Gizmodo, “The 10 Worst Hacks of All Time” (6.14.12)

Marconi telegraph hack (1903)

In 1903 the physicist John Ambrose Fleming began a demonstration of Guglielmo Marconi’s wireless telegraph for the benefit of the Royal Institution. 300 miles away, Marconi himself was to send a message to Fleming to prove the efficacy of his invention.

As the eminent scientists of the Royal Institution waited, the telegraph receiver suddenly burst into life, tapping out the Morse Code for a poem, “There was a young fellow of Italy, who diddled the public quite prettily.” The wireless had been hacked by Nevil Maskelyne, a music hall magician and would-be wireless tycoon, who had been frustrated by Marconi’s broad patents on telegraphy tech.

This is arguably the first network ‘hack’ and even though it didn’t really affect many people (it took place during a product demo), it did spectacularly demonstrate for the first time that networked communications were not inherently secure. Better still, it was done for the LULZ.

Affected: One person. Two if you count Marconi.

Project Chanology (2008-present)

When a video of Tom Cruise espousing his belief in the Church of Scientology was leaked to YouTube in 2008, the Church attempted to shut it down. This annoyed members of anarcho-hacktivist group Anonymous and led to the formation of Project Chanology, an anti-Scientology movement that has launched many cyber attacks and hacks against the celeb-addled religion.

Hacks documented so far include numerous denial of service attacks that have shut down the Scientology website; several e-thefts of Scientology documents and emails, and much cheekiness like gaming Google’s search algorithms to make Scientology the number one result for “dangerous cult” and anti-Scientology site Xenu.net the top result for searches about the religion.

Affected: unknown numbers of Scientologists. Tom Cruise.

Captain Zap’s phone hack (1981)

Ian Murphy (aka Captain Zap), along with three friends, hacked the telephone billing server used by AT&T to meter people’s calls. Murphy inverted the metering clock, giving cheap rate calls to everyone at peak times and bumping up the charges on anyone trying to save money by calling late at night.

Now reformed, Murphy runs a security consultancy and claims to be the inspiration for the movie “Sneakers”.

Affected: millions of AT&T customers.

Morris Worm (1988)

In 1988 Robert Tappan Morris, a graduate student at Cornell University, wrote the first worm — a form of computer virus designed to copy itself across the internet. Morris claims he was merely performing an experiment to map the size of the early internet but his creation quickly got out of control and infected at least 6,000 UNIX servers.

This may not sound a lot, but at the time it was equivalent to roughly one tenth of the internet. The Morris worm took years to completely eradicate and caused damage estimated at around $10,000,000 (around £6.4m)

Affected: 6,000 Unix boxes. The innocence of the early internet.

Conficker Worm (2008)

In November of 2008, a few eagle-eyed IT-types spotted that Windows PCs on their network were infected with what looked like a run-of-the-mill Worm. It quickly became apparent that not only was this a particularly slippery and hard to stamp out infection, but one that carried a rather nasty payload.

The Conficker worm quietly recruits the infected PC into the world’s largest botnet, responsible for distributing viruses, malware and taking part in massive denial of service attacks on behalf of their masters.

The source of the Conficker worm and its many variants is unknown, although some researchers believe it originated in the Ukraine. Microsoft has a standing bounty of $250,000 (£161,000) for information leading to the arrest of its creators.

Affected: at least 15 million PCs. Untold damage caused by secondary infections and subsequent denial of service attacks.

TiGER-MATE’s world record hack (2011)

A Bangladeshi hacker calling himself TiGER-MATE set a new record for the most websites hacked in a single attack. By targeting the data centre of web hosting company InMotion, TiGER-MATE was able to deface the home page of 700,000 sites in one fell stroke.

Affected: 700,000 sites. Whichever poor sod had to restore all that data.

Sony Playstation Network double-whammy (2011)

To suffer one hack against your Network is careless, Mr Sony. To suffer two…

Sony was forced to take down its own Playstation Network (PSN) in April last year after it suffered a security breach that the company initially described as “an external intrusion”. Over the following month, a succession of Sony spokespeople stared at the floor and picked at their fingernails while slowly revealing that over 77 million user accounts had been compromised.

It was a PR disaster for Sony. Not only did 77 million customers face the possibility of fraud or identity theft (or at least the loss of their PSN account) but Sony’s failure to admit the scale of the problem straight away and the extensive downtime that kept people out of PSN for weeks all added up to a problem that must NEVER happen again.

Shame they were hacked again a couple of months later, really.

Affected: over 77 million PSN users. Sony canteen completely out of humble pie for most of 2011.

Verisign Hack (2010)

Verisign is one of the most important companies on the internet. It is a key part of the Domain Name System, which associates hostnames (like “gizmodo.co.uk” or “google.com”) with their numerical IP addresses. Without it, the internet wouldn’t work very well.

As a company, it specialises in the SSL certificates that enable e-commerce sites to process payments via encrypted HTTPS. It is a business built entirely on trust.

Sooooo it was a bit worrying that in 2011, Reuters investigators discovered a series of serious security breaches that VeriSign had been less than forthcoming about. Some of these hacks had taken place two years earlier, with senior management at Verisign not being made aware of them until 2010. Even then, the hacks were not made public until Reuters spotted a mention of them hidden away in an SEC filing.

The full extent of the Verisign hack is not clear. The hackers may have fiddled around with Domain Name resolution, redirecting certain sites at will. More seriously, they could have compromised SSL certificates — something that could have huge financial ramifications if it was to be exploited. We just don’t know.

Affected: hard to say. Possibly, er, everybody.

Operation Shady RAT (2006-present)

This is the big one. In 2011 a researcher for antivirus and security company McAfee picked up the trail of a huge number of hacks and security breaches involving multiple hackers and targeting private companies; governments all over the world and even the International Olympic Committee. Defence contractors; entertainment companies; the United Nations and other groups have all been hacked by an army of nerds as part of what McAfee calls “a five year targeted operation by one specific actor.”

Nobody will come out and say exactly who or what this actor is but most people agree that it rhymes with “Beeples Shmepublic of Whiner.”

Affected: at least 74 governments, multinational companies and NGOs.

Gawker Media Comments Failstravaganza (2010)

Yeah. Ok. We know.

Back in 2010 hackers calling themselves ‘Gnosis’ kicked in the electronic back door of Gawker Towers with…umm…big cyber boots. Gnosis swiped the login details for thousands of reader accounts for sites including Gawker, Jezebel, io9, Kotaku and (hey!) Gizmodo US. The cheeky bastards then posted a story about the hack on Gawker’s front page.

All the data was encrypted, but weak passwords could be worked out from the stolen data by trial and error. It was all a bit embarrassing. Can we change the subject now?

Affected: Look! A monkey! *runs away*