NIPC ADVISORY 99-024

"RingZero Trojan Program"

October 22, 1999

RingZero demonstrates a new, aggressive reconnaissance technique that is currently being used to map target systems and could be used to support malicious activities. Large numbers of government and commercial sites have seen an unusual amount of network scans coming from multiple origins in the past two months. This activity involves a windows-based Trojan program called Ring Zero that is designed to infect client machines without the users' knowledge.

This Trojan appears to be a remote controlled distributed scanning engine that is configured to scan ports 80 (common port for World Wide Web), 8080 (common port for World Wide Web Proxy Services), and 3128 (common squid proxy services) and send collected IP addresses and open port information to what appears to be a data collection script running on a machine located at **www.rusftpsearch.net** .

Its origins are currently unknown, but unconfirmed reports indicate that it was distributed initially via e-mail, possibly with another program such as a screen saver or game. Although Ring Zero appears to contain no malicious code, each infected client machine continues to perform electronic reconnaissance every time it is turned on.

As cited by NSWC's John Green, this activity reflects a significant advance in distributed attack technology because of Ring Zero's transmission rate; dynamic configuration options (may be able to go from scanning to attacking); and automated result consolidation.

NIPC recommends using the system administration, networking and security (SANS) Institute published information to block unneeded services as a defense against the Ring Zero Trojan. If services on ports 80, 8080, and 3128 are used, system administrator personnel should examine outbound traffic originating from these ports that are directed to unknown or suspicious sites. The NIPC strongly recommends that activity of this nature be reported to the appropriate CERT organizations, information technology security organizations, or the NIPC.