

General AV LIST for Windows

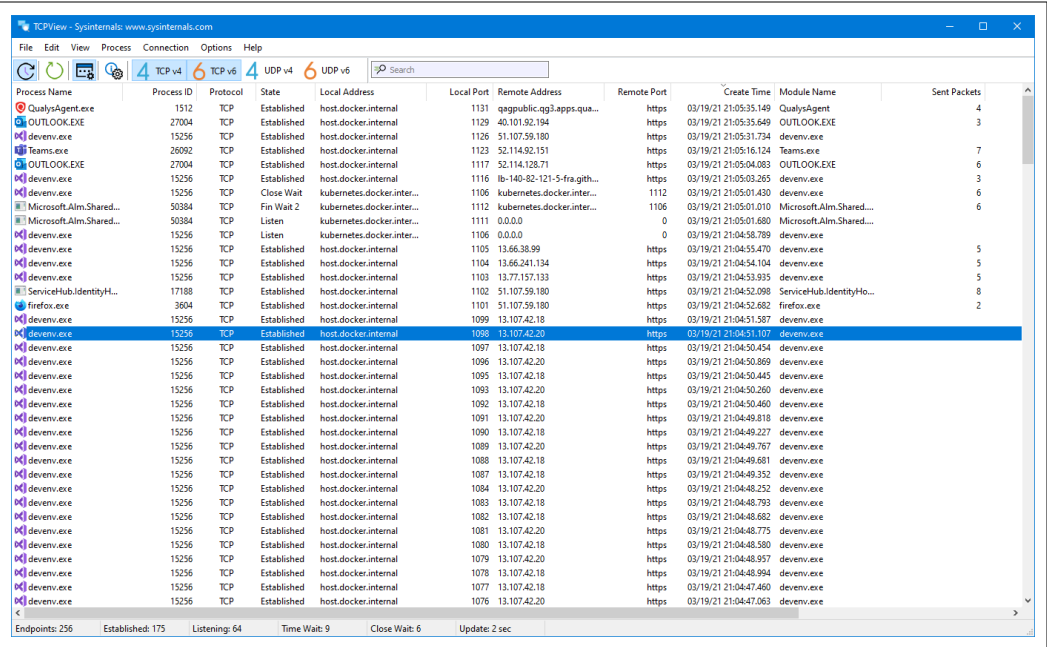
Malwarebytes RootKit	S	General Bet AV
Bitdefender	B	Random AV
Microsoft Malicious Software Removal Tool	B	Long very long and worse then MalwareBytes
Superantispyware	S	LOTS of useful tools and solid analysis the AV part is the worst part about this
KasperskyAV RootKiller	A	Best AV but this is paid
https://loaris.app	A	Trojan Remover Remove stuff very well better then even malwarebytes
ESET Online Scanner	B	Just Another AV

SysInternals

Sysmon	A	Monitors and reports key system activity via the Windows event log. Just use [name of the XDR product we plan to use]
AccessChk	S	AccessChk is a command-line tool for viewing the effective permissions on files, registry keys, services, processes, kernel objects, and more.
AccessEnum	S	This simple yet powerful security tool shows you who has what access to directories, files and Registry keys on your systems. Use it to find holes in your permissions.
AdExplorer	B	Active Directory Explorer is an advanced Active Directory (AD) viewer and editor.
AdInsight		An LDAP (Light-weight Directory Access Protocol) real-time monitoring tool aimed at troubleshooting Active Directory client applications. This might be useful for RVB
AdRestore	S	Undelete Server 2003 Active Directory objects. 1. To list all tombstoned objects without restoring: a. adrestore 2. To list all tombstoned objects with a name that starts with "User":

		<ul style="list-style-type: none"> a. adrestore User 3. To restore a specific object by its distinguished name (DN): <ul style="list-style-type: none"> a. adrestore "cn=John Doe,ou=Users,dc=example,dc=com" 4. To interactively restore tombstoned objects: <ul style="list-style-type: none"> a. adrestore -r
Autoruns	SS	See what programs are configured to startup automatically when your system boots and you login. Autoruns also shows you the full list of Registry and file locations where applications can configure auto-start settings.
Diskmon	B	This utility captures all hard disk activity or acts like a software disk activity light in your system tray.
FindLinks	B	FindLinks reports the file index and any hard links (alternate file paths on the same volume.md) that exist for the specified file. A file's data remains allocated so long as it has at least one file name referencing it.
Handle	S	<p>This handy command-line utility will show you what files are open by which processes, and much more.</p> <ul style="list-style-type: none"> 1. To display the list of all handles, simply run: <ul style="list-style-type: none"> a. handle 2. To display the handles belonging to a specific process, you can use the process ID (PID): <ul style="list-style-type: none"> a. handle -p <PID> 3. To search for all handles that contain a specific keyword, use: <ul style="list-style-type: none"> a. handle <keyword> 4. To display information about all handles for a specific type, such as files, use: <ul style="list-style-type: none"> a. handle -t File b. c.
ListDLLs	A	<p>List all the DLLs that are currently loaded, including where they are loaded and their version numbers.</p> <ul style="list-style-type: none"> 1. To report all DLLs loaded by processes: <ul style="list-style-type: none"> a. listdlls 2. To list DLLs loaded by a specific process (by name): <ul style="list-style-type: none"> a. listdlls notepad 3. To show the full path to each DLL: <ul style="list-style-type: none"> a. listdlls -c 4. a.
LogonSessions	A	<p>List the active login sessions on a system.</p> <ul style="list-style-type: none"> - Useful for nats
PortMon	A	Monitor serial and parallel port activity with this advanced monitoring tool. It knows about all standard serial and parallel IOCTLS and even shows you a portion of the data being sent and received. Version 3.x has powerful new UI enhancements and advanced filtering capabilities.
ProcDump	A	This command-line utility is aimed at capturing process dumps of otherwise difficult to isolate and reproduce CPU spikes. It also serves as a general process dump creation utility and can also monitor and generate

		process dumps when a process has a hung window or unhandled exception.
Process Explorer	SSSS SSSS SSSS	Find out what files, registry keys and other objects processes have open, which DLLs they have loaded, and more. This uniquely powerful utility will even show you who owns each process.
Process Monitor	SS	Monitor file system, Registry, process, thread and DLL activity in real-time.
PsExec	A	Execute processes on remote systems. - allows for priv esc / use of system account SEXXXX????
PsFile	?	See what files are opened remotely. - NATs?
PsGetSid	B	Displays the SID of a computer or a user.
PsKill	SSS	Terminate local or remote processes. - Usage: pskill process id
PsList	S	Show information about processes and threads.
PsLogList	A	Dump event log records.
RegDelNull	S	Scan for and delete Registry keys that contain embedded null-characters that are otherwise undeleteable by standard Registry-editing tools.
ShellRunas	LOL	Launch programs as a different user via a convenient shell context-menu entry.
SDelete	SS	Securely overwrite your sensitive files and cleanse your free space of previously deleted files using this DoD-compliant secure delete program.
Sigcheck	SSSS SSSS	Dump file version information and verify that images on your system are digitally signed. 1. To check signatures recursively in a directory, use: a. sigcheck -s <path to directory> 2. To check a file against the VirusTotal database using your private API key, use: a. sigcheck -vt <path to file> 3. To see the catalog for the file (if applicable): a. sigcheck -k <path to file> b. In the context of Microsoft Windows operating systems, a "catalog" file (with a .cat extension) is used to store a collection of digital signatures for a number of files, typically for driver packages. When you install a new hardware driver, Windows uses catalog files to validate that the files included in the driver package are signed and have not been tampered with. c.
TCPView	SSS	Active socket viewer.

		
--	--	--

Streams	S	<p>Reveal NTFS alternate streams.</p> <ul style="list-style-type: none">- streams [-s] [-d] <file or directory>- -s Recurse subdirectories.- -d Delete streams.- Streams takes wildcards e.g. 'streams *.txt'.-
---------	---	---

SecuiryXpload Upload Tools

Advanced Windows Service Manager	SSS	'Advanced Windows Service Manager' can help you to detect those Malicious services easily from hundreds of running services. You can then use integrated 'Online Scan' to further verify it through one of online services such as VirusTotal, ProcessLibrary, Google etc.
DLL Hijack Auditor		<p>DLL Hijack Auditor is the smart tool to Audit against the Dll Hijacking Vulnerability in any Windows application.</p> <p>This is one of the critical security issues affecting almost all Windows systems. Though most of the apps have been fixed, still many Windows applications are susceptible to this vulnerability which can allow any attacker to completely take over the system.</p>

DLL Finder		In the same
NoVirusThanks Tools		
https://www.usbradar.com	B	USB Radar is a service-only application that tracks USB device events on Windows OS, can track when a USB device is inserted /plugged-in, can track when a file is copied/moved from/to a USB device, can track files deleted on a USB device etc. USB Radar will also log the date and time, the PC username, useful device information, and the full file path of copied files. This is useful to completely track important
https://www.syshardener.com	A	Windows OS security application that allows you to harden Windows settings to mitigate cybersecurity threats. With this tool you can restrict functionalities of Windows and secure vulnerable applications (i.e Office and Adobe Reader). You can unassociate VBS, VBE, JS, ISO, IMG, MSI, CHM file type associations, disable Macros and ActiveX on Office, disable unused Windows Services, block outbound connections of specific programs via Windows Firewall,
https://www.osarmor.com	A	OSArmor is a Windows OS application that monitor and block suspicious processes behaviors to prevent infections by malware, ransomware, and other threats. This tool analyzes parent processes and prevents, for example, MS Word from running cmd.exe or powershell.exe. It prevents ransomware from deleting shadow copies of files via vssadmin.exe, blocks processes with double file extensions (i.e invoice.pdf.exe), blocks USB-spreading malware, and much more. It
Nirsoft Upload Tools (Fucking Amazing)		
AlternateStreamView v1.58	SSS	AlternateStreamView is a small utility that allows you to scan your NTFS drive, and find all hidden alternate streams stored in the file system. After scanning and finding the alternate streams, you can extract these streams into the specified folder, delete unwanted streams, or save the streams list into a text/html/csv/xml file.
PasswordFox v1.70	SS	PasswordFox is a small password recovery tool that allows you to view the user names and passwords stored by Mozilla Firefox Web browser. By default, PasswordFox displays the passwords stored in your current profile, but you can easily select to watch the passwords of any other Firefox profile. For each password entry, the following information is displayed: Record Index, Web Site, User Name, Password, User Name Field, Password Field, and the Signons filename. ChromePass v1.58
EncryptedRegView v1.05	SSS	EncryptedRegView is a tool for Windows that scans the Registry of your current running system or the Registry of external hard drive you choose and searches for data encrypted with DPAPI (Data Protection API). When it finds encrypted data in the Registry, it tries to decrypt it and displays the decrypted data in the main window of EncryptedRegView. With this tool, you may find passwords and other secret data stored in the Registry by Microsoft products as well as by 3-party products.
LoadedDllsView - Show in which processes every DLL is loaded		
WinPrefetchView v1.37	SSS	Each time that you run an application in your system, a Prefetch file which contains information about the files loaded by the application is created by Windows operating system. The information in the Prefetch file is used for optimizing the loading time of the application the next time that you run it.

		WinPrefetchView is a small utility that reads the Prefetch files stored in your system and displays the information stored in them. By looking in these files, you can learn which files every application is using, and which files are loaded on Windows boot.
EDR/SIEM		
AURORA	???	The AURORA Agent is a lightweight and customisable EDR agent based on Sigma. It uses Event Tracing for Windows (ETW) to recreate events that are very similar to the events generated by Microsoft's Sysmon and applies Sigma rules and IOCs to them. AURORA complements the open Sigma standard with "response actions" that allow users to react to a Sigma match.
https://heimdalsecurity.com/blog/open-source-edr-tools/		
https://wazuh.com/?utm_id=PM		Found this john hammond guide: https://www.youtube.com/watch?v=i68atPbB8uQ
https://www.nirsoft.net/utis/index.html way to many tools		