Detecting persistence with Kansa PowerShell framework

Dave Crim
Information Security Analyst
MISO
About: Dave Crim

- 35, married, two kids (twins)
- BS in Computer Science from Taylor University
- 13 years in IT, 10 in Cyber Security, 2 in Threat Hunting
The Problem

Malware evolves
The Solution

Use Kansa framework to scan and find persistence mechanisms.

- Build Foundation
- Gather Data
- Analyze Data
- Learn
Build Foundation
Gathering Data

On-Screen Keyboard: C:\Windows\System32\osk.exe
Magnifier: C:\Windows\System32\Magnify.exe
Narrator: C:\Windows\System32\Narrator.exe
Display switcher: C:\Windows\System32\DisplaySwitch.exe
App Switcher: C:\Windows\System32\AtBroker.exe
Sticky Keys: C:\Windows\System32\Sethc.exe
UtilMan: C:\Windows\System32\Utilman.exe
Gathering Data - Know your Organization

• Baselines
• Risk
• Capabilities
Gathering Data - Create a Module

PowerShell script that returns one or more objects with the data you want to analyze

<#
.SYNOPSIS
<Short summary>

.NOTES
The following line is required by Kansa.ps1, which uses it to determine how to handle the output from this script.
OUTPUT csv
Get-Data
#>
Let’s try it out
Analyzing Data - Stacking


• Pick a few variables, collect and group results by those variables, and then look for the unique or low-count results that stick out.

• Filter out noise such as unique usernames in path strings.
Let’s try it out
Analyzing Data – Asking Questions

- Get the raw data in something like a pivot table, or a BI tool.
- What if I stack by different fields, just one field?
- What if I only look at Windows 7 versus Windows 10 machines?
- What host has the most number of unique items?
- If I repeat this over time, how is the data changing?
- What if I compare other attributes such as task start time
What we have learned

• There is a LOT of noise, learning how to reduce and eliminate noise is critical to finding actionable intelligence.
• Find more misconfigurations, unwanted software, and change drift than actual malware.
• Automate analysis as much as possible.
• Quantitative analysis is difficult because so much of the data is qualitative. Can’t do statistics on registry keys.