

Product Solutions Resources Open Source Enterprise Pricing

Search

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

02cb591

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 / T1070.008 / T1070.008.md

Atomic Red Team doc generat... Generated docs from job=generate-doc... b1f3c96 · last year History

Preview

Code

Blame

239 lines (120 loc) · 6.77 KB

Raw

Copy

Download

Menu

T1070.008 - Email Collection: Mailbox Manipulation

Description from ATT&CK

Adversaries may modify mail and mail application data to remove evidence of their activity. Email applications allow users and other programs to export and delete mailbox data via command line tools or use of APIs. Mail application data can be emails, email metadata, or logs generated by the application or operating system, such as export requests.

Adversaries may manipulate emails and mailbox data to remove logs, artifacts, and metadata, such as evidence of [Phishing/Internal Spearphishing](#), [Email Collection](#), [Mail Protocols](#) for command and control, or email-based exfiltration such as [Exfiltration Over Alternative Protocol](#). For example, to remove evidence on Exchange servers adversaries have used the `ExchangePowerShell` [PowerShell](#) module, including `Remove-MailboxExportRequest` to remove evidence of mailbox exports.(Citation: Volexity SolarWinds)(Citation: ExchangePowerShell Module) On Linux and macOS, adversaries may also delete emails through a command line utility called `mail` or use [AppleScript](#) to interact with APIs on macOS.(Citation: Cybereason Cobalt Kitty 2017) (Citation: mailx man page)







Adversaries may also remove emails and metadata/headers indicative of spam or suspicious activity (for example, through the use of organization-wide transport rules) to reduce the likelihood of malicious emails being detected by security products. (Citation: Microsoft OAuth Spam 2022)

Atomic Tests

- [Atomic Test #1 - Copy and Delete Mailbox Data on Windows](#)
- [Atomic Test #2 - Copy and Delete Mailbox Data on Linux](#)
- [Atomic Test #3 - Copy and Delete Mailbox Data on macOS](#)
- [Atomic Test #4 - Copy and Modify Mailbox Data on Windows](#)
- [Atomic Test #5 - Copy and Modify Mailbox Data on Linux](#)
- [Atomic Test #6 - Copy and Modify Mailbox Data on macOS](#)

Atomic Test #1 - Copy and Delete Mailbox Data on Windows

Page 1 of 4

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

Copies and deletes mail data on Windows

Supported Platforms: Windows

auto_generated_guid: d29f01ea-ac72-4efc-8a15-bea64b77fabf

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

```
New-Item -Path "C:\Users\%env:USERNAME\AppData\Local\Comms\Unistore\data
Get-ChildItem -Path "C:\Users\%env:USERNAME\AppData\Local\Comms\Unistore
Remove-Item -Path "C:\Users\%env:USERNAME\AppData\Local\Comms\Unistore\d
```

Cleanup Commands:

```
Remove-Item -Path "C:\Users\%env:USERNAME\AppData\Local\Comms\Unistore\d
```

Atomic Test #2 - Copy and Delete Mailbox Data on Linux

Copies and deletes mail data on Linux

Supported Platforms: Linux

auto_generated_guid: 25e2be0e-96f7-4417-bd16-a4a2500e3802

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

```
mkdir -p /var/spool/mail/copy
for file in /var/spool/mail/*; do
    if [ "$(basename "$file")" != "copy" ]
    then
        cp -R "$file" /var/spool/mail/copy/
    fi
done
rm -rf /var/spool/mail/copy/*
```

Cleanup Commands:

```
rm -rf /var/spool/mail/copy
```

Atomic Test #3 - Copy and Delete Mailbox Data on macOS

Copies and deletes mail data on macOS

Supported Platforms: macOS

auto_generated_guid: 3824130e-a6e4-4528-8091-3a52eeb540f6

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

```
mkdir ~/Library/Mail/copy
cp -R ~/Library/Mail/* ~/Library/Mail/copy
rm -rf ~/Library/Mail/copy/*
```

Cleanup Commands:

```
rm -rf ~/Library/Mail/copy
```

Atomic Test #4 - Copy and Modify Mailbox Data on Windows

Copies and modifies mail data on Windows

Supported Platforms: Windows

auto_generated_guid: edddff85-fee0-499d-9501-7d4d2892e79b

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

```
New-Item -Path "C:\Users\%env:USERNAME\AppData\Local\Comms\Unistore\data"
Get-ChildItem -Path "C:\Users\%env:USERNAME\AppData\Local\Comms\Unistore\data"
Get-ChildItem -Path "C:\Users\%env:USERNAME\AppData\Local\Comms\Unistore\data"
```

Cleanup Commands:

```
Remove-Item -Path "C:\Users\%env:USERNAME\AppData\Local\Comms\Unistore\data"
```

Atomic Test #5 - Copy and Modify Mailbox Data on Linux

Copies and modifies mail data on Linux

Supported Platforms: Linux

auto_generated_guid: 6d99f93c-da56-49e3-b195-163090ace4f6

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

```
mkdir -p /var/spool/mail/copy
for file in /var/spool/mail/*; do
  if [ "$(basename "$file")" != "copy" ]
  then
    cp -R "$file" /var/spool/mail/copy/
    if [ -f "/var/spool/mail/copy/$(basename "$file")" ]; then
      echo "Modification for Atomic Red Test" >> "/var/spool/mail/copy/$(basename "$file")"
    fi
  fi
done
```

Cleanup Commands:

```
rm -rf /var/spool/mail/copy
```

Atomic Test #6 - Copy and Modify Mailbox Data on macOS

Copies and modifies mail data on macOS

Supported Platforms: macOS

auto_generated_guid: 8a0b1579-5a36-483a-9cde-0236983e1665

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

```
mkdir ~/Library/Mail/copy
cp -R ~/Library/Mail/* ~/Library/Mail/copy
echo "Manipulated data" > ~/Library/Mail/copy/manipulated.txt
```

Cleanup Commands:

```
rm -rf ~/Library/Mail/copy
```