Power(Shell)ing Through the Timeline

DISK ARTIFACT ANALYSIS AT SCALE WITH KANSA
Tradition!
...but?
Kansa
Get-MasterFileTable.ps1

Administrator: Windows PowerShell

PS C:\Source\Kansa\Modules\Disk> \Get-MasterFileTable.ps1 -Disk 0 -Partition 0 -Verbose | Export-Csv .\mft_0_0.csv

VERBOSE: Starting to process disk \\PHYSICALDRIVE0
VERBOSE: Disk sector size is 0x200 (512) bytes
VERBOSE: Grabbing first sector and analyzing master boot record.
VERBOSE: Found 2 partition entries.

<table>
<thead>
<tr>
<th>Bootable Type</th>
<th>FirstSector</th>
<th>Length</th>
</tr>
</thead>
<tbody>
<tr>
<td>True NTFS</td>
<td>0x800</td>
<td>0xAF000 sectors (350 MB)</td>
</tr>
<tr>
<td>False NTFS</td>
<td>0xAF800</td>
<td>0x74656DB0 sectors (931 GB)</td>
</tr>
</tbody>
</table>

VERBOSE: Starting to process partition entry 0.
VERBOSE: Verified partition entry 0 refers to an NTFS partition.
VERBOSE: Partition has 512 bytes per sector and 8 sectors per cluster.
VERBOSE: MFT is 0x74A0000 (122331136) bytes into the partition.
VERBOSE: MFT file records are 0x400 (1024) bytes long.
VERBOSE: MFT index records are 0x1000 (4096) bytes long.
VERBOSE: Parsing the MFT's self-referential entry.
Why this way?

PowerShell is installed by default on all systems since Windows Vista with 3.0 and later available since Windows 7.

No need for third-party disk drivers that can introduce instability or other issues, and the project is open-source so you can verify the code before you run it.

Kansa is agentless, so there’s nothing to install.

In short: If you’re running Windows, you already have everything you need to use it.
Analysis
SELECT

  TO_DATE(TO_TIMESTAMP([StdInfo: Created], 'yyyy-MM-ddTHH:mm:ssZ')) AS [SI Created Date],
  QUANTIZE([Entry Number], 1000) AS [Entry Group],
  COUNT(*) AS [Row Count]

INTO %myOutput%

FROM %myInput%

WHERE EXTRACT_EXTENSION([File Name]) = '%myExtension%'

GROUP BY

  TO_DATE(TO_TIMESTAMP([StdInfo: Created], 'yyyy-MM-ddTHH:mm:ssZ')),
  QUANTIZE([Entry Number], 1000)
Analysis

Least-frequency analysis
Large files (staged exfiltration)
Deleted executables
On-demand compiler residue
Etc...
Shortcomings & Future work

C#
Contact me!

Jon Turner
jturner@microsoft.com
@z4ns4tsu