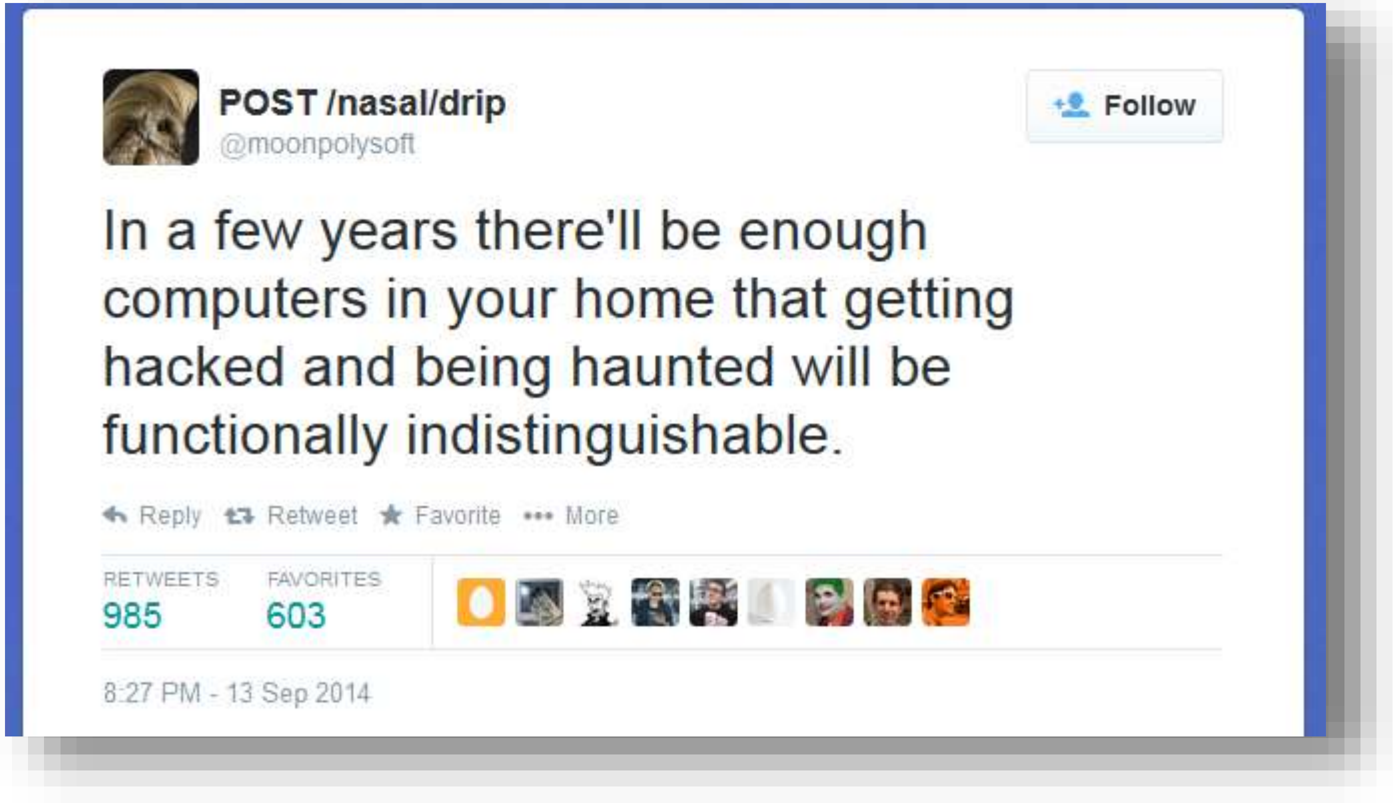
SECURITY IN THE AGE OF INTERNET OF THINGS

Janne Järvinen, Director External R&D Collaboration

2015-09-22

F-Secure



POST /nasal/drip
@moonpolysoft

In a few years there'll be enough computers in your home that getting hacked and being haunted will be functionally indistinguishable.

8:27 PM - 13 Sep 2014

TRENDS

CLOUDIFICATION

CONNECTED DEVICES

ADVANCED THREATS

INTERNET OF THINGS

NEEDS

- Protecting people and data
- Safeguarding all devices
- Incident prevention, detection and remediation
- Overall management of security risks

CUSTOMERS

CONSUMERS

CORPORATIONS

LARGE ENTERPRISES

More services included

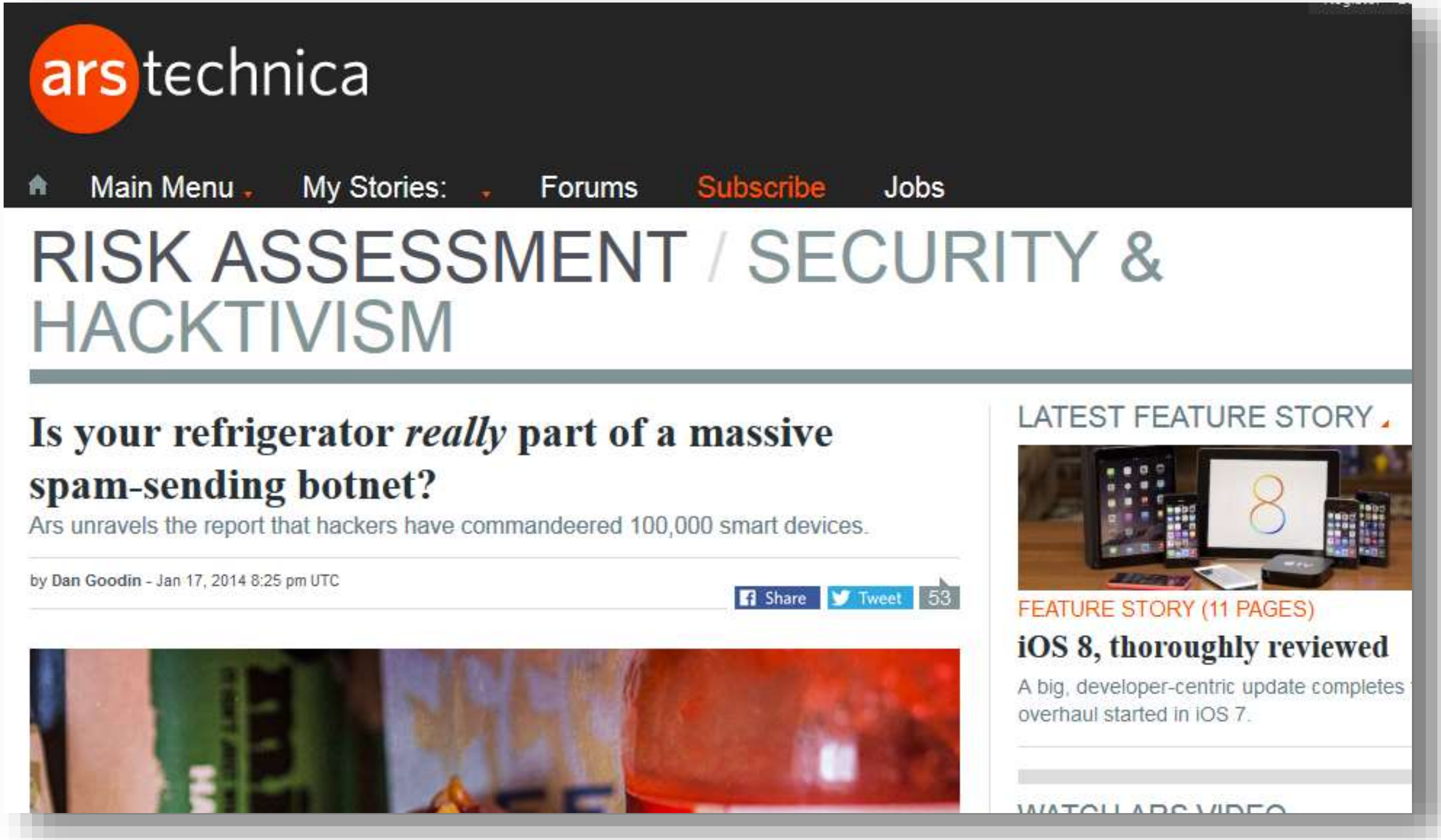
CHANNELS

WE WORK WITH
200+ OPERATORS
6,000+ RESELLERS
IN 40+ COUNTRIES

- OPERATORS
- SERVICE PARTNERS, RETAILERS AND IT RESELLERS
- DIRECT SALES

SECURITY FROM THE CLOUD

F-Secure



RISK ASSESSMENT / SECURITY & HACKTIVISM

Is your refrigerator *really* part of a massive spam-sending botnet?

Ars unravels the report that hackers have commandeered 100,000 smart devices.

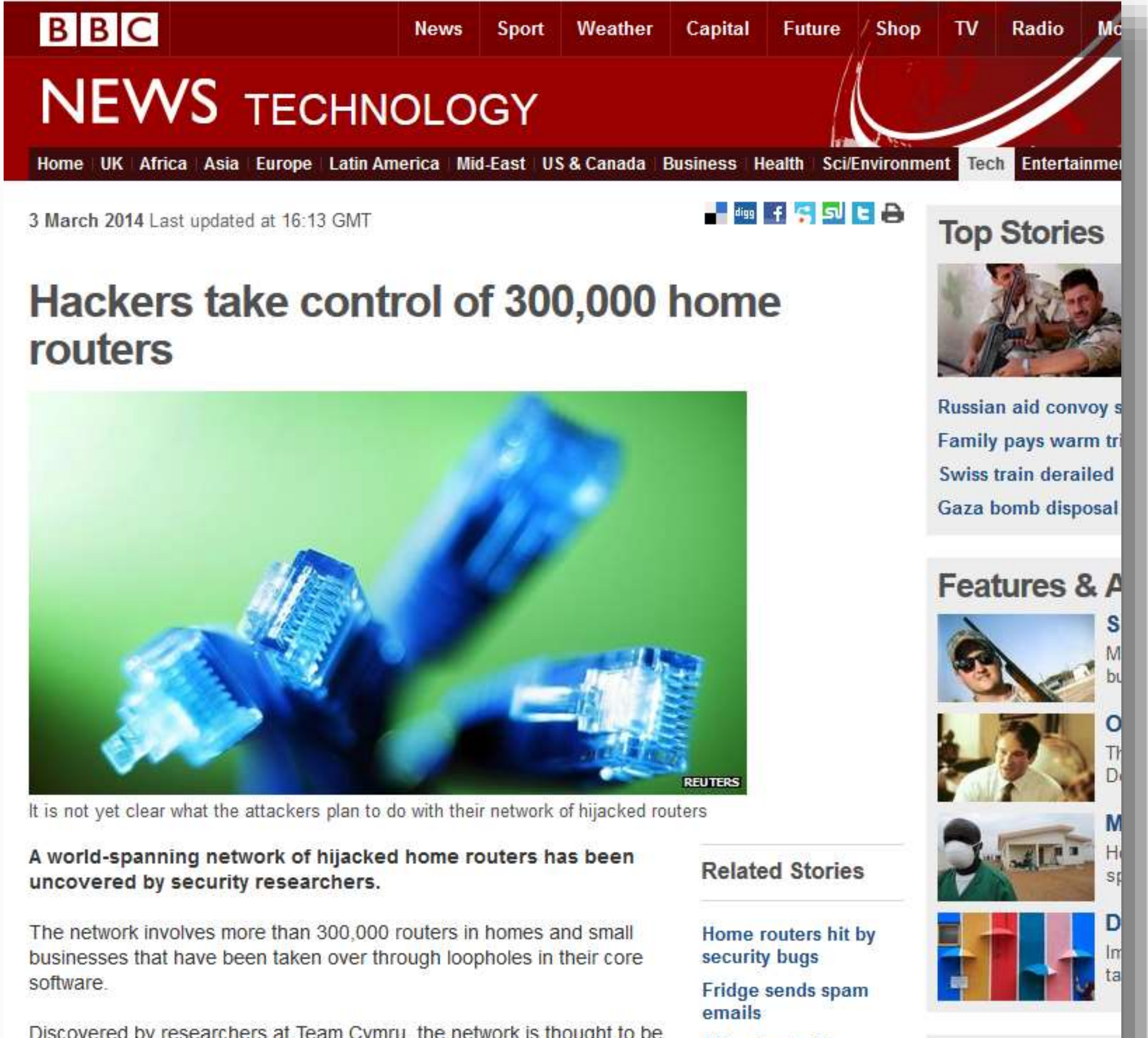
by Dan Goodin - Jan 17, 2014 8:25 pm UTC

LATEST FEATURE STORY

FEATURE STORY (11 PAGES)

iOS 8, thoroughly reviewed

A big, developer-centric update completes overhaul started in iOS 7.



3 March 2014 Last updated at 16:13 GMT

Hackers take control of 300,000 home routers

It is not yet clear what the attackers plan to do with their network of hijacked routers

A world-spanning network of hijacked home routers has been uncovered by security researchers.

The network involves more than 300,000 routers in homes and small businesses that have been taken over through loopholes in their core software.

Discovered by researchers at Team Cymru, the network is thought to be

Related Stories

Home routers hit by security bugs

Fridge sends spam emails

Top Stories

Russian aid convoy s

Family pays warm tri

Swiss train derailed

Gaza bomb disposal

Features & A

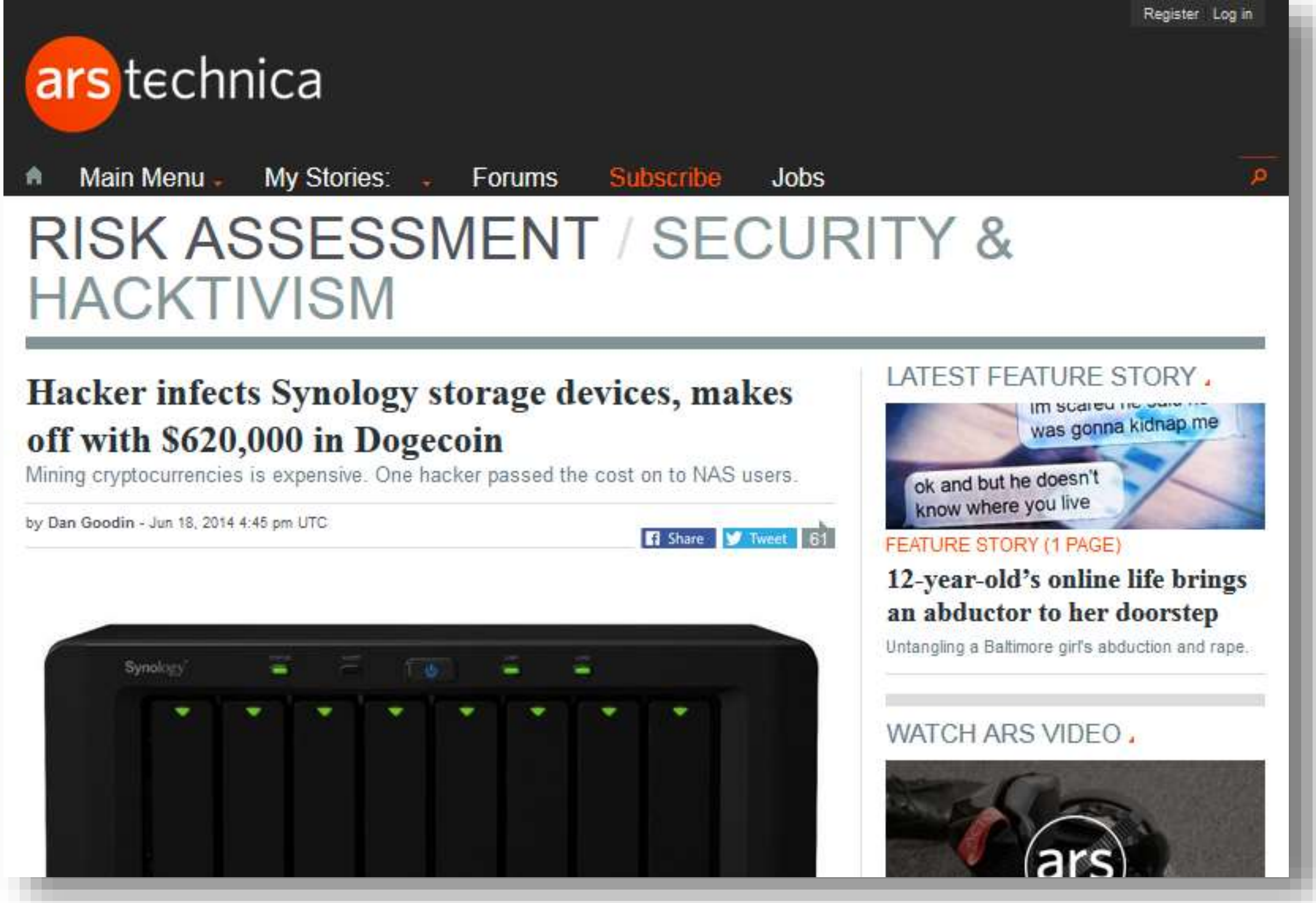
S
M
bu

O
Th
D

M
H
sp

D
Im
ta

F-Secure.



RISK ASSESSMENT / SECURITY & HACKTIVISM

Hacker infects Synology storage devices, makes off with $620,000 in Dogecoin

Mining cryptocurrencies is expensive. One hacker passed the cost on to NAS users.

by Dan Goodin - Jun 18, 2014 4:45 pm UTC

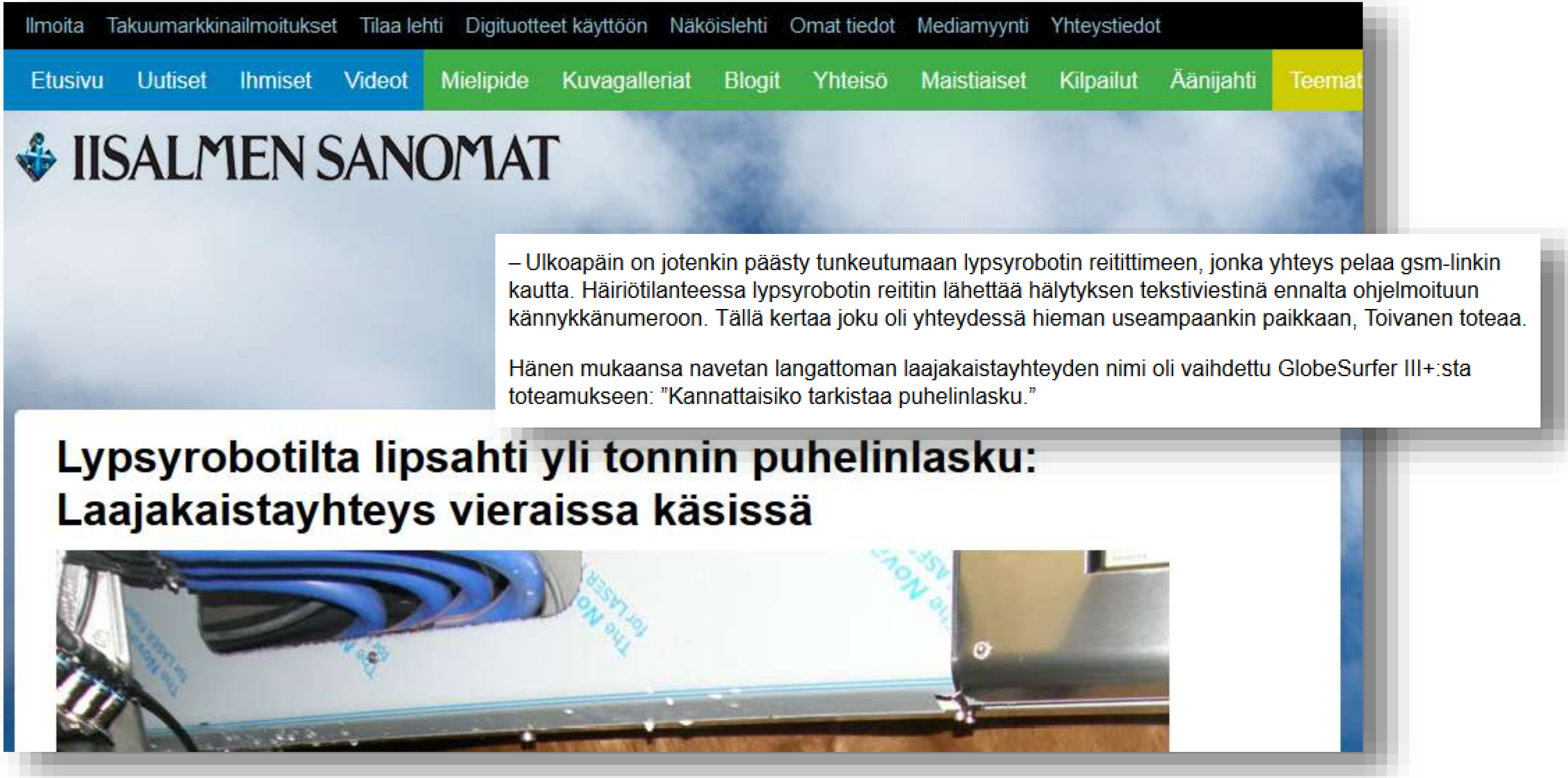
LATEST FEATURE STORY

FEATURE STORY (1 PAGE)

12-year-old's online life brings an abductor to her doorstep

Untangling a Baltimore girl's abduction and rape.

WATCH ARS VIDEO



– Ulkoapäin on jotenkin päästy tunkeutumaan lypsyrobotin reitittimeen, jonka yhteys pelaa gsm-linkin kautta. Häiriötilanteessa lypsyrobotin reititin lähettää hälytyksen tekstiviestinä ennalta ohjelmoituun kännykkänumeroon. Tällä kertaa joku oli yhteydessä hieman useampaankin paikkaan, Toivanen toteaa.

Hänen mukaansa navetan langattoman laajakaistayhteyden nimi oli vaihdettu GlobeSurfer III+:sta toteamukseen: "Kannattaisiko tarkistaa puhelinlasku."

Lypsyrobotilta lipsahti yli tonnin puhelinlasku: Laajakaistayhteys vieraissa käsissä

http://www.iisalmensanomat.fi/news/lypsyrobotilta-lipsahti-yli-tonnin-puhelinlasku-laajakaistayhteys-vieraissa-ksiss/

IoT risks

- Not secure by design
  - Focus is on easy deployability and UX – sort of opposite to security
- Typically not updated automatically
  - Manual updating may not be available to normal consumers either
  - Vulnerability in open source software (hearbleed, shellshock, etc) often affect IoT devices as well and don’t always require device-specific exploit code.
- Detection and remediation difficult or impossible
  - Consumers have no way of detecting their NAS box or Smart TV has malware on it
  - Even if a consumer suspects malware, how can they get rid of it? (even factory reset doesn’t always do the trick)

Example hack: Samsung Smart TV

- Samsung Smart TV is a pretty standard Linux machine
- Remote control devices (smart phone, tablet) etc. authenticated by MAC only – also, if you use NULL as MAC in the request, the weak authentication is bypassed completely.
- Remote control app can change the device into developer mode
- In developer mode the TV will allow running (root) applications from any selected web server

➔ Full compromise very simple without any overflows or such

Jeong Wook Oh, HP, VB2014

Jeep

Why hack a toaster?

- Making money
  - Spamming, DDoS, bitcoin mining, clickfraud
- Infrastructure and access
  - Bridgehead to other attacks, hosting malware, etc.
- Blackmail
  - *"If you don't pay up, I will burn down your house with the toaster"*
- Spying / voyerism
  - Many IoT devices has webcams – especially security cameras and nannycams but also things like Xbox Kinect and high end smart TVs
- Hiding your tracks
  - Criminals want to hide their tracks by proxying through hacked devices ("using neighbors Wifi")

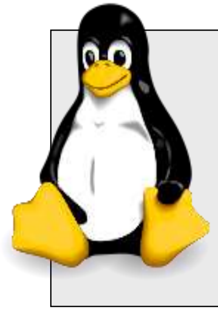
Differences between "any IoT device" and your PC

No (or very little) stored personal information

- People not expected to do online banking or reading emails on their refrigerator
- Typically nothing of value can be stolen from the device itself

Less CPU power

- And other resources



Linux OS (or no OS at all)

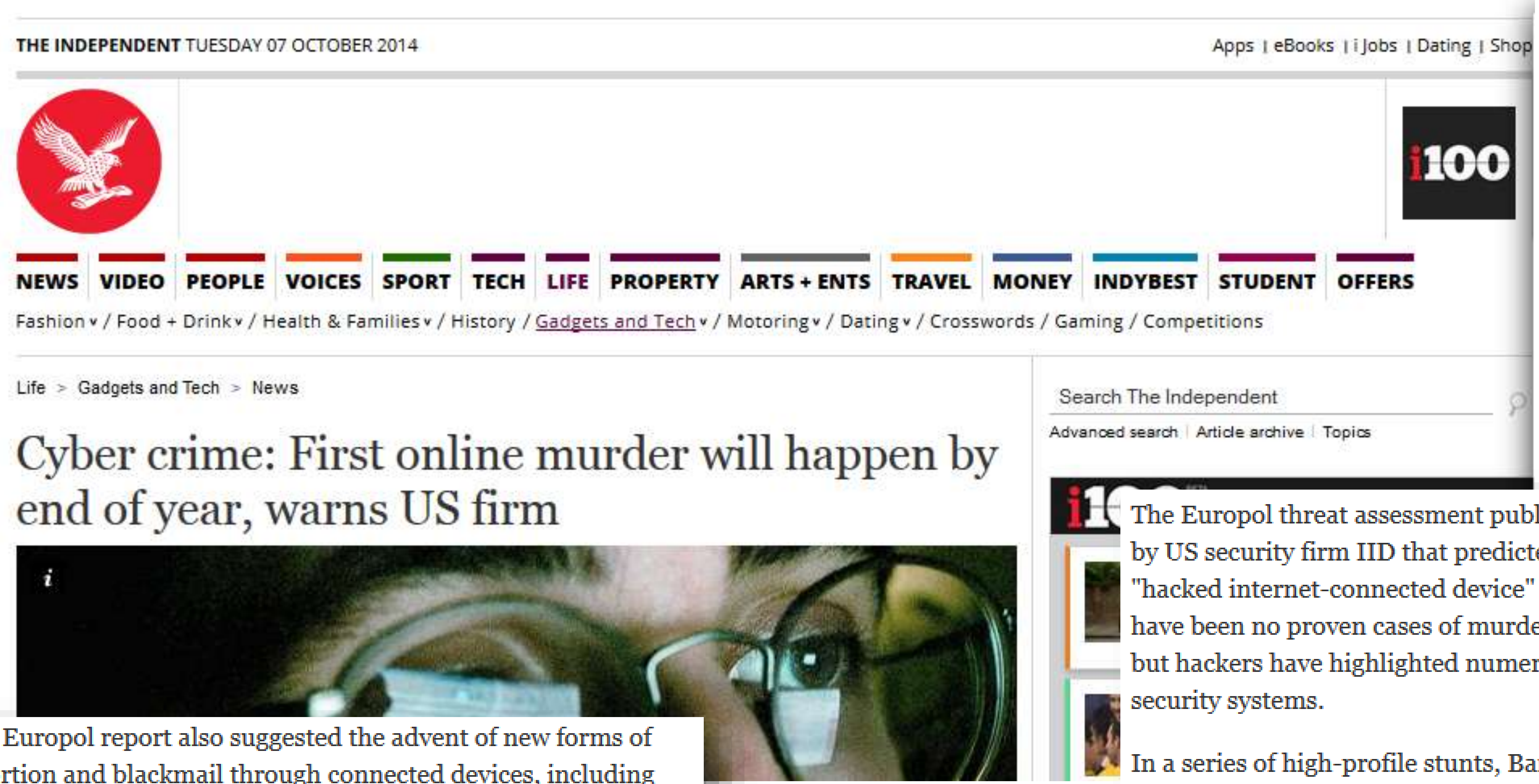
- Stripped down Linux
- Microcontroller-based devices typically have no OS at all

No display or keyboard

- Maybe some buttons and small led display but not a full display

More dramatic threats

- Murders by hacking pacemakers, burglaries by hacking locking systems, blackmail by hacking car control systems, etc.
- These will all happen, and not in too distant future
- However, they won’t be a threat to the average consumer during the next three years
    - They are targeted attacks: Not a problem for the masses but also really difficult to protect from



THE INDEPENDENT TUESDAY 07 OCTOBER 2014

Apps | eBooks | i Jobs | Dating | Shop

NEWS VIDEO PEOPLE VOICES SPORT TECH LIFE PROPERTY ARTS + ENTS TRAVEL MONEY INDYBEST STUDENT OFFERS

Fashion / Food + Drink / Health & Families / History / Gadgets and Tech / Motoring / Dating / Crosswords / Gaming / Competitions

Life > Gadgets and Tech > News

Search The Independent

Advanced search | Article archive | Topics

Cyber crime: First online murder will happen by end of year, warns US firm

The Europol threat assessment published last week cited a report by US security firm IID that predicted the first murder via "hacked internet-connected device" by the end of 2014. There have been no proven cases of murder by tampering with devices but hackers have highlighted numerous flaws in computer security systems.

In a series of high-profile stunts, Barnaby Jack hacked into cash machines to make them spew money, and exploited a flaw in an insulin pump. He died last year just before he was about to demonstrate how pacemakers could be hacked.

The former US vice-president Dick Cheney – who has a long history of heart problems – revealed last year that the wireless function had been disabled on his implanted defibrillator because of concerns that outsiders could hack the network and provoke a heart attack.

The Europol report also suggested the advent of new forms of extortion and blackmail through connected devices, including locking people out of their smart cars and homes before payment of a ransom. It said that new systems would increasingly rely on facial and speech recognition for security that were open to abuse without up-to-date security in place.

SWITCH ON FREEDOM