PRIVILEGED AND CONFIDENTIAL -- ATTORNEY CLIENT WORK PRODUCT

From: [redacted]
Date: May 1, 2003
RE: Cheley Non-Email Related Hacking

All of the following illegal accesses of the Near North systems put Cheley in a position to obtain internal information that stretches far beyond email. Depending on which user Cheley had chosen to impersonate for that given session, he would have had the same network access as that authorized person had been granted. For example, when he gained access into the system as Dan Watkins, he would have access to all of the Accounting file groups, and any files that Dan Watkins had saved to his personal network directories. *When Cheley logged in as Tony Swiantek (username: aswiante) or one of NN's network administrators (bwoll or ahuda), Cheley would have had complete access to all files and servers on the NN network.*

During these sessions, Cheley could easily run searches on the file servers, locate documents that met his search criteria, and then copy, print, retain, or even modify these files. Cheley's level of stolen access allowed him to be much more than a mere voyeur. It is interesting to make the distinction that this type of hacking gave Cheley "full administrative access" over the entire NN network. Cheley definitely had the appropriate access and opportunities to easily modify, delete, and/or move certain files from one location to another.

Once logged into the network in this fashion, Cheley could have also accessed and logged into any of the internal proprietary applications that NN uses. For instance, he could have accessed the Sagitta system to look up specific information, or even modified data inside these applications. One has to ask the question as to the credibility of any of the documents stored on the server, because Cheley could have modified these files at any point.

Cheley states in one email to Craig Jongsma his entire plan of manufacturing an email from Tony Swiantek, and then sending this email as Tony Swiantek to John Kass of the Chicago Tribune. He also talks about moving network files from one location to another – in an attempt to setup Swiantek. This comment, along with the access that Cheley had illegally obtained, proves that Cheley, at least, had thoughts of this type of active hacking. .

For our research, it also appears as though Cheley used these sessions to obtain new password lists so that he could continue to hack into the system -- even after individual users changed their passwords frequently.

The following list outlines the known times that Cheley infiltrated the NN system with a non-email purpose in mind. There are basically two types of entries:

1) RAS (remote access dial-in server). This is where Cheley would use a normal telephone line and dial into the NN servers. All of the instances documented here originate from Cheley's home telephone number (312.988.9608).

2) VPN (virtual private networking). All of the VPN activities listed here come from Cheley's home SprintBroadband account (66.1.214.97). This is a much quicker way to access the network. This type of access was not available until October 2001 (after Cheley was gone from NN), so Cheley either learned that this type of access was available by reading relevant IT email or from information shared by Craig Jongsma.

The following list demonstrates specific dates and times that Cheley accessed the NN network with full administrator privileges. The process used to compile this list is very tedious and time-consuming because of how the data is kept in the original computer logs. Undoubtedly, as we continue to analyse the logs and patterns, we will find additional unauthorized Cheley hacking into this part of the network. For not, this should be a decent sample so that one can comprehend how and when Cheley accessed the network in this fashion.

Saturday, August 18, 2001
08/18/01,22:07, RAS (Dial-In Server), 3129889608,0.6 minutes
08/18/01,22:08, RAS (Dial-In Server), 3129889608,2.3 minutes
08/18/01,22:19, RAS (Dial-In Server), 3129889608,6.3 minutes
08/18/01,22:30, RAS (Dial-In Server), 3129889608,1.7 minutes
08/18/01,22:37, RAS (Dial-In Server), 3129889608,76.1 minutes

Sunday, August 19, 2001
08/19/01,00:00, RAS (Dial-In Server), 3129889608,9.6 minutes
08/19/01,07:52, RAS (Dial-In Server), 3129889608,19.9 minutes
08/19/01,08:18, RAS (Dial-In Server), 3129889608,5.1 minutes

Tuesday, October 2, 2001
10/02/01,21:59, RAS (Dial-In Server), 3129889608,5 minutes
10/02/01,22:15, RAS (Dial-In Server), 3129889608,25.1 minutes

Saturday, December 23, 2001
12/23/01,19:16, RAS (Dial-In Server), 3129889608,4.1 minutes
12/23/01,19:21, RAS (Dial-In Server), 3129889608,4.1 minutes
12/23/01,19:29, RAS (Dial-In Server), 3129889608,2.3 minutes
12/23/01,19:44, RAS (Dial-In Server), 3129889608,10.3 minutes
12/23/01,19:16, RAS (Dial-In Server), 3129889608,4.1 minutes

Wednesday, January 9, 2002
01/09/2002,21:57:39,1,"NNI\msegal","NNI\msegal",,"66.1.214.97"
01/09/2002,21:57:57,1,"NNI\kgruca","NNI\kgruca",,"66.1.214.97"
01/09/2002,21:58:20,1,"NNI\jmicros","NNI\jmicros",,"66.1.214.97"
01/09/2002,21:58:31,1,"NNI\keads","NNI\keads",,"66.1.214.97"
01/09/2002,21:59:05,1,"NNI\jsegal","NNI\jsegal",,"66.1.214.97"
01/09/2002,22:00:11,1,"NNI\msoto","NNI\msoto",,"66.1.214.97"
01/09/2002,22:00:57,1,"NNI\kmcgee","NNI\kmcgee",,"66.1.214.97"
01/09/2002,22:01:30,1,"NNI\dsikora","NNI\dsikora",,"66.1.214.97"
01/09/2002,22:01:55,1,"NNI\admin","NNI\admin",,"66.1.214.97"
01/09/2002,22:02:14,1,"NNI\ahuda","NNI\ahuda",,"66.1.214.97"
01/09/2002,22:02:37,1,"NNI\aswiante","NNI\aswiante",,"66.1.214.97"
01/09/2002,22:03:47,1,"NNI\dcheleyorig","NNI\dcheleyorig",,"66.1.214.97"
01/09/2002,22:04:05,1,"NNI\djohnson","NNI\djohnson",,"66.1.214.97"
01/09/2002,22:04:53,1,"NNI\dwatkins","NNI\dwatkins",,"66.1.214.97"
01/09/2002,22:14:40,1,"NNI\bwoll","NNI\bwoll",,"66.1.214.97"
01/09/2002,22:16:28,4,"NNI\bwoll",,,"66.1.214.97"
01/09/2002,22:26:03,1,"NNI\bwoll","NNI\bwoll",,"66.1.214.97"
01/09/2002,22:27:07,1,"NNI\dwatkins","NNI\dwatkins",,"66.1.214.97"

01/09/2002,22:27:39,1,"dmi\dwatkins","DMI\dwatkins",,"66.1.214.97"
01/09/2002,22:29:07,1,"NNI\cjongsma","NNI\cjongsma",,"66.1.214.97"
01/09/2002,22:35:25,1,"NNI\bwoll","NNI\bwoll",,"66.1.214.97"
01/09/2002,22:47:51,4,"NNI\bwoll",,,"66.1.214.97"

Saturday, January 19, 2002
01/19/2002,21:01:36,1,"NNI\jmicros","NNI\jmicros",,"66.1.214.97"
01/19/2002,21:01:47,1,"NNI\msegal","NNI\msegal",,"66.1.214.97"
01/19/2002,21:03:37,4,"NNI\bwoll",,,"66.1.214.97"
01/19/2002,21:42:40,4,"NNI\bwoll",,,"66.1.214.97"

Sunday, January 27, 2002
01/27/2002,17:33:03,1,"NNI\bwoll","NNI\bwoll",,"66.1.214.97"

Sunday, February 9, 2002
02/09/2002,20:29:48,1,"NNI\bwoll","NNI\bwoll",,"66.1.214.97"
02/09/2002,20:32:58,1,"NNI\dwatkins","NNI\dwatkins",,"66.1.214.97"
02/09/2002,20:55:09,1,"NNI\msoto","NNI\msoto",,"66.1.214.97"
02/09/2002,21:53:31,4,"NNI\msoto",,,"66.1.214.97"

Wednesday, March 20, 2002
03/20/2002,22:51,RAS (Dial-In Server), 3129889608,1.9 minutes
03/20/2002,22:54,RAS (Dial-In Server), 3129889608,1.8 minutes
03/20/2002,23:02:47,1,"NNI\msoto","NNI\msoto",,"66.1.214.97"
03/20/2002,23:03:17,4,"NNI\dwatkins",,,"66.1.214.97"
03/20/2002,23:20:33,1,"NNI\aswiante","NNI\aswiante",,"66.1.214.97"
03/20/2002,23:21:53,1,"NNI\bwoll","NNI\bwoll",,"66.1.214.97"

Saturday, March 23, 2002
03/23/2002,20:36,RAS (Dial-In Server), 3129889608,2.3 minutes
03/23/2002,20:38,RAS (Dial-In Server), 3129889608,2.9 minutes
03/23/2002,20:49:50,1,"NNI\dwatkins","NNI\dwatkins",,"66.1.214.97"
03/23/2002,22:13:58,4,"NNI\dwatkins",,,"66.1.214.97"
03/23/2002,22:32:09,4,"NNI\dwatkins",,,"66.1.214.97"

Sunday, March 31, 2002
03/31/2002,21:22:38,1,"NNI\msoto","NNI\msoto",,"66.1.214.97"
03/31/2002,21:30:20,4,"NNI\msoto",,,"66.1.214.97"

Thursday, April 11, 2002
04/11/2002,22:01,RAS (Dial-In Server), 3129889608,2.9 minutes

Friday, April 19, 2002
04/19/2002,07:29,RAS (Dial-In Server), 3129889608,6.4 minutes