CERT Incident Note IN-98-07: Windows NT "Remote Explorer" Virus

The CERT Coordination Center publishes incident notes to provide information about incidents to the Internet community.

Windows NT "Remote Explorer" Virus

Recently, a Windows NT virus by the name of "Remote Explorer" or "RICHS" has received some public attention. Although this virus can modify files, our interaction with Microsoft leads us to belive that this virus is unable to gain any privileges beyond those of the user running the infected program. That is, the virus has only the capabilities, file permissions, etc.,of the person running it.

However, in addition to being an ordinary virus, Remote Explorer can also install itself as a Windows NT service if an infected file is run by someone with local administrator privileges. Once it has been installed as a service, Remote Explorer can impersonate anyone else who subsequently logs into the system, including domain administrators. Then, using the privileges of a domain administrator, Remote Explorer attempts to self-propagate by infecting other files on the network. Note that the ability to impersonate the currently-logged-in user is an ordinary function of any service that has been installed with privileges.

The additional ability to install itself as a service probably means that Remote Explorer can propogate somewhat faster than other viruses.

The CERT Coordination Center has not received any first-hand reports of this virus infecting systems or networks, though we have received one second-hand report of the infection of approximately 50 Windows NT servers and an undetermined number of Windows NT workstations.

You can identify machines infected by current strains of the virus by looking for a service running as "Remote Explorer" in the services control panel.

In general, we recommend that sites adhere to the following practices:

- Log in with administrative privileges only when needed. Avoid doing ordinary tasks with enhanced privileges.
- Log in as a Domain Administrator only from trusted workstations.
- Install and maintain anti-virus tools.
- Avoid running executables from unknown or untrusted sources.
- Educate users about anti-virus policies

Microsoft has provided some information regarding Remote Explorer. For more information, please see

> *http://www.microsoft.com/security/bulletins/remote.asp*

Contributors

Our thanks to Jason Garms of Microsoft for reporting this problem to us and providing technical assistance.