

DART Overview

CONTENT		
DART Number	DART Description	Page No.
0	Client Internal Error Log	9
6	Memory Statistics	9
8	Orphaned Log File Sent as Attachment	10
9	Scandisk Execution	10
10	Scandisk dialog box creation	10
12	Symantec Virus Definition Management	10
13	Virus Scan Dialog Box Creation	11
14	MS Internet Account Dialog Box Creation	11
15	Anti Virus Scan Execution	11
16	MS Internet Explorer History Folder Dialog Box Creation	11
17	Executable Detected	12
18	ReSOFT Client Shut-down / Re-start	12
19	Disk Defragmenter Execution (MS Windows 9x and Me)	12
20	Disk Defragmenter Dialog Box Creation	13
21	File / Folder Deletion Dialog Box Creation	13
24	Silent.log Check	13
26	Executable Usage Profiler	13
27	System Start-up Environment Control	14
38	Fault Detected	16
42	Password Lockout Resolution	16
43	ReSOFT Client Tools	16
45	Port Probe Detected	18

CONTENT (Contd...)		
DART Number	DART Description	Page No.
46	Error Dialog Box Creation	19
47	Warning Dialog Box Creation	19
48	Information Dialog Box Creation	19
49	Question Dialog Box Creation	19
50	Process Creation Detected	19
51	Process Completion Detected	19
60, 217, 218, 219, 220, 221	Clean Folders	19
61	System Survey	20
62	Scandisk Files Clean-up (MS Windows 9x and Me)	20
63	ReSOFT Client Start-up	21
64	ReSOFT Client Shut-down	21
65	Traceback Information on Client Internal Error	21
68	User Has Changed System Date and Time	21
69	Chkdsk Files Clean-up (MS Windows NT4, 2000, XP, and Server 2003)	22
70	Software Installation Detected	22
71	Software Removal Detected	23
72	Scandisk Log Produced at Start-up Found	24
73	System Restart	24
74	Printer Added / Removed	24
76	Netscape Preferences Dialog Box Creation	25
77	Windows Event Log Change Detected	25
79	Eudora Mail Preferences Dialog Box Creation Detected	25

CONTENT (Contd...)		
DART Number	DART Description	Page No.
80	Pegasus Mail Preferences Dialog Box Creation Detected	25
84	Network Connectivity Status	25
86	Synchronization of System Clock with Time Server	25
87	Difference between System and Time Server Clock Exceeds Configured Threshold	26
88	Network Devices and Services Availability	27
89, 151, 152, 153, 154, 155, 212, 213, 214, 215	Scheduled Program Execution	27
90	McAfee Virus Definition Management	28
92	Disk Defragmenter Execution (MS Windows NT4 and 2000)	29
93	Report running processes	29
94	Dialog Box Creation	29
95	Logical Disk Statistics	29
96	Processor Statistics	30
97	Physical Disk Statistics	30
98	Network Statistics	31
100	File Distribution and Retrieval	31
101	Printer Installation and Removal	32
111	HandsFree Client Network Deployment	32
156	Sequential Scheduled Program Execution	36
157	System Restore Point	37
160	Registry Management	37
CONTENT (Contd...)		

DART Number	DART Description	Page No.
161	Registry Protection Management	38
164	Email Attachment Filtering Log	39
165	File Download Filtering Log	39
174	User Logon-logoff Tracking	39
175	McAfee VirusScan Execution	40
176	Service Restart (MS Windows NT4, 2000, XP, and Server 2003)	40
177	DART Configuration Update	40
178	Microsoft Windows Networking Denied Access	41
187	Machine List Management	41
188	Email Attachment Filtering	41
189	File Download Filtering	42
191	TCP/IP Connectivity Problem Management	43
192	Program Execution Control	43
196	Software Patch Application	44
197	Network Configuration Change Detected	44
199	Registry Change Detected	45
207	Content Distribution	45
208	Software Update	46
211	Disk Defragmenter Execution (MS Windows XP, Windows Server 2003)	47
216	Print Queue Problem Resolution	47
222	Report File Attributes	48
225	Directory and File Protection Management	49
CONTENT (Contd...)		

DART Number	DART Description	Page No.
227	Process and Service Shutdown-Restart	50
228	Network Packet Filtering	52
231	Client Heartbeat	53
232	Intrusion Protection Control	53
233	System Start-up Environment Management	57
236	On-demand Remote Control	59
237	Microsoft Update Management	60
238	Symantec Anti Virus Definition Dates Log	61
239	McAfee Anti Virus Definition Dates Log	61
240	Intrusion Protection Management	61
241	Contact Information	64
242	eTrust Virus Definition Management	65
243	eTrust EZ Antivirus Scan Execution	65
244	eTrust EZ Antivirus Definition Dates Log	66
245	On-demand GoToAssist	66
246	Network Device Discovery	66
247	Trend Micro Virus Definition Management	67
249	Trend Micro Anti Virus Scan Execution	67
250	Trend Micro Anti Virus Definition Dates Log	68
251	IE Browser Optimization	68
252	Log File Retrieval and Logging	68
253	Defrager For 64-Bit OS	68
254	Rocket Dock Management	69
CONTENT (Contd...)		

DART Number	DART Description	Page No.
255	Contact Information	69
256	Client Uninstall	70
257	On-demand Repeater Connectivity	70
258	End-User Message - I	70
259	End-User Message - II	71
260	Sequential DART - I	71
261	Sequential DART - II	71
262	Sequential DART - III	72
263	Spybot Tool Management	72
264	3rd party Tools Installation - I	73
265	Fake AV Tool Management	73
266	Malwarebyte Tool Management (User Mode)	74
267	Trojan Remover Tool Management (User Mode)	75
268	Registry Healer Tool Management (User Mode)	75
269	Flash Player Plugin Management (User Mode)	76
270	JRE Plugin Management (User Mode)	76
271	Hitman Pro Tool Management (User Mode)	77
272	SafeMSI & rkill Tool Management (User Mode)	78
273	CCleaner Tool Management (User Mode)	78
274	RemoveIT Tool Management (User Mode)	79
275	3rd party Tools Installation - II (User Mode)	80
276	Superantispyware Tool Management (User Mode)	80
277	3rd party Patch Uninstallation - I	
CONTENT (Contd...)		

DART Number	DART Description	Page No.
278	3rd party Patch Uninstallation - II (User Mode)	81
279	3rd party Patch Uninstallation - III (User Mode)	82
280	Hardware Diagnostic Management (Scripts)	83
281	Hardware Diagnostic Management (Devices)	83
282	Windows Firewall Management	83
283	Windows Troubleshooter Management (Windows 7 & Vista)	83
284	Windows Fix-It Management (Windows XP)	84

DART 0 – Client Internal Error Log

DART 0 detects and reports the ReSOFT client internal errors.

DART 6 – Memory Statistics

DART 6 reports memory utilization statistics for each of the following classes of memory:

- Physical memory
- Virtual memory
- Swap space

The following utilization statistics are reported:

- Total (Kbytes)
- In use (Kbytes)
- Percentage in use (%)
- Free (Kbytes)
- Percentage free (%)

In addition, the following statistic is reported:

- Page reads per second

Note that memory utilization measurements are made at the time the DART is run. However, the "page reads per second" statistic must be averaged over a specific time period. That time period is one of the DART's configuration parameters, in mSec, with the default value set at 15000 Msec.

DART 6 can be used as an automated early warning system for low memory conditions. For page reads per second you can set a threshold that will trigger a DART log whenever page reads per second exceed it. This is recognized as one of the better indicators of degraded system performance due to low memory conditions.

In addition, for each type of memory monitored, users can set available memory thresholds as a percentage of the total amount of memory. When available memory falls below a threshold, a DART log is automatically created and uploaded to the log server. A support provider can then set up a notification that scans the log database every ten minutes and notifies him/her whenever a DART 6 log is found signaling a low-memory condition.

DART 8 – Orphaned Log File Sent as Attachment

DART 8 detects whether there are any files in the "temp" directory of the Client folder that aren't scheduled to be sent via e-mail. If there are any, it attaches them to an e-mail log, which causes them to be deleted when they are sent. This is helpful in diagnosing failures in the e-mail logging mechanism which cause logs to not be sent.

DART 9 - Scandisk Execution

DART 9 detects the execution of the Microsoft Scandiskw (the version of Scandisk running under Windows) program and reports its completion.

DART 10 – Scandisk dialog box creation

DART 10 detects and reports the content of the Microsoft Scandiskw (the version of Scandisk running under Windows) program completion dialog box and any dialog boxes displayed by the Scandisk program during its execution.

DART 12 - Symantec Virus Definition Management

DART 12 manages the Symantec virus definitions on all systems where it is enabled and configured accordingly. It ensures that at all times, all systems where it is enabled and configured accordingly, at the very least, will have the newest virus definitions available on each sub-net.

DART 12 accomplishes this goal by looking for the newest possible virus definitions in the following locations:

- Other systems on the same sub-net
- The location(s) of Norton Anti Virus on-site server(s)
- Symantec's site, using the LiveUpdate program

The above options for updating a system's Symantec virus definitions can be used independently, or in conjunction with each other. If they are used together, DART 12 executes each option in the order listed above.

DART 12 also automatically notifies you when The Symantec virus definitions are out of date for a period of time longer than the value of the **Maximum age of virus definitions in days** DART configuration parameter.

Whenever it runs, DART 12 automatically reports the Symantec virus definition dates from all systems on the sub-net. If so configured, DART 12 will also report if Norton Anti Virus is either not installed correctly or not at all on the system where the DART runs.

DART 13 – Virus Scan Dialog Box Creation

DART 13 detects and reports messages issued by the Norton Anti Virus program during its execution.

DART 14 – MS Internet Account Dialog Box Creation

DART 14 detects and reports user access to the Microsoft Internet Account Wizard.

DART 15 - Anti Virus Scan Execution

DART 15 initiates the silent execution of the Norton Anti Virus program and reports its completion.

If so configured, DART 15 will also report if Norton Anti Virus is either not installed correctly or not at all on the system where the DART runs.

DART 16 – File / Folder Deletion Dialog Box Creation

DART 16 detects and reports a user's attempt to delete MS Internet Explorer-related history or cookie files.

It does not report whether the attempted deletion was completed or the user chose to cancel the operation.

DART 16 will not detect an attempted deletion of the entire Internet Explorer History or Cookie folders located in the MS Windows directory. It would be detected by DART 21.

This DART is triggered by one of the following actions:

- Attempted deletion of an Internet Explorer history file located in the folder \Windows\History accessed directly either through "My Computer" or Windows Explorer.
- Attempted deletion of an Internet Explorer history file accessed through Internet Explorer, by clicking on **View, Explorer Bar, History**, or by clicking on the **History** icon on the Internet Explorer toolbar.
- Attempted deletion of an Internet Explorer cookie file accessed through Internet Explorer, by clicking on **Tools, Internet Options, Settings**, in the Temporary Internet Files section, and **View Files**.

DART 17 – Executable Detected

DART 17 detects and reports the execution of programs included in the **Executables to detect** list in its configuration file.

In some cases, executables whose execution you may want to detect are entered as parameters in the command line of a script or another executable.

For this reason, you can also enter the name of the executable in the **Command Line arguments to detect** list in DART 17's configuration file.

Note that Command Line arguments to detect entries don't have to be executables. You could use this parameter to enter any sequence of characters in the command line of an executable you want the DART to detect.

DART 18 - ReSOFT Client Shut-down / Re-start

DART 18 automatically shuts down and, optionally, restarts all the Automated Support Infrastructure clients in the local network.

DART 19 - Disk Defragmenter for MS Windows 9x and Me Execution

DART 19 executes the program Microsoft Disk Defragmenter on systems running the Microsoft Windows 9x or Me operating systems, and reports its completion status.

DART 20 - Disk Defragmenter Dialog Box Creation

DART 20 detects and reports the content of the Microsoft Disk Defragmenter program completion dialog box and any dialog boxes displayed by Disk Defragmenter program during its execution.

DART 21 - File / Folder Deletion Dialog Box Creation

DART 21 detects and reports a user's attempt to delete a file.

DART 24 - Silent.log Check

When an automated client update is performed, the installation is run in "silent" mode. If it encounters any errors or problems, it writes some diagnostic information in the file "silent.log" in the client directory. DART 24 looks for the "silent.log" file, and if it finds, sends the content of this file as part of a log. This is very useful for diagnosing problems that arise from the installation in a client update.

DART 26 – Executable Usage Profiler

DART 26 monitors the programs executed on a system on the local network from the time it was first enabled.

The list of the processes compiled by DART 26 can be used to identify changes in a system's configuration brought about by the installation of applications that don't use common installation executables.

This list would also be useful in identifying and analyzing system usage patterns.

The first time execution of a program is detected by DART 26, an event is logged on the log database. Another log of the execution of this program is recorded on the log database if its execution takes place more than 30 days since the last time it was executed.

The entry for a program in the list of executables maintained by DART 26 contains the last time execution of the program was detected by the DART.

At any time, while DART 26 is enabled, you can also get a complete list of the programs being tracked by this DART by enabling the **Dump process execution history** parameter.

DART 27 - System Start-up Environment Control

Overview

Managing and controlling system start-up helps minimize

- Slower system boot-up
- Ongoing startup performance problems
- Unwanted intrusion, and potentially even harm to the system
- Slower system performance
- ReSOFT features complete system start-up environment management and control.

We have two DARTs that perform these functions:

- DART 27 to control the content of a system's start-up environment. Depending on its configuration, it accepts, rejects, or disables any attempt to

add a new item to a system's start-up environment. If so configured, it performs all actions automatically. DART 27 can also prevent the removal of items from a system's start-up environment. In this way it neutralizes attempts to remove intrusion protection software such as virus scanners from running at system start-up.

- ▶ DART 233 to manage a system's start-up environment. DART 233 reports the content of a system's start-up environment, and disabled start-up items. It also lets you easily enable and disable start-up items on one, some, or all systems at a site.

Triggering and detection

DART 27 is triggered by changes to the relevant registry keys and file folders. These are registry keys and file folders that are used to control which applications are run when the system starts. When these are changed, the DART runs, examines their contents to see what has changed, and takes action to allow, disable, or remove a start-up environment change based on its configuration.

Due to a limitation in Microsoft Windows 95, DART 27 cannot be triggered by registry key changes on that operating system. Because of that limitation, and in order to avoid missing a change when the client is not running, the DART also runs at system startup, and whenever the ReSOFT client starts.

DART 27 also monitors, and lets you disable or remove pending file rename operations, which execute at system start-up. Operating system files that are loaded at system startup can't be deleted, replaced, or renamed when the operating system is running because it locks them. Pending file rename operations provide a mechanism to delete, replace, or rename these files by executing the action at system start-up before the files get loaded by the operating system. This mechanism can be exploited by someone with malicious intent.

DART 27 can also prevent the removal of items from a system's start-up environment. In this way it neutralizes attempts to remove intrusion protection software such as virus scanners from running at system start-up.

Actions

DART 27 monitors all mechanisms that can be used to run programs at startup. The areas protected include the Startup folder, the win.ini file, the system.ini file, and the registry keys described in <http://support.microsoft.com/default.aspx?scid=KB;en-us;q13736> and <http://support.microsoft.com/default.aspx?scid=kb;EN-US;314866>

Note that the DART does not monitor the "run once" keys, since those are primarily used for system operations, and will not cause changes that permanently affect system performance.

Whenever the list of items in any one of these locations changes; the DART notifies the support provider by posting an event log on the ReSOFT server. In addition, it can take one or more of the following actions:

- Delete the item from the start-up environment so that it will no longer run at startup
- Disable the item by moving it to a "holding area"
- Ask the system's user whether or not to delete/disable the item, if the user interface configuration option is enabled
- Prevent removal of an item from the system's start-up environment
- Do none of the above

Similarly, when DART 27 detects an attempt to add a pending file rename operation, it can automatically disable it, delete it, or ignore it. If the user interface option is enabled, the end-user has control over which of these actions should be taken.

Note that DART 27 will always log the detection of a new start-up item, the removal of an item from a system's start-up environment, or the addition of a pending file rename operation on the ReSOFT server, even if it is configured to do nothing to prevent these changes from taking place.

DART 38 – Fault Detected

DART 38 detects and reports faults. It provides detailed information about processes running on the system at the time of the fault. DART 38's output also includes the User Action Log (UAL).

The UAL contains a description of a user's 50 actions that preceded a fault. It captures a number of different types of actions, including:

- ➔ Running a program
- ➔ Dialog box creation
- ➔ Clicking on a button
- ➔ Selecting a menu item
- ➔ Entering text in a text box
- ➔ Shifting focus of top level window

It should be noted that the current version of DART 38 does not detect Microsoft Windows kernel faults, the ones that generate a blue screen.

DART 42 - Password Lockout Resolution

DART 42 detects and automatically resolves password lockout situations on systems running Microsoft Windows NT4, 2000, or XP operating system, and **Courion's Password Courier Direct** application.

DART 43 – ReSOFT Client Tools

DART 43 performs five functions:

- ➔ ReSOFT client configuration

Via the DART 43 configuration page you can change all ReSOFT client configuration parameters including the user id and password used to access the DART configurator directly, on a system-by-system basis. This means that security policies for accessing the DART configurator can match those you use for your organization as a whole.

DART 43 lets you also change the name of a site. We strongly advise against doing this because it would be difficult for you to maintain uniformity of site name particularly where systems belonging to a site are distributed across multiple local networks over a widely distributed area, or simply consist of remotely connected and/or mobile systems.

Additional complexity comes from having to make sure that when you change the name of the site via DART 43, the site parameter is set to **global**, or **local**, as needed, otherwise you would end up with systems reporting incorrect site information.

If you want to change the name of a site, the easiest and simplest way to do it is to change the site's name in its profile on the ReSOFT installation management facility. Doing it this way, avoids all the issues described in the two paragraphs above.

Please refer to the DART 43 configuration help files for a detailed description of all ReSOFT client configuration parameters, and instructions on how to change them, if necessary.

➤ Impersonation management

On NT based systems (MS Windows NT4, 2000, XP, and Server 2003) the ReSOFT client is logged in as local system administrator. This means that it cannot access shared resources on the local network.

In order to enable ReSOFT client's access to shared resources on the local network, we have implemented impersonation. Impersonation lets the ReSOFT client log onto the system where the shared resource is located as a user known by that system enabling it to access that shared resource.

You manage a site's impersonation settings including user id, password, and domain, if one is needed, via the impersonation parameters in the DART 43 configuration page.

➤ Network driver management

There may be circumstances when you might want to disable use of the ReSOFT network driver on a sub-net, either for troubleshooting, or because it may not be needed. DART 43 gives you the option to easily enable/disable, or remove the ReSOFT network driver. After you remove the ReSOFT network driver, if you decide to re-install it, this is easily accomplished with the click of a button on the DART 43 configuration page.

➤ ReSOFT client diagnostic information management

By simply checking boxes for the diagnostic information you need, and clicking on a few buttons, DART 43 will deliver to the ReSOFT server in-

depth diagnostic and error trace information from one, some, or all systems at a site. The diagnostic information logs produced include:

- Dumps of information related to the operation of the ReSOFT Client. Dumps produced are:
 - **Comm Dump:** A list a recent network communications between clients and or the server.
 - **Alist Dump:** A list of recent calls to add and remove machines from the client machine list.
 - **Sync Dump:** A list of sync objects in use. Used in client resource management.
 - **DART Dump:** A list of recently executed DARTs, DARTs currently being executed, and DARTs waiting to be run.
 - **Timer Dump:** A list of DARTs in the timer queue scheduled to be run.
- Error log files

DART 43 posts dumps and error log files onto the event log database on the ReSOFT server as SSL HTTP logs sent via port 80. Alternatively, it can also send dumps and error log files via e-mail.

➤ ReSOFT client uninstall

DART 43 lets you remove the ReSOFT Client from the system where the DART 43 configuration page is being accessed. Removal can be silent. ReSOFT client uninstall is not a site wide operation. This minimizes the risk of unintentionally removing the ReSOFT client from an entire site.

DART 45 - Port Probe Detected

When enabled, DART 45 monitors all IP ports on a system where the ReSOFT client is running.

It detects and reports any attempt by a device, whether on the local or other network, to open a TCP connection that is rejected by the local system because there is no process listening on that port.

Usually that indicates a "probe" or a "port scan" that could be the prelude to an unwanted intrusion.

DART 46 - Error Dialog Box Creation

DART 46 detects error dialog boxes and reports their content.

DART 47 - Warning Dialog Box Creation

DART 47 detects warning dialog boxes and reports their content.

DART 48 - Information Dialog Box Creation

DART 48 detects information dialog boxes and reports their content.

DART 49 - Question Dialog Box Creation

DART 49 detects question dialog boxes and reports their content.

DART 50 - Process Creation Detected

DART 50 detects and reports creation of a process.

DART 51 - Process Completion Detected

DART 51 detects and reports completion of a process.

DART 60, 217, 218, 219, 220, 221 - Clean Folders

DART 60 deletes files and directories specified in the DART's configuration page. All the configuration settings for DART 60 can be changed including file mask, locations, deletion of read-only files, and minimum age of files to be deleted. Its default settings are:

- Locations scanned: Those matching the TEMP environment variable
- Search criteria: [~*.~] [*.tmp] [\$.~]
- Removal criteria: older than 14 Days, 0 Hours, 0 Minutes, 0 Seconds
- Read-only files matching search criteria and aging criteria are not deleted

DART 61 – System Survey

DART 61 performs a detailed system hardware, software and configuration survey. It runs automatically after the ReSOFT Client is installed or updated on a system, and can be executed on a schedule, or on demand.

Information collected by DART 61 includes:

- BIOS information including serial number(s), service tag number, and other detailed hardware
- information
- Disk drive capacity and capacity utilization information
- Software version and license information
- Support and operations related information:
 - Detailed networking configuration information
 - Start-up environment information
 - E-mail client configuration information
 - Browser configuration information
 - Other application configuration information

DART 62 - Scandisk Files Clean-up on MS Windows 9x / Windows Me Systems

DART 62 deletes files created when Microsoft Scandisk finds an error on a drive and attempts to recover data before repairing the error. Its default parameters are:

- Location scanned: Root directory on all local drives
- Search criteria: file?????.chk
- Removal criteria: Older than 14 Days, 0 Hours, 0 Minutes, 0 Seconds

The value of the removal criteria parameter can be changed using the DART configuration module. All other parameters are fixed.

DART 63 – ReSOFT Client Start-up

DART 63 detects and reports start-up of the ReSOFT client. It can be used as an indicator of system start-up.

DART 64 – ReSOFT Client Shut-down

DART 64 detects and reports shut down of the ReSOFT client. It can be used as an indicator of system shut-down.

DART 65 – Traceback Information on Client Internal Error

DART 65 detects Client internal errors and logs traceback information in a text file that is uploaded to the log database.

DART 68 - User Has Changed System Date and Time

DART 68 detect and reports a user-produced change of system date and/or time. It takes no corrective action automatically because it does not presume that the change in system date and/or time was unintentional.

However, if the user interface feature is enabled when a user changes the system date and/or time, a dialog box will pop up listing the original and new time and date, and asking:

"Did you mean to change the time?"

Seeking a **Yes/No** response.

If the user interface is not enabled, DART 68 will detect the date/time change but will not take any action to reset it.

DART 68 also compares the time zone of the system on which it was triggered with that of the other systems on the local network where the ReSOFT client is active reporting any discrepancy and listing each system with its time zone.

DART 68 detects date/time changes of more than five hours. Any date/time change of five hours or less will be ignored.

Please note that DART 68 is triggered when a user accesses the calendar on his/her system by double-clicking on the time display at the lower right-hand corner of the system's desktop. When this happens DART 68 will report any date and/or time discrepancy, as discussed above, and time zone differences among systems on the local network.

This means that even if the user does not change the time or date on his/her system, if there are differences in time zones among systems on the local network, DART 68 will report these differences as long as they persist.

DART 69 - Chkdsk Files Clean-up on MS Windows NT4 / Windows 2000 Systems

DART 69 deletes files created when Chkdsk finds an error on a drive and attempts to recover data before repairing the error.

For every fixed disk drive in the system, DART 69 looks in the root directory for directories that match the mask "found.???". This is where Windows NT places any files produced by Chkdsk. It names these directories found.001, found.002, and so on, for the different runs of Chkdsk.

Inside the "found.???" directories, DART 69 selects files that match the "file*.chk" mask and directories that match "dir*.chk" mask.

Inside the "dir*.chk" directories, it examines all files and directories. It deletes any file that is as old as or older than the number of days entered in its configuration file. The default value of the removal criteria is 14 days. This means that DART 69 deletes any selected file that is at least 14 days old.

When it examines a directory, it checks to see if it is old enough. If it is, then it recursively descends into the directory and looks at everything inside it. If it ends up deleting everything inside the directory, then it also deletes that directory.

The value of the removal criteria parameter can be changed using the DART configuration module. The file and directory selection masks are fixed.

DART 70 – Software Installation Detected

DART 70 detects and reports software installations that take place on systems on which it is installed. The default values for the file masks used by DART 70 to detect installation of a software program are:

- ➔ _ins????_mp
- ➔ *setup*.exe
- ➔ appinst.exe
- ➔ ReSOFTnstal.exe
- ➔ inst*.exe
- ➔ load.exe
- ➔ run.exe
- ➔ startup.exe
- ➔ startwin.exe
- ➔ tuavinst.exe
- ➔ wininst.exe

- ➔ winload.exe
- ➔ winstart.exe
- ➔ wintst.exe
- ➔ wksbinst.exe
- ➔ msexec.exe
- ➔ Uedit32i.exe

The file masks can be changed using the DART configurator.

Once triggered, DART 70 checks the Microsoft registry for changes before reporting a successful software installation.

DART 71 – Software Removal Detected

DART 71 detects and reports the removal of software applications that when installed were registered and appear in the window of the Install/Uninstall tab of the Add/Remove Program Properties panel. This DART is triggered when the Client detects the execution of software removal programs that match the following masks:

- ➔ isuninst.exe
- ➔ uninst*.exe
- ➔ unwise*.exe
- ➔ msexec.exe

Once triggered, DART 71 checks the Microsoft registry for changes before reporting a successful software removal.

DART 72 – Scandisk Log Produced at Start-up Found

DART 72 detects and reports the content of log files produced by Microsoft Scandisk when executed at system start-up.

Typically these log files are produced as a direct consequence of an abnormal system shutdown.

DART 73 - System Restart

DART 73 can:

- Shut down, and then re-start a system.
- Shut down all processes running in the logon session of the process that called the ExitWindowsEx function, and then log the user off.
- Shut down a system, and turn off the power. The system must support, and have enabled the power-off feature.
- Shut down the system and then restart it, as well as any applications that have been registered for restart using the RegisterApplicationsRestart function.
- Shut down a system to a point at which it is safe to turn off the power. All file buffers have been flushed to disk, and all running processes have stopped.

DART 73 can perform the above functions on demand, or as scheduled through the DART configurator.

Before re-starting a system, DART 73 gracefully terminates execution of all processes listed in the DART's **Names of processes to shutdown** parameter.

DART 74 – Printer Added / Removed

DART 74 detects and reports the addition or removal of a printer.

DART 76 – Netscape Preferences Dialog Box Creation

DART 76 detects and reports user access to the Netscape Preferences module. It does not report whether the user actually made a change in his/her Netscape preferences.

DART 77 – Windows Event Log Change Detected

DART 77 detects and reports the addition of event logs to the Application, System and Security logs maintained on systems running Microsoft Windows NT4, 2000, or XP operating system.

You can use DART 77 to also monitor any custom logs that you may have created. To do this, you would simply add the name of the custom log you want this DART to monitor to the **Event logs to monitor for changes** list in the DART's configuration page.

DART 79 – Eudora Mail Preferences Dialog Box Creation Detected

DART 79 detects and reports user access to the Eudora Mail Preferences module. It does not report whether the user actually made a change in his/her Eudora Mail preferences.

DART 80 – Pegasus Mail Preferences Dialog Box Creation Detected

DART 80 detects and reports user access to the Pegasus Mail Preferences module. It does not report whether the user actually made a change in his/her Pegasus Mail preferences.

DART 84 – Network Connectivity Status

DART 84 detects any failure of a system's connection to the local sub-net. This DART can also be configured to notify the user when his/her system's connection to the local network fails, and when it is restored.

DART 86 - Synchronization of System Clock with Time Server

DART 86 synchronizes a system's clock in one of two ways:

- Using HCP from the system where the ReSOFT log server is located (this is the default option)
- Accessing a certified time server on the Internet. It uses port 37 to access the following time servers to adjust a system's clock:

- time.nist.gov
- time-a.nist.gov
- time-nw.nist.gov
- ntp2.usno.navy.mil

In case of failure to reach the first time server on the list above, it will attempt to reach the others in sequential order (i.e. 2nd, 3rd, etc., etc.)

If none of the time servers is available, the synchronization operation will be attempted again the next time DART 86 is scheduled to run.

You can modify the list of time servers used by DART 86, adding or deleting time servers.

DART 87 - Difference between System and Time Server Clock Exceeds Configured Threshold since Last Checked Twelve Hours Ago

DART 87 detects and reports the difference between a System's clock and an Internet time server's clock when it exceeds 15 minutes during the 12 hours since it was last executed.

In order to determine whether a system's clock is slow, DART 87 retrieves atomic time in one of two ways:

- Using HCP from the system where the ReSOFT log server is located (this is the default option)
- Accessing a certified time server on the Internet. It uses port 37 to access the following time servers to adjust a system's clock:
 - time.nist.gov
 - time-a.nist.gov
 - time-nw.nist.gov
 - ntp2.usno.navy.mil

In case of failure to reach the first time server on the list above, it will attempt to reach the others in sequential order (i.e. 2nd, 3rd, etc., etc.)

If none of the time servers is available, the synchronization operation will be attempted again the next time DART 87 is scheduled to run.

You can modify the list of time servers used by DART 87, adding or deleting time servers.

The number of minutes used by DART 87 to determine whether a system clock is slow or not, is a configurable parameter.

If the time reported by a system's clock is slower than the atomic time retrieved by DART 87 by a number of minutes greater than or equal to the value of the *Minimum difference (minutes)* to report parameter, DART 87 will reset the system's clock to match the atomic time.

DART 88 – Network Devices and Services Availability

DART 88 can be used to monitor the availability of all TCP/IP devices and services accessible from the local network

This DART generates a log only when a device or service it is configured to monitor fails to respond.

DART 88 supports ICMP and TCP/IP. The availability of devices you wish to monitor can be tested from one or more systems on the network eliminating dependence on a single point for monitoring network availability.

DART 89, 151-155, and 212-215 - Scheduled Program Execution

DART 89 executes the program entered in its configuration file on the schedule defined in the DART's schedule entry in its configuration file. You can enter just the executable name (ftp.exe) or a specified path (C:\download\internet\ftp.exe), and any combination of command line parameters allowed by the program you want to execute.

If the file name does not contain a directory path, the system searches for the executable file in the following sequence:

- The directory from which the application loaded

- The current directory for the parent process
- Windows 95/98: The Windows system directory using the GetSystemDirectory calls function to get the path of this directory.
- Windows NT/2000: The 32-bit Windows system directory using the GetSystemDirectory function to get the path of this directory. The name of this directory is System32
- Windows NT/2000: The 16-bit Windows system directory. There is no Win32 function that obtains the path of this directory, but it is searched. The name of this directory is System
- The Windows directory using the GetWindowsDirectory function to get the path of this directory
- The directories that are listed in the PATH environment variable

MS-DOS commands can be executed by DART 89 using the command.com executable. For example, if you wanted to copy some files using the **copy** command, you would type:

```
Command /c copy <cr>
```

Note that using the **/c** option will close the MS-DOS window as soon as the command is completed.

DART 90 - McAfee Virus Definition Management

DART 90 manages the McAfee VirusScan virus definitions on all systems where it is enabled and configured accordingly. It ensures that at all times, all systems where it is enabled and configured accordingly, at the very least, will have the newest virus definitions available on each sub-net.

DART 90 accomplishes this goal by looking for the newest possible virus definitions in the following locations:

- Other systems on the same sub-net
- The location(s) of McAfee VirusScan on-site server(s)
- Symantec's site, using the LiveUpdate program

The above options for updating a system's McAfee VirusScan virus definitions can be used independently, or in conjunction with each other. If they are used together, DART 90 executes each option in the order listed above.

DART 90 also automatically notifies you when The McAfee VirusScan virus definitions are out of date for a period of time longer than the value of the **Maximum age of virus definitions in days** DART configuration parameter.

Whenever it runs, DART 90 automatically reports the McAfee VirusScan virus definition dates from all systems on the sub-net.

If so configured, DART 90 will also report whether McAfee VirusScan is either not installed correctly or not at all on the system where the DART runs.

This DART can be configured to update the VirusScan virus definition database, or the virus database and the VirusScan software itself.

DART 92 - Disk Defragmenter for MS Windows NT, 2000 and XP Execution

DART 92 executes the program disk defragmenter on systems running the Microsoft Windows NT4 or 2000 operating systems, and reports its completion status.

DART 93 - Report running processes

DART 93 detects and logs on demand all the processes running on one of the systems on the local network.

DART 94 - Dialog Box Creation

DART 94 detects dialog boxes and reports their content.

DART 95 – Logical Disk Statistics

DART 95 reports the following logical disk (drive letters) statistics:

- Total disk space (Kbytes)
- Used (Kbytes)
- Percentage used (%)
- (Kbytes)
- Percentage free (%)

Note that all of these statistics are an instantaneous sample taken at the time the DART is run.

DART can be used to alert about high disk capacity utilization conditions thus averting problems that could cripple a system.

You can set a minimum free disk space threshold. If disk capacity falls below this threshold, DART 95 will instantly generate a log and send it to the log server where appropriately set notifications will generate an e-mail message for the designated support provider contact.

DART 96 – Processor Statistics

DART 96 reports processor statistics. Some of these statistics are available for both Windows NT (NT4, 2000, and XP) and Windows 9x (Windows 95/98/Me), and some are only available for Windows NT.

On both Windows NT and Windows 9x, the following statistic is reported:

- Processor utilization (%)
- On Windows NT only, the following statistics are reported:
 - Interrupt rate (per second)
 - Average queue length (items)

Note that all of these statistics must be averaged over a specific time period called Sampling Period. That time period is fixed for Windows 9x. For the Windows NT version, it's one of DART 96's configuration parameters.

DART 97 – Physical Disk Statistics

DART 97 reports physical disk statistics. These statistics are available only for Windows NT (NT4, 2000, and XP) systems. For each physical disk, the following statistics are reported:

- Percent busy time (%)
- Reads (per second)
- Writes (per second)
- Average queue length (items)

Note that all of these statistics must be averaged over a specific time period called the Sampling Period. That time period (in mSec) is one of DART 97's configuration parameters.

DART 98 – Network Statistics

DART 98 reports Network statistics. These statistics are available only for Windows NT (NT4, 2000, and XP) systems. For the entire local network, the following statistics are reported:

- Network utilization (%)
- For each network adapter, the following statistics are reported:
 - Bytes sent (per second)
 - Bytes received (per second)

Note that all of these statistics must be averaged over a specific time period called the Sampling Period. That time period (in mSec) is one of DART 98's configuration parameters.

DART 100 - File Distribution and Retrieval

DART 100 lets you retrieve and send any number of files, from anywhere on any system where the ReSOFT client is installed and running, to the e-mail box (es) identified in the **Email address group definitions** parameter in the DART's configuration page, or to the default e-mail address group as defined in the ReSOFT client initialization file.

Optionally, you can also select files to be retrieve based on their content matching one or more keywords contained in the **Keyword group definitions** parameter.

If the **Retrieve file by date** option is enabled, DART 100 will retrieve only files that match the files masks, and keywords, if any, and have a **Modified** date later than the date you set in the DART configuration.

DART 100 is also a powerful, yet simple, file distribution tool. If you want to distribute one ore more files, to one or more locations on one, some, or all systems at your site(s), all you need to do is use a location group instead of an e-mail group in the command line used by the DART.

You can easily and quickly define as many location groups as you like directly in the **File distribution. File location group definitions** on the DART 100 configuration page.

For each file retrieval and distribution operation, DART 100 generates one event log that summarizes the entire operation, listing all files retrieved based on the user defined criteria (Figure 1 below), and one event log for each individual file retrieval operation (Figure 2).

DART 101 – Printer Installation and Removal

DART 101 automates the following printer related system management tasks:

- Make a newly installed printer available (i.e. install the appropriate drivers and set up the needed port) to one, a subset, or all systems on a sub-net
- Make one, some or all printers on a sub-net available (i.e. install the appropriate drivers and set up the needed ports) to a newly installed system on the sub-net

- Remove a printer from the list of installed printers on systems on a sub-net when the printer is removed (physically or simply not made available to users any longer) from the sub-net
- Change the printers that are available (i.e. the appropriate driver is installed and needed port is set up) to one, some, or all systems on a sub-net

DART 111 - HandsFree Client Network Deployment

DART 111 automatically installs the ReSOFT client on all systems on the sub-net where the system on which DART 111 ran is located.

Whenever it runs, DART 111 either runs a networks survey (the first time it runs), or updates a network survey. Please note that you can also run the network survey action independently of the ReSOFT client deployment action by clicking on the Run network survey now Execute button in the DART's configuration page.

Whenever it runs, DART 111 generates a log reporting the actions it took and the contents of the survey of all network devices for which it found information in the system's ARP table, including additional information it retrieves from the devices directly.

HandsFree client network deployment function restrictions

DART 111 works on systems running a version of the Microsoft Windows 2000, XP, Server 2003, and Vista operating systems.

At locations where systems are running a version of the Microsoft Windows XP operating system, the HandsFree client network deployment function (DART 111) works if:

- Systems are in a domain
- File and print sharing is enabled

Please note the above restrictions apply only to systems running Microsoft Windows XP.

On sub-nets where systems running Microsoft Windows XP are not in a domain, in order for the HandsFree Client network deployment function to work, the following conditions must be met:

- Simple file sharing is disabled
- The Microsoft XP firewall is configured to allow file and print sharing

In addition to the above, In order to use the HandsFree client network deployment, you will need to provide a user name and password for an administrative account that works on all systems on the sub-net. If this is a domain account, you will also need to provide the domain name for the account. You will also need to check and make sure that the system you run the HandsFree network deployment function on is a member of the domain where you want to install the ReSOFT client.

Network survey output explained

For each system on the sub-net where the system on which DART 111 runs is located, DART 111 will report information as in the following example:

Name: MNMS

IP Address: 192.168.0.36

MAC Address: 00:20: AF: CD: 72:46

Time: 04/06/2007 13:40:38

Client: none

Testing for Network Share: \\MNMS\C\$\Program Files

Error: Bad network path.

Last changed from: 04/04/2007 12:32:56 to: 04/06/2007 13:40:38

Below, you will find an explanation of the content of the network survey produced by DART 111.

Name - NetBIOS name of the system surveyed IP address - IP address of system being surveyed

MAC address - MAC address of network interface card where the TCP/IP connection to the sub-net on the system being surveyed is enabled and active.

Time - The time at which the system being surveyed (in this example MNMS) was seen by the ReSOFT client. The time field reports when the machine was added to the ARP table of the system where DART 111 ran. When the ReSOFT client re-starts, it re-detects the ARP table. At that time, it re-detects the machine again, and sets the new time in its ARP table copy. The information in the log reports this change in time.

Client - The version of the client if it can be acquired at the time of the survey.

Testing for Network Share - The ReSOFT client looks for the "Programs Files" directory on available network shares. This field shows the path that the ReSOFT client used when it checked for the "Program Files" directory.

The result of network share test can be:

- **Directory exists.** or
- **Error:** followed by one of the following error messages:

Error: Directory does not exist.

The ReSOFT client was able to access the network share but the directory didn't exist. In this case the ReSOFT client will attempt to test network share D\$\ etc...

Error: Bad network path.

This error occurs when:

- The system being surveyed is turned off.
- The system being surveyed doesn't have Microsoft Windows installed.
- When a firewall is blocking file and printer sharing.

Error: Bad network password.

This error is reported when the password entered for the administrative user does not work.

Error: Access denied.

Typically, this error is reported when one or more of the following is true:

- "Simple file sharing" is enabled on the system being surveyed
- The administrative user account whose credentials you have entered does not exist
- File and print sharing for Microsoft networks is not enabled
- The file and print sharing exception in the Microsoft XP firewall has not been enabled.

Error: Bad network name.

This error occurs when the network share has been removed from the system being surveyed.

The network request is not supported

This error occurs when the device contacted by DART 111 although it is a valid IP device does not appear to run an operating system which supports the system access request performed by DART 111.

Logon failure: unknown user name or bad password.

This error is reported when the administrative user credentials either are incorrect, or the administrative user whose credentials you have entered is not active on the system being surveyed.

Network changes

After you trigger execution of the HandsFree client network deployment function (DART 111) either by using the **/DEPLOY=1** ReSOFT client installation executable command line option, or on demand by clicking on the Begin auto deploy Execute button in the DART 111 configuration page, the DART will run once, execute a network survey and beginning the ReSOFT client installation on systems in the sub-net.

After the initial execution, DART 111 will run every time a new device is added to the ARP table on the system where DART execution was triggered.

If you change the configuration of the network where you ran the HandsFree network deployment function in a way which you think may affect the ReSOFT client deployment,

you should run the HandsFree client network deployment function again on demand by clicking on the Begin auto deploy Execute button in the DART 111 configuration page.

When DART 111 runs a second time, it will update the network survey, and report changes it finds with messages such as the following:

➤ **Version installed changed from: 2.004.026.0177.00 to: 2.004.026.0182.00**

Or

➤ **NetBIOS name changed from: 192.168.0.116 to: AWIN**

The two messages above are examples of changes in the network environment reported by DART 111. In the first case the ReSOFT client was upgraded. In the second case DART 111 was able to resolve 192.168.0.116 to AWIN, the NetBIOS name of the system being surveyed.

Here is another example of the kinds of changes reported by DART 111 when it runs. On the system listed below the ReSOFT client was removed, and the system was re-started. When DART 111 ran the network survey after the ReSOFT client was removed from the system, it detected the fact that the ReSOFT client was removed, and that the DHCP server assigned a new IP address.

IP address changed from: 192.168.0.90 to: 192.168.0.125

Last changed from: 04/06/2007 13:28:58 to: 04/09/2007 09:10:52

NetBIOS name changed from: WXP-9QMN331 to: 192.168.0.125

Installed status changed from: 1 to: FALSE

Version installed changed from: 2.004.026.0176.00 to: none

DART 156 – Sequential Scheduled Program Execution

DART 156 executes multiple command line(s) entered in the “Executable” sequentially.

DART 156 executes the program entered in its configuration file on the schedule defined in the DART's schedule entry in its configuration file. You can enter just the executable name

(ftp.exe) or a specified path (C:\download\internet\ftp.exe), and any combination of command line parameters allowed by the program you want to execute.

If the file name does not contain a directory path, the system searches for the executable file in the following sequence:

- The directory from which the application loaded
- The current directory for the parent process
- Windows 95/98: The Windows system directory using the GetSystemDirectory calls function to get the path of this directory.
- Windows NT/2000: The 32-bit Windows system directory using the GetSystemDirectory function to get the path of this directory. The name of this directory is System32
- Windows NT/2000: The 16-bit Windows system directory. There is no Win32 function that obtains the path of this directory, but it is searched. The name of this directory is System
- The Windows directory using the GetWindowsDirectory function to get the path of this directory
- The directories that are listed in the PATH environment variable

MS-DOS commands can be executed by DART 156 using the command.com executable. For example, if you wanted to copy some files using the **copy** command, you would type:

```
Command /c copy <cr>
```

Note that using the **/c** option will close the MS-DOS window as soon as the command is completed.

DART 157 – System Restore Point

DART 157 (System Restore Point) creates a system restore point by name “HFN Restore Point”.

DART 160 - Registry Management

DART 160 (Registry Management) executes the registry management actions you configure on the ReSOFT server via the registry management console

[\[https://ReSOFTservername/main/regmgmt/rmgt.php\]](https://ReSOFTservername/main/regmgmt/rmgt.php). You can:

- Retrieve any portion of the registry from one, some, or all systems
- Add multiple registry keys to one, some, or all systems
- Change registry key content for multiple registry keys at the same time on one, some, or all systems
- Delete multiple registry keys simultaneously from one, some, or all systems.

DART 160 can run on demand, or on a schedule.

For more information about the ReSOFT registry management function please consult the online help file found at:

How to >>> Registry management -

<https://ReSOFTservername/main/howto/HFN%20ReSOFT%20registry%20management%20main%20help%20page.html>

DART 161 - Registry Protection Management

Overview

DART 161 is a powerful intrusion protection tool that also automatically performs a useful problem resolution function.

It lets you monitor registry keys on one, some, or all systems at a site, detect changes, and prevent them if configured to do so.

DART 161 Operations

You can configure DART 161 to monitor registry keys continuously, in which case the DART will detect changes to directories and files as they happen, or on a schedule, in which case it will check them at the time you define in the DART's configuration parameter.

If you enable DART 161's change prevention function, the DART will make a copy of the registry keys that you want to prevent from being changed, and store all the other relevant information. If you choose to protect a registry branch, it will copy the entire branch, and all its other relevant information.

DART 161 runs when one of the following events occurs:

- When the ReSOFT client starts up. When this happens it checks for changes
- When you click on the execute button to the right of the **Check monitored items now** label in the DART's configuration page. When this happens it checks for changes.
- At its scheduled time. When this happens it checks for changes
- When monitored item(s) change. When this happens it checks for changes.
- When one of its configuration parameter changes. When this happens it updates the configuration.
- When it is enabled/disabled. When this happens it updates the configuration.
- Checking for changes means - Determining if any files or directories have been removed, added or altered, and
- Updating the stored information about any item that has changed

Updating the configuration means updating the stored information about monitored item(s) to match their current state. If any existing stored information for monitored item(s) is still relevant, then it is re-used. If a new item is added, it means recording its information.

If DART 161 is configured to prevent changes, instead of updating the stored information about any item that has changed, it will restore the item to its pre-change state by overwriting the changed item with the copy that was stored when the item was first added to the **Monitored items** parameter as (part of) a command line.

This means that if a protected item is corrupted because of a system's software or hardware malfunction, and does not function properly any longer, if the ReSOFT client is operational, DART 161 will restore the protected item to its working state. In this scenario, the DART can be a useful automated problem resolution tool.

DART 164 - Email Attachment Filtering Log

DART 164 detects and logs all e-mail attachment filtering actions taken by DART 188.

The filtering of each file attached to a message generates a separate DART 164 log. For example, if an e-mail message has four attachments all of which are filtered based on the user configuration of DART 188, the filtering operation will generate four DART 164 logs.

DART 165 - File Download Filtering Log

DART 165 detects and logs all file download filtering actions taken by DART 189.

Each file download filtering action generates a DART 165 log.

DART 174 - User Logon-logoff Tracking

DART 174 is enabled by default. It detects and reports all user logon and logoff events.

DART 174 tracks and reports the amount of time a user is logged onto a system, and reports all information contained in the user profile.

When users shut down or re-start their systems, DART 174 will report the event as a logoff event when the system re-starts.

DART 175 - McAfee VirusScan Execution

DART 175 initiates the silent execution of the McAfee VirusScan program and reports its completion.

If so configured, DART 175 will also report if McAfee VirusScan is either not installed correctly or not at all on the system where the DART runs.

DART 176 - Service Restart

On systems running Microsoft Windows NT4, 2000, or XP operating system, DART 176 monitors services listed in the **Services** list on its configuration page, and re-starts them automatically if they stop running.

DART 176 can run on demand or on a recurring schedule.

DART 177 - DART Configuration Update

DART 177 retrieves DART configuration changes made using the server based ReSOFT site management facility, and propagates them to all systems on the local network.

Here is how it works:

- It makes a call to the server where the ReSOFT site management facility is located, passing it the client revision level, the PS revision level, the machine name, and the site name.
- The ReSOFT site management facility returns an indication of what to do. It will tell the client whether or not the client revision level and the PS revision level matches. After receiving this information, the ReSOFT client takes the following two steps, in order:
 - If the client revision level doesn't match, the ReSOFT client sends the DART templates to the ReSOFT site management facility.
 - If the PS revision level doesn't match, the ReSOFT client performs a DART configuration update operation retrieving the updated DART

configuration(s) from the ReSOFT site management facility and propagating it/them to all systems on the local network.

DART 178 – Microsoft Windows Networking Denied Access

DART 178 detects failure to access a shared resource on the network because access was denied. Typically, this happens when the wrong password is used to access the shared resource.

This DART can be a useful tool for detecting and tracking potentially unauthorized attempts to access a shared resource.

DART 178 is triggered on the system where the shared resource is located when it detects an **access denied** error code at the SMB protocol level.

DART 187 – Machine List Management

DART 187 reports the content of the Local Machines page accessed <http://localhost:2721>, on the system where the DART was executed.

DART 187 runs:

- When the ReSOFT client starts-up
- On demand, when a user clicks on one of the Execute buttons in the DART's configuration page

DART 188 -E-mail Attachment Filtering

DART 188 can be used to delete attachments from messages received on a system. You can enter the types of files you want DART 188 to delete using the DART configuration facility.

Attachments that are removed are replaced with a text file with the following content:

“The file attached to this message that was originally named “[file name]” has been removed due to the filtering policy set up by your system administrator.”

Because DART 188 operates on the system where the ReSOFT client is installed, it protects systems from potentially damaging attachments arriving from either POP based mail services, or Web based mail services (e.g. AOL Mail, Yahoo Mail, and Hotmail).

Local execution of DART 188 also makes it possible to customize attachment filtering policies on a system-by-system basis, or for subsets of systems.

DART 189 - File Download Filtering

DART 189 can be used to block downloading of files on a system. You can enter the types of files, or specific files, whose download you want DART 189 to prevent using the DART configuration facility.

Files whose download is prevented are replaced with a file whose name you enter in DART 189's configuration page.

If no such file name is entered, the file whose download was prevented is replaced with a file whose content is zeros.

It's important to note that DART 189 only replaces the content of the file whose download was blocked, not its name. Unless the end-user is informed on a timely basis that the file download filtering is enabled, this can lead to repeated attempts to download a file, and consequent frustration on the part of the end-user.

To minimize the potential for this to happen, we have included in the ReSOFT client directory a small program called block.exe (also in zipped form, block.zip) that when executed informs the end user about the file download blocking policy in effect with the following statement:

"Sorry, per company policy download of this file type is not allowed. Please contact your system administrator with any questions. Thank you."

You can use block.exe or block.zip as the files that replace blocked files when blocking files of type's .exe, or .zip, respectively.

DART 191 - TCP/IP Connectivity Problem Management

DART 191 detects, diagnoses, and manages the resolution of TCP/IP connectivity problems. Failure points covered by DART 191 include:

- Local connectivity
- Internet access gateway
- DNS server
- Target service port - DART 191 covers ALL TCP/IP ports / services

DART 191 uses the ReSOFT network driver to detect and diagnose TCP/IP connectivity problems on all ports, at a low level before they are detected by application software.

If the port of the service that failed is included in the User Interface enabled on failure of these ports list, DART 191 will inform the end-user about the problem with three dialog boxes:

- One dialog box that informs the user that a connectivity problem occurred
- A second dialog box that tells the end-user which problem occurred, and offers to notify him/her when the service is available again, and
- If the end-user clicked on the "OK" button in the second dialog box, a third dialog box that will notify the user that the failed service is back online.
- If the service that failed is not back online at the time of the last notification message, DART 191 will display a special message with instructions to the user on what he/she should do next that you specify when configuring DART 191.

You can configure DART 191 to exclude selected IP addresses and domains from user notification while still logging failure to access them. This function can be a powerful tool for identifying IP addresses and domains that may be accessed by a program that was installed without the end-user's knowledge (e.g. spyware, or other intrusion program).

DART 192 - Program execution control

DART 192 stops the execution of programs listed in the DART's configuration page. It has two modes of operation:

- Stop List (default)
- Run List

In **Stop List** mode, DART 192 will terminate the execution of any command line listed in its **Stop List**.

In **Run List** mode, DART 192 will only allow execution of programs listed in the **Run List** of commonly running programs and of programs entered manually by the user. The **Run List** of commonly running programs is created automatically from the list of processes running on the machine for which the DART is being configured.

DART 196 – Software Patch Application

DART 196 enables the automated application of software updates and patches on one, a subset, or all systems on the local network. This DART can be used to install or uninstall software updated and patches from any vendor.

Patches and software updates applied by DART 196 can be located on a shared network resource, an FTP Server, or Web server using HTTP or secure HTTP (the FTP server and Web server could be located on the same system as the ReSOFT server).

Patches and software updates can be applied selectively based on a system's operating system.

DART 196 automatically tracks the patches and software updates applied to each system. This means that:

- You have a readily accessible trace of the history of patches and software updates applied to each system in your network, and
- You don't have to actively manage the list of patches to apply on a system-by-system basis as DART 196 will automatically ignore an attempt to re-apply a patch or

software update to a system where it has already been installed, unless you want it to.

DART 197 – Network Configuration Change Detected

DART 197 detects and reports changes made to key components of a system's network configuration.

DART 197 detects and reports changes in a system's network configuration by monitoring the content of and reporting changes in a number of registry keys and all of their sub-keys.

The registry keys monitored by DART 197 on Microsoft Windows 9x and Me based systems are:

- HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\VxD\MSTCP
- HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Class\Net
- HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Class\NetClient
- HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Class\NetService
- HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Class\NetTrans

The registry keys monitored by DART 197 on Microsoft Windows NT4, 2000, and XP based systems are:

- HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\TcpIp
- HKEY_LOCAL_MACHINE\Software\Microsoft\WindowsNT\CurrentVersion\NetworkCards

DART 199 – Registry Change Detected

DART 199 detects and reports changes made to the registry. It covers all keys listed in the Registry **keys to monitor parameter** in the configuration entry for this DART, and their sub-keys.

Most changes made to applications' and the system's configuration and environment result in registry changes. This means that the registry changes frequently. To avoid generating a large volume of event logs, most of which are not very useful, it is important to be as specific as you possibly can when identifying the registry keys you would like DART 199 to monitor.

For example, if you want to monitor changes in Outlook Express account settings, it is probably more advisable to select the key for specific accounts.

```
HKEY_CURRENT_USER\Software\Microsoft\Internet Account  
Manager\Accounts\00000001,
```

Rather than the entire Internet Account Manager key
(HKEY_CURRENT_USER\Software\Microsoft\Internet Account Manager).

DART 207 - Content Distribution

DART 207 automates the distribution of content to all systems on a sub-net. By content distribution, we mean that this DART will automatically update one or more files on all systems on a sub-net to the latest version.

Latest version is determined by the latest *Last Modified* date of the files being distributed. DART 207 is designed to be easily extensible to base the determination of latest version on other parameters such as file version, file size, file creation date, and other file properties.

DART 207 leverages HandsFree Networks peer-to-peer architecture to deliver a very powerful content distribution and file synchronization mechanism minimizing bandwidth consumption, and requiring minimal configuration. For example, DART 100 (File Distribution and Retrieval) can be used to place the latest version of a file on one system on a sub-net. Then, DART 207 can be used to update that file on all systems on the same sub-net eliminating the need to go outside the sub-net (except for one system), and minimizing bandwidth consumption.

DART 208 - Software Update

The ReSOFT client uses DART 208 to retrieve software updates from the ReSOFT server.

When DART 208 is executed, it contacts the updates module in the ReSOFT site management facility identifying the site name, the system it originated from, and the version of the ReSOFT client running on that system.

In response to contact from DART 208, the updates module gives the DART an action code that determines which action the DART should take, the location of the software update executable, and command parameters to be used when running it.

Currently, the actions triggered by the action codes include:

- **0 - No update** - No action is taken. This can be the case when ReSOFT client from a new site contacts the updates module. In this case, new entries for the site and the system are added to the sites and machines lists, respectively, in the updates module. No action is taken also if no software update version is selected for the site the ReSOFT client is contacting the updates module from.
- **1 - Normal update** - A software update will be downloaded and installed automatically by the ReSOFT client if the software version number reported by the client and that associated with the site DART 208 originates from are different.
- **4 - Forced update** - You have the option to “force” the download and installation of a software update regardless of software version by selecting the force update option in a site’s machines configuration page on the updates module.

DART 211 - Disk Defragmenter Execution (MS Windows XP)

DART 211 executes the program disk defragmenter on systems running the Microsoft Windows XP operating system, and reports its completion status.

DART 216 - Print Queue Problem Resolution

Overview

The print queue problem resolution DART monitors print queues on systems that have an attached printer, or send jobs to be printed on a network printer. When the DART is enabled, it logs a system's printer configuration every time the ReSOFT client is restarted.

The DART performs two main tasks:

- Monitor print queues, detect all jobs being printed, and report their status
- Detect print jobs that are stuck in the process of being printed, stop the print queue, remove them, and re-start the print queue enabling other print jobs, if any, to be printed. Problem resolution is triggered when the maximum time that a job can be in the process of being printed, as set by IT personnel, is exceeded.

Automated print queue problem resolution

When the **Automated print queue problem resolution enabled** option is enabled, DART 216 will perform problem resolution whenever a job has been in the process of being printed for an amount of time equal, or in excess of the amount of time you specify in the **How long should the DART wait for a job to be in process before running automated problem resolution? (Enter time in minutes)** parameter.

Problem resolution takes place in three phases. Depending on the severity of the problem, the DART's actions escalate as follows:

- **Level I** - The DART detect the problem and uses spooler functionality to attempt to remove the job that's causing the problem from the queue while preserving the other jobs in the queue. The problem resolution steps carried out are:
 - Shut down of print spooler
 - Re-start of print spooler
- **Level II** - If Level I resolution does not resolve the problem, the DART performs the print job removal action directly, while still leaving untouched the other jobs in the queue. The problem resolution steps carried out are:
 - Shut down of print spooler
 - Deletion of job that has been in the process being printed for a time in excess of the number of minutes you specified in how long should the DART wait for a job to be in process before running automated problem resolution? (enter time in minutes)
 - Re-start of print spooler

- **Level III** - If the problem keeps recurring on the same queue, the DART restarts the system where the problem occurs (the problem may be caused by the print driver and restarting a system resolves most print driver related problems). Because this action, unlike the others, is very intrusive, level III problem resolution has to be explicitly enabled by IT personnel.

If it is enabled, before restarting the system, and the Third level problem resolution user interface enabled option is enabled, the DART will display a dialog box explaining to the user the reason for having to restart the system and asking the end-user to authorize system re-start via a yes/no dialog box. If the user clicks on the no button or ignores the dialog box, the DART will not restart the system. If the printing problem occurs again soon, the DART will once again ask the user for permission to restart the system. If the Third level problem resolution user interface enabled option is not enabled, DART 216 will perform third level problem resolution directly.

DART 222 – Report File Attributes

DART 222 reports the attributes of files and directories that match the mask specified in the DART's configuration page. All the configuration settings for DART 222 can be changed including file mask, and locations to be scanned. DART 222 reports the following attributes of a file:

- File Name
- File Version
- File Size
- File Creation Date
- File Last Modified

DART 222 reports also folder properties. However, you should keep in mind that the only directory properties are *Directory Name* and *Directory Creation Date*.

DART 225 - Directory and File Protection Management

Overview

DART 225 is a powerful intrusion protection tool that also automatically performs a useful problem resolution function.

It lets you monitor any file and/or directory on one, some, or all systems at a site, detect changes, and prevent them if configured to do so.

DART 225 Operations

You can configure DART 225 to monitor files and/or directories continuously, in which case the DART will detect changes to directories and files as they happen, or on a schedule, in which case it will check them at the time you define in the DART's configuration parameter.

If you enable DART 225's change prevention function, the DART will make a copy of the files that you want to prevent from being changed, and store all the other relevant information. If you choose to protect a directory, it will copy the entire directory, and all its other relevant information.

DART 225 runs when one of the following events occurs:

- When the ReSOFT client starts up. When this happens it checks for changes.
- When you click on the execute button to the right of the **Check monitored items** now label in the DART's configuration page. When this happens it checks for changes.
- At its scheduled time. When this happens it checks for changes.
- When monitored item(s) change. When this happens it checks for changes.
- When one of its configuration parameter changes. When this happens it updates the configuration.
- When it is enabled/disabled. When this happens it updates the configuration.
- Checking for changes means: Determining if any files or directories have been removed, added or altered, and

- Updating the stored information about any item that has changed.

Updating the configuration means updating the stored information about monitored item(s) to match their current state. If any existing stored information for monitored item(s) is still relevant, then it is re-used. If a new item is added, it means recording its information.

If DART 225 is configured to prevent changes, instead of updating the stored information about any item that has changed, it will restore the item to its pre-change state by overwriting the changed item with the copy that was stored when the item was first added to the **Monitored items** parameter as (part of) a command line.

This means that if a protected item is corrupted because of a system's software or hardware malfunction, and does not function properly any longer, if the ReSOFT client is operational, DART 225 will restore the protected item to its working state. In this scenario, the DART can be a useful automated problem resolution tool.

DART 227 - Process and Service Shutdown-Restart

Overview

DART 227 lets you shut down, and optionally restart, any combination of processes and services on one, some, or all systems at a site.

The shutdown and restart operations can be performed on demand, or on a schedule making this DART a powerful remote system management tool.

How it works

DART 227's structure follows a pattern that ReSOFT users will find familiar.

First you define, separately, process groups and service groups. As the names of these configuration parameters suggest, they let you, respectively, group processes that you may want to shutdown and/or restart together. Because we support standard MS-DOS wild card characters, and the exclusion character,!, you have great flexibility in managing the shutdown/restart of processes and services on systems at a site. Please refer to DART 227's configuration help file for detailed information on process and service group definition.

Next, you use the On-demand/Scheduled Shut down/Restart parameters (four in all) to define the lists of processes/services that you want to shutdown/restart on demand, or on a schedule. DART 227 lets you mix process and service groups in the shutdown/restart lists. You can also have the same process (es) and service(s) in different groups.

At this point, you set the schedule for the scheduled shutdown/restart operations and you are done.

DART 227 operations

DART 227 can have a **bimodal** mode of operation. It can be used to perform remotely and automatically the following functions:

- Scheduled shutdown. In this mode, DART 227 would be used, for example, to perform an orderly shutdown of all active applications before starting a regularly scheduled backup process. To use the DART this way, it is enabled, and the schedule is set up to run as desired.
- On-demand shutdown. In this mode, DART 227 would be used, for example, if a notification generated by the ReSOFT server, or other alert (or a phone call) informed an administrator that he/she needed to shut down certain process (es) and/or service(s) remotely. To use the DART to perform this action, it does not have to be enabled. The administrator simply clicks on the Execute button to the right of the Shut down processes now label to shut down the process (es) and/or service(s).
- Other elements of DART 227's function that make it a reliable and versatile system management tool include:
 - When shutting down an executable, DART 227 saves the exact location of the executable and its command line parameters, so that it could be restarted in a state that is as close as possible to its pre-shutdown state.
 - DART 227 shuts down services in the order in which they appear in a service group entry. It will restart them in the reverse order. In this way, dependent services are shut down first and restarted last.

- DART 227 will restart only one instance of each process it shut down, regardless of the number of instances that were running at the time. For example, if the DART shut down four copies of Microsoft Internet Explorer, it will restart only one.
- DART 227 will restart only processes that were successfully shut down.
- DART 227 lets you selectively restart processes that it shut down. For example, you can configure it to shut down *.exe but only restart foo.exe.

DART 228 - Network Packet Filtering

Overview

DART 228 performs an “in-depth” firewall function that is a last line of defense, rather than being an alternative to a corporate firewall, or to “personal” firewall products. It:

- Protects mobile machines, such as laptops, that sometimes operate outside the corporate firewall. These machines are usually unprotected when connected to a dial-up connection or a wireless connection in an airport or coffee shop.
- Limits the internal spread of a worm that gets inside the firewall. This can happen by physically bringing an infected machine into the network, or downloading and installing an infected executable.
- Reports an increase in firewall denials, which is an indicator that something is going on that merits investigation.

We don't intend to provide all the features of a “personal” firewall product. It would not add tangible values to the ReSOFT client. The major advantages that network packet filtering via DART 228 and the ReSOFT client have over those kinds of products include:

- Centralized configuration: the firewall configuration is controlled in one place, including any "exceptions". The entire facility is not open to a threat that exploits an unintentional weakness on a single machine.
- No configuration changes by end-users - Decisions on firewall policy are made by an informed system administrator who has a professional understanding of the security ramifications of the decisions, rather than being made by each end-user who just wants to complete a specific task

- **Centralized reporting:** All actions and events detected by DART 228 are logged on the ReSOFT server; including statistics on firewall deny operations that would alert a system administrator that the facility is under some kind of systematic attack.

How it works

DART 228 works by applying sequences of rules, which we call chains, to a system's networking connections, which we call adapter classes.

Rules specify deny traffic or allow traffic actions for source and destination IP addresses or ports. Please refer to DART 228's configuration help file for detailed information on rules.

Once you have defined a set of rules that you want to apply to your site(s), you are ready to assemble them into chains. Chains are simply comma-separated lists of rules. DART 228 applies the rules in a chain sequentially. It takes the action specified by the first rule in a chain that is matched by the packet. If no action is specified in the matching rule, or no rules match, then the default action (a configurable parameter), which is to deny a packet, is taken. Please refer to DART 228's configuration help file for detailed information on chains.

At this point, you are ready to tell DART 228 how to enforce the network packet filtering rules you have defined, i.e. how to apply chains of rules to a system's network connections as specified in its adapter classes. DART 228 supports the following adapter classes:

- **Hardwired** - An adapter that has a physical connection to a LAN
- **Wireless** - A wireless network adapter
- **Dial-up** - A dial-up connection through a modem
- **Default** - All of a system's networking connections

If you enable DART 228 and configure no adapter classes, or make a syntactical mistake in specifying rules, chains, and/or configuring adapter classes, the DART will log the configuration error and will not filter any packets.

DART 231 - Client Heartbeat

DART 231 runs on a schedule you select and simply posts a log onto the ReSOFT server signaling that the ReSOFT client is running and functioning normally.

Coupled with a notification triggered by the non-occurrence of an event (i.e. configured with notification triggering threshold equal to 0 and the Restricted option enabled), it provides a reliable mechanism for monitoring the availability of systems on which the ReSOFT client is installed, and of the ReSOFT client itself.

DART 232 - Intrusion Protection Control

Overview

DART 232 detects attempted configuration changes that can be used to execute unauthorized or malicious code. It can be configured to disable or delete these changes automatically without end-user intervention. If the user interface option is enabled, it alerts the end-user of such system configuration changes giving him/her the option to reject, disable (for future re-enabling if desired), or accept such changes.

The areas monitored by DART 232 are ones that are not normally covered by anti-virus and most other intrusion protection software. DART 232 focuses particularly on how a virus or other unauthorized code may be re-activated after an end-user or system administrator tries to terminate its execution and remove it. Typically, if an end-user or system administrator discovers an unauthorized executable running they may shut down the application, remove it, and possibly remove an entry for it from the system registry.

However it is possible, using shell extension handlers for example, to run a program every time a user right-clicks on a file which checks to see if the rogue application is installed and running, and if not, re-installs it and re-runs it. This type of re-activation can be very difficult to track down.

Malicious code can also be run at startup by using the Run registry keys, the startup folders, system.ini and win.ini. DART 27, (System Start-up Executable Management) protects these areas from intrusion. Though autoexec.bat can be used to run code at

startup, currently it's rarely used to do so. In autoexec.bat, we're more interested here in protecting the contents of the PATH environment variable. Rogue applications can use it to run unauthorized code. The system areas and object types currently protected by DART 232 include:

- Autoexec.bat
- Shell extension handlers Screen savers
- Open verb's command default value for executable files
- The Shell and Userinit values for the Winlogon key
- RunOnce, RunOnceEx, and RunServicesOnce registry keys
- Scrap Objects

How it works

DART 232 creates a hidden directory in the client dir called "232". When the DART first runs it creates in this hidden directory backup files of autoexec.bat, explorer.exe, and userinit.exe, using the .bak extension. DART 232 watches these files for tampering using checksums and should one of these files change the backup file in the hidden directory will be restored if the change is rejected (either silently, by dialog box timeout, or by user action). If a file changes and the change is accepted then the backup file is updated.

Further, if one of these files change and the chosen action is "Disable" then in addition to the backup file being restored the "disabled" version is archived in the hidden directory with the extension dbl. This is so a system administrator could examine the changed file after the backup is restored.

DART 232 coverage areas detail

In this section we describe in some detail the areas and object DART 232 protects from intrusion. For additional information on why and how configuration changes in these areas, and changes to these objects, can cause the execution of malicious code please refer to the article by Jason Fisher titled "Understand Common Virus Attacks Before They Strike to Better Protect Your Apps" at the following URL:

<http://msdn.microsoft.com/msdnmag/issues/03/05/VirusHunting/default.aspx>

Autoexec.bat can be used to run executable files on startup so we'll use a checksum to watch for changes in this config file. Also, the modification of the PATH environment variable is perhaps even more insidious than running executable code directly because it's less likely to be noticed as a potential risk. For example, when Microsoft Windows NT starts up it runs explorer.exe as the shell. This is because the "Shell" value of the "Winlogon" key is set to "explorer.exe". Now explorer.exe can't be replaced with a copy while Windows NT is running because it's protected by an operating system lock. However, there is no path given in the registry, so someone could replace explorer.exe with a copy stored somewhere on the system, and change the PATH variable so that Winds NT uses the copy instead of the original. What's worse is that the real explorer.exe is no longer protected by an operating system lock so it can now be overwritten.

Shell extension handlers (DLLs) can be set to run whenever any number of shell actions is initiated by the user, such as right clicking on an object to bring up the context menu or dragging and dropping. Since these handlers can execute malicious code, DART 232 monitored this area of the registry detecting (and rejecting/disabling them if so configured) any new ones that are installed and registered.

Screen savers. Screen savers are executable files. They are not locked by the operating system when they are not running so they can be replaced by files in screen saver format containing malicious code. When this happens, as soon as the screen saver is activated, the malicious code is executed.

Virus writers can implement attacks that exploit screen savers in two ways. First, they can find out what the currently selected screen saver is and replace the associated file with an infected copy. They can also copy a new screen saver (infected) to the system and programmatically make it the currently selected one.

To guard against these attacks DART 232 monitors the current screen saver selection for change. It also monitors the associated file for modification. It does not create backup files for screen savers because a typical machine can have over a dozen of them and users can install many more. Saving copies of all of them would unnecessarily clutter backup directories and these files are just not important enough to warrant that.

If the current screen saver selection is changed unknown to the user, DART 232 will change it back if it is configured to do so. If the file associated with the current screen saver selection is modified it cannot restore the original file because it keeps no backup.

Instead, DART 232 sets the screen saver selection to "None" so the malicious code won't execute. The DART will also post a log on the ReSOFT server warning you that the file associated with a screen saver was modified.

DART 232 only monitors the file associated with the screen saver currently selected by the end-user. To keep other (non-selected) screen saver files from being replaced, the DART I keep a list of their checksums. Whenever DART 232 runs, it compares the saved checksums with current ones. If it finds that one of the non-selected screen saver files has changed it posts a log on the ReSOFT server warning you that the file associated with a screen saver was modified. This should be sufficient because there is no immediate danger, since the screen saver associated with the modified file is not currently selected.

Open verb's command default value. There is a list of executable files (.exe, .com, .bat, etc.) that will run if the user double-clicks them. This is because their "open" verb's command default value in the registry is "%1" %*. These registry values can be changed to something like "VirusExecutable.exe %1". The result, as explained by Jason Fisher, would be this: "This allowed the virus program to run first any time the user attempted to execute any EXE program. The requested program was passed to the virus executable as a parameter, whereupon the virus could launch it, keeping the user largely in the dark about what was really going on." DART 232 monitors the open command's default value for executable files for attempts to modify them (rejecting/disabling them if so configured).

The "Shell" and "Userinit" values for the registry key "Winlogon" contains the name of executable files that are executed whenever a user logs on. The "Shell" value runs explorer.exe. "Userinit" runs userinit.exe on Microsoft Windows 2000, XP and 2003, and userinit.exe and nddeagnt.exe on systems running Microsoft Windows NT4. DART 232 monitors "Shell" and "Userinit". If so configured, it prevents them from being changed and, as further protection, records the checksums of the .exe files in case they get replaced with copies with the same name.

The RunOnce, RunOnceEx, and RunServicesOnce registry keys can be used to run a malicious executable at system start-up. What makes this type of intrusion particularly insidious is that after the malicious code runs at system start-up, the registry entries are automatically deleted, thus leaving no trace.

Scrap objects can be created for OLE (Object Linking and Embedding) purposes. Again, we'll just quote Jason Fisher's explanation: "[Scrap objects] are extremely dangerous because they can encapsulate executable code within a compound OLE document format."

Further: "There are two additional reasons these files are particularly risky, apart from the simple fact that they can hide executable code. First, they're often overlooked by antivirus software. Even if one of them is included in the list of executable application types, the other is often omitted. You should ensure that your antivirus program includes both file types. The second reason is much more subtle. As it turns out, the SHS and SHB extensions are always hidden by Explorer, even if you've configured Windows to display all file extensions. The reason is that the registry keys for these file types include an undocumented value, "NeverShowExt." If present, this value overrides global settings in Windows. For this reason, a virus writer can create a scrap object; give it an icon corresponding to an image, and then rename it something like "Look at This Funny Picture.jpg." Its actual file name, of course, is "Look at This Funny Picture.jpg.shs," but to the unsuspecting user it looks exactly like any other image. By the time the realization dawns that the file wasn't an image at all, the damage is done." Initially, DART 232 turns off the value NeverShowExt for scrap objects, making it less likely for a user to inadvertently execute one.

DART 233 - System Start-up Environment Management

Overview

Managing and controlling system start-up ensures that:

- Slower system boot-up
- Ongoing startup performance problems
- Unwanted intrusion and potentially even harm to the system
- Slower system performance is prevented.

- ReSOFT features complete system start-up environment management and control. We have two DARTs that perform these functions:
 - DART 27 to control the content of a system's start-up environment. Depending on its configuration, it accepts, reject, or disable any attempt to add a new item to a system's start-up environment. If so configured, it performs all actions automatically.
 - DART 233 to manage a system's start-up environment. DART 233 reports the content of a system's start-up environment, and disabled start-up items. It also lets you easily enable and disable start-up items on one, some, or all systems at a site.

How it works

DART 233 runs when one of the following events occurs:

- When you click on the execute button to the right of the Update startup items now label
- When a user logs on. Having DART 233 run when a user logs on has the side effect of having it run on ReSOFT client start-up. This is because the user that is currently active is seen as a new user when the ReSOFT client starts up.
- When it is enabled/disabled. When this happens it updates the configuration.
- At its scheduled time

When DART 233 runs the **Startup items to enable and Startup items to disable** parameters are processed first. After the appropriate start-up items are enabled or disabled as per the configuration, then the content of the **currently enabled startup items on this machine and currently disabled startup items on these machine parameters** is updated.

Enabling and disabling start-up items

The easiest way to disable a start-up item is to copy it from the **currently enabled startup items parameter**, and paste it into the **Startup items to disable** parameter. To re-enable an item you can move it from the Startup items to disable parameter to the **Startup items to enable parameter**.

While this method of enabling and disabling start-up items is certainly not the most elegant, it is straightforward and efficient.

DART 236 - On-demand Remote Control

Overview

DART 236 extend remote system control capabilities in a number of significant ways:

- It lets users control computers remotely without end-user intervention. This makes it ideal for remote control of unattended systems, e.g. servers.
- All aspects of remote control operations can be performed on demand, individually and in combination. This means that you can use DART 236 to install/remove the remote control utility, initiate/terminate a remote control session, or both (install/initiate a session, shutdown/remove) at any time.
- DART 236 brings scalability to remote control. The installation/removal of remote control software on one, some, or all systems on a sub-net is completely automated and managed via a single DART configuration page.

You can also initiate remote control sessions on one, some or all systems on a subnet with the click of a button on one system.

- With DART 236 remote control sessions are more secure:
 - The remote control session is initiated as an outbound transaction by the system you want to work on. This means that there is no need to open any ports for inbound traffic, which would pose a significant security risk.
 - DART 236 can be configured to automatically remove the remote control utility as soon as a remote control session is completed
 - There are no servers outside of your control that are used as intermediaries
 - The remote control session is completely self-contained every aspect of it is under your control including the installation and removal of the remote control utility

- DART 236 is designed to be used with any remote control utility. [Ultr@VNC](#) is the one initially supported both because it is popular, and it is open source

How it works

DART 236 performs four tasks:

- Installation and removal of the remote control utility (in the first version, VNC is the only supported remote control utility)
- Initiation and termination of a remote control session

Each task can be performed individually giving you flexibility on their sequence. For example, you could instruct DART 236 to install the remote control utility and begin a remote control session either immediately or at a different time. Depending on your choice, removal of the remote control utility can occur either right after a remote control session is over or at a later time.

You can perform both the installation and session initiation tasks in one step. You can also configure DART 236 to automatically remove the remote control utility as soon as the remote control session is completed.

When instructed to install the remote control utility, DART 236 downloads the software's installation executable from a URL of your choice. You can use an HTTP/HTTPS server, and FTP server, or shared network resource.

DART 237 - Microsoft Update Management

Overview

DART 237 performs two sets of actions:

- It retrieves and applies the Microsoft update management actions and configuration changes you set up via the Microsoft update management facility on the ReSOFT server
- Manages and controls the native Microsoft Automated Update client

How it works

DART 237 runs when one of the following events occurs:

- When you click on the **Execute** button for any of the following actions in the DART 237 configuration page:
 - Synchronize configuration with ReSOFT server now
 - Configure software updates now
 - Reset configuration now
- When it is enabled.
- At its scheduled time

DART 238 - Symantec Anti Virus Definition Dates Log

DART 238 reports the Symantec virus definition dates on the system where the DART is executed, and the latest virus definition dates on the sub-net where the system is located.

DART 238 can be executed on demand or on a schedule.

DART 239 - McAfee Anti Virus Definition Dates Log

DART 239 reports the McAfee VirusScan virus definition dates on the system where the DART is executed, and the latest virus definition dates on the sub-net where the system is located.

DART 239 can be executed on demand or on a schedule.

DART 240 - Intrusion Protection Management

Overview

ReSOFT features complete intrusion protection management and control. We have two DARTs that perform these functions:

- DART 232 controls the content of a system's areas that could be targeted by intruders. Depending on its configuration, it accepts, rejects, or disables any attempt

to modify the content of these areas. If so configured, it performs all actions automatically.

- DART 240 manages a system's configuration areas potentially affected by intruders. It reports the content of a system's intrusion related configuration variables, both enabled and disabled. It also lets you easily enable and disable these variables on one, some, or all systems at a site.

DART 240 coverage

System configuration variables managed by DART 240 are divided into two groups manipulated via different sets of configuration parameters.

The **Currently enabled items on this machine, currently disabled items on this machine, Items to enable**, and **Items to disable** configuration parameters manage the following system configuration variables:

- Autoexec.bat
- Shell= system.ini setting for systems running Microsoft Windows 9x based operating systems
- Shell extension handlers
- RunOnce
- RunOnceEx
- RunServicesOnce registry keys
- Browser Helper Objects
- Internet Explorer Bars
- Internet Explorer Extensions
- Internet Explorer Toolbars
- Hosts file

The **Current configuration settings on this machine and Configuration settings to enforce configuration parameters** manage the following system configuration variables:

- Start Page settings
- Search Pages settings
- Open verb commands
- Screen saver settings
- Critical Winlogon registry keys (shell and userinit) for systems running Microsoft Windows NT based operating systems (NT4, 2000, XP, or Server 2003)

How it works

DART 240 runs when one of the following events occurs:

- When you click on the execute button to the right of the Update **intrusion protection now label**
- When a user logs on. Having DART 240 run when a user logs on has the side effect of having it run on ReSOFT client start-up. This is because the user that is currently active is seen as a new user when the ReSOFT client starts up.
- When it is enabled/disabled. When this happens it updates the configuration
- At its scheduled time

When DART 240 runs, the **Items to enable, Items to disable, and Configuration settings to enforce** parameters are processed first. After the appropriate system configuration items are enabled or disabled as per the configuration, then the content of the **currently enabled items on this machine and currently disabled** items on these machine configuration parameters is updated.

Enabling and disabling items

DART 240 is a powerful management tool because in addition to providing you with information about enabled and disabled system configuration items that could be targeted by intruders, it lets you enable and disable these system configuration items on one, some, or all systems at a site, or at all your sites making the necessary changes only once.

In addition, like all other ReSOFT DARTs, DART 240 logs and reports all events it detects and actions it takes to the ReSOFT server where you can easily set up notifications and reports to

keep you and your users informed about intrusion protection management activities at your sites.

The easiest way to disable a system configuration item is to copy it from the **currently enabled items** configuration parameter, and paste it into the **Items to disable** configuration parameter. To re-enable an item you can move it (**cut and paste**) from the **Items to disable** configuration parameter to the items to enable configuration parameter.

While this method of enabling and disabling start-up items is certainly not the most elegant, it is straightforward and efficient. Depending on your needs, in order to disable a system configuration item on all systems at a site you only need to add an entry to the **Items to disable** configuration parameter on one system.

The **Configuration settings to enforce** configuration parameter provides you with a simple yet powerful tool for standardizing the value of critical system configuration settings such as browser and shell related variables at a site, and ensuring that they are protected from intruders.

The easiest way (and least prone to errors) to add to or modify the content of the **Configuration settings to enforce** configuration parameter is to copy entries with the desired value from the **Current configuration settings on this machine configuration parameter**.

DART 241 - Contact Information

DART 241 lets you build a contact database for each of your sites. Either at installation time, or on-demand, you can ask a system's user to enter information that will make it easier to identify the system and its location, and contact the user in case of need.

DART 241 is persistent. You have complete control over its execution cycle. You can configure both the amount of time the dialog box asking an end-user for information is displayed on the screen, and the interval between requests for information, when the end-user cancels the request, or no action is taken on the dialog box.

The fields in the contact database built by DART 241 include some or all of the following:

- First name
- Last name
- Title
- Company
- Address
- City
- State
- Zip
- Country
- First phone
- Second phone
- Fax
- E-mail
- Cell phone
- Custom value 1
- Custom value 2
- Custom value 3
- Custom value 4

DART 242 - eTrust Virus Definition Management

DART 242 manages the eTrust Anti Virus definitions on all systems where it is enabled and configured accordingly. It ensures that at all times, all systems where it is enabled and configured accordingly, at the very least, will have the newest virus definitions available on each sub-net.

DART 242 accomplishes this goal by looking for the newest possible virus definitions in the following locations:

- Other systems on the same sub-net
- The location(s) of eTrust Antivirus on-site server(s)
- Computer Associate's site, using the eTrust virus definition update program

The above options for updating a system's eTrust Antivirus virus definitions can be used independently, or in conjunction with each other. If they are used together, DART 247 executes each option in the order listed above.

When the date of the eTrust Antivirus virus definition database files (last modified date of the virus definition files) is older than the current date by the number of days specified by the **Maximum days since last definitions update** configuration parameter, or more, DART 242 will post this information on the ReSOFT server.

Whenever it runs, DART 242 automatically reports the eTrust virus definition versions from all systems on the sub-net.

If so configured, DART 242 will also report if eTrust EZ Antivirus is either not installed correctly, or not at all on the system where the DART runs.

DART 243 - eTrust EZ Antivirus Scan Execution

DART 243 executes the silent execution of the eTrust EZ Antivirus scan, and reports its completion. If so configured, DART 243 will also report if eTrust EZ Antivirus is either not installed correctly, or not at all on the system where the DART runs.

DART 244 - eTrust EZ Antivirus Definition Dates Log

DART 244 reports the eTrust virus definition versions on the system where the DART is executed and the latest virus definition version on the sub-net where the system is located. This DART can be executed on a schedule or on demand.

DART 245 – On-demand GoToAssist

DART 245 automates the establishment of a GoToAssist remote control session adding a number of significant benefits to GoTo Assist functions:

- It lets users control computers remotely without end-user intervention. This makes it ideal for remote control of unattended systems, e.g. Servers.
- It lets users take remote control of systems even when they are logged off.
- DART 245 brings scalability to remote control. The GoToAssist configuration on one, some, or all systems on a sub-net is completely automated, and managed via a single DART configuration page.

DART 246 – Network Device Discovery

DART 246 reports the content of the ARP table listing all devices on the LAN the system where DART 246 runs is connected to.

DART 246 can run in one of three modes

- On a user defined schedule
- On demand, triggered by a user
- Triggered when the ReSOFT network driver dynamically detects a change in the ARP table

For each device on the LAN, DART 246 reports:

- The NetBIOS name or fully qualified domain name
- The IP address
- The MAC address of the devices network interface card
- ReSOFT client version number, if it is installed on the device

DART 247 - Trend Micro Virus Definition Management

DART 247 manages the Trend Micro Anti Virus definitions on all systems where it is enabled and configured accordingly. It ensures that at all times, all systems where it is enabled and configured accordingly, at the very least, will have the newest virus definitions available on each sub-net.

DART 247 accomplishes this goal by looking for the newest possible virus definitions in the following locations:

- ➔ Other systems on the same sub-net
- ➔ The location(s) of Trend Micro Anti Virus on-site server(s)
- ➔ Trend Micro's site, using the Trend Micro virus definition update program

The above options for updating a system's Trend Micro Anti Virus definitions can be used independently, or in conjunction with each other. If they are used together, DART 247 executes each option in the order listed above.

When the date of the Trend Micro Anti Virus definition database files is older than the current date by the number of days specified by the **maximum days since last definitions update** configuration parameter, or more, DART 247 will post this information on the ReSOFT server.

Whenever it runs, DART 247 automatically reports the Trend Micro Anti Virus virus definition versions from all systems on the sub-net.

If so configured, DART 247 will also report if Trend Micro Anti Virus is either not installed correctly or not at all on the system where the DART runs.

DART 249 - Trend Micro Anti Virus Scan Execution

DART 249 executes the Trend Micro Anti Virus scan, and reports its completion.

If so configured, DART 249 will also report if Trend Micro Anti Virus is either not installed correctly or not at all on the system where the DART runs.

DART 250 - Trend Micro Anti Virus Definition Dates Log

DART 250 reports the Trend Micro Anti-virus definition dates on the system where the DART is executed, and the latest virus definition dates on the sub-net where the system is located.

This DART can be executed on a schedule or on demand.

DART 251 - IE Browser Optimization

DART 251 has the options to delete cookies, history, temporary internet files, toolbars, form data, password, files and settings stored by add-ons. Also re-registers IE files.

This DART can be executed on a schedule or on demand.

DART 252 - Log file Retrieval and Logging

DART 252 is used for reading the log files stored in any of the locations in the local drives and writing the file contents to DART 252's events.

This DART can be executed on a schedule or on demand.

DART 253 - Defrager for 64-bit OS

This Dart is used to defrag all the drives in the system.

- It checks the Architecture of the system (32-bit or 64-Bit).
- If the System is 32-bit then this dart will take the help of Disk Defragmenter Execution (MS Windows XP, and Server 2003) - Dart 211.
- If the System is 64-bit then this dart will check for the file df64.exe on location C:\Program Files (x86)\Handsfree\client\Tools\df64.exe.
- If the file exists then this DART will take help of df64bit - Shortcut batch file to defragment all the drives in the machine.

- If the file doesn't exist, then this DART will download the df64.exe from the FTP location to the C:\Program Files (x86)\Handsfree\client\Tools\df64.exe and start the defragmentation for all the drives.

DART 254 – Rocket DOCK Management

DART 254 is used to configure the DOCK icons in Rocket DOCK. There are 16 icons that can be configured. For instance,

- Icon 1: By default – Disabled
 - If enabled- then icon 1 will appear On the Dock.
 - Icon Label: Name to display on Icon 1.
 - File or command for Icon: Link or path of the file to be opened.

In the same way, all other DOCK icons can also be configured.

DART 255 – Contact Information

For each system where it runs, DART 255 displays the information entered by an end user in the following local configuration parameters:

- First name
- Last name
- Email ID
- Address Line 1
- Address Line 2
- City
- State
- Country
- First Phone Number
- Second Phone Number
- Zip Code
- Support Plan
- Transaction ID

- Plan Value
- Purchase Date
- Discount

DART 256 – Client Uninstall

DART 256 stores the client installation date and calculates the client uninstallation date based on the value given in the parameter “No of days to uninstall” and uninstalls the HFN client on the calculated date automatically.

In the parameter “Darts to run sequentially”, required DARTs can be specified which needs to be executed during HFN client uninstallation.

DART 257 – On-demand Repeater Connectivity

The entry in the “Domain Name” configuration parameter would be service.provider.com (or its public IP address). In addition, the firewall on your network would be configured to forward incoming port 5500 (or whichever port you have specified in the Listener port (Blank defaults to 5500) configuration parameter) traffic to the device at 192.168.1.250 (the private IP address of your computer).

The Listener port (Blank defaults to 5500) configuration parameter lets you identify an IP port different from the default (5500) for the remote control software on the target computer to use to communicate with the remote computer.

The value of the Listener port (Blank defaults to 5500) configuration parameter can be different for each remote computer. In this way, you can have multiple systems at your site conducting remote control sessions with different target computers at the same time.

DART 258 – End-User Message - I

When this DART is enabled, then a message box is displayed on the screen with the “Title” given in parameter “Message Box Title” and also with the “Text” given in parameter “Message Description”. The message-box will contain two buttons: “Ok” and “Cancel”. If the second

parameter “Enable Time Out For User” is checked, then the message box will wait for the user interaction only for the time period given in “No. of seconds to wait for user interaction” . After that time period, the message box gets closed automatically.

Note: - If the second parameter “Enable Timeout for user” is disabled, then the message box requires user interaction to proceed further, it will not close by itself.

DART 259 – End-User Message - II

When this DART is enabled, then a message Box is displayed on the screen with the “Title” given in parameter “Message Box Title” and also with the “Text” given in parameter “Message Description”. The message-box has two buttons named as “Ok” and “Cancel”. If the second parameter “Enable Time Out For User” is enabled, then this message box will wait for the user interaction only for the time period given in “No. of seconds to wait for user interaction”. After that time period, the message box gets closed automatically.

Note: - If the second parameter “Enable Timeout for user” is disabled, then the message box requires user interaction to proceed further, it will not close by itself.

DART 260 – Sequential DART - I

This DART will take the list of DARTS which needs to run in sequential way with the message to be displayed with each of them.

Below is the syntax that needs to be followed:

➔ DART number

For instance,

251

252

253

254

DART 261 – Sequential DART - II

This DART will take the list of DARTS which needs to run in sequential way with the message to be displayed with each of them. Below is the syntax that needs to be followed:

➔ DART number

For instance,

251

252

253

254

DART 262– Sequential DART - III

This DART will take the list of DARTS which needs to run in sequential way with the message to be displayed with each of them.

Below is the syntax that needs to be followed:

➔ DART number

For instance,

251

252

253

254

DART 263– Spybot Tool Management

DART 263 enables the automated application of software updates and patches on one, a subset, or all systems on the local network. This DART can be used to install or uninstall software updated and patches from any vendor.

Patches and software updates applied by DART 263 can be located on a shared network resource, an FTP Server, or Web server using HTTP or secure HTTP (the FTP server and Web server could be located on the same system as the ReSOFT server).

Patches and software updates can be applied selectively based on a system's operating system.

DART 196 automatically tracks the patches and software updates applied to each system. This means that:

- You have a readily accessible trace of the history of patches and software updates applied to each system in your network, and
- You don't have to actively manage the list of patches to apply on a system-by-system basis as DART 263 will automatically ignore an attempt to re-apply a patch or software update to a system where it has already been installed, unless you want it to.

DART 264- 3rd party Tools Installation - I

DART 264 enables the automated application of software updates and patches on one, a subset, or all systems on the local network. This DART can be used to install or uninstall software updated and patches from any vendor.

Patches and software updates applied by DART 264 can be located on a shared network resource, an FTP Server, or Web server using HTTP or secure HTTP (the FTP server and Web server could be located on the same system as the ReSOFT server).

Patches and software updates can be applied selectively based on a system's operating system.

DART 264 automatically tracks the patches and software updates applied to each system. This means that:

- You have a readily accessible trace of the history of patches and software updates applied to each system in your network, and

- You don't have to actively manage the list of patches to apply on a system-by-system basis as DART 264 will automatically ignore an attempt to re-apply a patch or software update to a system where it has already been installed, unless you want it to.

DART 265- Fake AV Tool Management

DART 265 enables the automated application of software updates and patches on one, a subset, or all systems on the local network. This DART can be used to install or uninstall software updated and patches from any vendor.

Patches and software updates applied by DART 265 can be located on a shared network resource, an FTP Server, or Web server using HTTP or secure HTTP (the FTP server and Web server could be located on the same system as the ReSOFT server).

Patches and software updates can be applied selectively based on a system's operating system.

DART 265 automatically tracks the patches and software updates applied to each system. This means that:

- You have a readily accessible trace of the history of patches and software updates applied to each system in your network, and
- You don't have to actively manage the list of patches to apply on a system-by-system basis as DART 265 will automatically ignore an attempt to re-apply a patch or software update to a system where it has already been installed, unless you want it to.

DART 266- Malwarebytes Tool Management (User Mode)

DART 266 enables the automated application of software updates and patches on one, a subset, or all systems on the local network. This DART can be used to install or uninstall software updated and patches from any vendor.

Patches and software updates applied by DART 266 can be located on a shared network resource, an FTP Server, or Web server using HTTP or secure HTTP (the FTP server and Web server could be located on the same system as the ReSOFT server).

Patches and software updates can be applied selectively based on a system's operating system.

DART 266 automatically tracks the patches and software updates applied to each system. This means that:

- You have a readily accessible trace of the history of patches and software updates applied to each system in your network, and
- You don't have to actively manage the list of patches to apply on a system-by-system basis as DART 266 will automatically ignore an attempt to re-apply a patch or software update to a system where it has already been installed, unless you want it to.

DART 267- Trojan Remover Tool Management (User Mode)

DART 267 enables the automated application of software updates and patches on one, a subset, or all systems on the local network. This DART can be used to install or uninstall software updated and patches from any vendor.

Patches and software updates applied by DART 267 can be located on a shared network resource, an FTP Server, or Web server using HTTP or secure HTTP (the FTP server and Web server could be located on the same system as the ReSOFT server).

Patches and software updates can be applied selectively based on a system's operating system.

DART 267 automatically tracks the patches and software updates applied to each system. This means that:

- You have a readily accessible trace of the history of patches and software updates applied to each system in your network, and

- You don't have to actively manage the list of patches to apply on a system-by-system basis as DART 267 will automatically ignore an attempt to re-apply a patch or software update to a system where it has already been installed, unless you want it to.

DART 268- Registry Healer Tool Management (User Mode)

DART 268 enables the automated application of software updates and patches on one, a subset, or all systems on the local network. This DART can be used to install or uninstall software updated and patches from any vendor.

Patches and software updates applied by DART 268 can be located on a shared network resource, an FTP Server, or Web server using HTTP or secure HTTP (the FTP server and Web server could be located on the same system as the ReSOFT server).

Patches and software updates can be applied selectively based on a system's operating system.

DART 268 automatically tracks the patches and software updates applied to each system. This means that:

- You have a readily accessible trace of the history of patches and software updates applied to each system in your network, and
- You don't have to actively manage the list of patches to apply on a system-by-system basis as DART 268 will automatically ignore an attempt to re-apply a patch or software update to a system where it has already been installed, unless you want it to.

DART 269- Flash Player Plugin Management (User Mode)

DART 269 enables the automated application of software updates and patches on one, a subset, or all systems on the local network. This DART can be used to install or uninstall software updated and patches from any vendor.

Patches and software updates applied by DART 269 can be located on a shared network resource, an FTP Server, or Web server using HTTP or secure HTTP (the FTP server and Web server could be located on the same system as the ReSOFT server).

Patches and software updates can be applied selectively based on a system's operating system.

DART 269 automatically tracks the patches and software updates applied to each system. This means that:

- You have a readily accessible trace of the history of patches and software updates applied to each system in your network, and
- You don't have to actively manage the list of patches to apply on a system-by-system basis as DART 269 will automatically ignore an attempt to re-apply a patch or software update to a system where it has already been installed, unless you want it to.

DART 270– JRE Plugin Management (User Mode)

DART 270 enables the automated application of software updates and patches on one, a subset, or all systems on the local network. This DART can be used to install or uninstall software updated and patches from any vendor.

Patches and software updates applied by DART 270 can be located on a shared network resource, an FTP Server, or Web server using HTTP or secure HTTP (the FTP server and Web server could be located on the same system as the ReSOFT server).

Patches and software updates can be applied selectively based on a system's operating system.

DART 270 automatically tracks the patches and software updates applied to each system. This means that:

- You have a readily accessible trace of the history of patches and software updates applied to each system in your network, and

- You don't have to actively manage the list of patches to apply on a system-by-system basis as DART 270 will automatically ignore an attempt to re-apply a patch or software update to a system where it has already been installed, unless you want it to.

DART 271- Hitman Pro Tool Management (User Mode)

DART 271 enables the automated application of software updates and patches on one, a subset, or all systems on the local network. This DART can be used to install or uninstall software updated and patches from any vendor.

Patches and software updates applied by DART 271 can be located on a shared network resource, an FTP Server, or Web server using HTTP or secure HTTP (the FTP server and Web server could be located on the same system as the ReSOFT server).

Patches and software updates can be applied selectively based on a system's operating system.

DART 271 automatically tracks the patches and software updates applied to each system. This means that:

- You have a readily accessible trace of the history of patches and software updates applied to each system in your network, and
- You don't have to actively manage the list of patches to apply on a system-by-system basis as DART 271 will automatically ignore an attempt to re-apply a patch or software update to a system where it has already been installed, unless you want it to.

DART 272- SafeMSI & Rkill Tool Management (User Mode)

DART 272 enables the automated application of software updates and patches on one, a subset, or all systems on the local network. This DART can be used to install or uninstall software updated and patches from any vendor.

Patches and software updates applied by DART 272 can be located on a shared network resource, an FTP Server, or Web server using HTTP or secure HTTP (the FTP server and Web server could be located on the same system as the ReSOFT server).

Patches and software updates can be applied selectively based on a system's operating system.

DART 272 automatically tracks the patches and software updates applied to each system. This means that:

- You have a readily accessible trace of the history of patches and software updates applied to each system in your network, and
- You don't have to actively manage the list of patches to apply on a system-by-system basis as DART 272 will automatically ignore an attempt to re-apply a patch or software update to a system where it has already been installed, unless you want it to.

DART 273- CCleaner Tool Management (User Mode)

DART 273 enables the automated application of software updates and patches on one, a subset, or all systems on the local network. This DART can be used to install or uninstall software updated and patches from any vendor.

Patches and software updates applied by DART 273 can be located on a shared network resource, an FTP Server, or Web server using HTTP or secure HTTP (the FTP server and Web server could be located on the same system as the ReSOFT server).

Patches and software updates can be applied selectively based on a system's operating system.

DART 273 automatically tracks the patches and software updates applied to each system. This means that:

- You have a readily accessible trace of the history of patches and software updates applied to each system in your network, and

- You don't have to actively manage the list of patches to apply on a system-by-system basis as DART 273 will automatically ignore an attempt to re-apply a patch or software update to a system where it has already been installed, unless you want it to.

DART 274- RemoveIT Tool Management (User Mode)

DART 274 enables the automated application of software updates and patches on one, a subset, or all systems on the local network. This DART can be used to install or uninstall software updated and patches from any vendor.

Patches and software updates applied by DART 274 can be located on a shared network resource, an FTP Server, or Web server using HTTP or secure HTTP (the FTP server and Web server could be located on the same system as the ReSOFT server).

Patches and software updates can be applied selectively based on a system's operating system.

DART 274 automatically tracks the patches and software updates applied to each system. This means that:

- You have a readily accessible trace of the history of patches and software updates applied to each system in your network, and
- You don't have to actively manage the list of patches to apply on a system-by-system basis as DART 274 will automatically ignore an attempt to re-apply a patch or software update to a system where it has already been installed, unless you want it to.

DART 275- 3rd party Tools Installation - II (User Mode)

DART 275 enables the automated application of software updates and patches on one, a subset, or all systems on the local network. This DART can be used to install or uninstall software updated and patches from any vendor.

Patches and software updates applied by DART 275 can be located on a shared network resource, an FTP Server, or Web server using HTTP or secure HTTP (the FTP server and Web server could be located on the same system as the ReSOFT server).

Patches and software updates can be applied selectively based on a system's operating system.

DART 275 automatically tracks the patches and software updates applied to each system. This means that:

- You have a readily accessible trace of the history of patches and software updates applied to each system in your network, and
- You don't have to actively manage the list of patches to apply on a system-by-system basis as DART 275 will automatically ignore an attempt to re-apply a patch or software update to a system where it has already been installed, unless you want it to.

DART 276– Superantispyware Tool Management (User Mode)

DART 276 enables the automated application of software updates and patches on one, a subset, or all systems on the local network. This DART can be used to install or uninstall software updated and patches from any vendor.

Patches and software updates applied by DART 276 can be located on a shared network resource, an FTP Server, or Web server using HTTP or secure HTTP (the FTP server and Web server could be located on the same system as the ReSOFT server).

Patches and software updates can be applied selectively based on a system's operating system.

DART 276 automatically tracks the patches and software updates applied to each system. This means that:

- You have a readily accessible trace of the history of patches and software updates applied to each system in your network, and

- You don't have to actively manage the list of patches to apply on a system-by-system basis as DART 276 will automatically ignore an attempt to re-apply a patch or software update to a system where it has already been installed, unless you want it to.

DART 277– 3rd party Patch Uninstallation - I

DART 277 enables the automated application of software updates and patches on one, a subset, or all systems on the local network. This DART can be used to install or uninstall software updated and patches from any vendor.

Patches and software updates applied by DART 277 can be located on a shared network resource, an FTP Server, or Web server using HTTP or secure HTTP (the FTP server and Web server could be located on the same system as the ReSOFT server).

Patches and software updates can be applied selectively based on a system's operating system.

DART 277 automatically tracks the patches and software updates applied to each system. This means that:

- You have a readily accessible trace of the history of patches and software updates applied to each system in your network, and
- You don't have to actively manage the list of patches to apply on a system-by-system basis as DART 277 will automatically ignore an attempt to re-apply a patch or software update to a system where it has already been installed, unless you want it to.

DART 278– 3rd party Patch Uninstallation - II (User Mode)

DART 278 enables the automated application of software updates and patches on one, a subset, or all systems on the local network. This DART can be used to install or uninstall software updated and patches from any vendor.

Patches and software updates applied by DART 278 can be located on a shared network resource, an FTP Server, or Web server using HTTP or secure HTTP (the FTP server and Web server could be located on the same system as the ReSOFT server).

Patches and software updates can be applied selectively based on a system's operating system.

DART 278 automatically tracks the patches and software updates applied to each system. This means that:

- You have a readily accessible trace of the history of patches and software updates applied to each system in your network, and
- You don't have to actively manage the list of patches to apply on a system-by-system basis as DART 278 will automatically ignore an attempt to re-apply a patch or software update to a system where it has already been installed, unless you want it to.

DART 279– 3rd party Patch Uninstallation - III (User Mode)

DART 279 enables the automated application of software updates and patches on one, a subset, or all systems on the local network. This DART can be used to install or uninstall software updated and patches from any vendor.

Patches and software updates applied by DART 279 can be located on a shared network resource, an FTP Server, or Web server using HTTP or secure HTTP (the FTP server and Web server could be located on the same system as the ReSOFT server).

Patches and software updates can be applied selectively based on a system's operating system.

DART 279 automatically tracks the patches and software updates applied to each system. This means that:

- You have a readily accessible trace of the history of patches and software updates applied to each system in your network, and

- You don't have to actively manage the list of patches to apply on a system-by-system basis as DART 279 will automatically ignore an attempt to re-apply a patch or software update to a system where it has already been installed, unless you want it to.

DART 280- Hardware Diagnostic Management (Scripts)

If PC Doctor 3.0 is installed in the machine, when this DART is triggered it runs hardware diagnostic tests for an individual item or multiple items which includes motherboards, CPUs, hard drives, system factory etc.

The result will be stored in the Handsfree folder and also displayed in DART 280's event.

DART 281- Hardware Diagnostic Management (Devices)

If PC Doctor 3.0 is installed in the machine, when this DART is triggered it runs hardware diagnostic tests for an individual item or multiple items which includes keyboard, mouse, printer, camera etc. The result will be stored in the Handsfree folder and also displayed in DART 280's event.

DART 282- Windows Security Management

This DART is used to turn on / off Windows Firewall.

DART 283- Windows TroubShooter Management (Windows 7 & Vista)

This DART runs various diagnostic steps in Windows 7 / Vista OS machines:

- Network Diagnostics
- Device Diagnostic
- Home Group Diagnostic
- Network Diagnostics Inbound
- Network Diagnostics Web
- IE Diagnostic
- IE Security Diagnostic
- Network Diagnostics Network Adapter

- Performance Diagnostic
- Audio Playback Diagnostic
- Power Diagnostic
- PCW Diagnostic
- Printer Diagnostic
- Audio Recording Diagnostic
- Search Diagnostic
- Network Diagnostics File Share
- Maintenance Diagnostic
- Windows Media Player DVD Diagnostic
- Windows Media Player Library Diagnostic
- Windows Media Player Configuration Diagnostic
- Windows Update Diagnostic

DART 284– Windows Fix-It Management (Windows XP)

This DART runs the following fixit in Windows XP OS machines:

- Aero
- Audio Play back
- Audio Recording
- Codec
- Devices
- DVD
- Home group
- IE Add-on
- IE Performance
- Maintenance
- MSN Client
- Performance
- Pictures
- Power
- Printing
- Setup TV Tuner

- Time Zones
- Windows Firewall
- Windows Update
- Windows file Folder
- Windows Security

To learn more about HandsFree Networks and our solution, visit www.handSFreenetworks.com, send us an e-mail or call



HandsFree Networks Inc
1021 Main Campus Drive, Suite 300
Raleigh, NC 27606 (US)

HandsFree Networks Pvt. Ltd.,
4th Floor, Concorde Block, UB City,
Vittal Mallya Road, Bangalore-560001 (INDIA)

HandsFree Networks and related HandsFree Networks Inc. logos are registered trademarks of HandsFree Networks Inc. Copyright ©2009 HandsFree Networks. All rights reserved. All other company, product and brand names are trademarks of their respective owners.

Find out how HandsFree Networks can automate
your software support process.