Judge in FBI Hacking Case uncertain on How FBI Hacking Works

Legal Monitor Worldwide

January 29, 2016 Friday

Length: 464 words

Body

Over the years, the FBI in particular has launched several drives to obtain data from suspects' computers via malware, often using the term Network Investigative Technique (NIT), to describe the software being used. As criminals continue to protect themselves with encryption and anonymization tech, cops are moving to hacking as an investigatory tool. When court cases relating to hacking come up, the judges face a major problem in understanding, even general terms used, like what is a hacking tool, and how does it work, what they do. The Department of Justice and the FBI have outlined and referred to NIT in legal documents, hence, some judges may not fully comprehend the power and scope of these searches that they authorize.

During a hearing was held in Seattle dealing with the case of Jay Michaud, a Vancouver, Washington public school administration worker arrested on child pornography charges last year. He was charged after FBI investigators seized Playpen, a Tor hidden service, and then hosted it from their own servers. From here, the FBI deployed a NIT designed to target users of the site and return their real IP address, amongst other technical information. The judge during the hearing failed to understand how a NIT, more broadly, a piece of information-siphoning malware works. There was

confusion in understanding certain parts of the documents, the language used in NIT warrants and supporting documents. The words like hack, malware or exploit are never used for that matter. Instead, the procedure of malware being downloaded to a target's computer is largely used in unclear language. Sometimes the judge completely failed to understand the terms and language used in the documents. He finds it extremely difficult to conceptualize where the data obtained from malware is sourced from, and where it goes. In short, the Judge, in spite of hearing the views of those who took part in the investigation, and having read the briefs submitted by the defense and prosecution several times, could not fully grasp what the NIT was doing.

Nate Wessler, staff attorney at the American Civil Liberties Union (ACLU), mentioned that if a smart federal judge still has trouble understanding after hours of expert testimony what is actually going on, then the average judge signing warrant applications has little hope of truly understanding what the FBI is proposing, he further stated that it appears in this case, and in other cases seen elsewhere in the country involving use of malware, the government explanations and warrant applications are quite unclear, which does not fully explain to judges how these technologies work He further state that it was important that the government be very careful to explain itself fully and precisely. 2016 Legal Monitor Worldwide.

Amy Strickling

Classification

Language: ENGLISH

Publication-Type: Newspaper

Journal Code: 1258

Subject: LAW ENFORCEMENT (90%); SPECIAL INVESTIGATIVE FORCES (90%); ARREST WARRANTS (89%); CRIMINAL INVESTIGATIONS (89%); INVESTIGATIONS (89%); COMPUTER CRIME (78%); ARRESTS (78%); JUSTICE DEPARTMENTS (78%); JUDGES (76%); WITNESSES (76%); LAWYERS (74%); TESTIMONY (71%); HUMAN RIGHTS ORGANIZATIONS (70%); PORNOGRAPHY (68%); CHILD PORNOGRAPHY (53%); EDUCATION ADMINISTRATION (53%); PUBLIC SCHOOLS (53%)

Industry: MALICIOUS SOFTWARE (90%); COMPUTER NETWORK SECURITY (90%); COMPUTER SOFTWARE (78%); COMPUTER EQUIPMENT (78%); COMPUTER CRIME (78%); HIDDEN WEB (77%); LAWYERS (74%); PUBLIC SCHOOLS (53%)

Geographic: SEATTLE, WA, USA (79%); WASHINGTON, USA (92%); UNITED STATES (92%)

Load-Date: January 29, 2016