

6:08-587

**AFFIDAVIT**

I, ROBERT G. HAMOD, being duly sworn hereby depose and state:

I am a duly appointed Special Agent of the FBI currently assigned to the Greenville, South Carolina, Resident Agency and have been so employed for the past sixteen years. Upon accepting a position with the FBI, your affiant underwent an extensive sixteen week training course involving investigations of federal crimes, to include Computer Intrusion. Your affiant has personally been involved with the investigation of Harold Anthony Trout, also known as Tony Trout, in the Greenville, South Carolina area involving computer intrusion.

The statements contained in this affidavit are based in part on information provided by witnesses and State Law Enforcement Officers. Since this affidavit is being submitted for the limited purpose of securing a search warrant, I have not included each and every fact known to me concerning this investigation. I have set forth only the facts that I believe are necessary to establish probable cause to believe that evidence of violations of Title 18, United States Code, Section 1030 are located at 107 Silver Ridge Court, Greer, South Carolina.

**STATUTORY AUTHORITY**

This investigation concerns alleged violations of Title 18, United States Code, Sections 1030(a)(2)(C), concerning the unauthorized access of a computer.

**DEFINITIONS**

The term "computer," as used herein, is defined pursuant to Title 18, United States Code, Section 1030(e)(1), as "an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device."

Your Affiant knows that computer hardware and computer software may be utilized to store records which include but are not limited to those relating to business activities, criminal activities, associate names and addresses and the identity and location of assets illegally gained through criminal activity.

The terms "records," "documents," and "materials" include all information recorded in any form, including electronic, visual or aural, and including the originals and all non-identical

copies thereof, whether different from the original by reason of any notation made on such copies or otherwise, including, but not limited to the following:

Written or printed matter of any kind, correspondence, memoranda, notes, diaries, statistics, letters, telephone toll records, telegrams, contracts, reports, checks, statements, receipts, summaries, pamphlets, books, ledgers, journals, registers, records, vouchers, slips, bills, calendars, pads, notebooks, files, logs, lists, bulletins, credit materials, data bases, teletypes, telefaxes, invoices, worksheets;

Graphic records or representations, photographs, slides, drawings, designs, graphs, charts, pictures, sketches, images, films, videotapes; and aural records or representations, tapes, records, discs.

The terms "records," "documents," and "materials" include all of the foregoing in whatever form and by whatever means the records, documents, or materials, their drafts, or their modifications may have been created or stored, including (but not limited to) any handmade form (such as writing, drawing, painting, with any implement on any surface directly or indirectly); any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, photocopies); any mechanical form (such as phonograph records, printing, or typing); any electrical, electronic, or magnetic form (such as tape recordings, cassettes, compact discs, or any information on an electronic or magnetic storage device, such as floppy diskettes, hard disks, hard drives, CD-ROMs, optical discs, printer buffers, smart cards, memory calculators, electronic dialers, Bernoulli drives, or electronic notebooks, as well as printouts or readouts from any magnetic storage device).

The term "Internet Service Provider" (ISP) refers to an entity which provides access to a host computer, from which electronic contact can be made to literally millions of computers around the world. A host computer is one that is attached to a dedicated network and serves many users. These host computers are sometimes commercial concerns, such as CompuServe and America-Online which allow subscribers to dial a local number and connect to a network which is in turn connected to their host systems. These service providers allow electronic mail service between subscribers and sometimes between their own subscribers and those of other networks.

The term "Internet Protocol" (IP) address is a unique identifier for a computer on a network. The format of an IP address is a 32-bit numeric address written as four sequences of numbers separated by periods.

A “domain name” identifies a computer or group of computers on the Internet, and corresponds to one or more IP addresses within a particular range. Domain names are typically strings of alphanumeric characters, with each “level” of the domain delimited by a period (e.g., Computer.networklevel1.networklevel2.com). A domain name can provide information about the organization, ISP, and physical location of a particular network user.

### **SOURCES OF INFORMATION**

Information was received from a witness, who is in a position to obtain this information, that Tony Trout utilized a computer monitoring software which he surreptitiously implanted onto a computer owned by the County of Greenville, South Carolina but in the possession of Joe Kernell, County Administrator, to gain access to and obtain information from this computer. Trout is currently an elected Councilman for Greenville County, South Carolina. In his capacity as a councilman, Trout has made allegations of fraud against Kernell in regards to the granting of road paving contracts in the County of Greenville.

Sometime in April 2008, the witness had a meeting with Trout, at Trout’s residence, in which Trout revealed that he had accessed Kernell’s county computer. Trout explained to the witness that he had used a commercial software product called “Remote Spy,” available at <http://www.remotespy.com/>, to access information on Kernell’s computer. Trout was able to implant the software on Kernell’s computer by first sending it attached to an e-mail to Butch Kirven, another County Councilman. Kirven then forwarded the e-mail to Kernell. When Kernell opened the e-mail the program was then installed on his computer. This software takes periodic screen shots of the target computer. It then sends this information to a server where the user can then gain access to it.

Trout then accessed his computer, in the presence of the witness, and showed him the information he had obtained. Included in this information was a log of the date/time that the screen shot was taken as well as a description of the item that was being viewed. The witness also viewed several of the screen shots which appeared to come from Kernell’s computer concerning county business. As well as this it appeared that Trout was able to obtain Kernell’s user names and passwords for a number of accounts. Trout then printed copies of the screen shots that the two viewed and provided them to the witness. The witness provided these copies to your affiant.

Trout then told the witness that he had used the information gathered by the software on Kernell’s computer to obtain Kernell’s user name and password for his e-mail account. Trout used

this information to access Kernell's e-mail account and download the information to his own computer. Trout showed several of the e-mails which he thought would be of interest to the witness. Trout also provided copies of these e-mails to the witness. The witness provided these copies to your affiant.

Trout has spoken to the witness several times about this matter. Trout has sent several more items obtained from Kernell to the witness via e-mail. The witness printed several of these items and provided them to your affiant.

The witness has told your affiant that Trout has installed spy software on more than one council member's computer.

A news article posted on a Web site run by WYFF, the Greenville, South Carolina, affiliate of NBC, available at [www.wyff4.com/politics/16575112/detail.html](http://www.wyff4.com/politics/16575112/detail.html), reads in part, "Trout denies looking at Kirven's computer, but admits to snooping on Kernell and said he has every right to do so. He said he consulted an attorney before looking at any computer files and was assured what he was doing was legal." The article quotes Trout saying "I was able to access what is going on because he is an employee of mine."

A check of public records revealed that the Internet domain name remotespy.com is registered to Tracer Spence, CyberSpy Software, LLC, 1512 E. Jefferson Street, Orlando, Florida 32801, with telephone number (321) 945-5394. The web site for the Florida Department of State, Division of Corporations shows that CyberSpy Software, LLC is registered with that same address, and also lists Tracer Spence's name in association with that company.

The witness has shown your affiant screen shots provided him by Trout that show the "Remote Spy" logo on them, leading me to conclude they were printed from that web site or from software provided by Remote Spy. One of those screen shots has notation at the top that says, "Toggle User:" followed by what appears to be drop-down box with "JKernell on COUNTY ADM01" selected.

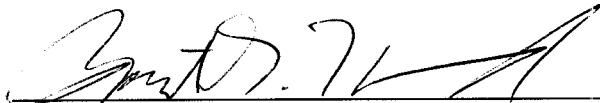
Individuals in the Greenville County, South Carolina, Information Systems Department, after being notified of this matter, conducted a search of their computer network for any malicious software. They were able to identify the Remote Spy software using their Anti-Virus software. The Anti-Virus software placed the Remote Spy software into a quarantine file. These individuals then removed the Remote Spy software from this file and installed it on an isolated computer to monitor how the software operated. They were able to determine that the software connected to the Remote Spy website through the internet. The software then began transmitting information from the infected

computer to this website. They were also able to determine that the information was being sent to an account with a username of "fiddlestix1."

Based on the above information, I believe that there is probable cause to believe that Title 18, United States Code, Section 1030(a)(2)(C), which makes it a federal crime for any person to intentionally access a protected computer without authorization and obtain information from that computer using an interstate or international communication, has been violated, and that evidence of that violation is in the possession of CyberSpy Software, LLC, 1512 E. Jefferson Street, Orlando, Florida 32801.

The evidence is believed to be concealed in records associated with the username "fiddlestix1" and/or Harold Anthony Trout (Tony Trout) or any account that is associated with the monitoring of "JKernell on COUNTY ADM01. Information obtained pursuant to this Search Warrant will be used only in connection with the investigation of this matter and it will not be disclosed to third parties except as needed to conduct the investigation and then only after giving warnings to any person to whom information is disclosed that such information is not to be further disseminated.

In consideration of the foregoing, your affiant respectfully requests that this Court issue a search warrant under 18 U.S.C. §§ 2703(a) & (c)(1)(A). If issued, the search warrant would be executed under those sections by compelling CyberSpy Software to produce to the FBI the items described in Attachment A.



ROBERT G. HAMOD, Special Agent  
Federal Bureau of Investigation

Sworn to before me this  
17<sup>th</sup> day of June, 2008.



William M. Catoe  
United States Magistrate Judge