Hackers and Media Hype

Big Hacks That Never Really Happened

Presented by:

C.Thomas

"Space Rogue"

Who Am I?

- C. Thomas aka “Space Rogue”

Who Am I?

- Space Rogue
  - Member of L0pht Heavy Industries

Who Am I?

- Space Rogue
  - Creator of the Whacked Mac Archives

Who Am I?

- Space Rogue
  - Testified to US Congress on “Weak Computer Security in Government”

Who Am I?

- Space Rogue
  - Editor in Chief of The Hacker News Network

Who Am I?

- Space Rogue
  - Threat Intelligence Manager @ Trustwave SpiderLabs

Who Am I?

- C. Thomas aka "Space Rogue"
  - Member of L0pht Heavy Industries
  - Creator of the Whacked Mac Archives
  - Testified to US Congress on "Weak Computer Security in Government"
  - Defcon, SOURCE, HOPE – MTV, ABC News, CNN
  - Editor in Chief of The Hacker News Network
  - Threat Intelligence Manager for Trustwave SpiderLabs

cthomas@trustwave.com @spacerog

Hackers and Media Hype

- What is Media Hype
- Cover Several Examples in Depth
- How to Identify HYPE
- How to be part of the REALITY

Hackers and Media Hype

Media *noun* - the means of communication, as radio and television, newspapers, and magazines, that reach or influence people widely

Hype *verb* – 1. to stimulate, excite, or agitate 2. to create interest in by flamboyant or dramatic methods 3. to intensify by ingenious or questionable claims or methods

Hackers and Media Hype

- Example Notes
  - Examples are not presented in any sort of order
  - Older stories harder to research - HYPE easier than REALITY
  - Hype happens daily, these examples are just some of the biggest
  - My apologies in advance to any journalists in the audience
  - Not including hype over theoretical attacks (i.e. printers catching fire, ATM jackpotting, wireless car attacks, etc…

Kevin Mitnick and NORAD

HYPE

New York Times – *July 04, 1994*

"As a teen-ager he used a computer and a modem to break into a North American Air Defense Command computer, foreshadowing the 1983 movie "War Games."[1]

St. Petersburg Times – *February 18, 1995*

'Mitnick, as a teenager in Sepulveda, Calif., infiltrated the North American Air Defense Command computer system."[2]

CNN.com – *March 18, 1999*

"Mitnick first received national attention in 1982 when he hacked into the North American Defense Command (NORAD), a feat that inspired the 1983 film "War Games."[3]

Kevin Mitnick and NORAD

REALITY

Chicago Tribune - February 1, 1996

"Ms. Hafner said she could find no evidence that the NORAD story was anything but myth."[4]

Kevin Mitnick -

"Leon Wheidman made one of the most outrageous statements that have probably ever been uttered by a Federal prosecutor in court: he told magistrate Tassopiulos that I could start a nuclear holocaust. "He can whistle into a telephone and launch a nuclear missile from NORAD," he said."[5]

Satellite Held for Ransom - 1999

HYPE

First reported by the Sunday Business

Reuters

Orlando Sentinel

Hackers Seize Britain's Military Satellite[6]

Fox News

Britian's Military Satellite held by Hackers[7]

Slashdot

Crackers Reportedly take Brit Mil Satellite[8]

Satellite Held for Ransom - 1999

SUNDAY BUSINESS - LONDON Hackers have seized control of one of Britain's military communication satellites and issued blackmail threats, The Sunday Business newspaper reported.

The newspaper, **quoting security sources**, said the intruders **altered the course** of one of Britain's four satellites that are used by defense planners and military forces around the world.

The sources said the satellite's course was changed just over two weeks ago. The hackers then issued a blackmail threat, demanding money to stop interfering with the satellite.

"This is a nightmare scenario," **said one intelligence source**. Military strategists said that if Britain were to come under nuclear attack, an aggressor would first interfere with military communications systems.

"This is not just a case of computer nerds mucking about. This is very, very serious and the blackmail threat has made it even more serious," **one security source said.**

Police said they would not comment as the investigation was at too sensitive a stage. The Ministry of Defense made no comment.

Satellite Held for Ransom - 1999

REALITY

Reuters

British Defense Ministry Dismisses Hacker Report[9]

ZD Net

Our Satellites are Hack Proof[10]

Satellite Held for Ransom - 1999

REALITY

Reuters

British Defense Ministry Dismisses Hacker Report[9]

ZD Net

Our Satellites are Hack Proof[10]

PCMag.com September 26, 2008

"*The 10 Most Mysterious Cyber Crimes"*

#2 Ministry of Defense Satellite Hacked

A small group of hackers traced to southern England gained control of a MoD Skynet military satellite and signaled a security intrusion characterized by officials as "information warfare," in which an enemy attacks by disrupting military communications. In the end, the hackers managed to reprogram the control system before being discovered. Though Scotland Yard's Computer Crimes Unit and the U.S. Air Force worked together to investigate the case, no arrests have been made.[11]

Al Quaeda Uses Steganography

HYPE

USA Today February 5, 2001

Terror groups hide behind Web encryption

"Hidden in the X-rated pictures on several pornographic Web sites...may lie the encrypted blueprints of the next terrorist attack against the United States or its allies."[12]

"You very well could have a photograph and image with the time and information of an attack sitting on your computer, and you would never know it."

Wired February 07, 2001

Bin Laden: Steganography Master?[13]

Crypto-Gram Newsletter September 30, 2001

Terrorists and Steganography[14]

Al Quaeda Uses Steganography

REALITY

Center For Information Technology Integration

August 31, 2001

Niels Provos, Peter Honeyman

Detecting Steganographic Content on the Internet

Downloaded over 2,000,000 images and scanned them for steganography – found nothing[15]

NewScientist September 25, 2001

Massive search reveals no secret codes in web images[16]

Al Quaeda Uses Steganography

HYPE

Zeit Online March 15, 2012

Documents reveal al Qaeda's plans for seizing cruise ships, carnage in Europe

"German investigators discovered encoded inside the actual video a treasure trove of intelligence -- more than 100 al Qaeda documents" [41]

REALITY

?????

CNN does not report until May 1st [42]

Only one named source (a reporter)

Bin Laden was found with porn but no mention of Steganography

Nothing new mentioned (Cruise ship attacks, city wide rampages, etc.)

Brazil Blackout

HYPE

Wired October 28, 2009

"We can look forward to the kind of things happening here that happened to Brazil, where hackers successfully brought down the power," says Richard Clarke[17]

60 Minutes November 8th, 2009

"We know that cyber intruders have probed our electrical grid, and that in other countries cyber attacks have plunged entire cities into darkness," the president said.

"President Obama didn't say which country had been plunged into darkness, but **a half a dozen sources** in the military, intelligence, and private security communities have told us the president was referring to Brazil.[18]

Brazil Blackout

REALITY

Wired November 9, 2009

Brazilian Blackout Traced to Sooty Insulators not Hackers

"Raphael Mandarino Jr., director of the Homeland Security Information and Communication Directorate, told the newspaper Folha de S. Paulo that he's investigated the claims and found no evidence of hacker attacks, adding that Brazil's electric control systems are not directly connected to the internet."[19]

"Brazil's independent systems operator group later confirmed that the failure of a 345-kilovolt line "was provoked by pollution in the chain of insulators due to deposits of soot"[20]

The National Agency for Electric Energy, Brazil's energy regulatory agency, concluded its own investigation in **January 2009** and fined Furnas $3.27 million (US Dollars) for failing to maintain the high-voltage insulators on its transmission towers.[20]

Twitter or: Hackers Shot My Weiner

HYPE

NBC4 New York May 30, 2011

Lewd Photo Sent Over Rep. Weiner's Hacked Twitter Account

"A computer hacker had apparently gained access to Weiner's Facebook and Twitter accounts and posted the picture, a spokesman for Weiner told the Post."[21]

Reuters May 31, 2011

NY Rep. Weiner hires lawyer after alleged Twitter hacking

"Democratic Representative Anthony Weiner has hired an attorney to investigate the hacking of his Twitter account after a lewd photo was sent to one of his followers, his office said on Tuesday.[22]

Huffington Post May 31, 2011

Anthony Weiner Hires Lawyer After Alleged Twitter Hack

"After Congressman Anthony Weiner's Twitter feed was allegedly hacked… Weiner has hired a lawyer."[23]

Twitter or: Hackers Shot My Weiner

REALITY

ABC News June 6, 2011

Rep. Anthony Weiner: 'The Picture Was of Me and I Sent It'

"Rep. Anthony Weiner of New York said… that he publicly lied about a photo of himself sent over Twitter to a college student in Seattle over a week ago."

"I take full responsibility for my actions," Weiner said. "The picture was of me, and I sent it."[24]

Twitter – Not the only Weiner

Halley Williams, the lead singer for the band Paramore blamed hackers after she tweeted a topless picture of herself.[25]

Paul Pierce of the Boston Celtics blamed hackers after a tweet calling for broom showed up in his twitter stream. The broom comment being in reference to possibly sweeping the Orlando Magic.[26]

Jaber Gafney of the Washington Redskins tweeted a series of profane tweet about his wife and other family members. Then later said *"This is the real Jabar and my acct was hacked that wasn't me saying all of that so disreguard whatever u read."*[27]

Satellite Hack 2010

HYPE

BusinessWeek October 27, 2011

Chinese Military Suspected in Hacker Attacks on U.S. Satellites

"Computer hackers, possibly from the Chinese military, **interfered** with two U.S. government satellites four times in 2007 and 2008 through a ground station in Norway, according to a congressional commission."[28]

"**may have** used an Internet connection at the Svalbard Satellite Station in Spitsbergen, Norway"[28]

BusinessWeek referenced a draft report from the "U.S.-China Economic and Security Review Commission." (ummm, who?)

Satellite Hack 2010

REALITY

NASA Watch October 31, 2011

"NASA experienced two suspicious events with the Terra spacecraft in the summer and fall of 2008. There was no manipulation of data, no commands successfully sent to the satellite, and no data captured."[29]

Reuters October 31, 2001

China denies it is behind hacking of U.S. satellites

Beijing on Monday denied a U.S. commission's claim that China may have been responsible for hacking incidents on U.S. environment-monitoring satellites, saying that the committee had "ulterior motives" in writing such a draft report[30]

Illinois Water Utility

HYPE

The Register November 17, 2011

Water utility hackers destroy pump, expert says

"Hackers destroyed a pump used by a US water utility after gaining unauthorized access to the industrial control system it used to operate its machinery, **a computer security expert said.**"[31]

Wired November 18, 2011

H(ackers)$_2$O: Attack on City Water Station Destroys Pump[32]

Krebs on Security November 18, 2011

Cyber Intrusion Blamed for Hardware Failure at Water Utility[33]

"Threat Level was unable to reach anyone at the utility company Thursday night to confirm the breach."

DHS spokesman Peter Boogaard. "At this time there is no credible corroborated data that indicates a risk to critical infrastructure entities or a threat to public safety."

Illinois Water Utility

REALITY

Washington Post November 25th 2011

Water-pump failure in Illinois wasn't cyberattack after all

"A water-pump failure in Illinois was initially mistaken to be the first foreign cyberattack on a public utility in the United States because **a plant contractor traveling in Russia remotely logged in to the plant's computer system**, according to a person familiar with a federal investigation of the incident."[34]

Northwest Railway

HYPE

nextGov.com 2012.01.23

Hackers manipulated railway computers, TSA memo says[37]

"Hackers, possibly from abroad, executed an attack on **a Northwest rail company's** computers that disrupted railway signals for two days in December"[37]

"train service on the unnamed railroad "was slowed for a short while" and rail schedules were delayed about 15 minutes after the **interference**, stated a Transportation Security Administration **summary of a Dec. 20 meeting** about the episode… The following day, shortly before rush hour, a "second event occurred" that did not affect schedules, TSA officials added."[37]

InfoSecurity.com 2012.01.25

Pacific Northwest train signals disrupted by hacker, says TSA[38]

Northwest Railway

REALITY

Wired January 26, 2012

Railroad Association Says Hack Memo Was Inaccurate

"There was no **targeted** computer-based attack on a railroad… The memo on which the story was based has numerous inaccuracies." [40]

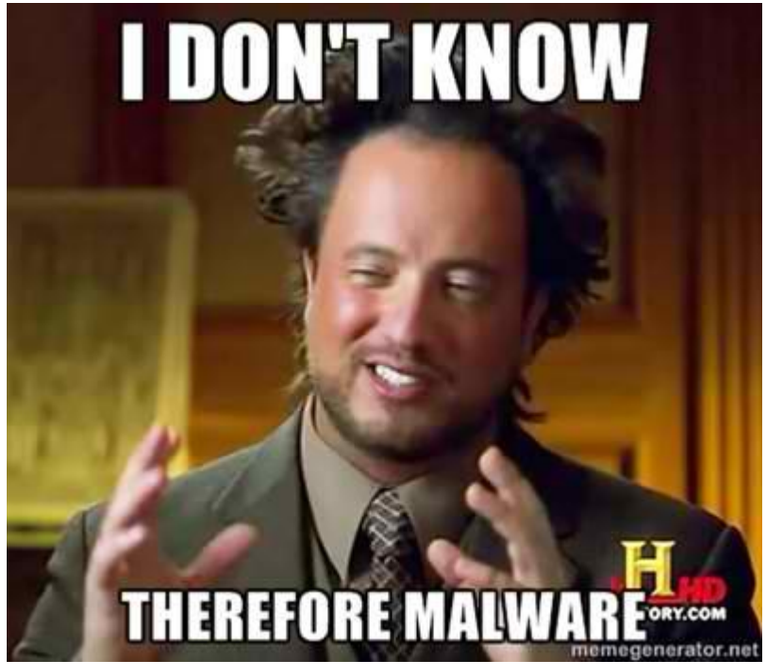
Northwest Railway

REALITY

Wired January 26, 2012

Railroad Association Says Hack Memo Was Inaccurate

"There was no **targeted** computer-based attack on a railroad… The memo on which the story was based has numerous inaccuracies." [40]



US Hacks Al-Qaeda

HYPE

ABC News 2012.05.24

Hillary Clinton: U.S. hacked Yemen al-Qaida sites

"a top U.S. official has explicitly acknowledged that the U.S. government hacked into websites run by al-Qaida's affiliate in Yemen" [43]

Huffington Post 2012.05.24

Yemen Al Qaeda Websites Hacked By U.S. State Department, Clinton Says

"Secretary of State Hillary Rodham Clinton says cyber experts based at the State Department hacked Yemeni tribal websites" [44]

Northwest Railway

REALITY

Hillary Clinton 2012.05.23

Remarks at the Special Operations Command Gala Dinner

"For example, a couple of weeks ago, al-Qaida's affiliate in Yemen began an advertising campaign on key tribal web sites bragging about killing Americans and trying to recruit new supporters. Within 48 hours, our team *plastered the same sites with altered versions of the ads* that showed the toll al-Qaida attacks have taken on the Yemeni people." [45]

Washington Post 2012.05.23

"A previous version incorrectly said that cyber experts had hacked into al-Qaeda sites … they did not engage in "hacking," [46]

More Recent Examples

Ars Technica 2011.01.17
Israeli and Palestinian hackers trade DDoS attacks in rising cyber-gang war[35]

Gizmodo 2012.01.22
Anonymous Just Deleted CBS.com and Took Down Universal[36]

I Don't Know…Therefore Malware
Air Raid Sirens in IL – hacked?

San Diego Fireworks – virus?

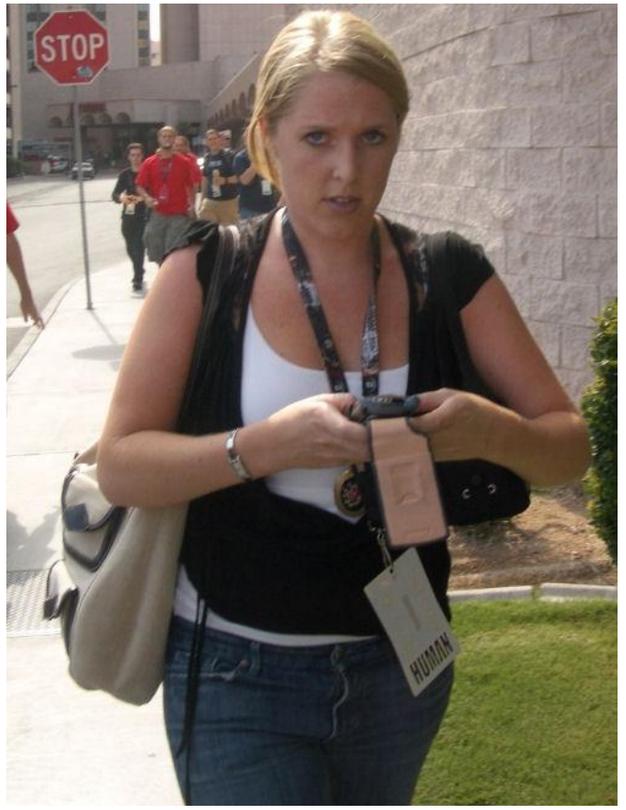
The Michelle Madigan Affair

- Associate Producer for NBC Universal
  - Dateline NBC

"Madigan was reportedly working on a piece aimed at showing middle America the *criminal hacker underground*. Madigan was noted as saying, "People in Kansas would be very interested in what is going on at Defcon." [37]

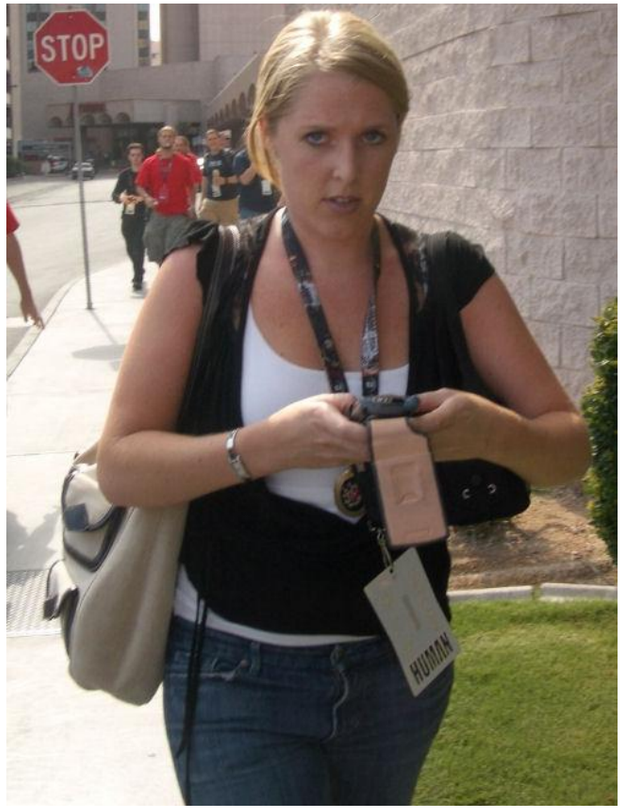
The Michelle Madigan Affair

- Associate Producer for NBC Universal
  - Dateline NBC
- Attended Defcon 15 in 2007
  - Did not get press credentials



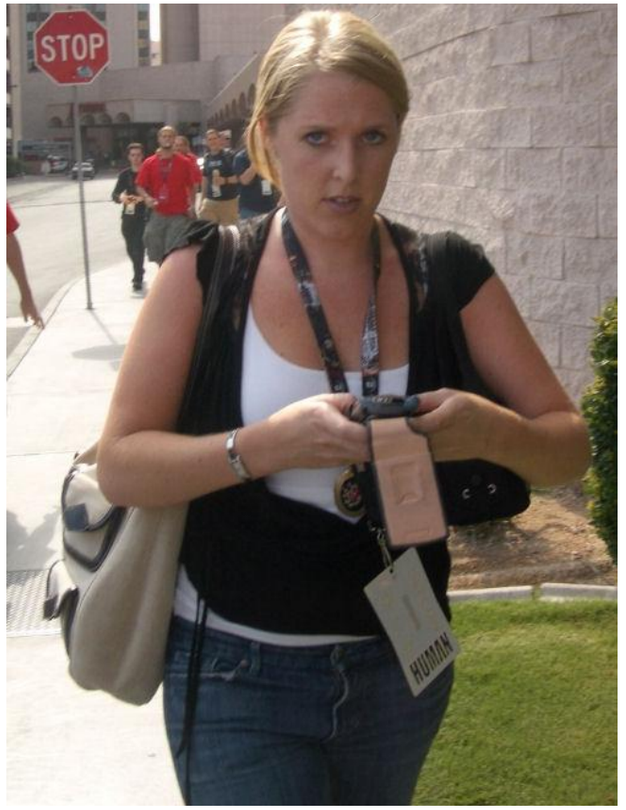
The Michelle Madigan Affair

- Associate Producer for NBC Universal
  - Dateline NBC
- Attended Defcon 15 in 2007
  - Did not get press credentials
- Defcon Found Out
  - Asked her numerous times to get press credentials [38]
  - She Refused
  - Was escorted (chased) out of the con



The Michelle Madigan Affair

- Associate Producer for NBC Universal
  - Dateline NBC
- Attended Defcon 15 in 2007
  - Did not get press credentials
- Defcon Found Out
  - Asked her numerous times to get press credentials
  - She Refused
  - Was escorted (chased) out of the con
- Not an isolated case



The CyberCrime Wave that Wasn't [39]

- New York Times Sunday Review
  - 2012.04.14
  - Dinei Florencio and Cormac Herly

- annual direct consumer losses at $114 billion worldwide.
- cybercrime estimates use bad statistical methods, making them unreliable
- numbers based on surveys and not facts
- 90% of estimates come from the answers of one or two individuals.
- Credentials and stolen credit-cards sold for pennies on the dollar for the simple reason that they are hard to monetize.
- No Cybercrime billionaires
- Know anyone who has lost billions due to cybercrime?

The REALITY of HYPE

- Hype can be used to raise awareness

- Chicken Little Effect (Oh my god the sky is falling!)
- Boy Who Cried Wolf Effect
- Used by PR flaks/Politicians to sell FUD/Pass Laws
- Makes us (hackers, Security Professionals etc..) look bad

Identifying HYPE

- Just because story is everywhere doesn't make it true
- No way to verify story (nameless quotes)
- Unknown entity is blamed (i.e. hackers or China)
- Vague details – Few actual facts
- Sensational claims (Hackers control satellites)
- Trusted sources may not be

Question Everything!

Don’t Be a Part of the HYPE

- Security Professionals / Law Enforcement
  - Vet Reporters
  - If you can’t go on the record then don’t
  - Be careful when making sensational statements

- Journalists
  - Verify your sources
    - If they can’t/wont go on record ask why?
    - Find someone who will go on the record
  - Is it better to be first or better to be right?

Be Part of the REALITY

- **If you see something, say something**
  - Comment on the article
  - Tweet
  - Write a blog post
  - Make a YouTube Video

SAY SOMETHING!

Bibliography

[1] http://www.nytimes.com/1994/07/04/us/cyberspace-s-most-wanted-hacker-eludes-fbi-pursuit.html?pagewanted=all&src=pm

[2] http://pqasb.pqarchiver.com/tampabay/access/21058219.html?dids=21058219:21058219&FMT=ABS&FMTS=ABS:FT&type=current&date=Feb+18%252C+1995&author=&pub=St.+Petersburg+Times&desc=Authorities+restrict+hacker's+phone+use&pqatl=google

[3] http://www.cnn.com/SPECIALS/1999/mitnick.background/

[4] http://pqasb.pqarchiver.com/chicagotribune/access/17175772.html?dids=17175772:17175772&FMT=ABS&FMTS=ABS:FT&type=current&date=Feb+01%2C+1996&author=Elizabeth+Weise%2C+Associated+Press.&pub=Chicago+Tribune+(pre-1997+Fulltext)&desc=SOME+CALLING+SUPER+HACKER+MORE+MYTH+THAN+A+DANGER&pqatl=google

[5] Mitnick, Kevin *Ghost in the Wires* 2010 pg. 85

[6] http://pqasb.pqarchiver.com/orlandosentinel/access/40380067.html?dids=40380067:40380067&FMT=CITE&FMTS=CITE:FT&type=current&date=Mar+01%2C+1999&author=&pub=Orlando+Sentinel&desc=HACKERS+SEIZE+BRITAIN'S+MILITARY+SATELLITE+REPORT&pqatl=google

[7] http://greenspun.com/bboard/q-and-a-fetch-msg.tcl?msg_id=000YIG

[8] http://slashdot.org/story/99/02/28/1037229/crackers-reportedly-take-brit-mil-satellite

[9] http://www.shmoo.com/mail/cypherpunks/mar99/msg00049.html

Bibliography

[10] http://web.archive.org/web/20011127170846/www.zdnet.com/zdnn/stories/news/0,4586,2217730,00.html

[11] http://www.pcmag.com/article2/0,2817,2331225,00.asp

[12] http://www.usatoday.com/life/cyber/tech/2001-02-05-binladen.htm

[13] http://www.wired.com/politics/law/news/2001/02/41658?currentPage=all

[14] http://www.schneier.com/crypto-gram-0109a.html#6

[15] http://www.citi.umich.edu/techreports/reports/citi-tr-01-11.pdf

[16] http://www.newscientist.com/article/dn1340-massive-search-reveals-no-secret-code-in-web-images.html

[17] http://www.wired.com/threatlevel/2009/10/smartgrid/

[18] http://www.cbsnews.com/stories/2009/11/06/60minutes/main5555565.shtml

[19] http://www.wired.com/threatlevel/2009/11/brazil_blackout/

[20] http://www.aneel.gov.br/cedoc/adsp2009278_1.pdf

[21] http://www.nbcnewyork.com/news/local/Lewd-Photo-Sent-Over-Rep-Weiners-Hacked-Twitter-Account-122799269.html

[22] http://www.reuters.com/article/2011/05/31/us-weiner-twitter-idUSTRE74U4OD20110531

[23] http://www.huffingtonpost.com/2011/05/31/anthony-weiner-twitter_n_869008.html

Bibliography

[24] http://abcnews.go.com/Politics/rep-anthony-weiner-picture/story?id=13774605#.TwZKeCNrNfI

[25] http://www.pedestrian.tv/entertainment/news/hayley-williams-accidentally-tweets-topless-photo-/16201.htm

[26] http://www.boston.com/sports/basketball/celtics/extras/celtics_blog/2010/05/paul_pierce_sho.html

[27] http://mashable.com/2012/04/12/jabar-gaffney-tweets/

[28] http://www.businessweek.com/news/2011-10-27/chinese-military-suspected-in-hacker-attacks-on-u-s-satellites.html

[29] http://www.nasawatch.com/archives/2011/10/did-china-hack.html

[30] http://www.reuters.com/article/2011/10/31/us-china-us-hacking-idUSTRE79U1YI20111031

[31] http://www.theregister.co.uk/2011/11/17/water_utility_hacked/

[32] http://www.wired.com/threatlevel/2011/11/hackers-destroy-water-pump/

[33] http://krebsonsecurity.com/2011/11/cyber-strike-on-city-water-system/

[34] http://www.washingtonpost.com/world/national-security/water-pump-failure-in-illinois-wasnt-cyberattack-after-all/2011/11/25/gIQACgTewN_story.html?wpisrc=al_national

[35] http://arstechnica.com/business/news/2012/01/israeli-and-palestinian-hackers-trade-ddos-attacks-in-rising-cyber-gang-war.ars

[36] http://gizmodo.com/5878238/anonymous-deleted-cbscom

Bibliography

[37] http://blog.engagepr.com/blog/2007/08/as-the-media-tu.html

[38] http://www.zdnet.com/blog/ou/undercover-nbc-dateline-reporter-bolts-from-defcon-2007/653

[39] http://www.nytimes.com/2012/04/15/opinion/sunday/the-cybercrime-wave-that-wasnt.html?_r=1

[40] http://www.wired.com/threatlevel/2012/01/railroad-memo/

[41] http://www.zeit.de/2012/12/Al-Kaida-Deutschland/seite-1

[42] http://edition.cnn.com/2012/04/30/world/al-qaeda-documents-future/

[43] http://news.yahoo.com/secretary-hillary-clinton-hacked-yemen-al-qaeda-sites-020500553--abc-news-topstories.html

[44] http://www.huffingtonpost.com/2012/05/24/yemen-al-qaeda-hacked_n_1542313.html

[45] http://www.state.gov/secretary/rm/2012/05/190805.htm

[46] http://www.washingtonpost.com/world/national-security/us-hacks-web-sites-of-al-qaeda-affiliate-in-yemen/2012/05/23/gJQAGnOxlU_story.html

Hackers and Media Hype

Big Hacks That Never Really Happened

Presented by:
C.Thomas
"Space Rogue"

cthomas@trustwave.com @spacerog