****

**EMBAROGED UNTIL 12:01AM GMT 18 MARCH 2015**

Contact:

Mike Rispoli

+44 (0) 7557 793878

press@privacyinternational.org

**UK government claims power for broad, suspicionless hacking of computers and phones**

The British Government has admitted its intelligence services have the broad power to hack into personal phones, computers, and communications networks, and claims they are legally justified to hack anyone, anywhere in the world, even if the target is not a threat to national security nor suspected of any crime.

These startling admissions come from a government court document published today by Privacy International. The document was filed by the government in response to two court cases initiated last year against GCHQ that challenge the invasive state-sponsored hacking revealed by Edward Snowden. In the document, the Government outlines its broad authority to infiltrate personal devices and the networks we use everyday.

Buried deep within the document, Government lawyers claim that while the intelligence services require authorisation to hack into the computer and mobile phones of “intelligence targets”, GCHQ is equally permitted to break into computers anywhere in the world even if they are not connected to a crime or a threat to national security.

Such powers are a massive invasion of privacy. Hacking is the modern equivalent of entering someone’s house, searching through her filing cabinets, diaries and correspondence, and planting devices to permit constant surveillance in future. If mobile devices are involved, the government can obtain historical information including every location visited in the past year and the ongoing surveillance will capture the affected individual wherever they go.

Additionally, the intelligence services assert the right to exploit communications networks in covert manoeuvres that severely undermine the security of the entire internet. The deployment of such powers is confirmed by recent news stories detailing how GCHQ hacked into Belgacom using the malware Regin, and targeted Gemalto, the world’s largest maker of SIM cards used in countries around the world.

The court document relies heavily on a draft code on “equipment interference”, which was quietly released to the public on the same day that the Investigatory Powers Tribunal found that GCHQ had previously engaged in unlawful information sharing with the United States’s National Security Agency.

For the past decade, GCHQ have been involved in state-sponsored hacking, or “Computer Network Exploitation”, without this code being available to the public. This lack of transparency is a violation of the requirement that the intelligence services act in accordance with law. The draft code has not yet been approved by Parliament, and is open for public comment until 20 March 2015.

Last week's ISC report admits for the first time that GCHQ relies on security vulnerabilities, including, zero-day vulnerabilities, for its CNE operations, but redacts the exact number of vulnerabilities disclosed.

Privacy International assisted in filing two separate complaints to the IPT challenging GCHQ’s widespread hacking. The first, in which Privacy International is the claimant, centres around GCHQ and the NSA’s reported power to infect potentially millions of computer and mobile devices around the world with malicious software that gives them the ability to sweep up reams of content, switch on users' microphones or cameras, listen to their phone calls and track their locations. It is the first UK legal challenge to the use of hacking tools by intelligence services.

The second complaint was filed by seven internet service and communications providers from around the world, who are calling for an end to GCHQ’s exploitation of network infrastructure in order to unlawfully gain access to potentially millions of people’s private communications. The complaint, filed by Riseup (US), GreenNet (UK), Greenhost (Netherlands), Mango (Zimbabwe), Jinbonet (Korea), May First/People Link (US), and the Chaos Computer Club (Germany), is the first time that internet and communication providers have taken collective action against GCHQ’s targeting, attacking and exploitation of network communications infrastructure.

Eric King, Deputy Director of Privacy International, said:

“The Government has been deep in the hacking business for nearly a decade, yet they have never once been held accountable for their actions. They have granted themselves incredible powers to break into the devices we hold near and dear, the phones and computers that are so integral to our lives. What’s worse is that without any legitimate legal justification, they think they have the authority to target anyone they wish, no matter if they are suspected of a crime. This suspicionless hacking must come to an end and the activities of our intelligence agencies must be brought under the rule of law."

Cedric Knight of GreenNet said:

“Our joint action has already resulted in the intelligence services publishing their interpretation of UK law. Unfortunately what has been revealed is not pretty. There is nothing in GCHQ's response to reassure us that they are not targeting our staff or equipment. We remain extremely concerned that Ed Snowden was right about GCHQ having the most intrusive capabilities of any security agency, and about exactly how widespread their computer network exploitation may be, and the risks to network security and the privacy, freedom and safety of internet users around the world.”

Jan Girlich, spokesperson for the Chaos Computer Club, Germany, said:

"It is apparent that GCHQ feels it has unlimited powers and does not care to work within its legal framework. Hacking of network infrastructure and people's phones and devices for claimed national security reasons is actually undermining the IT security on a structural level. It leaves our infrastructure vulnerable and the people's personal information in the hands of a secret service not bound to the law, wielding massive power over everybody they wish. Declaring infiltration and hacking of arbitrary computers worldwide legal by publishing the rules under which these activities happen, does not make it right. Mass surveillance and hacking is still wrong and must be stopped."

May First/People Link said:

"The Internet is a technology that breaks through the destructive barriers of national borders by providing each of us access to the thinking and experiences of the rest of humanity but some governments use this borderless state to abuse rights and effectively pervert the concept of access to experience. May First joins with our colleagues in combating that perversion."

Korean Progressive Network Jinbonet said:

"It's really surprising that the British Government claims that they can lawfully hack anyone in the world even without any suspicion. Intelligence agencies of each country including GCHQ and National Intelligence service of Korea seem to forget for whom and for what they have to serve. National security which is not based on rule of law and human rights would serve only the interest of the powerful."

***Note for editors for additional background:***

Given the long and complex nature of the both the Government’s Open Response and the ISC Report, we include below a brief guide to some of the most interesting sections of the documents with regard to the government’s hacking powers.

Government’s Open Response (see full document attached below)

·      Paragraphs 20 to 23:  The government describes its CNE activities.

·      Paragraph 65 to 66:  The draft Equipment Interference Code was published the same day the Open Response was served.  It had previously been secret policy.

·      Paragraph 77:  The intelligence services are claiming the power to hack “individuals who are not intelligence targets in their own right.”

·      Paragraph 83:  A warrant permitting hacking within the UK need only identify the person who will be affected by the hacking “where known,” permitting targeting of unknown persons.  Whether the target is suspected of or committed an offence only needs to be revealed “where relevant”, emphasizing that suspicionless people may be targets of hacking, as revealed in paragraph 77.

·      Paragraph 89:  Information obtained via hacking may be disclosed “outside the service.”

·      Paragraphs 91 to 99:  Hacking outside the British Islands is subject to a much lower standard for approval, requiring only that a “broad class of operations” be authorized by the Secretary of State.  There is no requirement that the specific target of any of theses operations be identified, much less explicitly connected to a threat to national security or a serious crime.

ISC Report (find full document here: http://isc.independent.gov.uk/news-archive/12march2015)

·      Page 14, footnote 13:  The Report’s terminology for hacking is “IT Operations.”  It also makes reference to the draft Equipment Interference Code.

·      Pages 63 to 69:  Describes, with much redaction, the intelligence services’ hacking and encryption undermining activities

Pages 87 to 89:  Addresses “class authorisations” issued pursuant to Section 7 of the Intelligence Services Act.  These broad authorisations allegedly permit the intelligence services to hack anyone outside of the British Isles.  As of October 2014, GCHQ only had *five* of them that “remove liability under UK law for some activities, including those associated with certain types of intelligence gathering and interference with computers, mobile phones and other electronic equipment.” (Para. 234)