Maldetect: Detecting Unknown Malware

Processos Maliciosos Encontrados:

PID	process_name	ranking	anomaly_description	log_information
1476	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: 053b6d67b0d4e2702ce466fef9d61fa60bff0657ecc6e777409d2d6264cb4c42, nÃ£o encontrado na base do virustotal!
1344	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	3	Porta ou conexão suspeita! Porta ou conexão suspeita! Área de memória com flag de write_exec!	
252	svchost.exe	2	Porta ou conexão suspeita! Porta ou conexão suspeita!	
1800	svchost.exe	1	Área de memória com flag de write_exec!	
1548	msiexec.exe	1	Área de memória com flag de write_exec!	
2404	mscorsvw.exe	1	Área de memória com flag de write_exec!	
2628	mscorsvw.exe	1	Área de memória com flag de write_exec!	

472	conhost.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
252	svchost.exe	TCPv4	-	49268	127.0.0.1	80	CLOSED
1928	explorer.exe	TCPv4	-	49267	127.0.0.1	80	CLOSED
252	svchost.exe	TCPv4	-	49264	224.0.0.22	80	CLOSED
1928	explorer.exe	TCPv4	-	49266	255.255.255.255	80	CLOSED

Histórico de Acessos do iexplore.exe:

pid	url

Histórico de Comando do cmd.exe:

****

CommandProcess: conhost.exe Pid: 644
CommandHistory: 0x356650 Application: cmd.exe Flags: Allocated, Reset
CommandCount: 1 LastAdded: 0 LastDisplayed: 0
FirstCommand: 0 CommandCountMax: 50
ProcessHandle: 0x60
Cmd #0 @ 0x3551c0: ipconfig
Cmd #15 @ 0x300158: 6
Cmd #16 @ 0x355950: 5

****

CommandProcess: conhost.exe Pid: 2636
CommandHistory: 0xb6700 Application: DumpIt.exe Flags: Allocated
CommandCount: 0 LastAdded: -1 LastDisplayed: -1

FirstCommand: 0 CommandCountMax: 50

ProcessHandle: 0x60

Cmd #15 @ 0x60158:

Cmd #16 @ 0xb5030: