M E M O R A N D U M

TO: JODY CLIFTON Total Pages: 4

FROM: BRADLEY KERTH, RICHARD SMITH

COPIES:
MONTEREY: SUE MAGIOTTE, JOE TAGLIA, PETE DICORTI
EDC: JOHN CONSTANT

DATE: 9 JANUARY, 1991

RE: DR DOS 6.0 SECURITY

Jody,

Now that DR DOS 6.0 has been shipping for several months, it has become clear that GPOS Technical Support needs some defined procedure through which a customer can remove the security from their drive. In the past several weeks, customers have become EXTREMELY aggravated when they are faced with a security login that they either can not disable through SETUP or to which the password is unknown. These situations have arisen for various reasons:

- A virus moving into the partition table in the area used by security. Since the system sees the drive as secure, virus checkers can not get at the virus.

- A glitch in any software or hardware that inadvertently overwrites the password. Suddenly the valid password is no longer valid.

- The unfortunate situation that allowed the master and user password to be the same thus preventing a customer from removing the security (this has been corrected in the December 1991 BUS, but there is a lot of August 1991 software still out there.)

- An customer having crashed about on the drive and no longer has access to bootable DR DOS 6.0 disks (they may have returned the product) and did not disable security.

- IDE drives are coming fresh from factories with the manufacturer's testing data still on the uninitialized drive. DR DOS 6.0 sees this data as security information and demands a password when the user is attempting to install.

While DRI did not create most of these situations (which are rare), our lack of assistance in removing security has REALLY aggravated customers, some threatening legal action. While the legal action will most likely be unsuccessful, great expense will be incurred defending ourselves not to mention the poor public

EXHIBIT
435
PENGAD-Bayonne, N.J.

Plaintiff's Exhibit
5213
Comes V. Microsoft

2/4

relations created with the customer. Thus, we would like to propose the following policy be defined and implemented:

1. Two utilities be developed that will remove security. The most commonly used version, KILLDISK, will remove ALL THE DATA ON THE DRIVE by clearing the partition table entries and then shelling to FDISK forcing the customer to reformat. The less commonly used version, OPENDISK, will simply remove the security without affecting the data. We have a very complete working model of OPENDISK that we created on our own time as an educational exercise. We can produce KILLDISK very easily based on the work done for OPENDISK. The technical details of OPENDISK are attached. It is designed to protect itself from misuse 3 ways from Tuesday. Before being used, the utilities will be submitted to the EDC.

2. KILLDISK would be available to a customer ONLY on supervisor's or manager's approval. OPENDISK would be available ONLY on a manager's approval. Authorizing parties would take reasonable measures to ensure that the customer is in fact the owner of the hardware involved. The floppy carrying the utility will be returned to DRI so that we can recover the data from that partition table for EDC's investigation.

3. The Legal Department should produce a document that the customer would complete PRIOR to receiving either utility that would state the customer is the owner of or the person responsible for the hardware and that they realize that data will/may be lost by using these utilities. Attached is a sample document that Legal has produced for this purpose.

With a little work (the software engineering is done), we can create an efficient security removal policy that will satisfy most customers while recovering for EDC that type of information that is causing these problems for security without having to give the customer any information about how our security works. Everybody wins.

C0253278

OPENDISK 1.0

Hunting mosquitoes with a bazooka

OPENDISK is designed to remove DR DOS 6.0 security from drives while protecting itself from misuse or unauthorized dissemination. OPENDISK must be run from the bootable, copy protected floppy on which the utility is provided. Below is a description of its behavior:

1. When first starting, OPENDISK checks to see that it has loaded in the expected area of memory. This is to prevent someone watching its behavior with a SID, DEBUG, SOFT ICE, etc.

2. It then checks to see that it is running under the special version of IBMBIO.COM that has been harmlessly altered. It also checks that the floppy from which it is running is the original floppy provided by DRI. The floppy is copy protected and has the customers serial number encrypted. This is to make sure that the OPENDISK file is not moved to another disk or to a BBS. Because of the copy protection, a disk image can not be created with normal utilities like DISKCOPY or DIMAGE.

3. The customer is then warned that data may be lost and that backups should be made if possible. They are asked if they want to proceed and must enter "YES" in its entirety. This is to prevent the accidental striking of "Y".

4. OPENDISK then reads the Partition Table from the first drive and writes it to an absolute sector on the floppy. This is so that we can capture the data for EDC's use to make a determination as to what was causing the problem when the disk is returned to us. Since the data does not appear in a file, the customer will have little idea what information we are saving. If there are 2 physical drives, both partition tables are saved. When the floppy is returned to DRI, it will be scanned for viruses. The recovered data will then be examined and relayed to EDC if desired.

5. OPENDISK then looks for data in the area that normally holds the encrypted passwords and clears that area. The partition descriptor bytes are then checked for expected DR DOS 6.0 security values and restored to standard DOS values if needed. Since we have found situations that have one piece of data and not the other, the two areas of the partition table are treated separately.

6. OPENDISK writes the corrected data to the drive and then checks for a second physical drive. If one is found, it goes through the same process.

7. OPENDISK finally terminates telling the customer to reboot the system.

: am a licensed owner of DR DOS 6.0. I have installed security on ny system and it is now no longer working. I have been talking extensively with (tech support agent), a Digital Research :echnician. I am authorized to use the computer on which the DR DOS 6.0 program is installed, and I have some very important iata that I need to have access to as soon as possible. Enclosed is a photocopy of my identification for your reference.

Digital Research has made me aware that they have a program called OPENDISK which is designed to remove security and may enable me to have access to my data. I have requested Digital Research to provide me w.th the OPENDISK software, and I understand that it is beta software which has not been fully tested, and that it will be provided to me on an "as is" basis, without any warranty of any kind, expressed or implied. I also understand that after using this software, I must return it to Digital Research as soon as possible so that they may look at the files and make a determination as to the cause of the problem. I also understand that I may not discuss the existance or performance of OPENDISK with any person not employed by Digital Research.

Sincerely,

(Customer Signature)
DATE

C0253280