5.3 Delwin

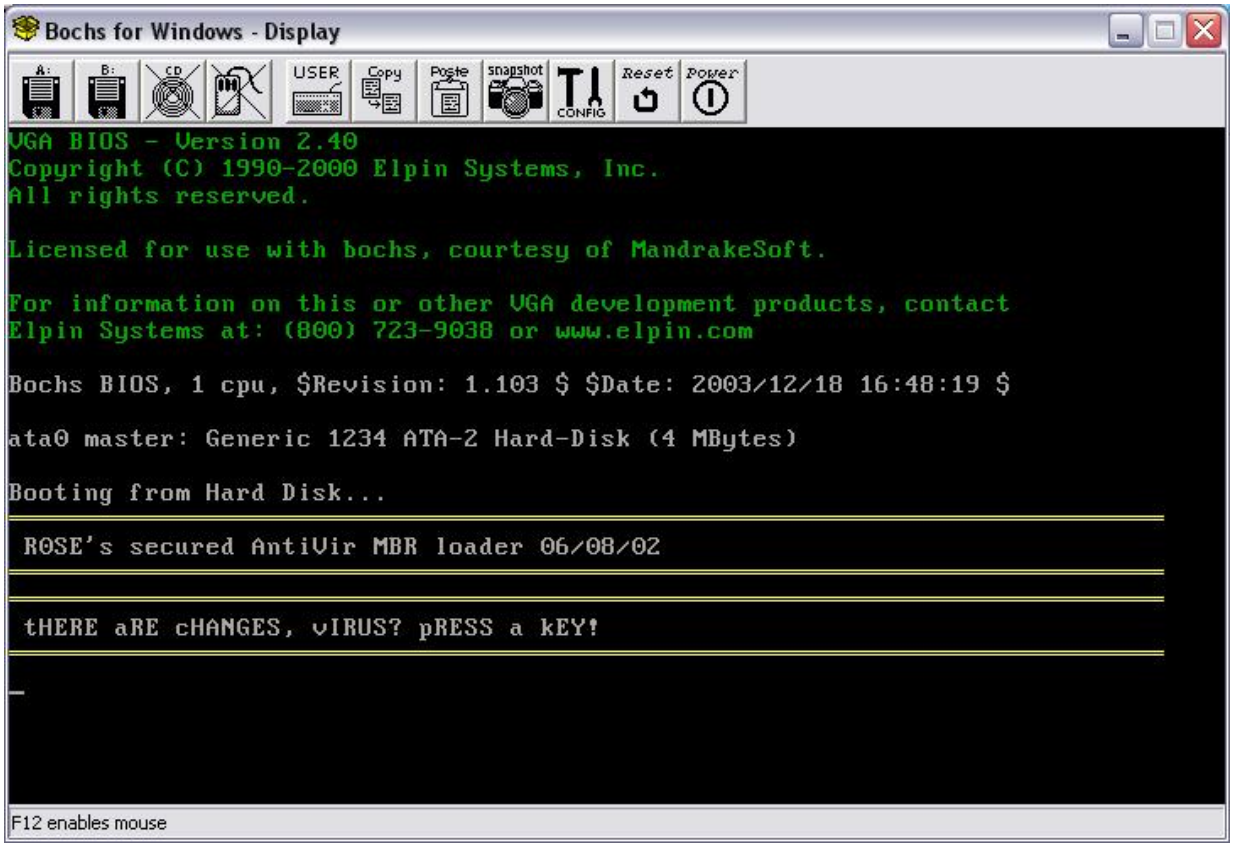
Name:	Delwin.1759, Goblin.1759
Virentyp:	Residenter EXE / MBR-Infektor, Verschlüsselt, Stealth
Größe:	EXE-Programme 1759 Bytes
Sektoren:	1+4+1 Sektoren (MBR / Code / Kopie)
Infiziert:	EXE-Programme ("EXE"-Endung und "MZ"-Test) sowie den MBR
Symptome:	Bildschirmflackern, falsche DOS-Version wird gemeldet
Status:	In Deutschland ist die 1759 Variante stark verbreitet.

Varianten: Von DelWin existieren zur Zeit zwei Varianten, einmal Delwin.1199 der auch als Goblin.1199 bekannt ist und Delwin.1759. Nur die 1759-Byte Variante ist in Deutschland sehr stark verbreitet, sie unterscheidet sich von der 1199-Byte Variante durch die Datei-Stealthfunktionen, die in der kürzeren Variante fehlen. Delwin.1759 enthält den Text "DELWIN", Delwin.1199 den Text "GOBLIN".

Infektionsmechanismus: Wird ein mit DelWin infiziertes Programm gestartet, entschlüsselt sich der Virus zunächst einmal im Speicher. Der Code ist nur mit einer statischen Verschlüsselungsroutine kodiert (XOR [1199] bzw. SUB [1759]), der Virus kann also leicht anhand einer Signatur gefunden werden. Mit der selbst definierten Interrupt 21h-Funktion AX=FD1Ch erkennt der Virus, ob er bereits im Speicher aktiv ist (Rückgabewert: AX=02E3h). Die 1199-Variante verwendet die Werte: AX=E67E -> AX=1981? Ist DelWin bereits aktiv, überspringt er seine Installationsroutine und springt sofort zum ursprünglichen Programmstart des infizierten Wirtprogramms. Ist der Virus noch nicht aktiv im RAM, ermittelt DelWin per INT 21h, AH=52h das DOS-Segment, installiert eine eigene INT 1-Routine (CPU-Einzelschrittmodus) und versucht durch Tracing den ursprünglichen INT 13h (Festplatte / Diskette) zu ermitteln. Als Dummy-Funktion für den Tracer benutzt DelWin ein Lesezugriff auf den Partitionssektor. Anhand des eingelesenen Sektors erkennt DelWin ob die Partition bereits infiziert wurde, ist das nicht der Fall verseucht der Virus nun den Partitionssektor. Der ursprüngliche Sektor wird nach Spur 0, Kopf 0, Sektor 2 kopiert (0/0/2), der Viruscode (4 Sektoren) nach 0/0/3. Eventuell. dort vorhandene Daten, wie etwa ein Partitionsmanager werden hierbei überschrieben. Der MBR-Code wird infiziert, indem die ersten 46 Bytes durch Viruscode ersetzt werden (Loader). Bevor der Viruscode in die Spur 0 geschrieben wird, ermittelt der Virus das aktuelle Systemdatum, ermittelt ein Datum ungefähr 5 Monate in der Zukunft und speichert diesen Wert im zu sichernden Code ab. Zum Ermitteln des Wertes liest der Virus die Werte der internen Uhr direkt aus dem CMOS aus.

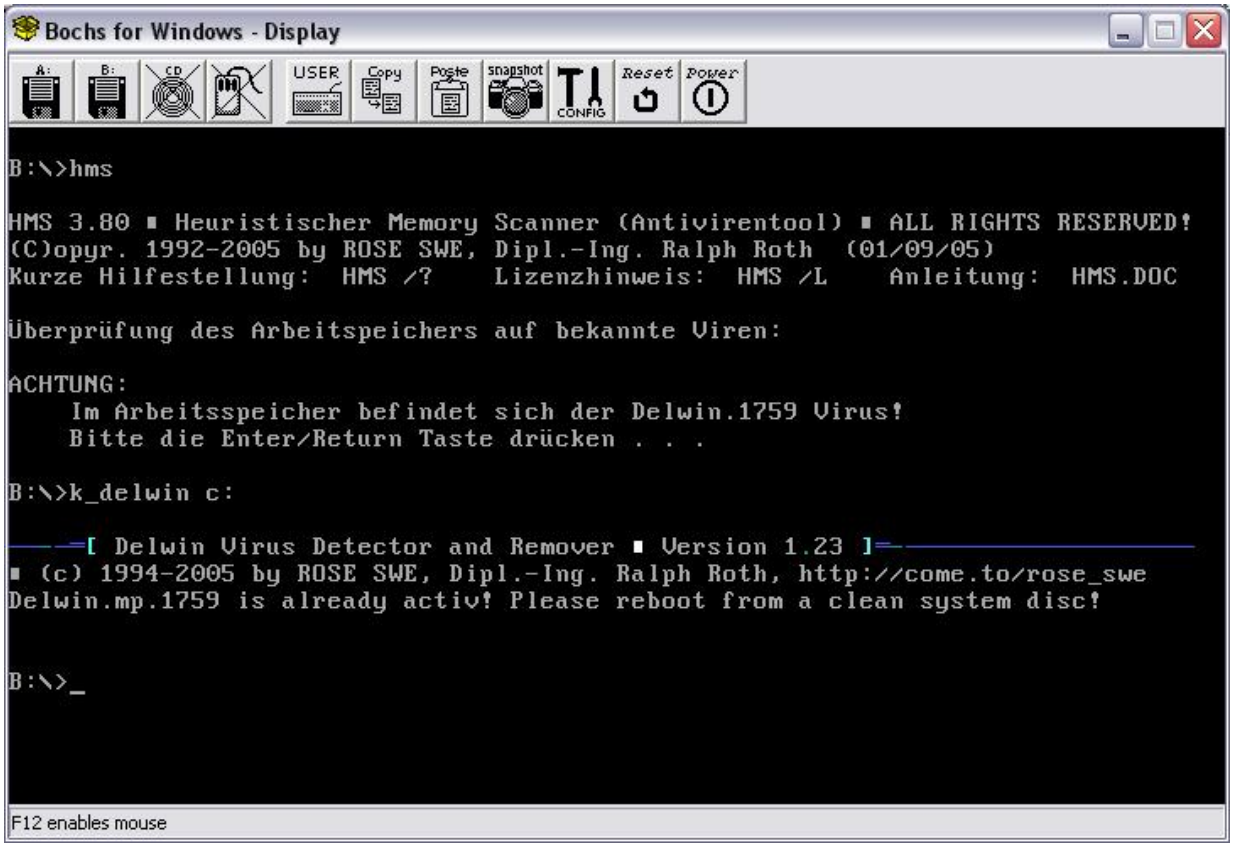
Nachdem das Infizieren abgeschlossen wurde, wird das Wirtprogramm gestartet. DelWin wird durch das Starten von infizierten EXE-Programmen nicht resident. Wird der Rechner neu gestartet, bleibt der Viruscode aus dem Partitionssektor resident im Speicher. Der DOS-Speicher wird dadurch um 2048 Bytes reduziert und der Interrupt

13h (Sektorzugriffe) belegt. Der Virus wartet dann solange bis DOS geladen wird (INT 21h-Segment unterhalb von 800h) und klinkt sich dann in den INT 21h (Dateistealth, Infektion), INT 13h (Sektorstealth-Routinen) und INT 1Ch (Schadensfunktion) ein. INT 1Ch wird nur dann belegt, wenn das beim Infizieren der Partition festgelegte Systemdatum erreicht ist. Die zweite INT13h-Routine beinhaltet die Stealthfunktion für den Partitionssektor, sämtliche Zugriffe auf den infizierten MBR werden auf die bei Spur 0, Kopf 0, Sektor 2 gespeicherte saubere Kopie umgeleitet. Wichtig: Ist der Virus aktiv kann also der verseuchte Partitionssektor weder erkannt noch gereinigt werden! Mit MBR-Kill behandelte Festplatten erkennen jedoch DelWin, wie folgende Abbildung zeigt:



Infektionsstrategie: DelWin infiziert Programme beim Öffnen (AH=3Dh, 6Ch), beim Umbenennen (AH=56H), Starten (AX=4B00h) sowie unter bestimmten Umständen beim Setzen des Dateidatums (AX=5701). INT 24h wird ausgeschaltet um Fehlermeldungen auf schreibgeschützten Disketten zu vermeiden. Der Virus infiziert EXE-Programme, wobei Programm die mit "SC" (SCAN) und "VI" anfangen nicht infiziert werden. Der Virus infiziert nur EXE-Dateien, die ".EXE" als Dateiendung haben, prüft aber auch noch ob die EXE-Signatur "MZ" vorhanden ist. Zusätzlich muss das Programm länger als 2048 Bytes sein und darf keine internen Overlays enthalten (Windows-EXE werden somit nicht infiziert). Der Virus setzt das Sekundenfeld von infizierten auf 62 und benutzt diesen Wert als Selbsterkennung beim Infizieren und für die Stealthfunktionen. Der Virus umgeht die Dateiattribute von

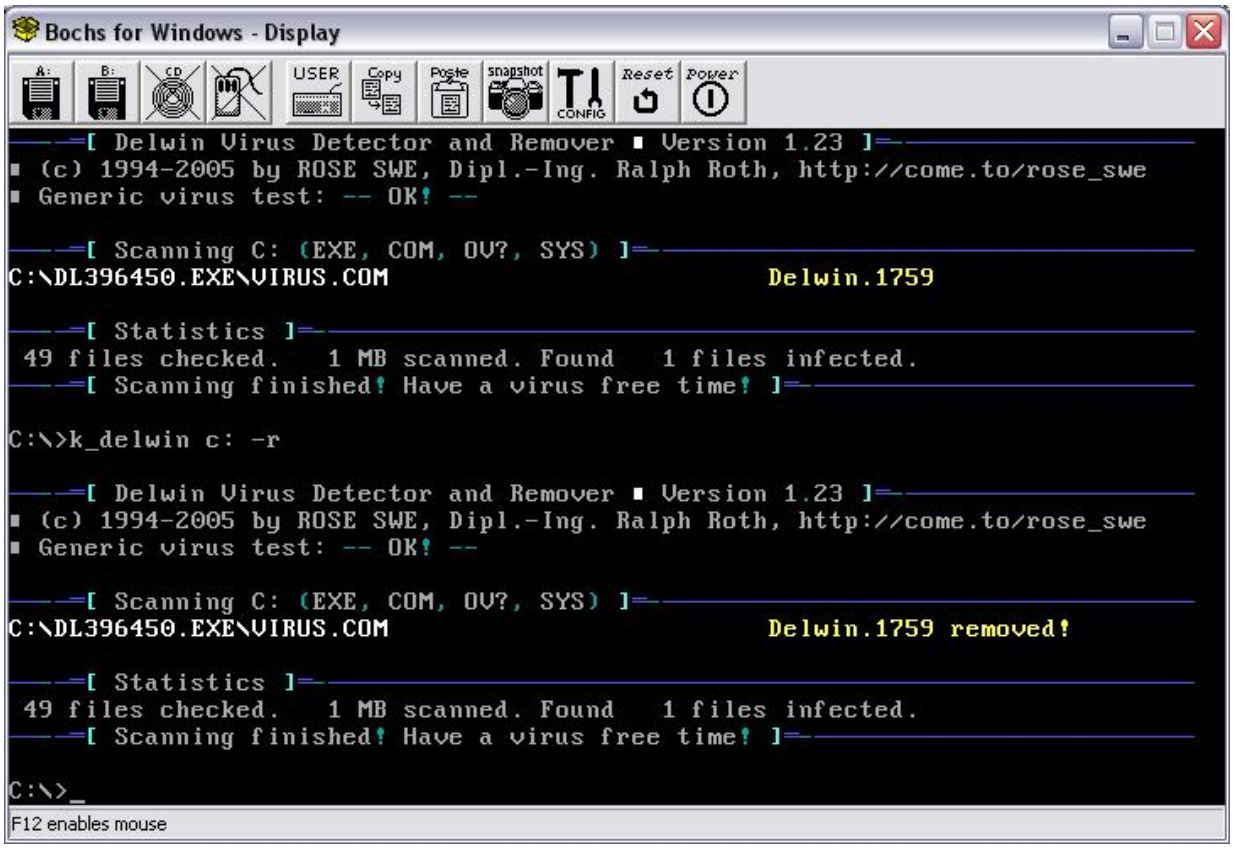
DOS und behält bis auf die Änderung des Sekundenfeldes auf 62 die alte Dateiuhrzeit bei. Ist der Virus aktiv im Speicher filtert er alle Zugriff auf infizierte Programme so, das die Dateien sauber erscheinen und den alten Inhalt und die alte Dateilänge haben. Die Funktion zum Korrigieren der Dateilänge prüft ob das aktuell laufende Programm im MCB-Namen den Eintrag "DS" enthält. Damit wird vermieden das CHKSDK durch die Stealthfunktionen des Virus irrtümlich Fehler im Dateisystem findet ('Ungültige Programmgröße').



Schadensfunktion: Wird ein Programm mit dem Namen "WIN????" gestartet (Windows, WIN.COM) gibt der Virus bei der DOS-Funktion AH=30h (DOS-Versionsnummer ermitteln) die DOS-Version 2.10, Hersteller IBM an. Dieser Wert wird normalerweise von OS/2 zurückgeliefert, Windows bricht deshalb den Startvorgang ab. Die Zeitgeber Routine von DelWin verändert in Abhängigkeit des Systemzeitgebers (Daily Counter bei 40:6Ch) das Register 0Fh des CRT Controllers. Das Resultat ist ein schnelles vertikales Flackern der Bildschirmanzeige.

Entfernung: Der Virus muss zuerst aus dem Partitionssektor entfernt werden. Dies erfolgt durch das Programm MBR-Kill. Anschließend von einer virenfreien Diskette booten und den Delwin-Killer "K-DELWIN" mit folgenden Parametern starten:

```
k-delwin c: -r
```


Bochs for Windows - Display
A:
B:
CD
USER
Copy
Paste
snapshot
CONFIG
Reset
Power
-=[Delwin Virus Detector and Remover ▪ Version 1.23]=-
▪ (c) 1994-2005 by ROSE SWE, Dipl.-Ing. Ralph Roth, http://come.to/rose_swe
▪ Generic virus test: -- OK! --
-=[Scanning C: (EXE, COM, OV?, SYS)]=-
C:\DL396450.EXE\VIRUS.COM Delwin.1759
-=[Statistics]=-
49 files checked. 1 MB scanned. Found 1 files infected.
-=[Scanning finished! Have a virus free time!]=-
C:\>k_delwin c: -r
-=[Delwin Virus Detector and Remover ▪ Version 1.23]=-
▪ (c) 1994-2005 by ROSE SWE, Dipl.-Ing. Ralph Roth, http://come.to/rose_swe
▪ Generic virus test: -- OK! --
-=[Scanning C: (EXE, COM, OV?, SYS)]=-
C:\DL396450.EXE\VIRUS.COM Delwin.1759 removed!
-=[Statistics]=-
49 files checked. 1 MB scanned. Found 1 files infected.
-=[Scanning finished! Have a virus free time!]=-
C:\>_
F12 enables mouse