Maldetect: Detecting Unknown Malware

Processos Maliciosos Encontrados:

PID	process_name	ranking	anomaly_description	log_information
172	mspaint.exe	21	Filho de Processo suspeito! Área de memória com flag de write_exec! Load DLL num contexto suspeito! Load DLL num contexto suspeito! Load DLL num contexto suspeito! Processo realiza um hook suspeito na função: wow64.dll!Wow64PrepareForDebuggerAttach at 0x74c3d438! Processo realiza um hook suspeito na função: wow64.dll!Wow64SuspendLocalThread at 0x74c3c174!	Hash sha256: 4f07feaa03f508604e0fc4b09b1137aebc1d4121e4aa4d41450c97308db28ef3, nÃ£o encontrado na base do virustotal!
2784	svchost.exe	19	Pai não encontrado! Caminho incorreto! username incorreto Falta parâmetro -k Área de memória com flag de write_exec! Processo realiza um hook suspeito na função: wow64.dll!Wow64PrepareForDebuggerAttach at 0x74c3d438! Processo realiza um hook suspeito na função: wow64.dll!Wow64SuspendLocalThread at 0x74c3c174!	Hash sha256: 8ed2590e4c84962eed302f05aec191dcf470286224f14b04a3ba61fae83618cc Detected by: 0 / 57
2528	calc.exe	17	Área de memória com flag de write_exec! Load DLL num contexto suspeito! Load DLL num contexto suspeito! Load DLL num contexto suspeito! Processo realiza um hook suspeito na função: wow64.dll!Wow64PrepareForDebuggerAttach at 0x74c3d438! Processo realiza um hook suspeito na função: wow64.dll!Wow64SuspendLocalThread at 0x74c3c174!	Hash sha256: a06fa2f5d0f25939bbb3bc954dff7ba2e141ee872e0168f02c48dfb2b6e26a1e, nÃ£o encontrado na base do virustotal!

2840	DumpIt.exe	15	Este artefato esta sendo executado a partir da pasta users! Processo realiza um hook suspeito na função: wow64.dll!Wow64PrepareForDebuggerAttach at 0x74c3d438! Processo realiza um hook suspeito na função: wow64.dll!Wow64SuspendLocalThread at 0x74c3c174!	
1928	explorer.exe	1	Área de memória com flag de write_exec!	
1800	svchost.exe	1	Área de memória com flag de write_exec!	
1860	cmd.exe	1	Caminho incorreto!	

DLLs Maliciosas Encontrados:

base	DLL	ranking	anomaly_description

Atividades de Rede Suspeitas:

PID	process_name	protocol	local_ip	local_port	remote_ip	remote_port	state

Histórico de Acessos do iexplore.exe:

pid	url

Histórico de Comando do cmd.exe:

****

CommandProcess: conhost.exe Pid: 1244

CommandHistory: 0x86700 Application: DumpIt.exe Flags: Allocated

CommandCount: 0 LastAdded: -1 LastDisplayed: -1

FirstCommand: 0 CommandCountMax: 50

ProcessHandle: 0x60

Cmd #15 @ 0x30158:

Cmd #16 @ 0x85030: