

Maldetect: Detecting Unknown Malware

Processos Maliciosos Encontrados:

PID	process_name	ranking	anomaly_description	log_information
3028	jackal.exe.exe	31	Cria um filho cmd.exe!Cria um filho cmd.exe!Mutex malicioso! mutex__Dassara__Malware family =jackalPorta ou conexão suspeita!Backdoor!Hash sha256: 4810c6ed3fef2a571dad00f20e8f9262cb866c642da8dc7bf73add7aca4ec4c3 Detected by: 12 / 57Load DLL num contexto suspeito!Load DLL num contexto suspeito!	http://download.microsoft.com/download/A/6/A/A6AC035D-DA3F-4F0C-ADA4-37C http://download.microsoft.com/download/7/0/A/70AABEC5-CCC0-40C8-BC09-CAE http://download.microsoft.com/download/9/7/E/97ED8B6B-C021-4D4B-A33E-CB4 http://146.82.77.59/s91911/klsjall/filter.txt http://go.microsoft.com/index.html http://128.134.176.126/exists/Pasadena.doc http://128.134.176.126/index.html Visited: Daniel@ http://go.microsoft.com/favicon.ico Visited: Daniel@ http://go.microsoft.com/fwlink/?LinkId=69157 Visited: Daniel@ https://ieonline.microsoft.com/favicon.ico Visited: Daniel@ http://go.microsoft.com/fwlink/?LinkId=191282 Visited: Daniel@ http://go.microsoft.com/index.html?LinkId=69157 Visited: Daniel@ http://go.microsoft.com/index.html?LinkId=69157 Visited: Daniel@ http://go.microsoft.com/index.html?LinkId=191282
1084	cmd.exe	7	Pai incorreto!Backdoor!	
1608	cmd.exe	5	Utiliza técnicas de ocultação de processos!Pai incorreto!	
244	smss.exe	4	Caminho diferente. Processo suspeito!Utiliza técnicas de ocultação de processos!	
3116	svchost.exe	4	Utiliza técnicas de ocultação de processos!Área de memória com flag de write_exec!	
4	System	3	Utiliza técnicas de ocultação de processos!	
336	csrss.exe	3	Utiliza técnicas de ocultação de processos!	
376	csrss.exe	3	Utiliza técnicas de ocultação de processos!	
480	services.exe	3	Utiliza técnicas de ocultação de processos!	
488	lsass.exe	3	Utiliza técnicas de ocultação de processos!	
496	lsm.exe	3	Utiliza técnicas de ocultação de processos!	
384	wininit.exe	1	Caminho suspeito!	
308	conhost.exe	1	Caminho incorreto!	
2544	explorer.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
3028	jackal.exe.exe	TCPv4	0.0.0.0	9090	0.0.0.0	0	LISTENING

Histórico de Comando do cmd.exe:

history
***** CommandProcess: conhost.exe Pid: 1652 CommandHistory: 0x30f498 Application: cmd.exe Flags: Allocated, Reset CommandCount: 1 LastAdded: 0 LastDisplayed: 0 FirstCommand: 0 CommandCountMax: 50 ProcessHandle: 0x5c Cmd #0 @ 0x306ba8: c:\windows\system32\jackal.exe Cmd #19 @ 0x300030: ***** CommandProcess: conhost.exe Pid: 1652 CommandHistory: 0x30f658 Application: jackal.exe Flags: Allocated CommandCount: 0 LastAdded: -1 LastDisplayed: -1 FirstCommand: 0 CommandCountMax: 50 ProcessHandle: 0x54 ***** CommandProcess: conhost.exe Pid: 1652 CommandHistory: 0x30f7c8 Application: cmd.exe Flags: Allocated CommandCount: 0 LastAdded: -1 LastDisplayed: -1 FirstCommand: 0 CommandCountMax: 50 ProcessHandle: 0xd8