Maldetect: Detecting Unknown Malware

Processos Maliciosos Encontrados:

PID	process_name	ranking	anomaly_description	log_information
2920	DumpIt.exe	15	Este artefato esta sendo executado a partir da pasta users! Processo realiza um hook suspeito na função: wow64.dll!Wow64PrepareForDebuggerAttach at 0x74bfd438! Processo realiza um hook suspeito na função: wow64.dll!Wow64SuspendLocalThread at 0x74bfc174!	Hash sha256: ab09696fd64d0e11bf2a903f8bad39ce781721a00cd94affc033bae09134478b, nÃ£o encontrado na base do virustotal!
3012	MALDETECT-PC.e	8	Este artefato esta sendo executado a partir da pasta appData! Área de memória com flag de write_exec! Load DLL num contexto suspeito!	Hash sha256: 140a0a7092379fb60f9126c17c8fe04f97ace77097f30383dd2c03994272ddcb, nÃ£o encontrado na base do virustotal!
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!	Hash sha256: c22455ffd59e88e375aa8e4e6cec82e3c573de525d0fcfd5940a1766296f4814, nÃ£o encontrado na base do virustotal!
1376	iexplore.exe	1	Área de memória com flag de write_exec!	Hash sha256: 1b8614fde6c1b314847fc0e0d248b4139d6673db1525c4fa427a9851e3448b26, nÃ£o encontrado na base do virustotal!
2384	iexplore.exe	1	Área de memória com flag de write_exec!	

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	224.0.0.252	80	CLOSED
252	svchost.exe	TCPv6	-	0	-	0	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: 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:
```