**ASSUMPTION**: ***Trojan.Worktrik (Variant) – Trik Bot***

1. What is the general functionality of the sample?

Trojan.Wortrik is a Trojan horse that sends spam email messages from the compromised computer. It’s mode of operation is to use instant messaging systems to propagate.

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.)?

* WS2\_32.dll
* WININET.dll
  + The WinInet API is a convenience API which simplifies the interaction to higher level protocols such as HTTP, FTP and even GOPHER! To begin using the WinInet API to talk to a remote host you first need to call InternetOpen() followed by InternetConnect() or InternetOpenURL(). Once the internet has been opened and a connection established, to perform and HTTP request you can call the functions HttpOpenRequest() to make a request handle and HttpSendRequest()to send the request.  InternetReadFile() may then be called to read any response from the server. It can also be used to read data from an FTP session. The InternetWriteFile() function can also be used generically in place of any protocol specific function where data needs to be sent across the wire. The HTTP functions provide the programmer the ability to configure most of the options one would expect in an HTTP request header such as the User-Agent string. Not all of these values have to be specified though, and the system default will be used if none is specified. The malware programmer doesn't have as much flexibility to introduce subtle anomalies in the request structures though like they can with sockets, and left with default settings the malware's HTTP requests will look virtually identical to legitimate Internet Explorer traffic on the network.
* SHLWAPI.dll
* URLMON.dll
  + The URL Monikers API provided by the DLL urlmon.dll provides yet another API for performing internet communications. In the back end it uses COM but I choose to list this as a separate category from the later discussion of COM because using this API is an abstraction away from the ugly, obscure-t0-reverse methods of direct COM interaction. The most popular function in the URLMon arsenal, from a malware perspective, is the one-punch knockout function URLDownloadToFile(). Rarely in the Win32 API does one function do so much work. You provide this function a URL (for any protocol IE understands), a filename and it uses COM to force Internet Explorer to download the resource to the specified filename. This is very popular with dropper malware which simply needs to download an EXE from a website and launch it. You might also run into the URLDownloadToCacheFile() function which will download a specified URL to the browser cache and return the name of the file it downloaded to.  URLOpenStream() and URLOpenPullStream() can be used to download a URL to a buffer in memory, but these functions are rarely used in malware.
* KERNEL32.dll
* USER32.dll
* ADVAPI32.dll
* SHELL32.dll
* OLE32.dll
* MSVCRT

1. 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.)