50 lines (27 loc) · 2.02 KB

Preview Code Blame Raw

T1137 - Office Application Startup

Description from ATT&CK

> Adversaries may leverage Microsoft Office-based applications for persistence between startups. Microsoft Office is a fairly common application suite on Windows-based operating systems within an enterprise network. There are multiple mechanisms that can be used with Office for persistence when an Office-based application is started; this can include the use of Office Template Macros and add-ins.
> A variety of features have been discovered in Outlook that can be abused to obtain persistence, such as Outlook rules, forms, and Home Page.(Citation: SensePost Ruler GitHub) These persistence mechanisms can work within Outlook or be used through Office 365.(Citation: TechNet O365 Outlook Rules)

Atomic Tests

- Atomic Test #1 - Office Application Startup - Outlook as a C2

Atomic Test #1 - Office Application Startup - Outlook as a C2

As outlined in MDSEC's Blog post https://www.mdsec.co.uk/2020/11/a-fresh-outlook-on-mail-based-persistence/ it is possible to use Outlook Macro as a way to achieve persistance and execute arbitrary commands. This transform Outlook into a C2. Too achieve this two things must happened on the syste

- The macro security registry value must be set to '4'
- A file called VbaProject.OTM must be created in the Outlook Folder.

Supported Platforms: Windows

auto_generated_guid: bfe6ac15-c50b-4c4f-a186-0fc6b8ba936c

Attack Commands: Run with `command_prompt`!

```
reg add "HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Security\Level"
mkdir  %APPDATA%\Microsoft\Outlook\ >nul 2>&1
echo "Atomic Red Team TEST" > %APPDATA%\Microsoft\Outlook\VbaProject.OTM
```

Cleanup Commands:

```
reg delete "HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Security\Leve
del %APPDATA%\Microsoft\Outlook\VbaProject.OTM >nul 2>&1
```