**ASSUMPTION**: *W32/Rbot-XC Trojan Worm*

1. What is the general functionality of the sample?

It is programmed with Trojan functionality, allowing it to remotely access the infected computer via IRC channels while running quietly in the background as a service. W32/Rbot-XC duplicates itself on the infected computer and creates entries in the registry to run itself on system startup.

1. What are the indicators that this sample is malicious?

* winmgr.exe is a new running process
* share.exe file properties changed from 882 Bytes 🡪 32 KB
* update.exe disappeared after running

1. How does this sample interact with the local system (e.g., system DLLs, files, etc.)?
2. What files and registry keys does this sample create, modify and access?
3. What is the network behavior (including hosts, domains and IP addresses accessed)?
4. What are the time and local system dependent features?
5. What is method and means by which this sample communicates to the external environment?
6. What is the original infection vector and propagation methodology?

* Trojan Worm

1. What use does this sample make of encryption for storage, communication?
2. What self-modifying or encrypted code does this sample employ?

* share.exe file properties changed from 882 Bytes 🡪 32 KB
* update.exe disappeared after running

1. What ancillary information is available concerning the development of this sample (compiler type, country of origin, author names/handles, etc.)