Threat Expert BLOG
A Blog about an automated threat analysis
..and the bad guys it targets
Trojan/Zombie Rootkit Backdoor Spyware Virus

WEDNESDAY, JANUARY 13, 2010

Trojan.Hydraq Exposed

The post describes functionality (static analysis) of the trojan that was reported in the recent targeted attacks against some large companies.

Trojan.Hydraq trojan is a DLL that runs as a service within the context of the system process `svchost.exe`.

In order to be executed within the process `svchost.exe` at the system startup, the trojan employs no injection techniques - this is achieved with the steps described below.

Firstly, the trojan registers itself as a system service `RaS[4 random characters]` by creating registry entries under the newly created key:

`HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\RaS[4 random characters]`

The `"ImagePath"` value of its service registry key is set to start `svchost.exe`, as shown below:

`"ImagePath"` = `%SystemRoot%\system32\svchost.exe -k netsvcs`
`HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\RaS[4 random characters]`

This will force the system process `svchost.exe` to look up its multi-string value `"netsvcs"`, load all services specified in it into its address space, and then call their `ServiceMain()` exports.

To make `svchost.exe` aware of its existence and be loaded too, the trojan adds its service name into the list of strings (service names) stored in the value `"netsvcs"` of the registry key:
`HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SvcHost`

To make sure its service name is added to the list of services only once, the trojan queries the contents of the value `"netsvcs"` to make sure that the multiple strings stored in that value do not contain any string that starts from `"RaS"` (case-sensitive).

Other parameters of the newly installed service are specified in the values:

`ObjectName` = `LocalSystem`
`Type` = `dword:0x20` (a win32 service that can share a process with other win32 services)
`Start = 2` (to be loaded automatically for all startups)

of the registry key:

`HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\RaS[4 random characters]`

Finally, to let `svchost.exe` process know where to load the DLL from, the image path of the trojan's service DLL is saved by setting the value:

`ServiceDll` = `[path to trojan DLL]`

of the registry key:

`HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\RaS[4 random characters]\Parameters`

The file name of the trojan DLL is retrieved by calling `GetModuleFileNameA()` API, as the trojan knows its name may vary.

For instance, the trojan can create a copy of itself under a random filename in the `%TEMP%` directory; if it locates a file `%TEMP%\c_1758.nls`, it may rename that file under a different file name.

NOTE: `%TEMP%` is a variable that refers to the temporary folder in the short path form. By default, this is C:\Documents and Settings\[UserName]\Local Settings\Temp\ (Windows NT/2000/XP), or C:\User\[UserName]\AppData\Local\Temp (Windows Vista, Windows 7).

The Hydraq trojan installs a backdoor trojan that listens for incoming commands. The commands allow the trojan to perform multiple actions - the trojan organizes them into groups - these commands are enlisted below with the [group number].[internal command number] prefixes:

- `[0.0]` adjust token privileges
- `[0.1]` terminate processes

BLOG ARCHIVE

- ▼ 2010 (7)
  - ► October (1)
  - ► August (2)
  - ► May (1)
  - ► April (1)
  - ▼ January (2)
    - Trojan.Hydraq - Part II
    - Trojan.Hydraq Exposed
- ► 2009 (17)
- ► 2008 (41)

ABOUT THREATEXPERT™

ThreatExpert is an advanced automated threat analysis system designed to analyze and report the behavior of computer viruses, worms, trojans, adware, spyware, and other security-related risks in a fully automated mode.

LINKS

ThreatExpert
PC Tools
ThreatFire Blog

- [1.0] enumerate name and status for all system services
- [1.1] control arbitrary services
- [1.2] query status for arbitrary services

- [2.0] receive remote file and save it as %TEMP%\mdm.exe, then launch it by using command control program %SYSTEM%\cmd.exe

- [3.0] enumerate registry keys under the specified key
- [3.1] enumerate registry values for the specified key
- [3.3] query registry values
- [3.4] set registry values conditionally
- [3.5] set registry values unconditionally
- [3.6] delete registry keys
- [3.7] create registry keys conditionally
- [3.8] create registry keys unconditionally

- [4.0] retrieve the list of logical drives on a system
- [4.1] read files from the local file system
- [4.2] execute arbitrary files
- [4.3] copy files in the local file system
- [4.4] delete arbitrary directories
- [4.5] rename files
- [4.6] change file attributes

- [5.1] power off computer
- [5.2] reboot Windows
- [5.3] uninstall itself by deleting the registry key HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\RaS[4 random characters]
- [5.5] clear all system event logs (application, security, and system pools)

- [6.0] enumerate files in the specified path

- [7.11] check if %SYSTEM%\acelpvc.dll is present - if it is present, load it and call its EntryMain() export; check the presence of the DLL %SYSTEM%\VedioDriver.dll

- [9.1] open the file %SYSTEM%\drivers\etc\networks.ics and read 616 bytes from it
- [9.2] delete the file %SYSTEM%\drivers\etc\networks.ics

In addition to the commands enlisted above, the trojan retrieves CPU speed by querying the "~MHz" value from the registry key:
HKEY_LOCAL_MACHINE\HARDWARE\DESCRIPTION\System\CentralProcessor\0

The stolen details are then delivered to the remote site.

Hydraq trojan is capable to keep inter-process communications with other components via a named pipe - a separate thread is spawned for that purpose.

Internal data or configuration is stored by the trojan in the values "IsoTp" and "AppleTlk" in the dedicated registry key:
HKEY_LOCAL_MACHINE\Software\Sun\1.1.2

Continued in part II.

POSTED BY SERGEI SHEVCHENKO AT 5:49 PM
LABELS: TROJAN.HYDRAQ

Newer Post Home Older Post