(TS//SI) Efforts Against Virtual Private Networks Bear Fruit

FROM: [redacted] VPN Working Group Chair, NAC (SSG2)
and SIGINT Communications
Run Date: 03/23/2006

(TS//SI) The Network Analysis Center has been working on VPNs for over three years -- and now a number of high-potential VPNs have been identified and decrypted.

(TS//SI) Organizations around the world want the best of both worlds. On the one hand, they want to be able to communicate among themselves via a private, secure network. On the other, they want to communicate with coworkers who may be located far away, and to do so economically, which means using public networks. How can they have their cake and eat it, too? The solution for many is a virtual private network, or VPN. Although VPNs pose special challenges for SIGINT collection and processing, we've recently had notable success in exploiting these communications.

(U) How a VPN Works (In Brief)

(U//FOUO) Although a VPN rides on a public network, it maintains privacy for its users by creating a "tunnel" through which their data can pass securely. As described in a Yakima Research Station tutorial :

"(U) A "tunnel" is constructed by establishing an authenticated connection between two gateway devices, usually either gateway routers or firewall appliances or both... Packets that do not originate from the gateway devices and do not contain packets of the private network protocol are not permitted through the gateways.

(U) For the connection between the gateways to be considered secure, the gateways must be able to authenticate themselves to each other, denying access to any device that cannot authenticate correctly. While not required, the private network packets can be encrypted for further security."

(U//FOUO) Graphic courtesy of NSA VPN Working Group

(TS//SI) Success in Exploiting VPNs for SIGINT

(TS//SI) The Network Analysis Center (NAC) has been focusing on VPN SIGINT Development (SIGDev) for over three years now, and the investment is paying off! By working with NSA's extended enterprise for collection, and with various SIGINT product lines and the Office of Target Pursuit (S311), we have identified several important targets using VPNs. What are the results? **Recently, NSA has decrypted a number of interesting targets** (thanks to decryption capabilities engineered by Network Security Products (S31213)) **deemed by product lines to have high potential as sources of intelligence:**

- Iraqi Ministry of Defense and Ministry of Interior
- [redacted]
- Iraqi State Controlled Internet Service (SCIS)
- airline reservation services:
    - Iran Air
    - Paraguayan SABRE
    - Aeroflot
    - Russian Galileo
- Al Jazeera Broadcasting internal communications

(TS//SI) Decrypted traffic has been provided to the product lines and is being evaluated for intelligence content. Hundreds of additional VPN links have also been identified and are being investigated.

(TS//SI) Work is underway at Cryptologic Centers as well. During a VPN Bootcamp held at the NSA-Georgia in early December, SIGDev analysts at Ft Gordon found a VPN target of interest within Iraqi networks already being worked there.

(U) How to Get Involved

(U//FOUO) If your target may be using VPNs, take some time to learn more. VPN Bootcamps will be held at NSA-Hawaii in May and at NSAW in June (watch for future announcements). In addition, NSA and the Second Party Partners will meet for a VPN Conference at Cheltenham in October, and a VPN Working Group meets regularly. Please join in the collaboration.

(U//FOUO) For more information, visit the NAC VPN Webpage or contact [redacted] [redacted] .

"(U//FOUO) SIDtoday articles may not be republished or reposted outside NSANet without the consent of S0121 (DL sid_comms)."