Known DLLs				
advapi32.dll	clbcatq.dll	combase.dll	COMDLG32.dll	difxapi.dll
gdi32.dll	gdiplus.dll	IMAGEHLP.dll	IMM32.dll	kernel32.dll
LPK.dll	MSCTF.dll	MSVCRT.dll	NORMALIZ.dll	NSI.dll
ole32.dll	OLEAUT32.dll	PSAPI.DLL	rpcrt4.dll	sechost.dll
Setupapi.dll	SHELL32.dll	SHLWAPI.dll	user32.dll	WLDAP32.dll
Wow64.dll	Wow64cpu.dll	Wow64win.dll	WS2_32.dll	

API Calls	Possible Trojan Functionality
GetSystemDirectoryA **GetDriveTypeA** **GetLogicalDrives** **DeleteFileA** **FindNextFileA** **FindFirstFileA** **CreateFileA** **WriteFileA** **CopyFileA**	File system traversal and file manipulation such as creating, editing, deleting, or searching for files
TerminateProcessA **Process32First** **Process32Next** **ShellExecuteA** **CreateProcessA**	Process termination, enumeration, or creation
RegSetValueA **RegDeleteKeyA** **RegCreateKeyExA** **RegOpenKeyExA** **RegQueryInfoKeyA** **RegCloseKeyA**	Registry enumeration/manipulation
RegisterServiceCtrlHandlerA **CreateServiceA** **StartServiceA** **QueryServiceStatus** **SetServiceStatus** **OpenSCManagerA**	Windows service enumeration/creation/config
InternetReadFile **InternetOpenA** **InternetConnectA** **InternetConnectA** **InternetOpenUrlA** **HttpSendRequestA** **HttpOpenRequestA**	HTTP related API calls

File Analysis Columns	Tracking Analysis Columns	Tasks Analysis Columns	Autoruns Analysis Columns
Filename	**Source Module Filename**	**Source Module Filename**	**Source Module Filename**
File size	**Event**	**Event**	**Event**
Machine Count	**Target Module Filename**	**Target Module Filename**	**Target Module Filename**
Packed	**Target Module Path**	**Target Module Path**	**Target Module Path**
Signature	**Source Command Line**	**Arguments**	**Arguments**
Full Path	**Hidden**	**Registry Path**	**Registry Path**
Days Since Compilation			
Section Names			
Hidden			

IR ECAT Hunting Guide Cheat Sheet

Instant IOCs	Potential Impact
Suspicious SVCHOST running	A running SVCHOST.exe module that is not signed by Microsoft
Suspicious services registry entry	An ACCESS DENIED message from a @ImagePath or @ServiceDll entry
Hidden & Beacon	The file or directory the process is running from is hidden from the user and the module is contacting the internet at regular intervals
Suspect thread & Network access	Threads in floating code or where or threads whose service table was hooked. Could indicate process injection of malicious code that contacts the network
Floating code & suspect thread	A thread in floating code indicates process injection of malware. PlugX and Duqu 2.0 are two Examples of malware that will use this technique to hide from User space tools
Suspect thread & Hooking	Thread in floating code or where or threads whose service table was hooked that hooks another module. Could represent rootkit activities
Floating module in browser process	A module that has no image on disk and is loaded into a browser could represent memory resident malware from an exploit or code injection from another module.
Unsigned run key present once in environment	An unsigned Registry Run key that is not found elsewhere in the environment. This could represent an advanced adversary with a beachhead in the environment or commodity malware.
Written by blacklisted module	A previously blacklisted module that writes a new module. If there is an ongoing investigation and the malware has been identified this represents the attacker dropping more tools or malware onto the system.
Services in program data	A Windows service should never be run out of the ProgramData directory and is nearly always malicious.
Unsigned creates remote thread	An unsigned module creating a remote thread is an indicator of code injection. This can be a Trojans method of hiding from User land tools or password dumping if the target process is lsass.exe
Unsigned copy itself as AutoStart	This is indicative of a dropper entrenching itself in the filesystem and then registering an autorun mechanism
Unsigned writes executable to startup directory	This is indicative of a dropper entrenching itself in the filesystem by unpacking a Trojan to the startup directory
Directory hidden	Module exists within a hidden directory, a common way to hide from User land tools.
Runs NET.EXE	Cmd.exe will likely have many hits for this IOC but reconnaissance batch files or small executables running recon commands will execute this
Runs AT.EXE	Indicates possibly lateral movement. If cmd.exe is triggered, the analyst should pivot into the host and examine the Tasks under Scan Data to get the arguments and determine severity.
Runs CMD.EXE	There will be many hits for this IOC. Explorer.exe and vmwaretools.exe will run cmd.exe for legitimate purposes. Other modules running cmd.exe should be examined especially if they are HTTP daemons, scripting language interpreters like powershell.exe, cscript.exe or wmiprsrve.exe.
Unsigned writes executable to UNC	This is indicative of lateral movement in the environment but could also be benign. Examine what binaries were copied over and to what directories on the remote host
Autorun unsigned ServiceDLL	Service DLL's are generally digitally signed by the authoring organization. Printer and camera drivers often show up with this IOC but there shouldn't be many to sort through
Floating module in OS process	A module that has no image on disk and is loaded into an OS process could represent code injection
Floating module & Network access	A module in memory that has no image on disk. This could represent memory resident only malware. Oftentimes it is an AV product
Reads document	Many legitimate applications will be reading documents. The analyst should examine the binaries reading the documents as this could indicate packaging and staging of exfil data