Maldetect: Detecting Unknown Malware

Processos Maliciosos Encontrados:

PID	process_name	ranking	anomaly_description	log_information
2784	svchost.exe	9	Pai não encontrado!Caminho incorreto!username incorretoFalta parâmetro -kÁrea de memória com flag de write_exec!	Hash sha256: 8ed2590e4c84962eed302f05aec191dcf470286224f14b04a3ba61fae83618cc Detected by: 0 / 57
172	mspaint.exe	5	Filho de Processo suspeito!Área de memória com flag de write_exec!	Hash sha256: 4f07feaa03f508604e0fc4b09b1137aebc1d4121e4aa4d41450c97308db28ef3, não encontrado na base do virustotal!
4	System	3	Utiliza técnicas de ocultação de processos!	
220	smss.exe	3	Utiliza técnicas de ocultação de processos!	
296	csrss.exe	3	Utiliza técnicas de ocultação de processos!	
340	csrss.exe	3	Utiliza técnicas de ocultação de processos!	
2072	chrome.exe	3	Utiliza técnicas de ocultação de processos!	
2840	DumpIt.exe	3	Utiliza técnicas de ocultação de processos!	
1928	explorer.exe	1	Área de memória com flag de write_exec!	
1800	svchost.exe	1	Área de memória com flag de write_exec!	
2528	calc.exe	1	Área de memória com flag de write_exec!	
1860	cmd.exe	1	Caminho incorreto!	

Atividades de Rede Suspeitas:

PID	process_name	protocol	local_ip	local_port	remote_ip	remote_port	state

Histórico de Comando do cmd.exe:

history

```
**********************************************
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:
```