Maldetect: Detecting Unknown Malware

Processos Maliciosos Encontrados:

PID	process_name	ranking	anomaly_description	log_information
3012	MALDETECT-PC.e	8	Este processo esta sendo executa a partir da pasta appData!Load DLL num contexto suspeito!Área de memória com flag de write_exec!	Hash sha256: 140a0a7092379fb60f9126c17c8fe04f97ace77097f30383dd2c03994272ddcb, 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!	
252	svchost.exe	2	Porta ou conexão suspeita!Porta ou conexão suspeita!	
1928	explorer.exe	1	Área de memória com flag de write_exec!	
1800	svchost.exe	1	Área de memória com flag de write_exec!	
684	iexplore.exe	1	Área de memória com flag de write_exec!	
1376	iexplore.exe	1	Área de memória com flag de write_exec!	
2384	iexplore.exe	1	Área de memória com flag de write_exec!	

Atividades de Rede Suspeitas:

PID	process_name	protocol	local_ip	local_port	remote_ip	remote_port	state

252	svchost.exe	TCPv4	-	49268	224.0.0.252	80	CLOSED
252	svchost.exe	TCPv6	-	0	-	0	CLOSED

Histórico de Comando do cmd.exe:

history

```
**************************************************
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: 5
Cmd #16 @ 0x355950: 5
**************************************************
CommandProcess: conhost.exe Pid: 472
CommandHistory: 0xc6740 Application: DumpIt.exe Flags: Allocated
CommandCount: 0 LastAdded: -1 LastDisplayed: -1
FirstCommand: 0 CommandCountMax: 50
ProcessHandle: 0x60
Cmd #15 @ 0x70158:
Cmd #16 @ 0xc5070:
```