FEDERAL BUREAU OF INVESTIGATION
SITUATIONAL INFORMATION REPORT
Cyber Activity Alert
Albany Division

29 June 2011

(U//LES) Going Dark: Law Enforcement Problems in Lawful Surveillance

(U) Overview

(U//LES) 'Going Dark' is a Law Enforcement (LE) initiative to address the gap between the legal authority and practical ability of LE to conduct lawfully-authorized electronic surveillance. Problems highlighted by the Going Dark initiative include LE's difficulty in receiving information from some technology companies, and criminal's use of advanced technologies and techniques that can complicate carrying out of lawfully-authorized court orders to conduct electronic surveillance.

(U) This Situational Information Report (SIR) is being provided to state and local Law Enforcement Officers (LEO) in response to questions asked about the Going Dark initiative. The intent of this document is to explain basic information on the initiative and a small sampling of the technologies and techniques that may pose problems during lawfully-authorized electronic surveillance. This product reflects the views of FBI Albany on problems state and local LE may encounter and has not been vetted by FBI Headquarters.

(U) Law Enforcement Sensitive: This information is the property of the FBI and may be distributed to state, tribal, or local government law enforcement officials with a need-to-know. Further distribution without FBI authorization is prohibited. Precautions should be taken to ensure this information is stored and/or destroyed in a manner that precludes unauthorized access.

(U) Warning: This is an information report, not finally evaluated intelligence. It is being shared for informational purposes but has not been fully evaluated, integrated with other information, interpreted, or analyzed. Receiving agencies are cautioned not to take actions based solely on this raw reporting unless the information is independently verified. A presumption of innocence still exists for any person being reported on in this report.

(U) Note: This product reflects the views of FBI Albany and has not been vetted by FBI Headquarters.

(U) Details

(U) There are many sophisticated technologies and techniques that can complicate lawfully-authorized electronic surveillance. Additionally, it is possible to use these technologies and techniques in tandem, for instance, a criminal may encrypt their web traffic and use a proxy server to hide their location.

(U) Compliance Issues

(U//LES) LE's ability to monitor sophisticated technologies is complicated by the companies that sell the technologies. Some companies are unable to comply with LE requests for lawful intercepts due to a lack of knowledge regarding LE authority, a belief that they are not subject to the laws providing LE intercept authority, or a lack of technical capability to provide the requested information. Due to the Internet and the ease with which consumers are able to purchase/use items from around the world, other companies are sometimes located outside the United States and not subject to US electronic surveillance legislation. Additionally, some companies simply do not keep the documentation necessary to comply with legal requests, either because they are not aware of the requirements or because they purposely seek to protect privacy or impede LE activities.

(U) Hiding Data

(U//LES) Encryption is one of the most common techniques and it is extremely difficult for LE to decrypt information without cooperation. Encryption is the process of applying an algorithm to a set of data that alters the data into an unrecognizable format. Only users with the decryption keys are able to decrypt the data. Through the use of hardware and software-based encryption, consumers are able to use encryption to secure individual files, hard drives, removable media (CDs, USB sticks, etc.), e-mails, instant messages, text messages and even phone calls. Encryption can be achieved through a wide variety of software and smartphone applications, that are typically user friendly. LE may be able to decrypt some data without cooperation due to poor user practices, including notes and e-mails containing passwords, and decryption keys contained in computer memory (RAM); however, frequently LE receives encrypted data, but has no way to decrypt it.

UNCLASSIFIED

(U) Examples of VoIP include Skype, Vonage, and Magic Jack. Pictured above is a Vonage phone (orange USB stick). Vonage USB sticks turn any computer with Internet access into a telephone.

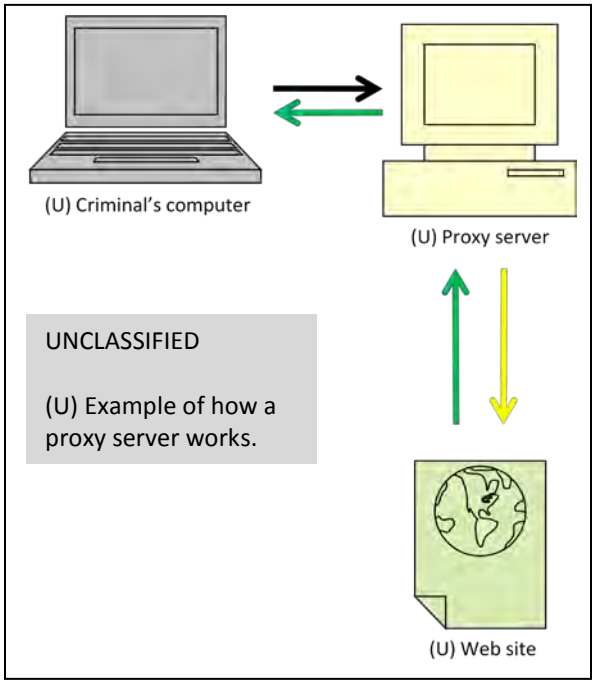
(U//LES) Steganography is a tool that physically embeds a set of data within another set of data. Methods exist to embed data inside of digital images and may allow for steganography to be applied to streamed content, like videos, music, and phone calls. The existence of the embedded data is invisible to a user unless the LEO has special training in what indicators to look for, and even if LE knows about the data, it may be impossible to retrieve the embedded data.

(U//LES) Some Voice over Internet Protocol (VoIP) services encrypt voice traffic. The use of these technologies means that criminals carry on phone conversations that LE has difficulty intercepting, and

even if the calls are intercepted, LE some data may be encrypted and unable to be analyzed.

(U) Hiding Originator Information

(U//LES) When encryption and steganography is deployed, LE can determine who the sender and receiver is, however, there are technologies and techniques that prevent LE from determining who sent and/or received the information. A Proxy server is an intermediary for another computer to connect to the Internet. Typically, the destination computer only sees that the request came from the proxy server and does not know who originated the request. To find both the destination and originator information, LE must identify and work with the proxy server owner, who could be in another country, and are frequently unwilling to cooperate with LE requests. Proxy servers may or may not keep log files that can aid Law Enforcement in determining where the traffic originated. The Onion Router (Tor) is a sophisticated network of proxy servers that allow Internet users to route their traffic through multiple intermediaries (Tor nodes), completely masking the originating computer. Tor is specifically designed so that no single computer in the chain knows both the destination and origination information, and the Tor network is comprised of multiple home and business users throughout the world, making it almost impossible to find the originating and/or destination computer.



(U//LES) While not always considered Going Dark issues, the following are worth mentioning due to their use in recent local cases and the difficulties they caused investigators.

(U//LES) Anonymous remailers prevent the identification of an e-mail writer, allowing the writer to send an e-mail without any originating information. The program accepts the properly formatted e-mail and forwards it to the recipient without any information about the sender. Some remailers will forward the e-mail at a random date and time, up to seven days after the writer hits "send" to prevent anyone from using the date-time stamp to identify the sender. Many of these services do not keep log files, which can make it impossible to trace the e-mail back to the sender.

(U//LES) Communication companies offer phone number spoofing and voice changing services, which allow callers to mask their identities. When a phone number spoofer is used, the application/service hides the number of the caller and provides false caller identification information. Some applications allow the caller to choose what number they want displayed, which makes it easy to impersonate another person or company.

(U//LES) FBI Albany is interested in information regarding criminal use of sophisticated tradecraft to counter LE activity.

(U) This report has been prepared by the Albany Division of the FBI. Comments and queries may be addressed to the Albany Field Intelligence Group at (518) 465-7551.