(TS//SI) A Tough Targeting Challenge: Skype

FROM: [redacted]
CT's Target Discovery (S2I61)
Run Date: 11/29/2005

(TS//SI) NSA is faced with a tough new targeting challenge: Skype, a free, software-based multimedia communications tool. Easily downloaded from the Internet, it allows a user to place a free call from his computer to another Skype user anywhere in the world, or to a traditional phone anywhere in the world for generally pennies per minute. Skype permits a user to purchase a phone number and, for around 40 Euros (@$47) per year, allows that number, when called from the Public Switched Telephone Network, to ring to the Skype account.

(U//FOUO) Skype also permits file sharing and chat, and will soon offer live video communications between Skype users. Skype communications are encrypted with combinations of two advanced encryption standards, AES and RSA, which makes the IP/Internet side of a Skype communication very secure.

(TS//SI) The Skype application, by nature, defeats conventional intelligence targeting practices in the following ways:

(S) **Target Identification:** Skype requires no user information upon registration other than a username and a password. Therefore, a Skype user can remain completely anonymous while on the Skype network. If a user wishes to utilize Skype's paid services, a credit card is used. However, it is easy for targets to avoid detection by using false or stolen credit cards.

(TS//SI) **Target Collection:** Skype uses peer-to-peer networking. This means that the packets from the same voice call will take different network paths to their destination. This requires multiple SIGINT collection sites to be able to recognize and collect packets from the same voice call. Skype also attempts to resolve latency issues in packet transmission, which means that, as much as possible, Skype packets will keep to fiber- optic and other types of land-based infrastructure for transmission purposes. As the Skype network and the global Internet grows, only limited amounts of Skype traffic will be available over traditional FORNSAT collection.

(TS//SI) **Target Tracking:** Skype can be implemented, without further modification, as a call center. A Skype user can be simultaneously logged on to the same Skype account on multiple computers in multiple places around the world. When a call is placed to that account, it rings to all of those computers - completely independent of geographic constraints - at the same time. Only when the user answers the call would a third party be able to identify the user's location based on the user's IP address. The effectiveness of this method, however, is hindered by the ability for a second individual, using the same account but different computer, to either make or answer a call. Therefore, the call metadata would reflect the same account being active in two simultaneous call events from possibly two geographically separate locations. This will render conventional target tracking analysis ineffective because both sets of metadata would be, in this case, true.

(U//FOUO) **Content Decryption:** Skype communications are encrypted by default. According to a four month open-source assessment of Skype by Tom Berson of Anagram Labs (www.anagram.com): *"The designers of Skype did not hesitate to employ cryptography widely and well in order to establish a foundation of trust, authenticity, and confidentiality for their peer-to-peer services. The implementers of Skype implemented the cryptographic functions correctly and efficiently. As a result, the confidentiality of a Skype session is far greater than that offered by a wired or wireless telephone call, or by email and email attachments."*

(TS//SI) The Skype application has swept the Internet in the past two years. Users are attracted to Skype's free services, extremely low costs (where costs are incurred), high call quality, and responsive support. At this time, SIGINT targets have a method to freely obscure their

communications on the global Internet, thus hindering our ability to collect vital communications intelligence. Greater analyst awareness of this and similar emerging technologies is what will lead to effective solutions for this problem in the years to come.

(U//FOUO) For more information, please visit " Go Skype " on NSANet.
