National Sovereignty intimidated by Dark Web Policing, Researcher disputes

Legal Monitor Worldwide

March 16, 2016 Wednesday

Length: 870 words

Body

As crime carry on to reproduce on the so-called dark web, law enforcement agencies sometimes have to work outside of their jurisdiction. When a suspected criminal acts on the dark web, authorities are unlikely to know where in the world he or she is physically located. So if they then attempt to take action, they might be inadvertently carrying out an operation that crosses borders.

In a working paper, one researcher argues that this raises serious concerns around national sovereignty, and could even lead to retaliation from affected countries or prosecution of investigators.

Basically, it's like playing Russian Roulette with cross-border cyber operations, Ahmed Ghappour, visiting assistant professor at UC Hastings College of Law and author of the paper Searching Places Unknown: Law Enforcement Jurisdiction on the Dark Web, told Motherboard in a phone call.

In response to dark web-related crime, law enforcement agencies have moved to more non-traditional means of identifying suspects, in some cases directly hacking criminals computers to circumvent the protections given by the Tor anonymity network.

But, because it's largely impossible to know where a target computer is located before it's been hacked, the FBI and other bodies are sometimes breaking into computers overseas, without explicit consent of the host country. At bottom, no country has consented to us hacking them, or hacking their citizens, in the same way that we haven't consented to another country to hack us, Ghappour said.

In a recent case, the FBI used a network investigative technique (NIT)the agency's euphemism for a hacking toolto identify visitors of child pornography site Playpen. When users clicked on specific forum threads, the NIT would grab their IP and MAC address, as well as other technical information about their system, and send it all to a US government facility.

Motherboard found that those hacked computers weren't just in the US, though; the operation also hit computers in Greece, Chile, and likely the UK.

Some of these cyber operations might be landing in countries that we're in conflict with; that introduces a whole new set of problems

One problem, in Ghappours eyes, is that rank and file″ investigators are often left with the discretion to carry out operations that involve hacking computers abroad.

Amy Strickling

They simply lack the information and competence to make decisions that are broader than the immediate needs of a criminal investigation, Ghappour added. This is not to say that FBI agents don't know what they're doing, technologically speaking, but that the ramifications could go beyond their own work. (Usually data sharing agreements, such as Mutual Legal Assistance Treaties (MLATs), which allow law enforcement to request data from overseas, are negotiated by the State Department and implemented by the Department of Justices Office of International Affairs.)

Ghappour suggests possible ramifications from overseas hacking could include the prosecution of investigators for violating domestic laws of affected countries; he points to a 2002 case where Russia's Federal Security Service (FSB) filed charges against the FBI for remotely siphoning data from servers in Chelyabinsk. Ghappour writes that affected countries may also take counter-measures against the US, and that operations may result in diplomatic fallout.

He said I think there's a significant risk. Some of these cyber operations might be landing in countries that we're in conflict with; that introduces a whole new set of problems.

He is also concerned that this sort of activity could establish norms, and allow other countries to hack suspects in the US without consent. Ghappour said, having US law enforcement taking these steps doesn't put us in a good place to be doing this, or in a defensible position. If anything, this practice only normalizes other nations doing it to us.

Indeed, in December 2014, an unnamed foreign law enforcement agency hacked a visitor of another child porn site. That user, it turned out, was in the US.

At the moment, public documents indicate that the majority of the information collected by the FBI's NITs, such as in the case of Playpen, is fairly limited, consisting mostly of IP addresses and other technical information. But as more invasive techniques are used, the chance of these risks will likely increase.

Ghappour added If I was to actually control your computer to do something, like surveil you for a month, that also becomes a very questionable practice.

Ghappour, in his paper, lays out a set of possible solutions, such as explicitly limiting the types of crimes these tools can be used to combat or the sort of information they can collect, and shifting oversight of the operations to bodies of government such as the US Attorney General. Rather than waiting for a really problematic case to come up, perhaps it would be better to consider these solutions now.

Ghappour asked Nobody denies that the concepts of territoriality and sovereignty are changing in cyberspace. The question is, who should take the lead in that charge? Should it be led by the immediate needs of criminal investigation, or should be driven by diplomacy and higher echelons of government? 2016 Legal Monitor Worldwide.

Classification

Language: ENGLISH

Publication-Type: Newspaper

Journal Code: 1258

Subject: LAW ENFORCEMENT (91%); CRIMINAL INVESTIGATIONS (89%); INVESTIGATIONS (89%); SPECIAL INVESTIGATIVE FORCES (89%); CRIMINAL LAW (78%); COMPUTER CRIME (78%); AGREEMENTS (77%); TERRITORIAL & NATIONAL BORDERS (76%); FOREIGN RELATIONS (75%); STATE DEPARTMENTS & FOREIGN SERVICES (75%); LAW SCHOOLS (73%); US FEDERAL GOVERNMENT (71%); PORNOGRAPHY (65%); INTERNATIONAL ASSISTANCE (61%); COLLEGE & UNIVERSITY PROFESSORS (54%); CHILD PORNOGRAPHY (50%)

Industry: COMPUTER EQUIPMENT (90%); COMPUTER NETWORK SECURITY (90%); HIDDEN WEB (90%); COMPUTER CRIME (78%); INTERNET & WWW (78%); LAW SCHOOLS (73%); COLLEGE & UNIVERSITY PROFESSORS (54%)

Geographic: UNITED STATES (92%); UNITED KINGDOM (79%)

Load-Date: March 16, 2016