Hacking Goes Mainstream

William Gibson's cyberpunk novel "Neuromancer", predicted a future where much, if not all, of our lives are conducted online. Groups of shadowy hackers operate underground, using their skills to steal data and money, and their influence to manipulate individuals, corporations, or in some cases the world.

In the 1980s, 1990s and even through the first decade of the 21st century this science fiction seemed far removed from reality. Yet many of us now live much of our lives online; we access our bank accounts, pay our bills, taxes, and mortgages online. Many of us shop for everything from books to groceries online. Our social life has gone online as we instant message, use social networking sites and play games with friends all over the world online. More and more of our data, be it personal data, business data, or anything in between, is being stored and accessed online.

facebook

Facebook helps you connect and share with the people in your life.

Sign Up

Suddenly the future described in Neuromancer does not seem so farfetched. The reality is more down to earth, admittedly: none of us have to physically connect and "jack in" ourselves to the internet yet, although given how many seem almost surgically attached to their smartphones and iPads this can't be far off! It is however hard to deny that our lives are now lived, to a greater or lesser extent, online. What was not truly appreciated until recently was how vulnerable these lives could be.

The Beginning: Sony v. GeoHot

On 2 January 2011, enterprising young hacker George Hotz, better known as "GeoHot", published the root keys of Sony's Playstation 3 (PS3) on his website. On 11 January 2011 Sony filed an application for a temporary restraining order against Hotz. They then sued him, alleging, breaches of the Digital Millennium Copyright Act, breach of contract (in respect of the Playstation Network User Agreement), tortuous interference, trespass, computer fraud and copyright infringement. The restraining order was granted on 27 January 2011, but Hotz went on and posted details of why he had hacked the PS3 on his blog. On 11 April 2011, it was revealed that a settlement had been reached between Hotz and Sony, which included a permanent injunction preventing Hotz from taking part in hacking activities relating to any Sony product. This, however, did not mark the end of Sony's problems.

"Anonymous"

Anonymous is an internet-based group known for initiating civil disobedience against a wide range of targets as diverse as Scientology, YouTube and the Australian government. When the Recording Industry Association of America (RIAA) began its heavily publicised campaign of commencing legal proceedings against file-sharers who had allegedly shared music online, Anonymous became, in its eyes at least, a defender of freedom of speech and internet freedom. Many of the group's activities throughout the last few years encompassed attacks, such as distributed denial of service (DDoS) attacks, against the websites of individuals and organisations who allied themselves with the RIAA's stance on file sharing. These were an esoteric mix encompassing everyone from law firms who partook in legal claims against file sharers to musicians outspoken on the topic such as Gene Simmons of the rock band KISS.

Anonymous v. Sony

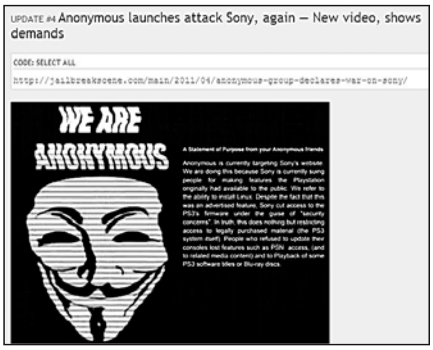
Anonymous responded to Sony's lawsuit against George Hotz by describing it as "offensive against free speech and internet freedom". Part of the lawsuit saw Sony being granted details of the IP addresses of everyone who had accessed George Hotz's blog, and on 4 April 2011 Anonymous issued the following statement:

"Congratulations, Sony. You have now received the undivided attention of Anonymous. Your recent action against our fellow hackers, GeoHot and Graf_Chokolo, has not only alarmed us, it has been deemed wholly unforgivable.

You have abused the judicial system in an attempt to censor information on how your products work…Now you will experience the wrath of Anonymous…"

Anonymous announced its intention to hack Sony's websites. Then, on 17 April 2011, shortly before Easter, the Sony's PlayStation Network (PSN) was compromised. On 20 April 2011 it was taken offline.

PSN allows users of Sony PS3s and PlayStation Portables to play games and socialise online. It also provides a platform for the preview and purchase of content. The PSN remained offline throughout the Easter holiday, causing considerable inconvenience to users and generating negative publicity for Sony. More troubling though were the reports, which initially came through piecemeal, that in the course of the outage personal information had been compromised, including names, postal and e-mail addresses and credit card information. Anonymous denied (and continues to deny) involvement in the outage, and the stories of theft of personal information were dismissed as pure rumour, spread online by those disgruntled by the lack of PSN facilities.



UPDATE #4 Anonymous launches attack Sony, again – New video, shows demands

CODE: SELECT ALL

http://jailbreakscene.com/main/2011/04/anonymous-group-declares-war-on-sony/

A Statement of Purpose from your Anonymous friends

Anonymous is currently targeting Sony's website. We are doing this because Sony is currently suing people for making features the Playstation originally had available to the public. We refer to the ability to install Linux. Despite the fact that this was an advertised feature, Sony cut access to the PS3's firmware under the guise of "security concerns". In truth, this does nothing but restricting access to legally purchased material (the PS3 system itself). People who refused to update their consoles lost features such as PSN access, (and to related media content) and to Playback of some PS3 software titles or Blu-ray discs.

However, on 4 May 2011, Sony confirmed the worst. Personally identifiable information from 77 million PSN user accounts had been stolen during the hack. It was discovered that in many cases personal data was unencrypted. The PSN remained down until 15 May 2011, and the cost to Sony was a reported US$171 million. This, combined with the unprecedented loss of personal data on an incredible scale, made the hack of PSN the biggest breach of online security to date. Hacking was catapulted into the public eye, and this was just the beginning.

All Aboard The "LulzBoat"

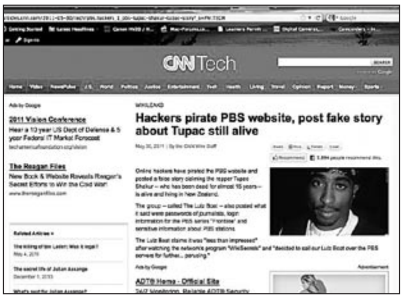
Anonymous has become, ironically, the most well-known hacker group. But in the wake of the Sony hack stories of increasingly disconcerting hacks, the perpetrators of which were often unknown, flooded the media. Some were true, and some were mere scare stories. DDoS attacks were instigated against the United States Senate, and defence giant Lockheed Martin was hacked and had data stolen. The National Health Service in the United Kingdom was notified that it had a vulnerability but that the hackers in question meant it "no harm". Reports that the entire database from the United Kingdom 2011 census had been stolen were found to be untrue. Online stores worldwide were compromised when a major database provider was hacked, with user information such as usernames, e-mail addresses and postal addresses released into the public domain. It suddenly seemed that no-one was safe online.

Out of the chaos emerged a new hacker group. Lulz Security, better known as LulzSec, used the motto "Laughing at your security since 2011!". They claimed to be hacking high profile website and organisations "for the lulz" (for the laughs) and delighted in publicly embarrassing, often via their Twitter feed, the weaknesses in the online security of large corporations and governments. They described themselves as sailing in the "LulzBoat" from hack to hack.

The first LulzSec attack took place in May 2011, when they attacked Fox.com and leaked internal passwords and the names of contestants of the talent show "X Factor". They then gained notoriety for hacking the website of American public broadcaster PBS and posting a fake story which claimed deceased rapper Tupac Shakur was in fact still alive and living in a small resort in New Zealand which had also housed another very well-known and also very deceased rapper Notorious BIG. From there, LulzSec's activities became a daily source of amusement for onlookers and of horror for security professionals as the group claimed responsibility for hacking organisations affiliated with the FBI, Sony Pictures, pornography websites (releasing usernames and e-mail addresses), and the website of the CIA. LulzSec also released into the public domain a list containing a random assortment of 62,000 usernames and passwords which they encouraged users to plug into sites to see if they could gain access.

Motivation and Damage

The interesting factor in the activities of LulzSec is the lack of a clear motivator. Whilst some members of LulzSec claimed that they were interested in bringing the public's attention to the security flaws they had uncovered, the



Ads by Google

2011 Vision Conference

Hear a 10 year US Dept of Defense & 5 year Federal IT Market Forecast

The Reagan Files

New Book & Website Reveals Reagan's Secret Efforts to Win the Cold War!

WIKILEAKS

Hackers pirate PBS website, post fake story about Tupac still alive

May 30, 2011 | By the CNN Wire Staff

Online hackers have pirated the PBS website and posted a false story claiming the rapper Tupac Shakur – who has been dead for almost 15 years – is alive and living in New Zealand.

The group – called The Lulz Boat – also posted what it said were passwords of journalists, login information for the PBS series "Frontline" and sensitive information about PBS stations.

The Lulz Boat claims it was "less than impressed" after watching the network's program "WikiSecrets" and "decided to sail our Lulz Boat over the PBS servers for further... perusing."

Related Articles »

The killing of bin Laden: Was it legal?
May 4, 2011

The secret life of Julian Assange
December 1, 2010

What's next for Julian Assange?

Ads by Google

ADT® Home - Official Site

24/7 Monitoring. Reliable ADT® Security

targets of LulzSec's attacks seemed to be selected at random and the group in fact seemed only to relish in the chaos it was causing. Whilst occasionally there appeared to be some political motivation in place, there was certainly no financial motivation. Indeed, when a small security firm issued a challenge to hack its website, with a prize for US$10,000 for doing so, LulzSec hacked the site and posted the message upon it: "Done, that was easy. Keep the money, we do it for the lulz."

The concern is, of course, that there are many who do not do it for "the lulz". These hackers do not necessarily want their activities to be publicized and may well be hacking for financial gain. Whatever one's view of the activities of Anonymous or LulzSec, the truth is that both of these groups have shown how fragile online security can be. Whilst hackers themselves are not invulnerable (suspected members of both Anonymous and LulzSec have been apprehended), by their very nature hackers are difficult to trace, and often will not be identified (let alone stopped) until some damage has been caused.

Breaches of online security are damaging to organizations and individuals. Sony is on the record for stating that the PSN breach cost US$171 million. That sum does not factor in the damage to Sony's goodwill, loss of consumer confidence, or fines that may be imposed upon the company for breaches of applicable data protection legislation, or indeed legal claims brought by those affected by the hack. Many smaller organisations may struggle to survive an attack such as that suffered by Sony. For individuals, the personal impact of a hack could be greater since loss of data, especially personal data, brings with it the risk of bank or credit card fraud, identity theft, and indeed damage to reputation: consider what havoc could be caused if someone had access to your Facebook, Twitter or LinkedIn account.

The News International Scandal

Thus far this article has only considered the issues and consequences of hackers acting alone, be it for their own personal or financial gain. One of the great themes of the science fiction mentioned at the start of this article was the use of hackers by corporations and businesses. Whilst such use has often been suspected, and there have been many reports of countries engaging in war via cyberspace through the likes of DDoS attacks, it was only recently that one of the largest media conglomerates in the world was implicated in the hacking of individuals' voicemail accounts, bank and medical records and e-mail accounts.

NEWS OF THE WORLD

FREE INSIDE 56-PAGE WORLD CUP MAGAZINE

CASH FOR ROYAL ACCESS SENSATION

FERGIE 'SELLS' ANDY FOR £500k

She makes bogus claims he'll help business deals

Takes $40k cash deposit & demands share of profits

EXCLUSIVE

News International's British News of the World newspaper was shut down in the wake of allegations that the newspaper employed private investigators to use hacking to gain information on individuals ranging from the victims of the 9/11 terror attacks to prominent celebrities, to the British Prime Minister and the Royal Family. The intention behind the hacks appears to have been to gain access to information to produce stories for publication. Investigations are ongoing.

Taking Responsibility For One's Own Security

In just six months, it seems that hacking, and its uses, has been thrust into the public eye. It would be naive to assume that hacking incidents have simply increased sharply: rather such activities have been going on for years, if not decades. The difference now is that the media is simply paying more attention to them. The increased awareness must be a positive sign. We have a duty as organizations and individuals to ensure that our data is encrypted, that we do not use the same password for every single online service we use, and that we do not allow our personal data and credit card information to be stored across the internet.

These steps are rudimentary, but they are our first line of defence and surprisingly few take them. Data will never be truly safe online, and never can be truly hacker proof, but we can at least ensure that gaining access to our business and personal data is not as easy as the likes of Anonymous and LulzSec have shown.

Paul Haswell
Senior Associate, Pinsent Masons