicinarlo senza disturbarlo e registrare la comunicazione criptata tra il pacemaker e il programmatore professionale usato dai medici.



**Era il primo obiettivo da raggiungere  
per mettere in scena il suo piano**



Per recuperare tutti i dati che gli servivano doveva conoscere qual era la marca e il modello del pacemaker che il presidente aveva impiantato nel petto.



## Indagò come fa un hacker

Cercò le tracce lasciate dall'amministrazione dell'ospedale e dal reparto di ingegneria clinica dove aveva lavorato per tanti anni, e lo fece accedendo ai computer ancora in servizio, che lui stesso aveva configurato.



Attraverso il sito web aziendale, indagò sui resoconti degli acquisti fatti negli ultimi anni e trovò la lista dei produttori di pacemaker e dei defibrillatori impiantabili che stavano usando.

Per trovare il modello esatto Mario cercò tra le tracce che il presidente lasciava sui social network, incrociandole con le e-mail private che incurante della sicurezza informatica, continuava a usare senza autenticazione, usando l'indirizzo pubblico dell'azienda.

In una delle email che conservava sul suo account condiviso, trovò il **nome** e il **codice** del pacemaker che gli avevano impiantato; un device sofisticato ma soggetto a numerose regolazioni per potersi adattare allo stile di vita dell'ospitante.

Alla fine Mario scoprì anche le date di tutti gli appuntamenti che il presidente aveva già programmati nell'ospedale.

**Ma per registrare e decodificare le comunicazioni digitali via radiofrequenza la cosa fu articolata.**

I due si conoscevano e per non farsi scoprire, nascose il registratore di segnali, nella scatola di uno smartphone, che consegnò a uno sbandato del suo quartiere, promettendogli una ricca ricompensa in cambio di un “lavoretto pulito”.

L’incaricato, si sarebbe dovuto avvicinare con la scatola a un locale dell’ospedale indicato da Mario, in un giorno e a un’ora precisa, per registrare i rumori ambientali.

Lo sbandato, ignaro di quello a cui si sarebbe prestato, acconsentì.

Il giorno del controllo del pacemaker era tutto pronto.

Il presidente come faceva da alcuni mesi tornò al laboratorio di aritmologia dell’ospedale per farsi riprogrammare il suo prezioso dispositivo in modo che si adattasse al suo stile di vita.

Anche il presidente era ignaro di quello che gli stava per accadere. In una stanza attigua al laboratorio, dietro una parete fuori dalla vista del medico, lo sbandato registrò il traffico dati prezioso per Mario, quella comunicazione speciale con cui il professionista di fiducia del presidente, riconfigurava tutti i pacemaker, come faceva sempre, ogni giorno in buona fede.

Mario era entrato in possesso di quello streaming di dati digitali pronto per essere dato in pasto al suo vecchio e glorioso software di analisi.



**Sapeva tutto:** il modello del pacemaker e del programmatore, il tipo di modulazione in radiofrequenza usato, le codifiche e i protocolli usati perché erano descritti nei manuali accessibili in rete e sui motori di ricerca.



Ora toccava a Mario.

Iniziò il suo lavoro di hacker con l'acquistare tutto l'hardware necessario su **ebay**.

Non fu il traffico SSL a fermarlo, perché erano anni che i nerd sapevano come de-cryptarlo; serviva solo tempo e lui ne aveva tanto.

Ci vollero settimane di prove per trovare una logica in quella sequenza di dati criptati che avrebbe dovuto scambiare con il pacemaker.

Condition see all  
New (3)  
Used (8)

Price  
\$ [ ] to \$ [ ]

Format see all  
All Listings (11)  
Auction (0)  
Buy It Now (11)

Item Location see all  
Default

**St. Jude Medical (EX-1150) Merlin Home Transmitter**  
**\$10.99**  
Buy It Now

**Merlin @ Home Transmitter St Jude Medical EX1150**  
**\$22.99**  
or Best Offer

Utilizzando lo stesso lettore di tracciati ed eventi usato dal presidente a casa sua e che Mario aveva comprato su eBay, disassemblò il firmware, entrò come **root** e scoprì le chiavi di comunicazione private, grazie al tracciato registrato con il suo dispositivo.

On the right a screenshot evidencing Muddy Waters got root on Merlin@home devices (using exploits developed by MedSec):

apps dev mnt sbin vpd

```
root@(none):# cd etc
root@(none):/etc# ls -a
.
..
PWD.lock
.tantobasic_release
Wireless
adjtime
chatscripts
cron.daily
default
devfs
dhcpc
fstab
gateways
group
hhl-arch
host.conf
hosts
hotplug
hotplug.d
init.d
root@(none):/etc#
```

Muddy Waters Research - Due diligence-based investment research - Mozilla Firefox  
Muddy Waters Rese... x +  
www.muddywatersresearch.com

what time is it - Google Search - Mozilla Firefox  
what time is it -Goo... x +  
https://www.google.com/search?client=ubuntu&

MUDDY WATERS RESEARCH

2:12 PM

Wednesday, July 6, 2016 (PDT)

Poi, grazie al calendario delle visite all'ospedale del presidente, Mario riuscì a programmare più tentativi per testare le modifiche che stava introducendo nello streaming di cui aveva fatto il reverse engineering e finalmente riuscire ad imbrogliare il pacemaker da controllare.

Anche trovare un trasmettitore di segnali radio adeguato, in grado di convincere il pacemaker da colpire di essere lo stesso programmatore usato dai medici dall'ospedale non fu facile; ma ormai con quello che Mario sapeva, ci riuscì.

### ***Il primo tentativo di hackeraggio che organizzò fu un fallimento***

Mario era nelle vicinanze della sala di attesa del reparto di aritmologia, solo, al buio, nel ripostiglio della ditta delle pulizie, ma la prima volta la comunicazione nemmeno iniziò.

Registrò una nuova sequenza e dopo averla analizzata, al secondo tentativo, dopo essersi di nuovo appostato nelle vicinanze della sala di attesa, il **sistema** e il **pacemaker** del presidente parlarono.



Mario inviò i nuovi codici al dispositivo impiantato nel petto del presidente senza conoscerne gli effetti.

Pochi minuti dopo il presidente iniziò a sentirsi male.

Si alzò dalla sala di attesa barcollando, in cerca di aiuto, ed era in stato confusionale, quando incontrò Mario diretto verso l'uscita, pronto a cantar vittoria.

Mario era un nerd, ma infondo era anche una brava persona e non se la sentì di lasciare il suo ex-presidente in quello stato.

Lo prese sottobraccio e l'accompagnò nel laboratorio di elettrofisiologia chiedendo aiuto al posto suo.

I medici prestarono assistenza al presidente, lo portarono in sala operatoria e riprogrammarono il pacemaker impazzito, cancellando tutte le tracce dello sforzo di Mario.

Pur sapendo di rischiare di essere scoperto, Mario decise di pubblicare la storia, su come aveva riprogrammato il pacemaker del presidente e la inviò al giornale del suo paese.

Il giornalista ricevuta l'auto-denuncia, per verificare le notizie contenute nell'articolo, contattò il medico di fiducia del presidente, il quale, rivoltosi alla ditta produttrice del pacemaker, dopo aver ricevuto una lunga e convincente spiegazione da parte della multinazionale sulla sicurezza dei dispositivi in commercio, convinse il giornalista a non pubblicare nulla.

Passarono pochi giorni e Mario si rese presto conto della beffa che aveva subito: niente articolo pubblicato sul giornale e soprattutto, il giornale locale a cui si era rivolto, improvvisamente, aveva iniziato una nuova stagione editoriale: la rubrica sulle denunce dei cittadini era stata soppressa, e il giornalista zelante fu spostato alla cronaca.

Per quel suo gesto sconsiderato, l'unico a rimetterci era stato il giornalista strapazzato dal suo editore.

Mario avvilito, era ripiombato nella depressione, e prima di scomparire, decise di scrivere la sua storia con dovizia di particolari, adattandola per un social network frequentato dai professionisti della sicurezza informatica.

Sapeva benissimo che piacenti o non piacenti, quei suoi discorsi sulla sicurezza avrebbero fatto arrabbiare le multinazionali.

Ormai non gli importava più nulla.

Sentitosi minacciato, Mario condivise la sua storia su di un cloud; mentre una copia della storia completa, la condivise via tor nel darkweb frammentata su centinaia di migliaia di server in tutto il mondo.

Disperato e contro ogni logica razionale era pronto a condividere il suo ultimo sforzo.

Aggiustò la grafica, evidenziò le parole chiave usando gli hashtag, le graticole usate per indicizzare i testi sui motori di ricerca. Era pronto a fare il suo click, a mandare in rete tutto il veleno che aveva in corpo.

Lo faceva per ammonire e rendere consapevoli tutti quei medici sempre compiacenti con le multinazionali, sulla sicurezza di quei dispositivi che impiantavano nei pazienti, con tanta leggerezza.

Improvvisamente il suono di un sms, accese per un attimo il display del suo smartphone.:

***“Mario, sappiamo dove sei,  
non ti muovere e non inviare nulla in rete”***

Tutte le comunicazioni erano controllate ma decise di regalare a tutti la sua storia.

Cliccò sul pulsante “**Invia**” e tutte le prove finirono frammentate in tanti parti diverse di un film porno condiviso su di uno dei tanti server tor.

*E il seguito, direte voi...*

Come tutte le storie, anche questa ebbe un seguito.

Del nostro Mario non si seppe più nulla.

Da quando accaddero quegli eventi nel gennaio 2016, quanti nerd come Mario ci provarono ancora, non è dato saperlo.

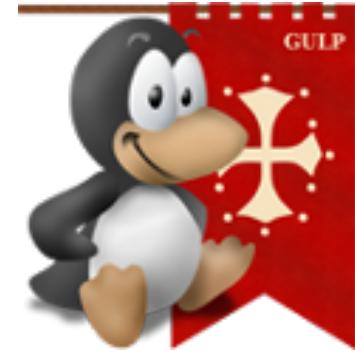
D'altra parte, **prima addestriamo i nostri professionisti della sicurezza a spese della comunità, poi li sotto inquadriamo e li sottopaghiamo, e infine li facciamo fuori nella speranza che nelle nostre organizzazioni vada sempre tutto bene.**

Quanti “**Mario**” disperati potranno in futuro mettere in pericolo la vita di altri cittadini e per di più a loro insaputa?

Domande a cui i medici da sempre sono stati addestrati a risponderci con parole rassicuranti, e noi non sapremo mai la verità.



[mazzaris@ifc.cnr.it](mailto:mazzaris@ifc.cnr.it)  
[mazzaris@mac.com](mailto:mazzaris@mac.com)  
[mazzaris@gmail.com](mailto:mazzaris@gmail.com)  
<https://it.linkedin.com/in/mazzaris>



## Grazie della vostra attenzione

**Alessandro Mazzarisi** - Senior Technician at National Research Council Institute of Clinical Physiology, Co-reviewed Articles, International Conference Papers, Full-Texts, I am a visionary technician with over thirty years of experience working with teams whose focus is on integrating technology into our healthcare systems. Passionate about innovation, as well as on improving healthcare and education, I have worked in different roles with public and private companies, government entities and universities in Europe. I have taken part in the growth of Italian biomedical engineering, ICT and EHR infrastructures. Currently, my focus is on developing effective software solutions for innovative EU-projects at the Italian National Council of Research. I have recently resolved to share my experience on Linkedin Network with weekly original articles.

... a seguire alcune slides di riferimento

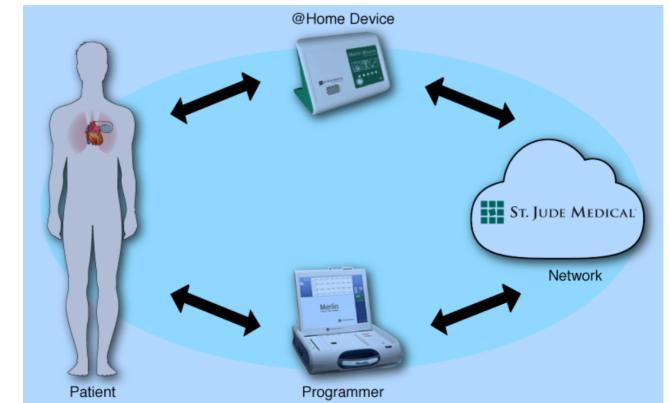
## August 25, 2016 hacker team demonstrations of two types of cyber attacks against implantable cardiac devices

<http://www.muddywatersresearch.com/research/stj/mw-is-short-stj/>



I Device Medicali controllati in remoto con Radio Frequenze, RF dovrebbero avere una serie di difese che includono:

- ☆ strong authentication,
- ☆ encrypted software and code,
- ☆ anti-debugging tools,
- ☆ and anti-tampering mechanisms.

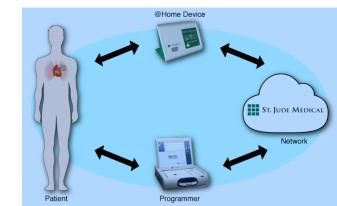


Inoltre i costruttori potrebbero richiedere meccanismi di attivazione dell'comunicazione RF molto lunghe per evitare attacchi ripetuti.

## August 25, 2016 hacker team demonstrations of two types of cyber attacks against implantable cardiac devices



**Vulnerabilità:** I programmatori dei Device Medicali generalmente possono comunicare agevolmente con i dispositivi cardiaci impiantabili perché di solito non c'è un'autenticazione forte implementata nei protocolli di comunicazione. Un malintenzionato che fa reverse engineering delle comunicazioni può accedervi e impersonare tutti gli attori dell'ecosistema.



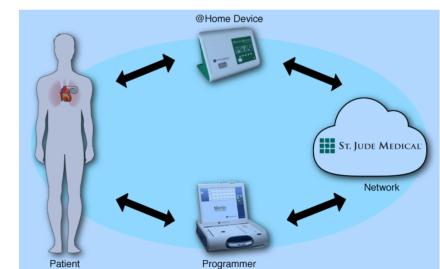
<http://www.muddywatersresearch.com/research/stj/mw-is-short-stj/>

# August 25, 2016 hacker team demonstrations of two types of cyber attacks against implantable cardiac devices



**Sono stati dimostrati due tipi di attacchi:**

- (a) Un attacco per far alterare il corretto funzionamento del device impiantato, incluso una stimolazione errata e fuori controllo.
- (b) Un attacco per scaricare brutalmente la batteria, scenario altrettanto pericoloso per la possibilità di essere eseguito all'insaputa dell'ospitante per prossimità.



<http://www.muddywatersresearch.com/research/stj/mw-is-short-stj/>