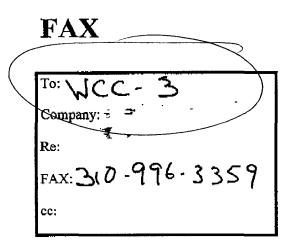
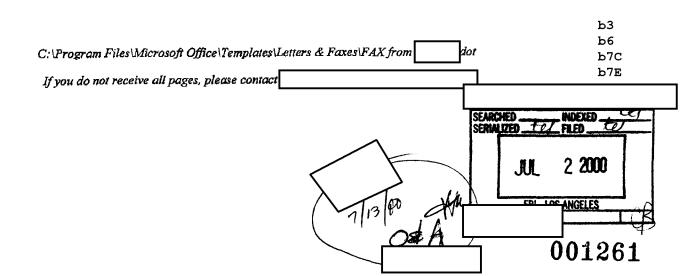
National Medical Review Offices, Inc.

5900 Wilshire Blvd., 22nd Floor Los Angeles, CA 90036



Date:	6 3	6	.2000	2	
Number o	of pages in	cluding	cover:	5_	
5900	Medical Wilshire	Blvd., 22		nc.	b6 b70
Phone:	2				
FAX:					



b6 b7С

b6 b7C

b6 b7C

Confidential	Page 2 of 4	06/30/00
We believe that	is a clue evidencing identity	of the hacker, because
by	the breach was conducted. This wered that password cracking rminal servers by	
Investigation of Netw	ork Security Breach, NMRO) — 6/17/2000
Results of the Investi	ation	
administrative passwor passwords, they had ac onto the NMRO domai mailbox using to email.	username/password. The username/password. The user retains copies of his elections user would be able to reacy	d access to these in. The hacker logged and created an email ser then gained access mail on the Microsoft
Chronology of Facts		
Saturday 6/17/2000		
Contacted by 6/17/2000, Someone fraccessing and forwardieschange mailb	om within or outside the NMR ing email from	ing email security O organization is

b6 b7C

b6 b7C

Confidential

Page 3 of 4

06/30/00

	rrived NMRO at 7:30 am and met with briefly concerning the nail security incident. met with behind closed doors about the incident.
fir	immediately began to investigate the incident. These were our ading:
1.	Someone had tampered with Windows NT Users and Groups permissions on the NMRO primary domain controller other than the authorized network security personnel.
	A user account that was disabled by after the individual left the company was enabled. The user was our After further investigation, several other users and groups have received domain administrator privileges not authorized by the Network Administrator Refer to the NMRO Security Update document for further reference.
2.	immediately revoked Admin privileges for all unauthorized users and groups and from the NMRO domain controllers and revoked remote access privileges to the

3. Focusing our attention on NMRO terminal servers, we discovered Lophtcrack 2.5 software (www.l0pht.com/l0phtcrack/) had been installed on Terminal Server (Frame 2). This software when placed and executed on a Windows NT server will crack all administrative and user passwords. A malicious hacker uses this software to gain password access in the domain. The Lophtcrack folders were deleted off the terminal servers yet the software was not removed properly from the ADD/Remove programs options in the Windows NT control Panel. Therefore leaving a trail that the software was loaded on the server.

Confidential

Page 4 of 4

06/30/00

4. Upon further investigation Lophtcrack 2.5 was brought into the organization by our	b6 b7С
END OF REPORT	
Please call me, oras soon as possible. Thank you in advance for your attention to this matter.	ь6 ь7с
Sincerely	

FEDERAL BUREAU OF INVESTIGATION

Date of transcription $07/19/2000$
was interviewed telephonically at After being advised of the official identity of the interviewing agent and the purpose of the interview, provide the following information:
is employed by National Medical Review Offices (NMRO) as has examined NMRO's event logs and security logs in an attempt to identify the origin of the intrusions into NMRO's computer system between April and June of 2000. could not identify a specific user responsible for these intrusions.
access to NMRO's system was disabled after his termination. subsequently examined the accounts of a number of people who are no longer employed by NMRO. Access to these accounts should have been disabled. However, on approximately 06/15/2000, found that the passwords and remote logon capabilities for approximately six of these accounts had been enabled. This included account. The majority of these had administrative privileges. These accounts would have to have been enabled from inside the company. However, it is difficult to determine how and when these accounts were enabled.
There were several instances between the middle of April 2000 and June, 2000 when NMRO's system had suspicious outages and went down. The system was down for a total of approximately three days. suspected that someone was hacking into NMRO's system in an attempt to shut it down.
The affected machine was NMRO's mail server. The intruder may have gained access through a program or batch file on the server. and would have had ample opportunity to install such a program on that server.
LOPHT is a hacker group that does not engage in criminal activity. This group created a program called LOPHTCRACKER that cracks system passwords. In told to run this program on NMRO's system in order to test the system.
stigation on 07/13/2000 at Los Angeles, California (telephonically)
Date dictated 07/19/2000
SA Ceb

This document contains neither recommendations nor conclusions of the FBI. It is the property of the FBI and is loaned to your agency; it and its contents are not to be distributed outside your agency.

b3

b6 b7C

b7E

b6 b7C

b6 b7C

To: NSD From: Losgeles Re:
these accounts had been enabled. This included account. The majority of these had administrative privileges. These accounts would have to have been enabled from inside the company. However, it is difficult to determine how and when these accounts were enabled.
There were several instances between the middle of April, 2000 and June, 2000 when NMRO's system had suspicious outages and went down. The system was down for a total of approximately three days. suspected that someone was hacking into NMRO's system in an attempt to shut it down.
The affected machine was NMRO's mail server. The intruder may have gained access through a program or batch file on the server. and would have had ample opportunity to install such a program on that server.
LOPHT is a hacker group that does not engage in criminal activity. This group created a program called LOPHTCRACKER that cracks system passwords. In
of NMRO's servers which are main domain controllers are named The Internet Protocol (IP) addresses for these servers are respectively.
Given that there has not been a verifiable financial

b3 b6 b7C b7E

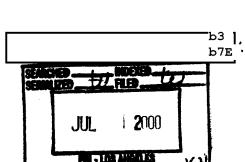
> b6 b7C b7E

Given that there has not been a verifiable financial loss to NMRO or theft of trade secrets, and because the intrusions are not ongoing, writer recommends that case be opened and closed. Investigation at Los Angeles complete.

(Title) b3
b6
b7C
b7E

Item	Date Filed	To be returned		Disposition
	Filed	Yes No		
1	7-31-00		notes re'	tel
		İ		
		j		
		İ		
		l		





*11/2 ml Construct

(experted value Mul to end 4/00 - prote ~ 6/15 - noticed Throughed 2 - 2'12 weeks after left to when deloved auts. - Mail server affect i flygetal - No commonder - mortes songuite or lather fighe Jungs - land ample of to instate - that softly of CAPHT - Clean haus group - Ive of the peop COPHT CRACKER for PUSS -Told to run it to test to to run it to test do Loguerde available Comp borne- Mould have loop Devel include from mile 4/2000 po mul 6/2000, Dusquour devays -down, 3dag