

Lessons Learned from Boston Children's: When Hacktivists Attack Your Hospital

Daniel Nigrin, MD, MS
SVP Information Services & CIO
Boston Children's Hospital



Boston Children's Hospital



HARVARD MEDICAL SCHOOL
TEACHING HOSPITAL

I have no relevant financial relationships to disclose



Boston Children's Hospital



HARVARD MEDICAL SCHOOL
TEACHING HOSPITAL

Case Study

What happened?

How did we respond?

What did we learn?

Could it happen again?

Postscript



A Shot Across Our Bow

- March 20, 2014 – notified by external cyber intelligence group about Twitter/Pastebin posting by Anonymous, threatening attack
 - result of highly publicized child custody case
 - Anonymous: loose and decentralized group of “hacktivist” individuals
- “d0x” of staff and presiding judge posted
- “Details” of BCH external web site posted





Was This the Real “Anonymous”?

- Not hard to get details they posted
- Not hard to post a video on YouTube
- Should we just discount it then?

NO!!

- Convened Hospital’s Incident Response Team, began forming contingency plans
 - Especially focused on potential need to “go dark”, cutting ourselves off from Internet if necessary
- Message to entire organization emphasizing vigilance, email security best practices
- Contacted authorities

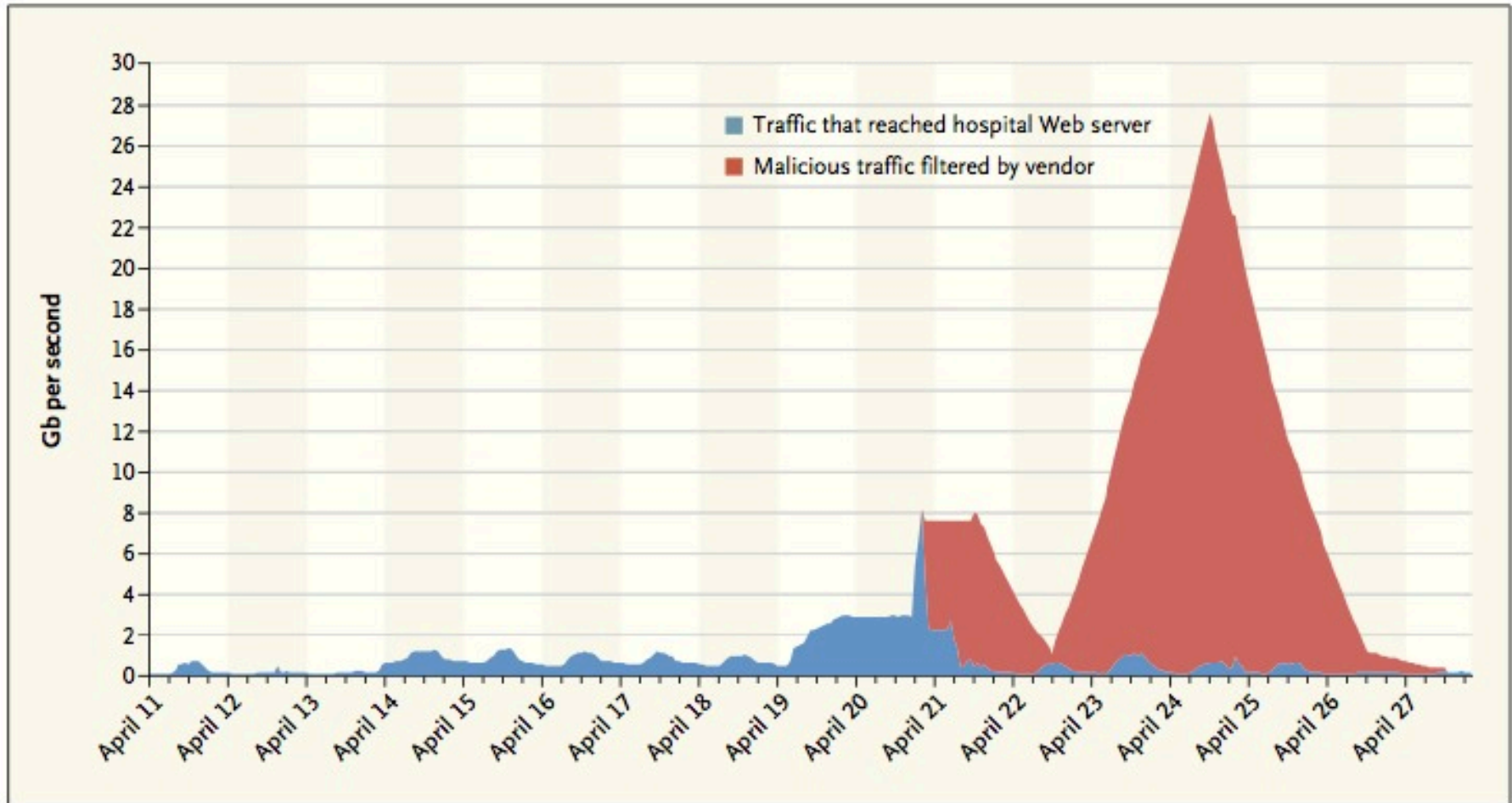


It Begins

- About 3 weeks later... low volume DDoS attack starts
- Mitigated by network changes
- Cat and mouse – we address attack, they change tactic/increase volume
- 1 week later, Easter/Patriot' Day weekend (Boston Marathon bombing 1 year anniversary)
 - Massive uptick in DDoS volume
 - Engaged 3rd party vendor to assist in filtering traffic



Internet Traffic During DDoS Attack



Nigrin, NEJM, July 31, 2014



Boston Children's Hospital



HARVARD MEDICAL SCHOOL
TEACHING HOSPITAL



[@MassMedical](#) No help to #FreeJustina means no website for you!
uptimestatistics.com/en/quicktest.p...
 We are #Anonymous. We give 0 fux.

Expand

Reply Retweet Favorite More



Retweeted by Anon Mercurial



Bennett Cláitor @THECIRCLEC · Apr 20

"This is not a political case -- it's a human rights case and a shocking example of government abuse of power." > [@HuckabeeShow](#) #FreeJustina

Expand

Reply Retweet Favorite More



Anon Mercurial @AnonMercurial · Apr 20

[@BostonChildrens](#) [@waysideyouthorg](#)
 #Anonymous & #AnonFamily will not let you continue your abhorrent practices.
 #FreeJustina & Expect us.

Expand

Reply Retweet Favorite More



Anon Mercurial @AnonMercurial · Apr 19

[@BostonChildrens](#) website Troubles? We Are #Anonymous #FreeJustinaNOW
 o d0xes of your staff are next. HIPAA breach thereafter. Test us.

Expand

Reply Retweet Favorite More



Retweeted by Anon Mercurial



HARBINGER @H4R81N93R · Apr 8

If saving a child's life makes us terrorists in your eyes then so f***ing be it. We give zero f***s.
 #Anonymous #OpJustina #GlovesOff

Expand

Reply Retweet Favorite More



Not Just DDoS...

- Direct penetration attacks on exposed ports, web sites
 - Proactively took down virtually all externally facing sites: research, philanthropy, patient and provider portals, etc...
- Massive influx of malware laden emails
 - Proactively shut down entire email system for ~24 hrs
 - Re-emphasized to staff to not open suspicious mails/attachments
 - Ensured no malware made it through filters
- Re-contacted authorities – advised no press!



BRUINS WIN IN OVERTIME, 3-2, PUSH RED WINGS TO THE BRINK — C1

The Boston Globe

FRIDAY, APRIL 25, 2014

In the news



Late shift

Friday: Turning rainy at night;
high 58-63, low 41-46

Saturday: Rainy, cooler;
high 47-52, low 39-44

High tide: 8:30 a.m., 9:04 p.m.

Sunrise: 5:48 Sunset: 7:37

Complete report, **B13**

Cyberattack hits Children's Hospital

May be the work
of group opposing
teen's treatment

By Michael B. Farrell
and Patricia Wen
GLOBE STAFF

The infamous computer hacker network known as Anonymous threatened to attack Boston Children's Hospital over the child custody case involving Justina Pelletier last month, just a few weeks before the medical center's website was subjected to numerous cyber-assaults.



The anti-authority members of Anonymous sometimes appear in Guy Fawkes masks.

Anonymous has made its interest in the case clear. Several weeks ago, the group claimed responsibility for an attack on the website of Wayside Youth and Family Support Network, the Framingham residential facility where 15-year old Justina has been living since January under state custody.

After the more recent attack on Children's, some patients and medical personnel could not use their online accounts to check appointments, test results, and other case information after the hospital shut down those Web pages.

The threats from Anonymous are the latest to emerge against

Firefight deal wo raise pa by 18.8

City's 6-year p
put at \$92.4m
is expected ne

By Meghan E. I



Boston Children's Hospital



HARVARD MEDICAL SCHOOL
TEACHING HOSPITAL



Anonymous

@YourAnonNews

Supports digital and AFK activists.
Right behind you. · youranonnews.org

TWEETS

91.2K

FOLLOWING

643

FOLLOWERS

1.24M



+ Follow



Anonymous @YourAnonNews · 8h

To all the "Anons" attacking the CHILDREN'S HOSPITAL in the name of Anonymous: - IT IS A HOSPITAL: STOP IT.

Expand

Reply Retweet Favorite



Boston Children's Hospital



HARVARD MEDICAL SCHOOL
TEACHING HOSPITAL

EXPECT US.

TWEETS

13

FOLLOWING

6

FOLLOWERS

6



Follow

Tweets



Anon Mercurial @AnonMercurial · 22h

@NSTAR_News We advise you to stop helping Boston Children's Hospital if you like your website to work: uptimestatistics.com/en/quicktest.p...



Boston Children's Hospital



HARVARD MEDICAL SCHOOL
TEACHING HOSPITAL

It Ends

- About 1 week after high volume DDoS started, it abruptly declined, to a low trickle
- Only gradually brought externally facing sites back online, after extensive 3rd party (re)penetration testing
- Took a deep breath!



Out of all bad things...
...good things come



Boston Children's Hospital



HARVARD MEDICAL SCHOOL
TEACHING HOSPITAL



The NEW ENGLAND JOURNAL of MEDICINE

I

Perspective
JULY 31, 2014

When 'Hacktivists' Target Your Hospital

Daniel J. Nigrin, M.D.

Earlier this year, Boston Children's Hospital was targeted in a sustained cyberattack purportedly instigated by the hacker group known as Anonymous. With cybersecurity becoming an increasingly im-

mation about the hospital's public-facing website, suggesting that it might become a target.

Several weeks later, the hospital began to experience a low-level "distributed denial of ser-



Boston Children's Hospital



HARVARD MEDICAL SCHOOL
TEACHING HOSPITAL

What Did We Learn

- DDoS countermeasures are critical!
- Know what systems (or features within systems) depend on Internet access, and have contingency plans for those
- Recognize importance of email, and need for alternate forms of communication
- Need to push through security initiatives – no excuses anymore
- Securing teleconference meetings
- Separating signal from noise



And Most Importantly

As an industry, we've got to pay closer attention to these threats, and prioritize our efforts against them, **far more** than we have done in the past



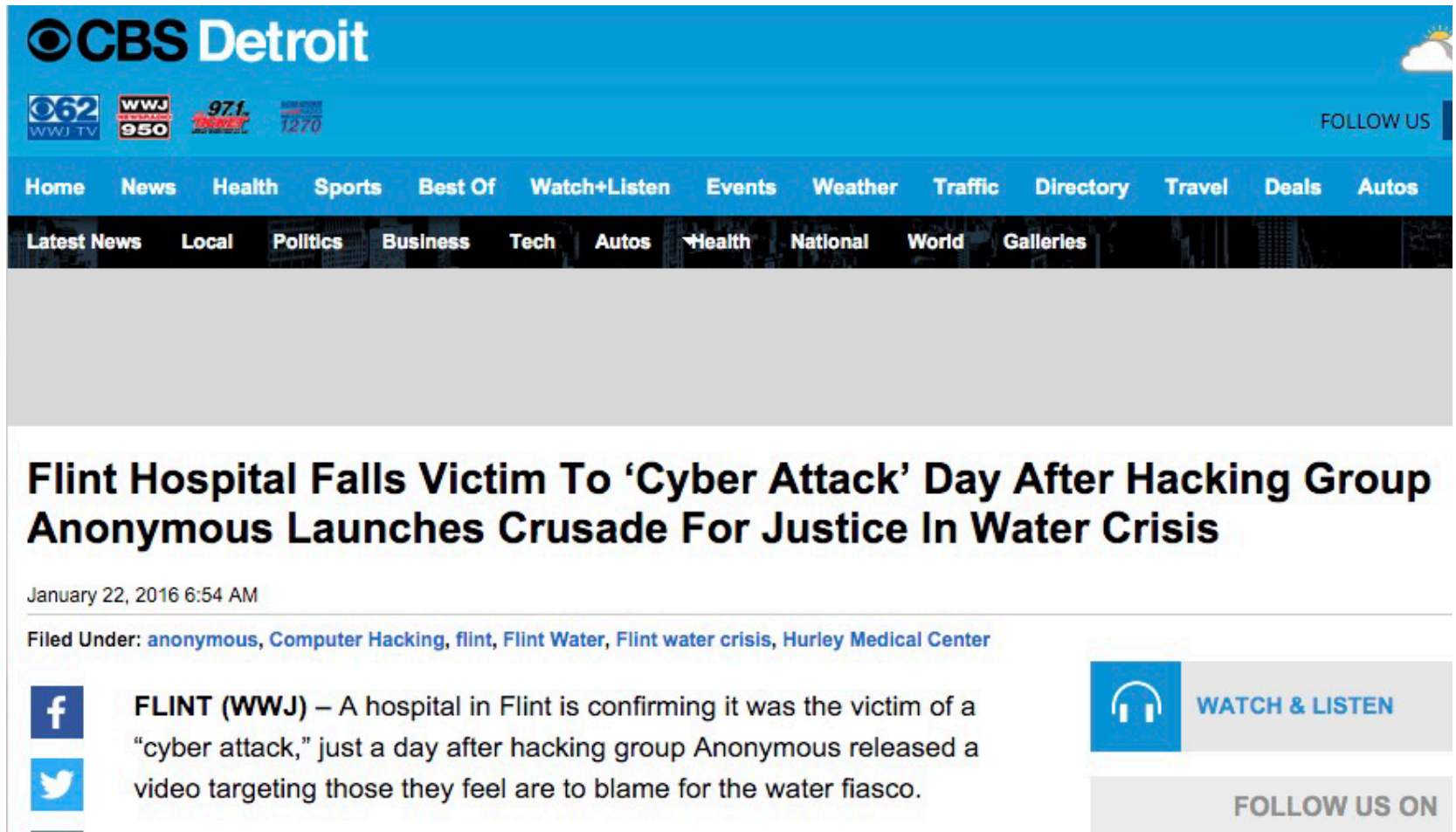
Boston Children's Hospital



HARVARD MEDICAL SCHOOL
TEACHING HOSPITAL

Postscript

Could it happen again?



The image is a screenshot of a news article on the CBS Detroit website. The header is blue with the CBS Detroit logo on the left and a weather icon on the right. Below the header is a navigation bar with various categories like Home, News, Health, Sports, etc. The main content area has a grey background. The article title is in large, bold black text. Below the title is the date and time. Underneath is a line of text indicating where the article is filed. At the bottom left, there are social media icons for Facebook and Twitter. At the bottom right, there are buttons for 'WATCH & LISTEN' and 'FOLLOW US ON'.

CBS Detroit

062 WWJ-TV, WWJ 950, 97.1 WJLW-FM, 1270 WJLB-AM

FOLLOW US


Home News Health Sports Best Of Watch+Listen Events Weather Traffic Directory Travel Deals Autos


Latest News Local Politics Business Tech Autos Health National World Galleries

Flint Hospital Falls Victim To 'Cyber Attack' Day After Hacking Group Anonymous Launches Crusade For Justice In Water Crisis

January 22, 2016 6:54 AM

Filed Under: [anonymous](#), [Computer Hacking](#), [flint](#), [Flint Water](#), [Flint water crisis](#), [Hurley Medical Center](#)

 **FLINT (WWJ)** – A hospital in Flint is confirming it was the victim of a “cyber attack,” just a day after hacking group Anonymous released a video targeting those they feel are to blame for the water fiasco.

 WATCH & LISTEN

FOLLOW US ON

Postscript #2

You can't make this stuff up

Postscript #2

Menu



Metro

SUBSCRIBE NOW



Get unlimited access to Globe.com for only 99¢

Subscribe
Starting at 99 cents

Somerville man accused of cyberattack on hospital picked up off Cuban coast



0

By **Steve Annear** | GLOBE STAFF FEBRUARY 17, 2016

A Somerville man who allegedly launched a cyberattack on a local hospital's website under the name of the hacker network Anonymous was picked up off the coast of Cuba this week when his boat experienced trouble on the open seas, federal prosecutors said.

Martin Gottesfeld, 31, was arrested by federal officials after he came ashore in

Top 10 Trending Article

Most Viewed

Most Commented

Officials search Boston Harbor for Harvard man

A father's worry, as his son goes

At UVM, substance-free dorm co-ordinator, personal trainer, nutrition coach

Donald Trump makes himself go viral with help from Jeb and W

Baby boomer retirements may slow economic growth

Boston Globe, February 17, 2016

ANONYMOUS HACKER INDICTED AS HUNGER STRIKE CONTINUES

BY ANTHONY CUTHBERTSON ON 10/21/16 AT 12:42 PM



TECH & SCIENCE

ANONYMOUS

A member of Anonymous has been indicted on hacking charges whilst on the third week of a prison hunger strike protesting perceived institutionalized torture and political prosecutions.

Martin Gottesfeld, 32, was charged this week in relation to the hacking of Boston Children's Hospital in 2014 following the alleged mistreatment of one of its patients. Gottesfeld has previously admitted to targeting the

Postscript #3

Newsweek.com, October 21, 2016

The Hacker Who Cared Too Much

When a programmer shut down a hospital website to defend a sick girl, he raised a crucial question: What are the bounds of protest in the digital age?



If convicted, Martin Gottesfeld could face up to 15 years in prison and \$500,000 in fines. Madeleine Hébert/Flickr

By David Kushner
June 29, 2017



One afternoon in a modest, hilltop home in West Hartford, Connecticut,

June, 2017

Postscript #5

VoteMartyG

Vote for the real Massachusetts native

MENU

 **MARTY**
GOTTESFELD
FOR SENATE **2018**

Home

"I'm campaigning from behind Harvard's bars"

Greetings from the Plymouth County Correctional Facility,

My name is Marty Gottesfeld and I'm proud to announce my candidacy for the U.S. Senate as a Republican in the 2018 race in Massachusetts. I believe in defending our freedom, our families, our Constitution and human rights.

February, 2018



Gottesfeld pictured in 2010. (Facebook)