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 / T1114.001 / **T1114.001.md**

```
64 lines (37 loc) · 2.54 KB
```

Preview Code Blame Raw

T1114.001 - Local Email Collection

Description from ATT&CK

> Adversaries may target user email on local systems to collect sensitive information. Files containing email data can be acquired from a user's local system, such as Outlook storage or cache files.
> Outlook stores data locally in offline data files with an extension of .ost. Outlook 2010 and later supports .ost file sizes up to 50GB, while earlier versions of Outlook support up to 20GB.(Citation: Outlook File Sizes) IMAP accounts in Outlook 2013 (and earlier) and POP accounts use Outlook Data Files (.pst) as opposed to .ost, whereas IMAP accounts in Outlook 2016 (and later) use .ost files. Both types of Outlook data files are typically stored in `C:\Users\<username>\Documents\Outlook Files` or `C:\Users\<username>\AppData\Local\Microsoft\Outlook`.(Citation: Microsoft Outlook Files)

Atomic Tests

- Atomic Test #1 - Email Collection with PowerShell Get-Inbox

Atomic Test #1 - Email Collection with PowerShell Get-Inbox

Search through local Outlook installation, extract mail, compress the contents, and saves everything to a directory for later exfiltration. Successful execution will produce stdout message stating "Please be patient, this may take some time...". Upon completion, final output will be a mail.csv file.

Note: Outlook is required, but no email account necessary to produce artifacts.

Supported Platforms: Windows

auto_generated_guid: 3f1b5096-0139-4736-9b78-19bcb02bb1cb

Inputs:

Name	Description	Type	Default Value
output_file	Output file path	String	$env:TEMP\mail.csv
file_path	File path for Get-Inbox.ps1	String	PathToAtomicsFolder\T1114.001\src

Attack Commands: Run with `powershell`!

```
powershell -executionpolicy bypass -command #{file_path}\Get-Inbox.ps1 -file #{out
```

Cleanup Commands:

```
Remove-Item #{output_file} -Force -ErrorAction Ignore
```

Dependencies: Run with `powershell`!

Description: Get-Inbox.ps1 must be located at #{file_path}

Check Prereq Commands:

```
if (Test-Path #{file_path}\Get-Inbox.ps1) {exit 0} else {exit 1}
```

Get Prereq Commands:

```
Invoke-WebRequest "https://raw.githubusercontent.com/redcanaryco/atomic-red-team/ma
```