EMBARGOED UNTIL 12PM BST 2 JULY

Global internet service and communications providers file complaint to end GCHQ attacks

Seven internet service and communications providers from around the world filed a legal complaint today, calling for an end to GCHQ's attacking and 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), along with Privacy International, is the first time that internet and communication providers have taken collective action against GCHQ's targeting, attacking and exploitation of networks maintaining communications infrastructure.

Lodged today in the Investigatory Powers Tribunal, the claimants assert that GCHQ's attacks on providers are not only illegal, but are destructive, undermine the goodwill the organisations rely on, and damage the trust in security and privacy that makes the internet such a crucial tool of communication and empowerment.[1] The claimants are demanding an end to such exploitation of internet and communication services, the targeting of their systems administrators and protections for their users whose rights may have been infringed.

The widespread nature of these attacks became known through a series of articles from Der Spiegel and the Intercept, which detailed GCHQ's illicit activities and targeting of providers. The articles outlined that:

- Employees of Belgian telecommunications company, Belgacom, were targeted by GCHQ and infected with malware through a highly developed attack called "Quantum Insert", in order to gain access to important network infrastructure.
- GCHQ and NSA have a range of network exploitation and intrusion capabilities, including a "Man on the Side" technique, which covertly injects data into existing data streams in order to create connections that will enable the targeted infection of users.
- The intelligence agencies utilize a technique through an automated system – codenamed TURBINE. TURBINE "*allow[s] the current implant network to scale to large size (millions of implants) by creating a system*

[1] The network providers' claims in this case are based on the following: 1) By interfering with network assets and computers belonging to the network providers, GCHQ has contravened the UK Computer Misuse Act and Article 1 of the First Additional Protocol (A1AP) of the European Convention of Human Rights (ECHR), which guarantees the individual's peaceful enjoyment of their possessions; 2) Conducting surveillance of the network providers' employees is in contravention of Article 8 ECHR (the right to privacy) and Article 10 ECHR (freedom of expression); 3) Surveillance of the network providers' users that is made possible by exploitation of their internet infrastructure, is in contravention of Arts. 8 and 10 ECHR; and 4) By diluting the network providers' goodwill and relationship with their users, GCHQ has contravened A1AP ECHR.

that does automated control implants by groups instead of individually," according to documents released by *The Intercept*.

- Other companies - including three German internet exchange points - were targeted by GCHQ. The joint NSA-GCHQ operation is directed at exchange points which spy on all internet traffic coming through the nodes, and identify 'important' customers of German teleport provider.

While the claimants were not directly named in the Snowden documents, the type of surveillance being carried out allows them to challenge the practices in the IPT because they and their users are at threat of being targeted. Given the interconnectedness of the internet, the surveillance being carried out by GCHQ and NSA detailed in the articles could be carried out against any internet and communications provider, not just simply the networks and companies named in the reports.

The case filed today comes on the heels of two other cases filed by Privacy International in the aftermath of the Snowden revelations - the first against the mass surveillance programmes TEMPORA, PRISM and UPSTREAM, and the second against the deployment by GCHQ of computer intrusion capabilities and spyware.

Eric King, Deputy Director of Privacy International, said:

"These widespread attacks on providers and collectives undermine the trust we all place on the internet and greatly endangers the world's most powerful tool for democracy and free expression. It completely cripples our confidence in the internet economy and threatens the rights of all those who use it. These unlawful activities, run jointly by GHCQ and the NSA, must come to an end immediately."

Cedric Knight, of GreenNet, said:

"Snowden's revelations have exposed GCHQ's view that independent operators like GreenNet are legitimate targets for internet surveillance, so we could be unknowingly used to collect data on our users. We say this is unlawful and utterly unacceptable in a democracy. Our long established network of NGOs and charities, or simply individuals who value our independent and ethical standpoint, rely on us for a level of integrity they can't get from mainstream ISPs. Our entire modus operandi is threatened by this illegal and intrusive mass surveillance."

Devin Theriot-Orr of Riseup.net said:

"People have a fundamental right to communicate with each other free from pervasive government surveillance. The right to communicate, and the ability to choose to do so secretly, is essential to the open exchange of ideas which is a cornerstone of a free society. GCHQ must stop its illegal monitoring activities."

Yeokyung Chang, ICT policy activist of Jinbonet, said :

"We are all equal users and citizens in the Internet. The right to privacy of users all over the world should be protected equally and should not be infringed on by any government."

Sacha van Geffen, CEO of Greenhost, said

“Greenhost provides critical infrastructure for journalists and activists working in the harshest conditions. Their lives and that of their colleagues and sources depend on a reliable communication network. Outsider intrusion such as that of the GCHQ criminalizes all the users of the network without legal ground and causes damage to fundamental processes that keep the network running. This illicit activity is not only a blatant violation of human rights but also endangers innocent lives. It must stop at once.”

Alfredo López, co-founder of May First/People Link, said:

“Using the Internet for surveillance and violations of privacy is an obscene betrayal of the reasons for the Internet's creation and development. The human race developed the Internet to communicate challenging borders, political and government obstructions and all other forms of repression. We have done this because we understand that open, world-wide communication among humans is critical to building the kinds of movements and collaborations necessary to save ourselves and our planet. Anything that contradicts this contradicts human progress and survival.”

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

"The GCHQ's dragnet surveillance takes away all citizens' privacy rights indiscriminately. Thus, not only lawyers, doctors, journalist, and many more people are robbed of their working basis, but everybody is stripped of his or her ability to object to their government's opinion without fear of retribution. Monitoring all communications secretively and without any effective control nor checks and balances breaks the foundations on which our modern democracies are based on. We are heading towards a police state and the only way to stop this is to bring mass surveillance to an end."

For more information from Privacy International, please contact Mike Rispoli, mike@privacy.org; +44 (0) 7557793878

Background on claimants

GreenNet is an “*ethical Internet Service Provider that has been connecting people and groups who work for peace, the environment, gender equality and human rights since 1986*".
http://www.gn.apc.org/
Contact: Cedric Knight, cedric@gn.apc.org +44 (0)20 7065 0935, +44 (0) 7962 637797

RiseUp provides "*online communication tools for people and groups working on liberatory social change. We are a project to create democratic alternatives and practice self-determination by controlling our own secure means of communications.*"
https://help.riseup.net
Contact: Devin Theriot-Orr, legal@riseup.net; +1 (206) 420-6607

Jinbonet, the Korean Progressive Network, is an organisation that "*aims to support the growth of civil activity and communication by providing network services such as web hosting, community, e-mail, blog, progressive meta blog, mailinglist, etc to civil society organizations, trade unions, individuals and progressive projects*."
http://www.jinbo.net/
Contact: Byoung-il Oh, antiropy@gmail.com

Greenhost offers "*a fresh approach to ICT and sustainability, and also supports various projects in the fields of education, culture and journalism. We are committed to a free and open internet and the security of our users."*
https://greenhost.net/
Contact: Douwe Schmidt, douwe@greenhost.nl, +31205682617

May First/People Link is "*a politically progressive member-run and controlled organization that redefines the concept of "Internet Service Provider" in a collective and collaborative way*," and notes that its members are "*organizers and activists*."
https://mayfirst.org/
Contact: Alfredo Lopez, alfredo@mayfirst.org

Chaos Computer Club is a non-profit association with 3,600 members which *"[f]or more than thirty years [has been] providing information about technical and societal issues, such as surveillance, privacy, freedom of information, hactivism,* [and] *data security."*
http://ccc.de/
Contact: Jan Girlich, presse@ccc.de