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

d0dad62

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 / T1124 / T1124.md

Atomic Red Team doc generat... Generated docs from job=generate-d... 3a6a696 · 2 years ago History

Preview Code Blame 139 lines (57 loc) · 3.46 KB Raw

T1124 - System Time Discovery

Description from ATT&CK

> An adversary may gather the system time and/or time zone from a local or remote system. The system time is set and stored by the Windows Time Service within a domain to maintain time synchronization between systems and services in an enterprise network. (Citation: MSDN System Time) (Citation: Technet Windows Time Service)
> System time information may be gathered in a number of ways, such as with Net on Windows by performing `net time \hostname` to gather the system time on a remote system. The victim's time zone may also be inferred from the current system time or gathered by using `w32tm /tz`. (Citation: Technet Windows Time Service)
>
> This information could be useful for performing other techniques, such as executing a file with a Scheduled Task/Job (Citation: RSA EU12 They're Inside), or to discover locality information based on time zone to assist in victim targeting (i.e. System Location Discovery). Adversaries may also use knowledge of system time as part of a time bomb, or delaying execution until a specified date/time.(Citation: AnyRun TimeBomb)

Atomic Tests

- Atomic Test #1 - System Time Discovery
- Atomic Test #2 - System Time Discovery - PowerShell
- Atomic Test #3 - System Time Discovery in macOS
- Atomic Test #4 - System Time Discovery W32tm as a Delay

Atomic Test #1 - System Time Discovery

Identify the system time. Upon execution, the local computer system time and timezone will be displayed.

Supported Platforms: Windows

auto_generated_guid: 20aba24b-e61f-4b26-b4ce-4784f763ca20

Inputs:

Name	Description	Type	Default Value

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

computer_name	computer name to query	String	localhost

Attack Commands: Run with `command_prompt`!

```
net time \\#{computer_name}
w32tm /tz
```

Atomic Test #2 - System Time Discovery - PowerShell

Identify the system time via PowerShell. Upon execution, the system time will be displayed.

Supported Platforms: Windows

auto_generated_guid: 1d5711d6-655c-4a47-ae9c-6503c74fa877

Attack Commands: Run with `powershell`!

```
Get-Date
```

Atomic Test #3 - System Time Discovery in macOS

Identify system time. Upon execution, the local computer system time and timezone will be displayed.

Supported Platforms: macOS

auto_generated_guid: f449c933-0891-407f-821e-7916a21a1a6f

Attack Commands: Run with `sh`!

```
date
```

Atomic Test #4 - System Time Discovery W32tm as a Delay

identifies DCRat delay time tactics using w32tm.
https://research.splunk.com/endpoint/b2cc69e7-11ba-42dc-a269-59c069a48870/
https://blogs.blackberry.com/en/2022/05/dirty-deeds-done-dirt-cheap-russian-rat-offers-backdoor-bargains

Supported Platforms: Windows

auto_generated_guid: d5d5a6b0-0f92-42d8-985d-47aafa2dd4db

Attack Commands: Run with `command_prompt`!

```
W32tm /stripchart /computer:localhost /period:5 /dataonly /samples:2
```