Your AV is Trying to Tell You Something: Registry

malwaremaloney.blogspot.com/2021/03/your-av-is-trying-to-tell-you-something_30.html

What research is complete without looking at the registry. There are a few interesting keys that can be found here. There is one that will tell you the worst infection type that occured on the endpoint, files that were quarantined and various other settings. This list is not complete but I tried to hit on some of the more interessting ones.

Registry Key Entries

Registry key entries are found in the following location:

- Hive: HKLM\SOFTWARE
- File: C:\Windows\System32\config\SOFTWARE

All registry subkeys are placed in the following location: **HKLM\SOFTWARE\Symantec\Symantec Endpoint Protection\CurrentVersion**, or under **HKLM\SOFTWARE\Wow6432Node\Symantec...** on a 64-bit OS.

Key	Name	Description
HKEY_LOCAL_MACHINE\SOFTWARE\Symantec\Symantec Endpoint Protection\AV	VirusEngine	DLL of virus engine
HKEY_LOCAL_MACHINE\SOFTWARE\Symantec\Symantec Endpoint Protection\AV	LocalMAC	MAC address of the computer
HKEY_LOCAL_MACHINE\SOFTWARE\Symantec\Symantec Endpoint Protection\AV	MyProcessID	Proccess ID of ccSvcHst.exe
HKEY_LOCAL_MACHINE\SOFTWARE\Symantec\Symantec Endpoint Protection\AV	LogFileRollOverDays	Number of days logs are kept
HKEY_LOCAL_MACHINE\SOFTWARE\Symantec\Symantec Endpoint Protection\AV	WorstInfectionType	"Severity of the worst detection that was made: 0 = (Severity 0) Viral 1 = (Severity 1) Non-viral malicious 2 = (Severity 2) Malicious 3 = (Severity 3) Antivirus - Heuristic 5 = (Severity 5) Hack tool 6 = (Severity 6) Spyware 7 = (Severity 7) Trackware 8 = (Severity 8) Dialer 9 = (Severity 9) Remote access 10 = (Severity 10) Adware 11 = (Severity 11) Jokeware 12 = (Severity 12) Client compliancy 13 = (Severity 13) Generic load point 14 = (Severity 14) Proactive Threat Scan - Heuristic 15 = (Severity 15) Cookie 9999 = No detections"
HKEY_LOCAL_MACHINE\SOFTWARE\Symantec\Symantec Endpoint Protection\AV	TimeOfLastVirus	The last time a virus was detected on the client computer (GMT)
HKEY_LOCAL_MACHINE\SOFTWARE\Symantec\Symantec Endpoint Protection\AV	TimeOfLastScan	The last scan time for this agent (GMT).
HKEY_LOCAL_MACHINE\SOFTWARE\Symantec\Symantec Endpoint Protection\AV\Quarantine	BackupItemPurgeAgeLimit	Maximum days to hold onto backup items

Key	Name	Description
HKEY_LOCAL_MACHINE\SOFTWARE\Symantec\Symantec Endpoint Protection\AV\Quarantine	BackupItemPurgeEnabled	To enable backup item purge: 0 = OFF 1 = ON
HKEY_LOCAL_MACHINE\SOFTWARE\Symantec\Symantec Endpoint Protection\AV\Quarantine	BackupPurgeBySizeDirLimit	Maximum size in Megabytes of the backup folder
HKEY_LOCAL_MACHINE\SOFTWARE\Symantec\Symantec Endpoint Protection\AV\Quarantine	BackupPurgeBySizeEnabled	To enable Sizing of backup folder: 0 = OFF 1 = ON
HKEY_LOCAL_MACHINE\SOFTWARE\Symantec\Symantec Endpoint Protection\AV\Quarantine	ForwardingEnabled	Enable forwarding of quarantine to central server: 0 = OFF 1 = ON
HKEY_LOCAL_MACHINE\SOFTWARE\Symantec\Symantec Endpoint Protection\AV\Quarantine	ForwardingPort	Port of forwarding server
HKEY_LOCAL_MACHINE\SOFTWARE\Symantec\Symantec Endpoint Protection\AV\Quarantine	ForwardingProtocol	Protocol of forwarding server
HKEY_LOCAL_MACHINE\SOFTWARE\Symantec\Symantec Endpoint Protection\AV\Quarantine	ForwardingServer	Path to forwarding server
HKEY_LOCAL_MACHINE\SOFTWARE\Symantec\Symantec Endpoint Protection\AV\Quarantine	QuarantinePurgeAgeLimit	Maximum days to hold onto quarantine files
HKEY_LOCAL_MACHINE\SOFTWARE\Symantec\Symantec Endpoint Protection\AV\Quarantine	QuarantinePurgeBySizeDirLimit	Maximum size in Megabytes of the quarantine folder
HKEY_LOCAL_MACHINE\SOFTWARE\Symantec\Symantec Endpoint Protection\AV\Quarantine	QuarantinePurgeBySizeEnabled	To enable Sizing of quarantine folder: 0 = OFF 1 = ON
HKEY_LOCAL_MACHINE\SOFTWARE\Symantec\Symantec Endpoint Protection\AV\Quarantine	QuarantinePurgeEnabled	To enable quarantine purge: 0 = OFF 1 = ON
HKEY_LOCAL_MACHINE\SOFTWARE\Symantec\Symantec Endpoint Protection\AV\Quarantine	RepairedItemPurgeAgeLimit	Maximum days to hold onto repaired items
HKEY_LOCAL_MACHINE\SOFTWARE\Symantec\Symantec Endpoint Protection\AV\Quarantine	RepairedItemPurgeEnabled	To enable repaired item purge: 0 = OFF 1 = ON
HKEY_LOCAL_MACHINE\SOFTWARE\Symantec\Symantec Endpoint Protection\AV\Quarantine	RepairedPurgeBySizeDirLimit	Maximum size in Megabytes of the repaired folder
HKEY_LOCAL_MACHINE\SOFTWARE\Symantec\Symantec Endpoint Protection\AV\Quarantine	RepairedPurgeBySizeEnabled	To enable Sizing of repaired folder: 0 = OFF 1 = ON
HKEY_LOCAL_MACHINE\SOFTWARE\Symantec\Symantec Endpoint Protection\AV\Quarantine\QRecords(10 digit numerical folder)	FName	Name of file that was quarantined
HKEY_LOCAL_MACHINE\SOFTWARE\Symantec\Symantec Endpoint Protection\CurrentVersion\public-opstate	AVRunningStatus	Registers whether Virus and Spyware Protection is enabled or disabled.
HKEY_LOCAL_MACHINE\SOFTWARE\Symantec\Symantec Endpoint Protection\CurrentVersion\public-opstate	LatestVirusDefsDate	Virus Definition date in use by client

Key	Name	Description
HKEY_LOCAL_MACHINE\SOFTWARE\Symantec\Symantec Endpoint Protection\CurrentVersion\public-opstate	LatestVirusDefsRevision	Virus Definition Revision number in use by client
HKEY_LOCAL_MACHINE\SOFTWARE\Symantec\Symantec Endpoint Protection\CurrentVersion\public-opstate	Infected	"Registers whether the client computer is infected with one or more risks that are detected by Virus and Spyware Protection. 0 = Not infected 1 = Infected"
HKEY_LOCAL_MACHINE\SOFTWARE\Symantec\Symantec Endpoint Protection\CurrentVersion\public-opstate	snac_enabled	Registers whether Symantec Network Access Control is enabled or disabled.
HKEY_LOCAL_MACHINE\SOFTWARE\Symantec\Symantec Endpoint Protection\CurrentVersion\public-opstate	FWRunningStatus	Registers whether firewall protection is enabled or disabled.
HKEY_LOCAL_MACHINE\SOFTWARE\Symantec\Symantec Endpoint Protection\CurrentVersion\public-opstate	LastServerIP	Registers the IP address of the most recent Symantec Endpoint Protection management server that the client connected to.
HKEY_LOCAL_MACHINE\SOFTWARE\Symantec\Symantec Endpoint Protection\CurrentVersion\public-opstate	ComputerID	Computer ID
HKEY_LOCAL_MACHINE\SOFTWARE\Symantec\Symantec Endpoint Protection\CurrentVersion\public-opstate	RebootReason	"Registers the reason for a restart of the client computer. 0=No reboot required. 1=Reboot required for threat remediation. 2=Reboot required for product patch. 3=Reboot required for content update. 4=Reboot required for install completion. 5=Reboot required by SEP manager command. 6=Reboot required due to catastrophic install failure. 7=Reboot required for driver config change."
HKEY_LOCAL_MACHINE\SOFTWARE\Symantec\Symantec Endpoint Protection\CurrentVersion\public-opstate	ASRunningStatus	"Registers whether Virus and Spyware Protection is enabled or disabled. Note: This subkey appears to be redundant with the following subkey."
HKEY_LOCAL_MACHINE\SOFTWARE\Symantec\Symantec Endpoint Protection\CurrentVersion\public-opstate	DeployStatus	"Registers details about the status of client software download, installation, upgrade, or patch. This is an integer sent by the client to represent the current deployment status. It can be generated by the client itself or by the installer. 302448896=Symantec Endpoint Protection Manager indicated an

Key	Name	Description
		upgrade package for the client. 302448897=The client decided to accept the upgrade package. 302448898=The client decided to reject the upgrade package. 302449152=The client has requested package information for the upgrade. 302449153=The client has received package information for the upgrade. 302449408=The client hasn't allowed the download of the upgrade package to start. 302449409=The client has successfully downloaded and verified the upgrade package. 302449664=The client failed to apply the upgrade package. 302449665=The client failed to patch the delta. 302449666=The client failed to launch the upgrade installer. 302449667=The client successfully launched the final upgrade installer. 302449920=The client is requesting the full version of the upgrade package due to the delta's failure. 302456832=Install successful. 302460928=Install repair successful. 302465024=Uninstall successful. 302469120=Install failed and rolled back. 302469121=Install failed due to insufficient disk space. 302469122=Install failed due to a launch condition. 302469123=Install failed; a consumer product was found. 302469124=Restart pending. 302456833=Files copied. 302469125=Install failed; a legacy enterprise edition was found. 302469126=Install failed due to non-elevated privileges. 302469127=Install failed due to an incompatible operating system."

Key	Name	Description
HKEY_LOCAL_MACHINE\SOFTWARE\Symantec\Symantec Endpoint Protection\CurrentVersion\public-opstate	InstallType	"Registers the type of installed client. 0=Standard 1=Embedded or VDI 2=Dark network"
HKEY_LOCAL_MACHINE\SOFTWARE\Symantec\Symantec Endpoint Protection\CurrentVersion\public-opstate	DeployMessage	This is a freeform, detailed message sent by the client to elaborate on the deployment status.
HKEY_LOCAL_MACHINE\SOFTWARE\Symantec\Symantec Endpoint Protection\CurrentVersion\public-opstate	DeployPreviousVersion	Registers the four-part version number of the Symantec Endpoint Protection client software that was previously installed on the client computer.
HKEY_LOCAL_MACHINE\SOFTWARE\Symantec\Symantec Endpoint Protection\CurrentVersion\public-opstate	DeployTargetVersion	Registers the four-part version number of the Symantec Endpoint Protection client software that is planned for future installation on the client computer.
HKEY_LOCAL_MACHINE\SOFTWARE\Symantec\Symantec Endpoint Protection\CurrentVersion\public-opstate	DeployRunningVersion	Registers the four-part version number of the Symantec Endpoint Protection client software that is currently installed on the client computer.
HKEY_LOCAL_MACHINE\SOFTWARE\Symantec\Symantec Endpoint Protection\CurrentVersion\public-opstate	DeployTimestamp	The time of the deployment action.
HKEY_LOCAL_MACHINE\SOFTWARE\Symantec\Symantec Endpoint Protection\CurrentVersion\public-opstate	LastSuccessfulScanDateTime	Date and Time of last successful scan
HKEY_LOCAL_MACHINE\SOFTWARE\Symantec\Symantec Endpoint Protection\CurrentVersion\SharedDefs\ACDefs	AC	Version of definition the client is currently using.
HKEY_LOCAL_MACHINE\SOFTWARE\Symantec\Symantec Endpoint Protection\CurrentVersion\SharedDefs\BASHDef	BASH	Version of definition the client is currently using.
HKEY_LOCAL_MACHINE\SOFTWARE\Symantec\Symantec Endpoint Protection\CurrentVersion\SharedDefs\ccSubSDK_SCD_Defs	ccSubSDK_SCD	Version of definition the client is currently using.
HKEY_LOCAL_MACHINE\SOFTWARE\Symantec\Symantec Endpoint Protection\CurrentVersion\SharedDefs\EDRDefs	EDR	Version of definition the client is currently using.
HKEY_LOCAL_MACHINE\SOFTWARE\Symantec\Symantec Endpoint Protection\CurrentVersion\SharedDefs\EfaVTDefs	SymEFA	Version of definition the client is currently using.
HKEY_LOCAL_MACHINE\SOFTWARE\Symantec\Symantec Endpoint Protection\CurrentVersion\SharedDefs\HIDefs	HI	Version of definition the client is currently using.
HKEY_LOCAL_MACHINE\SOFTWARE\Symantec\Symantec Endpoint Protection\CurrentVersion\SharedDefs\IPSDefs	Internet Security	Version of definition the client is currently using.
HKEY_LOCAL_MACHINE\SOFTWARE\Symantec\Symantec Endpoint Protection\CurrentVersion\SharedDefs\IronRevocationDefs	IronRevocation	Version of definition the client is currently using.
HKEY_LOCAL_MACHINE\SOFTWARE\Symantec\Symantec Endpoint Protection\CurrentVersion\SharedDefs\IronSettingsDefs	IronSettings	Version of definition the client is currently using.

Key	Name	Description
HKEY_LOCAL_MACHINE\SOFTWARE\Symantec\Symantec Endpoint Protection\CurrentVersion\SharedDefs\IronWhitelistDefs	IronWhitelist	Version of definition the client is currently using.
HKEY_LOCAL_MACHINE\SOFTWARE\Symantec\Symantec Endpoint Protection\CurrentVersion\SharedDefs\PCHDefs	PCH	Version of definition the client is currently using.
HKEY_LOCAL_MACHINE\SOFTWARE\Symantec\Symantec Endpoint Protection\CurrentVersion\SharedDefs\SDSDefs	APSCandShim56	Version of definition the client is currently using.
HKEY_LOCAL_MACHINE\SOFTWARE\Symantec\Symantec Endpoint Protection\CurrentVersion\SharedDefs\SDSDefs	DEFWATCH_10	Version of definition the client is currently using.
HKEY_LOCAL_MACHINE\SOFTWARE\Symantec\Symantec Endpoint Protection\CurrentVersion\SharedDefs\SDSDefs	NAVCORP_70	Version of definition the client is currently using.
HKEY_LOCAL_MACHINE\SOFTWARE\Symantec\Symantec Endpoint Protection\CurrentVersion\SharedDefs\SDSDefs	SRTSP	Version of definition the client is currently using.
HKEY_LOCAL_MACHINE\SOFTWARE\Symantec\Symantec Endpoint Protection\CurrentVersion\SharedDefs\SMDefs	SMR	Version of definition the client is currently using.
HKEY_LOCAL_MACHINE\SOFTWARE\Symantec\Symantec Endpoint Protection\CurrentVersion\SharedDefs\SRTSPSettingsDefs	SRTSPSettings	Version of definition the client is currently using.
HKEY_LOCAL_MACHINE\SOFTWARE\Symantec\Symantec Endpoint Protection\CurrentVersion\SharedDefs\STICDefs	STIC	Version of definition the client is currently using.
HKEY_LOCAL_MACHINE\SOFTWARE\Symantec\Symantec Endpoint Protection\CurrentVersion\SharedDefs\STICDefs	STIC_SCAN	Version of definition the client is currently using.
HKEY_LOCAL_MACHINE\SOFTWARE\Symantec\Symantec Endpoint Protection\CurrentVersion\SharedDefs\SymPlatformDefs	SymPlatform	Version of definition the client is currently using.
HKEY_LOCAL_MACHINE\SOFTWARE\Symantec\Symantec Endpoint Protection\CurrentVersion\SharedDefs\TDADDefs	TDAD	Version of definition the client is currently using.
HKEY_LOCAL_MACHINE\SOFTWARE\Symantec\Symantec Endpoint Protection\SMC	CurLocation	Currrent location of device
HKEY_LOCAL_MACHINE\SOFTWARE\Symantec\Symantec Endpoint Protection\SMC	EnableDebug802.1x	This debug setting is used to help isolate EAP 802.1x issues. The registry key causes the 802.1x EAP information to write to the standard debug.log file.
HKEY_LOCAL_MACHINE\SOFTWARE\Symantec\Symantec Endpoint Protection\SMC	smc_debug_level	"smc_debug_level affects the logging of virus and spyware events: • 2 - system debugger • 4 - transaction logs • 6 - everything"
HKEY_LOCAL_MACHINE\SOFTWARE\Symantec\Symantec Endpoint Protection\SMC	smc_debug_log_level	"smc_debug_log_level affects the logging of firewall events: • 0 - debug • 1 - info • 2 - warning • 3 - fatal"

Key	Name	Description
HKEY_LOCAL_MACHINE\SOFTWARE\Symantec\Symantec Endpoint Protection\SMC	smc_engine_status	To check if Network Threat Protection is installed and is Turned ON. 0 – means turned OFF 1- turned ON
HKEY_LOCAL_MACHINE\SOFTWARE\Symantec\Symantec Endpoint Protection\SMC\SSHelper	EnableScriptDebug	The Host Integrity is performed on the agent machine by a JavaScript file included in the policies downloaded from the policy manager. Normally this script is deleted once Host Integrity is done, but by setting this registry key the file is not deleted. Then you can review the script for troubleshooting.
HKEY_LOCAL_MACHINE\SOFTWARE\Symantec\Symantec Endpoint Protection\SMC\SYLINK\SyLink	DumpSylink	Sylink is the client component responsible for communication with the Symantec Endpoint Protection Manager (SEPM) server. The following debug setting is an alternative to running the SylinkWatcher/SylinkMonitor tool to log client-server communication.
HKEY_LOCAL_MACHINE\SOFTWARE\Symantec\Symantec Endpoint Protection\SMC\SYLINK\SyLink	HardwareID	To know the Hardware ID for the Client
HKEY_LOCAL_MACHINE\SOFTWARE\Symantec\Symantec Endpoint Protection\SMC\SYLINK\SyLink	PolicyMode	Client is communicating with SEPM or is OFFLINE 1 – means communicating 0- means offline
HKEY_LOCAL_MACHINE\SOFTWARE\Symantec\Symantec Endpoint Protection\SMC\SYLINK\SyLink	Preferredgroup	Which Group the client is pointing to
HKEY_LOCAL_MACHINE\SOFTWARE\Symantec\Symantec Endpoint Protection\SMC\SYLINK\SyLink	SerialNumber	Policy Serial Number on Client
HKEY_LOCAL_MACHINE\SOFTWARE\Symantec\Symantec Endpoint Protection\SMC\TSE	ExtendedDebug	Extended TSE debugging for Network Threat Protection
HKEY_LOCAL_MACHINE\SOFTWARE\Symantec\Symantec Endpoint Protection\SMC\Trident	AutoLocationDump	This debug setting makes the Symantec Endpoint Protection agent write AutoLocation switching information to the standard debug.log file.