DYNAMIC PAGE -- HIGHEST POSSIBLE CLASSIFICATION IS
TOP SECRET // SI / TK // REL TO USA AUS CAN GBR NZL

(S//SI//REL) '4th Party Collection': Taking Advantage of Non-Partner Computer Network Exploitation Activity

FROM: [redacted]
Menwith Hill Station (F77)
Run Date: 01/07/2008

(U//FOUO) This article is reprinted from Menwith Hill Station's Horizon newsletter, December edition.

(S//SI//REL) The Menwith Hill Station Computer Network Operations team has been working on developing methods of "4th Party Collection" - a technique that allows the Intelligence Community to take advantage of non-5-eyes computer network exploitation (CNE) activity. The exploitation activity may be state-sponsored or opportunistic, but when one target nation is gathering data on another target nation, the Intelligence Community (IC) may be able to use that information.

(S//SI//REL) Initial development in this arena has focused on developing capability against keyboard loggers (keyloggers), specifically attempts by the Kurdistan Democratic Party against several targets. A keylogger is software or hardware that has been installed, either co-operatively or maliciously, on a computer to capture key strokes, screen captures, chats, passwords, logins, etc. Keylogger activity is quite prevalent and is being used to identify activity on computers related to IC targets.

(S//SI//REL) MHS is interested not only in the data that is being ex-filtrated, but also in who is installing the keylogging software to initiate that ex-filtration. Some initial work has already identified a network believed to be associated with the Kurdistan Security Service. Research has shown that CNE activities targeting civilian and government individuals and computer networks are taking place in several locations: the northern Iraq city of Erbil,[1] various locations in Iran, and some Iraqi Ministry of Foreign Affairs computers.

(S//SI//REL) The method of exploitation involves the use of a commercial keylogger called "Perfect Keylogger." This keylogger records data from the computer it is installed on and emails the data to a configurable email address.[2] The data from these activities are being emailed to accounts that trace back to terminals believed to be associated with the Kurdistan Democratic Party (KDP).

(S//SI//REL) Image represents a sampling of the data taken from keylogger reports between the last week of November and the first week of December 2007.

(S//SI//REL) The computer networks being targeted appear to be internet cafés in both Iran and Iraq. Email addresses from at least five different private domains are receiving the keylogger reports. These domains are all registered in Erbil, Iraq. In all cases, the targeted individuals appear to be influential and were probably chosen because they have links with the Kurdistan Regional Government. At least one Iraqi Ministry of Foreign Affairs computer has also been compromised by this CNE activity. The keylogger reports that are targeting individuals are being sent to gmail accounts, which may indicate that the person receiving the ex-filtrated data wants to be able to access it from different locations. The email addresses of the person(s) receiving the keylogger reports have been associated to MAC addresses which are believed to belong to the KDP.

(S//SI//REL) Keyloggers can give analysts information such as login/passwords, additional email addresses, phone numbers, and documents that reside on the victim's computer that might never have been seen via traditional SIGINT. Information on the CNE activity by the KDP has been passed to the analysts in

production at MHS, the Kurd TOPI (Target Office of Primary Interest) at NSA Georgia, and the NSA/CSS Threat Operations Center.

(U//FOUO) For additional information on "4th party collection," contact the MHS CNO team at [redacted]

POC: [redacted]

(U) Notes:

[1] (U) Also called Irbil and Arbil

[2](U) Configurable - Registered domain on the internet that allows the owner to make their own email addresses.