Sign in

redcanaryco / **atomic-red-team** Public

Notifications Fork 2.8k Star 9.7k

Code Issues 6 Pull requests 4 Actions Wiki Security Insights

atomic-red-team / atomics / T1505.005 / **T1505.005.md**

```
54 lines (29 loc) · 3.31 KB
```

Preview Code Blame Raw

T1505.005 - Server Software Component: Terminal Services DLL

Description from ATT&CK

> Adversaries may abuse components of Terminal Services to enable persistent access to systems. Microsoft Terminal Services, renamed to Remote Desktop Services in some Windows Server OSs as of 2022, enable remote terminal connections to hosts. Terminal Services allows servers to transmit a full, interactive, graphical user interface to clients via RDP.(Citation: Microsoft Remote Desktop Services)
> Windows Services that are run as a "generic" process (ex: `svchost.exe`) load the service's DLL file, the location of which is stored in a Registry entry named `ServiceDll`.(Citation: Microsoft System Services Fundamentals) The `termsrv.dll` file, typically stored in `%SystemRoot%\System32\`, is the default `ServiceDll` value for Terminal Services in `HKLM\System\CurrentControlSet\services\TermService\Parameters\`.
>
> Adversaries may modify and/or replace the Terminal Services DLL to enable persistent access to victimized hosts.(Citation: James TermServ DLL) Modifications to this DLL could be done to execute

> arbitrary payloads (while also potentially preserving normal `termsrv.dll` functionality) as well as to simply enable abusable features of Terminal Services. For example, an adversary may enable features such as concurrent Remote Desktop Protocol sessions by either patching the `termsrv.dll` file or modifying the `ServiceDll` value to point to a DLL that provides increased RDP functionality.(Citation: Windows OS Hub RDP)(Citation: RDPWrap Github) On a non-server Windows OS this increased functionality may also enable an adversary to avoid Terminal Services prompts that warn/log out users of a system when a new RDP session is created.

Atomic Tests

- Atomic Test #1 - Simulate Patching termsrv.dll

Atomic Test #1 - Simulate Patching termsrv.dll

Simulates patching of termsrv.dll by making a benign change to the file and replacing it with the original afterwards. Before we can make the modifications we need to take ownership of the file and grant ourselves the necessary permissions.

Supported Platforms: Windows

auto_generated_guid: 0b2eadeb-4a64-4449-9d43-3d999f4a317b

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

```
$ACL = Get-Acl $fileName
$permission = "Administrators","FullControl","Allow"
$accessRule = New-Object System.Security.AccessControl.FileSystemAccessRule $permi
$ACL.SetAccessRule($accessRule)
Set-Acl -Path $fileName -AclObject $ACL

Copy-Item -Path "C:\Windows\System32\termsrv.dll" -Destination "C:\Windows\System3
Add-Content -Path "C:\Windows\System32\termsrv.dll" -Value "`n" -NoNewline -ErrorA
Move-Item -Path "C:\Windows\System32\termsrv_backup.dll" -Destination "C:\Windows\
```

Cleanup Commands:

```
Move-Item -Path "C:\Windows\System32\termsrv_backup.dll" -Destination "C:\Windows\
```