

## Maldetect: Detecting Unknown Malware

### Processos Maliciosos Encontrados:

PID	process_name	ranking	anomaly_description	log_information
3028	jackal.exe.exe	33	Cria um filho cmd.exe! Cria um filho cmd.exe! Mutex malicioso! mutex__Dassara__Malware family =jackal Backdoor! Porta ou conexão suspeita! Load DLL num contexto suspeito! Load DLL num contexto suspeito! Load DLL num contexto suspeito! Hash sha256: 4810c6ed3fef2a571dad00f20e8f9262cb866c642da8dc7bf73add7aca4ec4c3 Detected by: 12 / 57	
1084	cmd.exe	7	Pai incorreto! Backdoor!	
1608	cmd.exe	2	Pai incorreto!	
244	smss.exe	1	Caminho diferente. Processo suspeito!	
384	wininit.exe	1	Caminho suspeito!	
308	conhost.exe	1	Caminho incorreto!	
2544	explorer.exe	1	Área de memória com flag de write_exec!	
3116	svchost.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
3028	jackal.exe.exe	TCPv4	0.0.0.0	9090	0.0.0.0	0	LISTENING

**Histórico de Acessos do iexplore.exe:**

pid	url
3028	http://download.microsoft.com/download/A/6/A/A6AC035D-DA3F-4F0C-ADA4-37C8E5D34E3D/setup/SDKSetup.cab
3028	http://download.microsoft.com/download/7/0/A/70AABEC5-CCC0-40C8-BC09-CAE60F8E94E0/NrPolicy.cab
3028	http://download.microsoft.com/download/9/7/E/97ED8B6B-C021-4D4B-A33E-CB43D19859C7/NeutralMSU/x86fre/IE9-win7.msu
3028	http://146.82.77.59/s91911/klsjall/filter.txt
3028	http://go.microsoft.com/index.html
3028	http://128.134.176.126/exists/Pasadena.doc
3028	http://128.134.176.126/index.html
3028	Visited: Daniel@http://go.microsoft.com/favicon.ico
3028	Visited: Daniel@http://go.microsoft.com/fwlink/?LinkId=69157
3028	Visited: Daniel@https://ieonline.microsoft.com/favicon.ico
3028	Visited: Daniel@http://go.microsoft.com/fwlink/?LinkId=191282
3028	Visited: Daniel@http://go.microsoft.com/index.html?LinkId=69157
3028	Visited: Daniel@http://go.microsoft.com/index.html?LinkId=69157
3028	Visited: Daniel@http://go.microsoft.com/index.html?LinkId=191282

**Histórico de Comando do cmd.exe:**

\*\*\*\*\*

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