



The Internet of Everything: Fridgebots, Smart Sneakers & Data Protection

Jeff Greene

Senior Policy Counsel

Which of These Have Been Part of a Malicious Intrusion?



A



B



C

'London's creepiest startup' forced to pull 'spy' trash cans that could track London pedestrians via smartphones

NP

RAPHAEL SATTER, ASSOCIATED PRESS | 13/08/12 2:29 PM ET

[More from Associated Press](#)



A youth uses a trash bin in central London, Monday, Aug. 12, 2013. Officials say that an advertising firm must immediately stop using its network of high-tech trash cans, like this one, to track people walking through London's financial district

AP Photo / Lefteris Pitarakis

antec.

Glitches allow hackers to watch you through your 'smart' TV

Posted on: 6:33 am, August 3, 2013, by Matt Knight, *updated on: 06:34am, August 3, 2013*

[f Recommend](#) 169 [f](#) 169 [p](#) Pinterest 1 [+](#) Share 177 [t](#) Twitter 7 [e](#) Email

LAS VEGAS (CNNMoney) – Today's high-end televisions are almost all equipped with "smart" PC-like features, including Internet connectivity, apps, microphones and cameras. But a recently discovered security hole in some Samsung Smart TVs shows that many of those bells and whistles aren't ready for prime time.



TECH | 8/13/2013 @ 6:35PM | 36,917 views

How A Creep Hacked A Baby Monitor To Say Lewd Things To A 2-Year-Old

+ Comment Now + Follow Comments

Before I hacked a stranger's smart home, I asked [for permission](#). An anonymous creep who hacked a Texas family's baby monitor was not as polite. ABC News [reports](#) that a Houston couple heard an unfamiliar voice talking to their sleeping 2-year-old daughter on Saturday night and realized that a stranger had taken control of their camera-enabled monitor. And he wasn't a very nice stranger:



This looks like a Foscam baby monitor (via ABC News)

66 M. Gilman, "How A Creep Hacked A Baby Monitor To Say Lewd Things To A 2-Year-Old", 8/13/2013

Marketer of Internet-Connected Home Security Video Cameras Settles FTC Charges It Failed to Protect Consumers' Privacy

Hundreds of Camera Feeds for Home Security, Baby Monitoring Were Hacked, Posted Online

FOR RELEASE

September 4, 2013

TAGS: Technology | Bureau of Consumer Protection | Consumer Protection | Privacy and Security | Consumer Privacy | Data Security

A company that markets video cameras designed to allow consumers to monitor their homes remotely has settled Federal Trade Commission charges that its lax security practices exposed the private lives of hundreds of consumers to public viewing on the Internet. This is the agency's first action against a marketer of an everyday product with interconnectivity to the Internet and other mobile devices – commonly referred to as the "The Internet of Things"

The FTC's complaint alleges that TRENDnet marketed its SecurView cameras for purposes ranging from security to baby monitoring, and claimed in numerous product descriptions that they were "secure." The cameras had faulty software that left them open to online viewing, and in some instances listening to the cameras' Internet address.

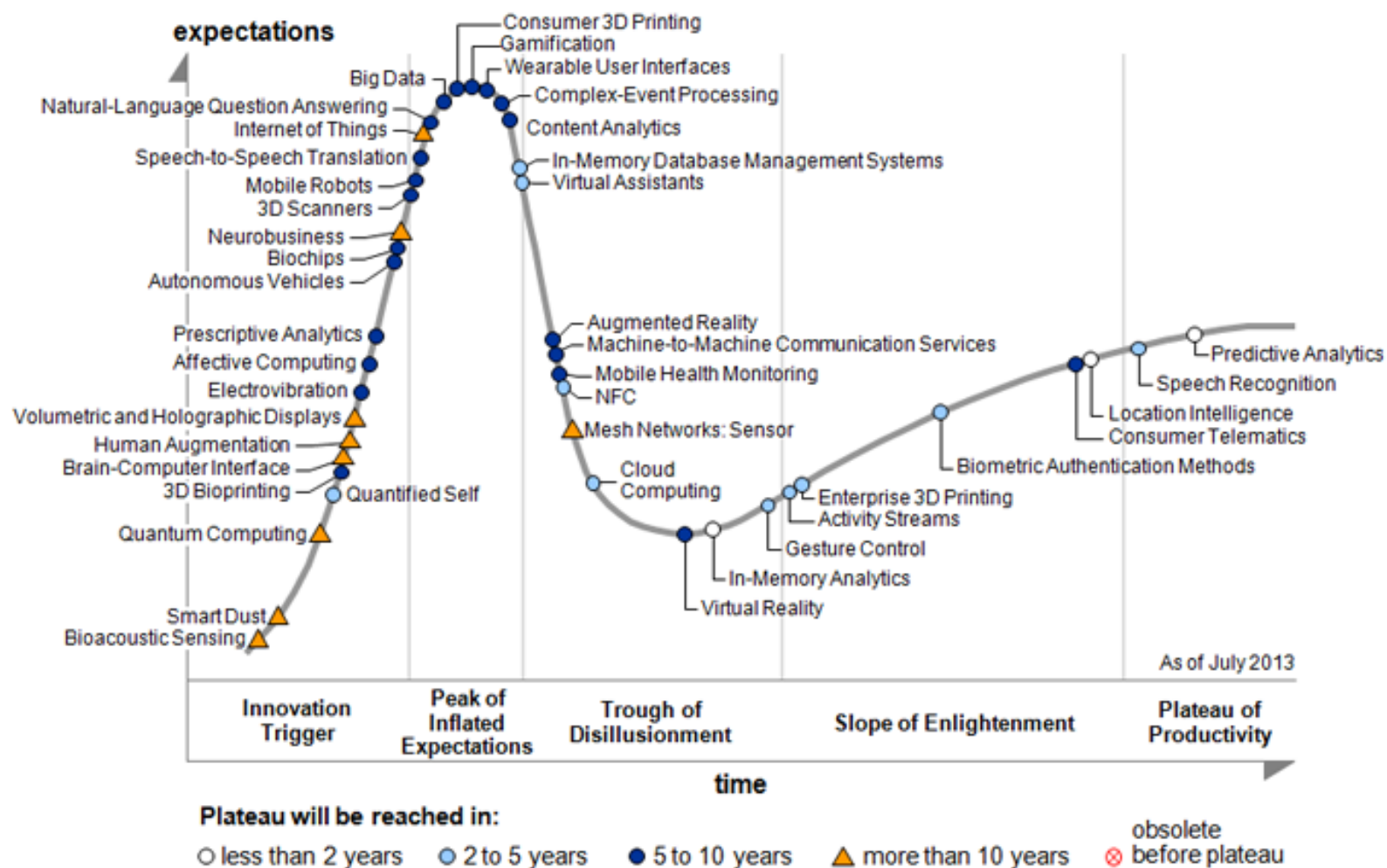
"The Internet of Things holds great promise for innovative consumer products and services. But privacy and security must remain a priority as companies develop more devices that connect to the Internet," FTC Chairwoman Edith Ramirez.



So what is the internet of things?

That's a really good question . . .

Gartner's 2013 Hype Cycle for Emerging Technologies



“

Trying to determine the market size of the Internet of Things is like trying to calculate the market for plastics, circa 1940. At that time, it was difficult to imagine that plastics could be in everything. If you look at information processing in the same way, you begin to see the vast range of objects into which logic, processors, or actuators could be embedded.

”

*Michael Nelson,
Bloomberg Government &
Georgetown University*

Home video games



Pong: 1975



Atari Video Game: 1977



Nintedo 64: 1996



PS2: 2000



PS4: 2013

Cameras



First commercial camera: 1839



Polaroid instant photo camera: 1948



First digital camera: 1988



iPhone: 2007

Music players



Musical clock: 1601



Music box: 1815



Phonograph: 1877



Cassette: 1964



CD: 1982



iPod: 2001



February 29th, 2009



This was my iPod until a few days ago. I was one of the first people with an iPod. I am normally *not* that trendsetting; my husband had heard about it at his high-tech workplace and got me one.

I remember, I kid you not, riding on Metro and people asking me what it was. Then Oprah featured it on her 'Favorite Things'... and Poof! Magic! You gotta love Oprah...

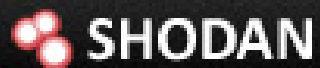
The same week Oprah declared the iPod one of her favorite things – 2 different people actually

stopped me on the street to confirm that what I had was 'the iPod that was on Oprah'.

That was many years ago and believe it or not, my iPod worked until about a month ago.

My husband got one a few years ago that was super-snazzy compared to mine, and much sleeker.





EXPOSE ONLINE DEVICES.

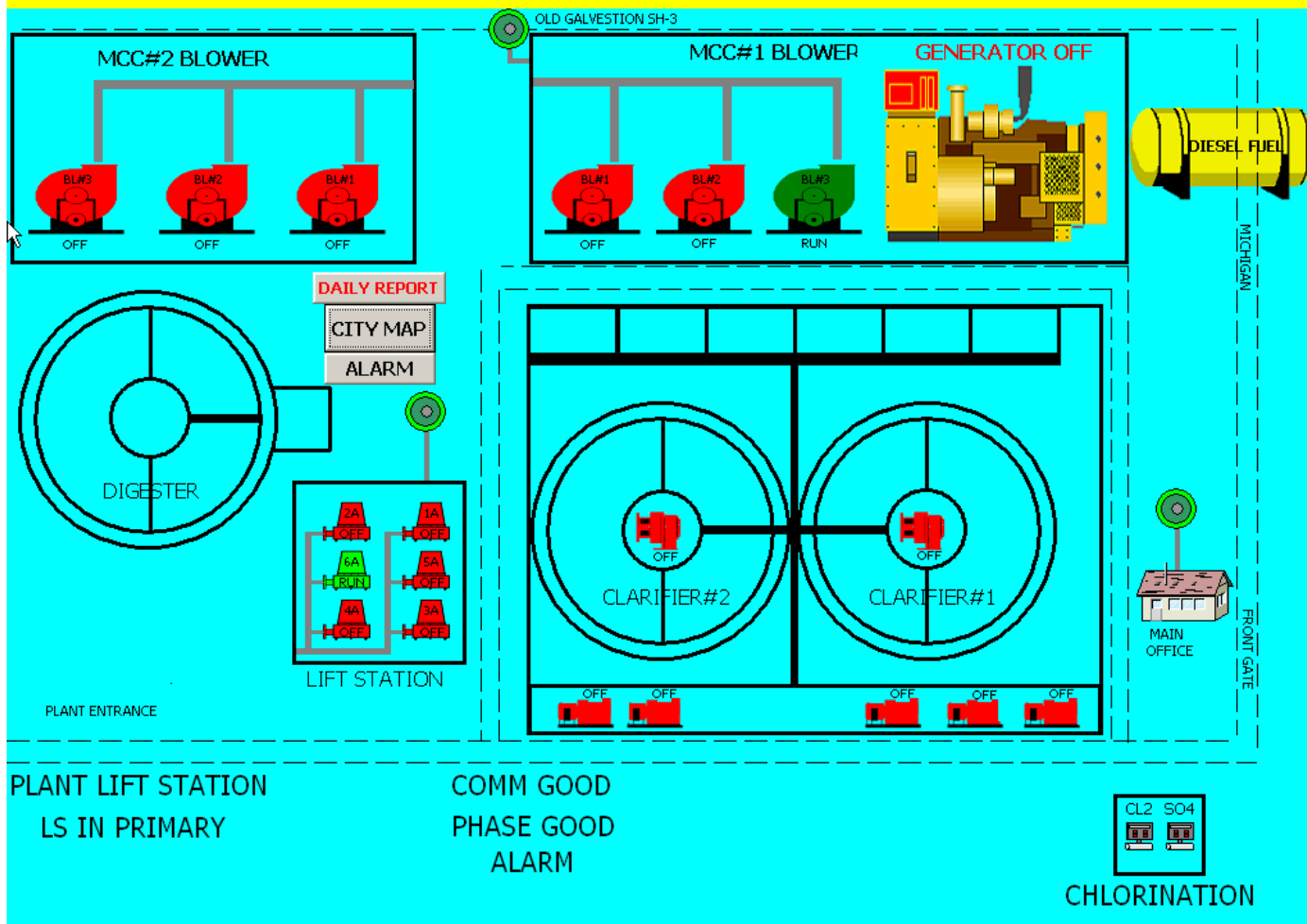
WEBCAMS. ROUTERS.

POWER PLANTS. IPHONES. WIND TURBINES.

REFRIGERATORS. VOIP PHONES.



CITY OF SOUTH HOUSTON WASTE WATER TREATMENT PLANT



“

This was barely a hack. A child who knows how the HMI that comes with Simatic works could have accomplished this. I'm sorry this ain't a tale of advanced persistent threats and stuff, but frankly most compromises I've seen have been have been a result of gross stupidity, not incredible technical skill on the part of the attacker. Sorry to disappoint."

”

***“Pr0f” in an e-mail
interview with
Threat Post.***

“

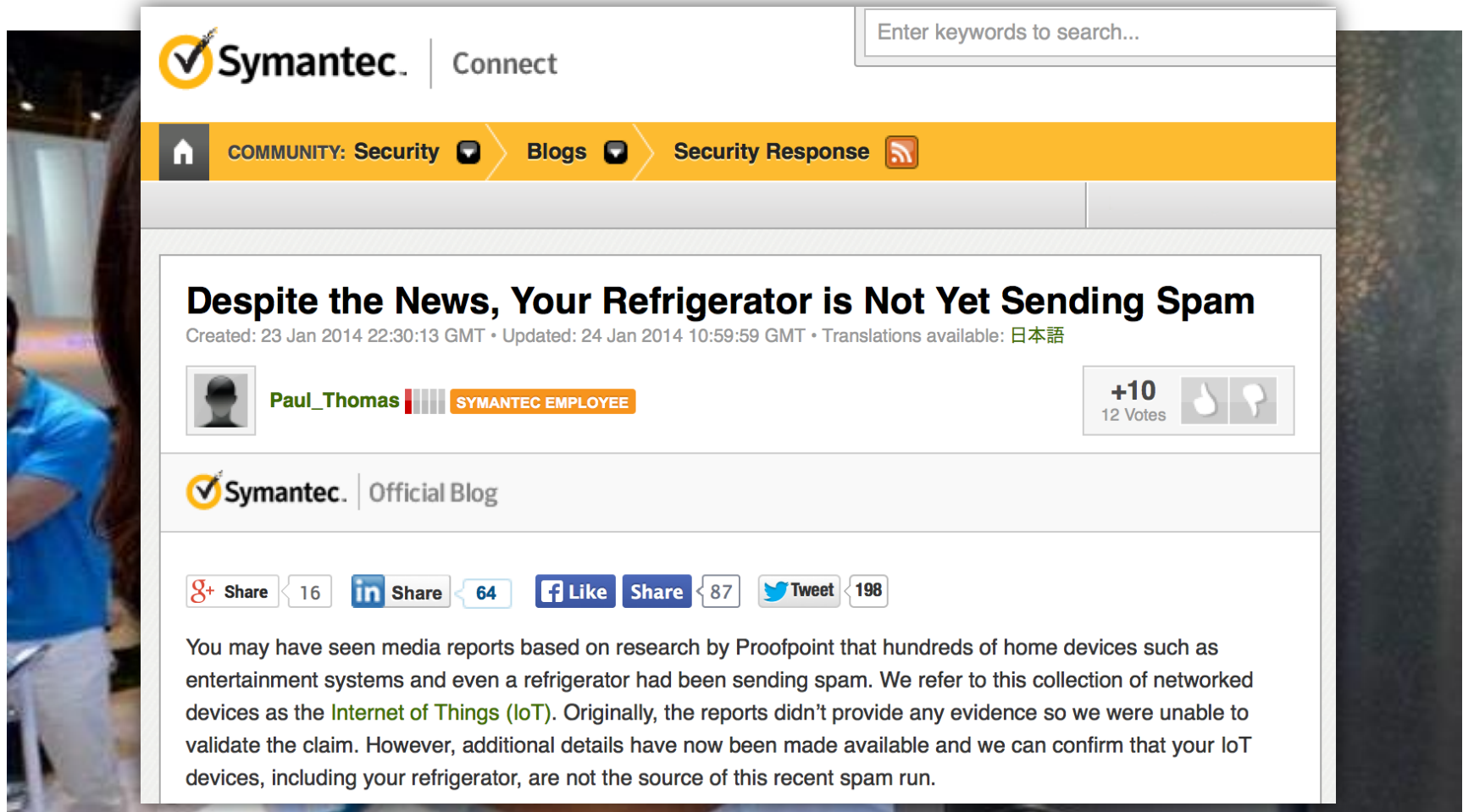
We're probably not the only one who is wide open. He caught everyone with our pants down.

”

***South Houston Mayor
Joe Soto***

Could your fridge send you spam?

Security researchers report 'internet of things' botnet



The screenshot shows a Symantec blog post. At the top is the Symantec logo and a search bar. Below is a navigation bar with links for 'COMMUNITY: Security', 'Blogs', and 'Security Response'. The main heading of the post is 'Despite the News, Your Refrigerator is Not Yet Sending Spam'. Below the heading is the creation and update information: 'Created: 23 Jan 2014 22:30:13 GMT • Updated: 24 Jan 2014 10:59:59 GMT • Translations available: 日本語'. The author is 'Paul_Thomas', a Symantec employee, with a profile picture and a 'SYMANTEC EMPLOYEE' badge. To the right of the author's name is a voting section showing '+10' and '12 Votes' with thumbs up and down icons. Below the author information is the Symantec 'Official Blog' logo. Further down are social sharing buttons for Google+, LinkedIn, Facebook, and Twitter, each with a share count. The main body of the post contains a paragraph explaining that while media reports claim IoT devices like refrigerators can send spam, Symantec can confirm that IoT devices are not the source of the recent spam run.

Despite the News, Your Refrigerator is Not Yet Sending Spam

Created: 23 Jan 2014 22:30:13 GMT • Updated: 24 Jan 2014 10:59:59 GMT • Translations available: 日本語

Paul_Thomas SYMANTEC EMPLOYEE

+10
12 Votes

Symantec Official Blog

Google+ Share 16 LinkedIn Share 64 Facebook Like Share 87 Tweet 198

You may have seen media reports based on research by Proofpoint that hundreds of home devices such as entertainment systems and even a refrigerator had been sending spam. We refer to this collection of networked devices as the **Internet of Things (IoT)**. Originally, the reports didn't provide any evidence so we were unable to validate the claim. However, additional details have now been made available and we can confirm that your IoT devices, including your refrigerator, are not the source of this recent spam run.

Source: <http://www.independent.co.uk/life-style/gadgets-and-tech/news/could-your-fridge-send-you-spam-security-researchers-report-internet-of-things-botnet-9072033.html>

So while IoT devices weren't to blame this time, we expect they probably will be to blame in the future.

“What is particularly worrisome about these kinds of threat is that, in many instances, the end user may have no idea that their device is running an operating system that could be attacked. The software is, by and large, hidden away on the device. Another potential issue is that some vendors don't supply updates, either because of hardware limitations or outdated technology, such as an inability to run newer versions of the software ”

Source: http://www.wired.com/beyond_the_beyond/2014/01/spime-watch-linux-darllaz-internet-things-worm/

WIRED

- “Should it be connected” – *NOT* “can it be connected.”
- Security in the IoT is a necessity and enabler, not a burden or a tax.
- Assume people will do wrong – think about how something could be used, not how you want it to be used.
- Consider security when you buy.



Thank you

Jeff Greene

jeff_green@symantec.com