**ASSUMPTION**: *~~W32/Rbot-XC Trojan Worm~~* ***Trojan.Worktrik***

1. What is the general functionality of the sample?

Trojan.Wortrik is a Trojan horse that sends spam email messages from the compromised computer.

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?

The Trojan creates the following registry entries so that it runs every time Windows starts:

* HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\Run\"Microsoft Windows Service" = "%Windir%\M-505045024322940506830284960384065\winsvc.exe"
* HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\"Microsoft Windows Service" = "%Windir%\M-505045024322940506830284960384065\winsvc.exe"
* HKEY\_USERS\S-1-5-21-2445195769-2503366633-525057035-500\Software\Microsoft\Windows\CurrentVersion\Run\"Microsoft Windows Service" = "%Windir%\M-505045024322940506830284960384065\winsvc.exe"

1. What is the network behavior (including hosts, domains and IP addresses accessed)?
2. What are the time and local system dependent features?
3. What is method and means by which this sample communicates to the external environment?
4. 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.)