NTI
Law Enforcement Systems and Services

Tel-Tales
Aug 2007

SpoofCard – Caller ID Spoofing

This is by no means the latest scam out there. Caller ID spoofing has been around for a long time and in many forms. Prepaid calling card systems are an easy way to offer a caller ID spoofing service to the public. I find that more and more people are using this service which is available from a number of different companies. Those that offer the service do it with impunity; they are very specific as to why they offer the service and how it can be used. Although they don't actually come out and say that bad guys could use their prepaid card to avoid detection of calls by law enforcement, it doesn't take much imagination for even your low-level street mope to figure out that this can work for him. Once upon a time everyone thought (and thankfully, many still do) that any calls made with a prepaid calling card purchased with cash are totally irretrievable by law enforcement. But many cases have now been made by many investigators – I have made my share of them – with subpoenaed call records from prepaid calling card companies. So now some of the more knowledgeable bad guys are getting wise to us and looking for a higher level of anonymity. They think spoof cards are the answer, and for all practical purposes they are right. But they are right for the wrong reasons. A spoof card call can be traced, but so few of us in law enforcement have ever done it or know how to do it that we throw up our hands and give up. In this issue we'll focus on remedying that situation.

> **Since this is a "sanitized" reprint of the August Tel-Tales per request of Direct Hit for distribution, the detail on Spoof cards has been redacted. For the full version of this and any other issue of Tel-Tales (they go back to January 2003) email Bob Lottero at rlottero@leo.gov and I'll send you the requested copies.**

Conclusion: By following the above procedure, you should be returned the telephone number (one of the telephone numbers) of the spoof card company. Depending on the circumstances, you may have to go through a few more iterations of the above, but once you get the telephone number of the spoof card company, the rest is easy. Just subpoena all their subscriber information and look particularly for the toll-free number a spoof card customer would have to use to place his call. Once you have the number (or numbers), subpoena calls to that toll-free number on the day(s) of the spoof calls to be traced. That subpoena will give you the actual originating number used by your target to place the call – actual/real caller ID cannot be blocked when dialing a toll-free number. Once you have the telephone number of your target, the rest is just plain ole detective work.

Finally, I'm using the THREADS system: A few months back I mentioned that a company in Florida, Direct Hit, Inc. (www.directhitinc.com) was nearing completion of THREADS a case management, analytical, and a full graphical/visualization system designed to be used by investigators (agents and detectives as well as analysts). This is the system for which I and my business partner, Bryan Shouldice (RCMP, retired), provided all specifications for telephonic intel

storage and advanced analysis as well as all other aspects of tactical intel storage and analysis and case management. Essentially, the design takes the case management, investigative, and analytical techniques that Bryan and I have used over our careers and clones them in an easy-to-use user interface with the look and feel of the web interface everyone is familiar with. We knew that analysts would use the system, but the one thing we both insisted on was that it had to be designed to be used by agents & detectives, the vast majority of whom have few if any analysts on staff.

We installed the system in our office and have been using it exclusively (we ran our old DOS-based system in parallel for a while) for a little over a month now. It only took a week for my staff to come up to speed and use the system effectively. I am happy to report that it has exceeded all expectations and has cut our analytical time by two-thirds [literally!] on the major federal investigations for which it has been employed. In the interest of full disclosure, I should tell you that Bryan and I get a royalty on sales of THREADS and that we have a contract with Direct Hit to provide all THREADS training – we didn't think anyone would want computer geeks training real investigators so we made sure that we would be the ones doing the training. I highly recommend it!

Help Wanted Department: Direct Hit's VP of Sales and Marketing tells me they are looking for experienced investigators and analysts to work out of their homes on a part or full time basis. If you are interested in selling THREADS software and training to law enforcement agencies, contact Kelly Solid at 321-956-2449 (Kelly.Solid@directhitinc.com).

More coming on Skype: In the June issue, I presented some preliminary research I did on Skype. At the end of the article, I asked for any input from Tel-Tales readers. The response was great; I am compiling all the information and will be presenting "Skype II", a detailed treatment of how to handle a case where Skype communication is involved. Stay tuned.

_____