VIRUS ANALYSIS 3

Bolzano Bugs NT

Péter Ször
Symantec

The first genuine Win32 virus – Win32/Cabanas – appeared at the end of 1997 (see *VB*, November 1997, p.10). From early July 1999 onwards we have been analysing six or seven of these viruses a week – a new 32-bit *Windows* virus almost every day! There are more than 200 variants now and shipment day for *Windows 2000* is getting very close.

Win32/Bolzano is a new virus that replicates under *Windows 95* and *NT*, infecting Portable Executable applications with EXE or SCR extensions. The virus does not infect if the size of the host program is less than 16 KB. We have received four different variants of Bolzano so far. A, B and D are very buggy, but the C variant is more stable. The size of D variant is the longest at 2716 bytes, but infected files will grow by at least 4 KB.

From the virus replication point of view there is nothing too remarkable about Bolzano. It is a simple, direct action appender. It adds its code to the end of the last file section and modifies the entry point of the program to point to the virus body (A, B and C variants). The D variant does not modify the entry point of PE files; instead, it searches for 12 possible CALL instructions inside the code section of the host and hooks the randomly selected CALLs to the entry point of the virus.

Fortunately, the D variant is not polymorphic; if it were, detection would be very difficult. The virus creates a thread in the infected process for itself and replicates in the background while it executes the host program (main thread). Therefore the user will not easily notice any delays. The B, C and D variants not only replicate but attack the *NT* file security system by using a new strategy which is likely to be used by other *NT* viruses in the future. This attack works on any version of *Windows NT* from 3.50 up to 4.0 with each service pack. It does not work on any betas of *Windows 2000*, but it remains feasible.

In order for the virus to attempt the attack, it needs administrative rights on an *NT* server or workstation during the initial infiltration. Therefore, it is not a major security risk, but still a potential threat. Viruses can always wait until the Administrator or someone with equivalent rights logs on. Then Bolzano has the chance to patch NTOSKRNL.EXE, the *NT* kernel, located in the WINNT\SYSTEM32 directory. The virus modifies just two bytes in an undocumented security API called SeAccessCheck that is a part of NTOSKRNL.EXE. In this way, the Bolzano virus is able to give all users full access to each file, regardless of its protection, whenever the machine is booted with the modified kernel.

This means that a Guest with the lowest possible rights on the system will be able to read and modify all files including those which are normally accessible only by the Administrator. This is a potential problem since the virus can spread everywhere it wants to regardless of the access restrictions on the particular machine. Furthermore, after the attack no data can be considered protected from any user. This is because the modified SeAccessCheck API is always forced to return 1, instead of 0 or 1. 1 means that the particular user has the necessary rights to access a particular file or directory placed on an NTFS partition while 0 means the user has no access. SeAccessCheck is called each time the file access rights should be checked.

Unfortunately, the consistency of NTOSKRNL.EXE is checked in only one place. The loader, NTLDR, is supposed to check it when it loads NTOSKRNL.EXE into physical memory during machine boot-up. If the kernel gets corrupted, NTLDR should stop loading NTOSKRNL.EXE and display an error message even before a 'blue screen' appears. In order to avoid this particular problem, Bolzano also patches the NTLDR so that no error message will be displayed and *Windows NT* will boot just fine even if its checksum does not match with the original.

Since no code checks the consistency of NTLDR itself, the patched kernel will be loaded without notification to the user. Since NTLDR is a hidden, system, read-only file Bolzano changes its attributes to 'archive' before trying to patch it. The virus does not change NTLDR's attribute back to its original value after the patch. Bolzano's B, C and D variants delete the contents of the \WINDOWS\Cookies and \WINNT\Cookies directories. Probably the virus writer wants to introduce the virus onto a machine he was using to cover where he was Web-surfing.

It is very likely that we are going to face other viruses that will be able to infect the *Windows NT* kernel and load themselves into the kernel memory area by using a similar attack. This would leave very little business for anti-virus companies that do not have an on-access, *Windows NT* driver-based scanner.

Win32/Bolzano

Infects:	Portable Executable files.
Self-check:	Time/Date stamp – not reliable, causes double infections.
Trigger:	Deletes \WINDOWS\COOKIES and \WINNT\COOKIES directory and patches NTLDR and NTOSKRNL.EXE.
Removal:	Delete infected files and use backups.