GlobalResearch
Center for Research on Globalization

Europol Warning: 'Internet of Everything' Could Lead to 'Online Murder' by End of 2014

By RT News
Global Research, October 08, 2014
RT News

Region: USA
Theme: Intelligence

The EU's chief criminal intelligence agency warms that the threat of "online murder" is set to rise, with cyber criminals increasingly targeting victims with internet technology.

The European Police Office (Europol) said governments are ill-equipped to counter the menace of *"injury and possible deaths"* spurred by hacking attacks on critical safety equipment, the UK Independent reported Sunday.

Security experts called for a paradigm shift in forensic science which would react to the 'Internet of Everything' (IoE) – the dawning era of technological interconnectedness where increasingly more human activity is mediated through computer networks.

"The IoE represents a whole new attack vector that we believe criminals will already be looking for ways to exploit," according to the Europol threat assessment.

> "The IoE is inevitable. We must expect a rapidly growing number of devices to be rendered 'smart' and thence to become interconnected. Unfortunately, we feel that it is equally inevitable that many of these devices will leave vulnerabilities via which access to networks can be gained by criminals."

Death online

In a world of smart cars, homes and even cities, the risk of hacking and cracking attacks will only increase as tens of billions of devices are expected to be accessible remotely in the coming decades. It's feared the attacks will not only be launched for financial gain, but also to inflict personal harm.

Citing a December 2013 report by US security firm IID, the Europol threat assessment warned of the first murder via "hacked internet-connected device" by the end of 2014.

The idea was widely popularized by the US spy drama Homeland, in which terrorists hacked into the pacemaker of Vice-President Walden, sending him into cardiac arrest. In the real world, a team of computer security researchers managed to gain wireless access to a combination heart defibrillator and pacemaker as far back as 2008.

At the time, the experiment required more than $30,000 worth of lab equipment and a sustained effort by a team of specialists from the University of Washington and the University of Massachusetts to interpret the data gathered from the implant's signals, the New York Times reported.

The risk, however, did not escape real-life former US Vice-President Dick Cheney, who admitted in October 2013 he harbored the exact same fear.

> "I was aware of the danger that existed," Cheney said. "I knew from the experience we'd had the necessity for adjusting my own device [pacemaker] that it [Homeland] was an accurate portrayal."

Former U.S. vice-president Dick Cheney (Reuters / Olivia Harris)

In Cheney's case, doctors opted to turn off the remote function in Cheney's pacemaker back in 2007.

Conspiracy theories have also surrounded the death of Rolling Stone and Buzzfeed journalist Michael Hastings, who died in a high-speed car crash on June 18, 2013.

Former US National Coordinator for Security, Infrastructure Protection, and Counter-terrorism Richard Clarke said that based on the available information, the crash was "consistent with a car cyber-attack."

> "There is reason to believe that intelligence agencies for major powers – including the United States – know how to remotely seize control of a car. So if there were a cyber-attack on [Hastings'] car – and I'm not saying there was, I think whoever did it would probably get away with it."

American journalist Michael Hastings reports from the Obama campaign trail the day before the general election November 5, 2012 in Des Moines, Iowa (AFP Photo / Chip Somodevilla)

Hastings, incidentally, was a vociferous critic of the US surveillance state. Just hours before his death, he sent an email to his colleagues warning of an FBI investigation and that he needed to *"go off the rada[r]" for a bit.*

That same month, the Food and Drug Administration (FDA) pressured the healthcare industry to seal up vulnerabilities in Internet-connected medical devices like pacemakers, "which could be hacked to send out lethal jolts of electricity, or insulin pumps, which can be reprogrammed to administer overdoses," the IID report said.

In another twist seemingly out of Hollywood, 35-year-old New Zealand hacker, programmer and computer security expert Barnaby Jack died in July 2013, just a week before he was to give a presentation on hacking heart implants at a computer security conference. Despite rumblings on the internet, Jack had already demonstrated this type of *"anonymous assassination"* by reverse-engineering a pacemaker transmitter that could deliver deadly electric shocks, the Daily Beast reported.

Barnaby Jack (Image from facebook.com)

Jack had done extensive research into the potential of exploiting medical devices including pacemakers and insulin pumps, prompting the FDA to change regulations regarding wireless medical devices in 2012.

Meanwhile, the latest cybersecurity threat assessment is the product of the 2015 Europol-INTERPOL cybercrime conference, which concluded at Europol's headquarters in The Hague on Friday.

The three-day conference brought together some 230 specialists from law enforcement, the private sector and academia "to review current trends and new modus operandi used by organized crime networks."

The conference named prevention, information exchange, investigation and capacity building as the four core elements needed to combat cybercrime.
