NIPC ADVISORY 00-035

"WIN9X Version of DDoS Tool"

February 18, 2000

The National Infrastructure Protection Center (NIPC) recently received information indicating the potential of a WIN9X version of distributed Denial of Service (DDoS) tools in the wild. The tool is initially believed to be similar to the "TRINO" and "Tribe Flood Network (TFN)" unique tools. NIPC determined that the tool was found on 16 Windows 98 machines on a university network and that the tools were initiating UDP packets. Each of the 16 systems were found to contain a copy of Back Orifice. The infected machines appear to have communicated with a controlling node using UDP packets and the 'PNG' and 'PONG' data using the following ports: 'PNG' received by infected machines on destination port 34555/UDP, 'PONG' sent back to controlling node on destination port 35555/UDP. These tools were detected by the system administrator due to a high volume of traffic.

Analysis determined that the TRINO-like agent appeared to be running as "SERVICE EXE," and that it started in the run registry entry, and listened on UDP port 34555 while running. Partial output of UNIX string command against the SERVICE.EXE binary included the following lines:

C:\1CC\TRINOO\NSFORK.C
LCCCRTO.C
,LOGICIELS/INFORMATIQUE 1CC-WIN32 VERSION 3.0
C:\1CC\TRINOO\1CC_.EXE
SOFTWARE\MICROSOFT\WINDOWS\CURRENTVERSION\RUN
PNG
BBB
AAA

The line "C:\1CC\TRINOO\1CC_.EXE" indicates on the infected machines the Back Orifice server file name is "_.EXE."

DDoS binaries have been disseminated to anti-virus vendors for possible design or modification of products to defeat this DDoS tool. Binaries have also been sent to Carnegie Mellon CERT/CC. NIPC requests that all computer network owners and organizations expeditiously examine their systems for evidence of this DDoS tool. Recipients are asked to report significant or suspected criminal activity to their local FBI office, NIPC Watch Warning Unit, computer emergency response support and other law enforcement agencies, as appropriate. The NIPC Watch and Warning Unit can be reached at (202) 323-3204/3205/3206, or nipc.watch@fbi.gov.