Building an Atomic Testing Program

Test. Measure. Improve.

ATT&CK CON
THE MITRE ATT&CK CONFERENCE

red canary

What is “atomic testing”?

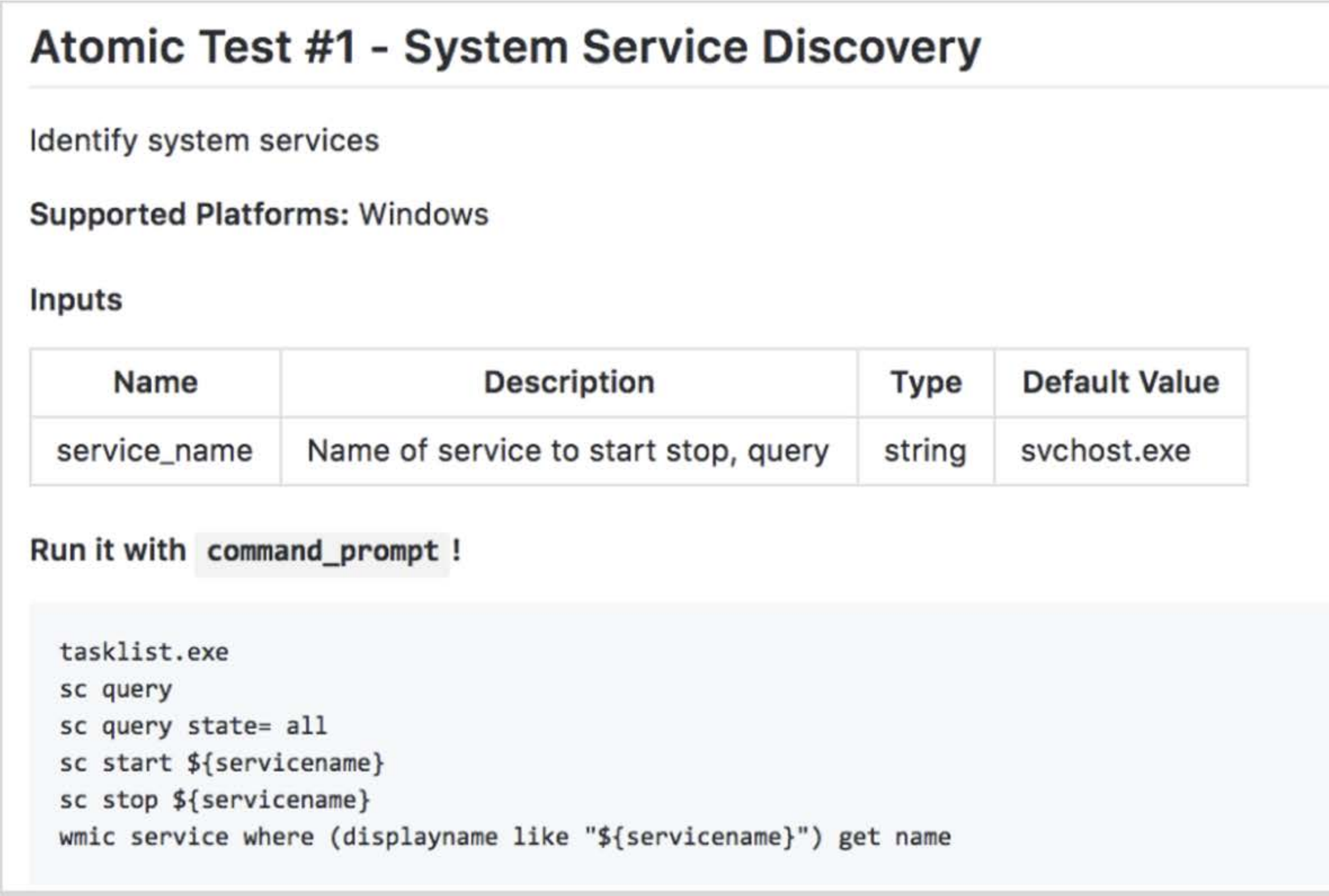
Think this

Not this

An atomic test is

1. Small (one ATT&CK technique)

2. Easy to execute



Atomic Test #1 - System Service Discovery

Identify system services

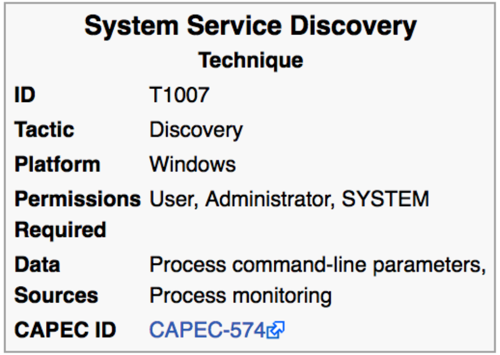
Supported Platforms: Windows

Inputs

Name	Description	Type	Default Value
service_name	Name of service to start stop, query	string	svchost.exe

Run it with `command_prompt` !

```
tasklist.exe
sc query
sc query state= all
sc start ${servicename}
sc stop ${servicename}
wmic service where (displayname like "${servicename}") get name
```



System Service Discovery

Technique

ID	T1007
Tactic	Discovery
Platform	Windows
Permissions Required	User, Administrator, SYSTEM
Data Sources	Process command-line parameters, Process monitoring
CAPEC ID	CAPEC-574

https://github.com/redcanaryco/atomic-red-team/blob/master/atomics/T1007/T1007.md

Why test atomically?

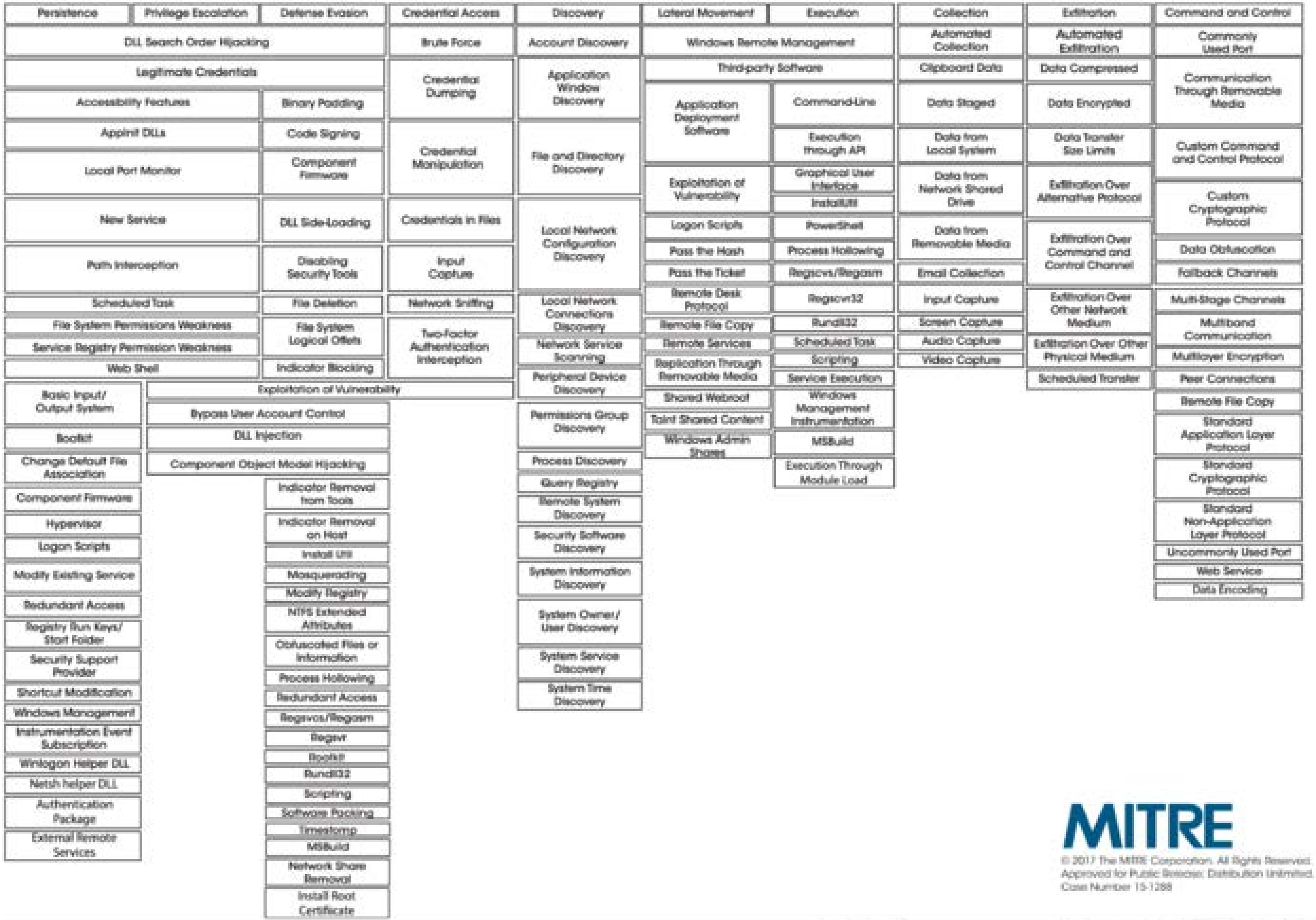
Testing your coverage is fundamental to improving your security outcomes.

Testing should be fast and easy.

Defenders need to keep learning how adversaries are operating.

> “*Another red team suggestion (hat tip: Tim McG—https://www.twitter.com/NotMedic) is to use ATT&CK before you even plan your next red team campaign.*
>
> ***Roll the dice*** *and randomly select 2–3 TTPs from each column and that becomes the fake adversary that you are emulating.*

https://medium.com/@malcomvetter/red-team-use-of-mitre-att-ck-f9ceac6b3be2



Persistence
Privilege Escalation
Defense Evasion

DLL Search Order Hijacking
Legitimate Credentials
Accessibility Features
AppInit DLLs
Local Port Monitor
New Service
Path Interception
Scheduled Task
File System Permissions Weakness
Service Registry Permission Weakness
Web Shell
Basic Input/ Output System
Bootkit
Change Default File Association
Component Firmware
Hypervisor
Logon Scripts
Modify Existing Service
Redundant Access
Registry Run Keys/ Start Folder
Security Support Provider
Shortcut Modification
Windows Management Instrumentation Event Subscription
Winlogon Helper DLL
Netsh helper DLL
Authentication Package
External Remote Services

Exploitation of Vulnerability
Bypass User Account Control
DLL Injection
Component Object Model Hijacking

Binary Padding
Code Signing
Component Firmware
DLL Side-Loading
Disabling Security Tools
File Deletion
File System Logical Offets
Indicator Blocking
Indicator Removal from Tools
Indicator Removal on Host
Install Util
Masquerading
Modify Registry
NTFS Extended Attributes
Obfuscated Files or Information
Process Hollowing
Redundant Access
Regsvcs/Regasm
Regsvr
Rootkit
Rundll32
Scripting
Software Packing
Timestomp
MSBuild
Network Share Removal
Install Root Certificate

Credential Access
Brute Force
Credential Dumping
Credential Manipulation
Credentials in Files
Input Capture
Network Sniffing
Two-Factor Authentication Interception

Discovery
Account Discovery
Application Window Discovery
File and Directory Discovery
Local Network Configuration Discovery
Local Network Connections Discovery
Network Service Scanning
Peripheral Device Discovery
Permissions Group Discovery
Process Discovery
Query Registry
Remote System Discovery
Security Software Discovery
System Information Discovery
System Owner/ User Discovery
System Service Discovery
System Time Discovery

Lateral Movement
Execution

Windows Remote Management
Third-party Software
Application Deployment Software
Exploitation of Vulnerability
Logon Scripts
Pass the Hash
Pass the Ticket
Remote Desk Protocol
Remote File Copy
Remote Services
Replication Through Removable Media
Shared Webroot
Taint Shared Content
Windows Admin Shares

Command-Line
Execution through API
Graphical User Interface
InstallUtil
PowerShell
Process Hollowing
Regscvs/Regasm
Regscvr32
Rundll32
Scheduled Task
Scripting
Service Execution
Windows Management Instrumentation
MSBuild
Execution Through Module Load

Collection
Automated Collection
Clipboard Data
Data Staged
Data from Local System
Data from Network Shared Drive
Data from Removable Media
Email Collection
Input Capture
Screen Capture
Audio Capture
Video Capture

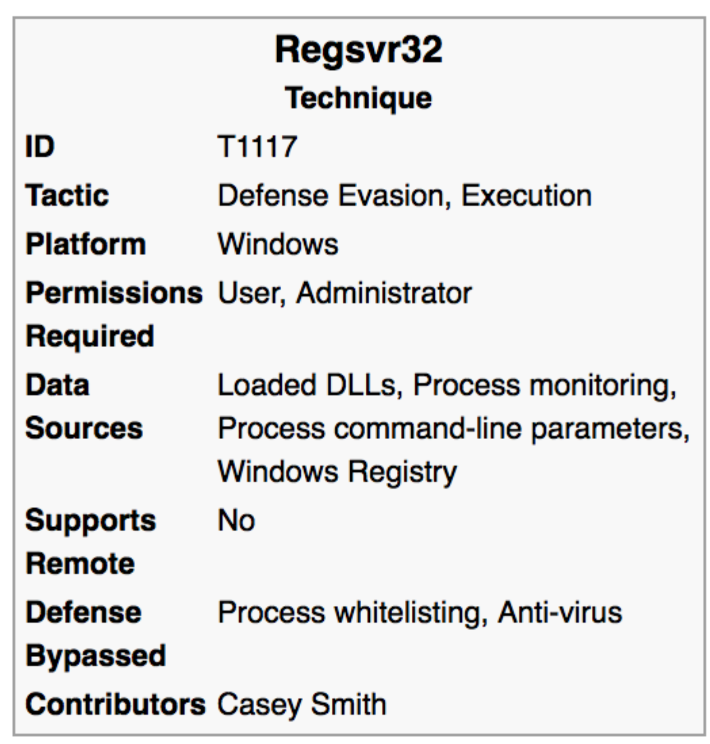
Exfiltration
Automated Exfiltration
Data Compressed
Data Encrypted
Data Transfer Size Limits
Exfiltration Over Alternative Protocol
Exfiltration Over Command and Control Channel
Exfiltration Over Other Network Medium
Exfiltration Over Other Physical Medium
Scheduled Transfer

Command and Control
Commonly Used Port
Communication Through Removable Media
Custom Command and Control Protocol
Custom Cryptographic Protocol
Data Obfuscation
Fallback Channels
Multi-Stage Channels
Multiband Communication
Multilayer Encryption
Peer Connections
Remote File Copy
Standard Application Layer Protocol
Standard Cryptographic Protocol
Standard Non-Application Layer Protocol
Uncommonly Used Port
Web Service
Data Encoding

MITRE

red canary

“Probably useful”

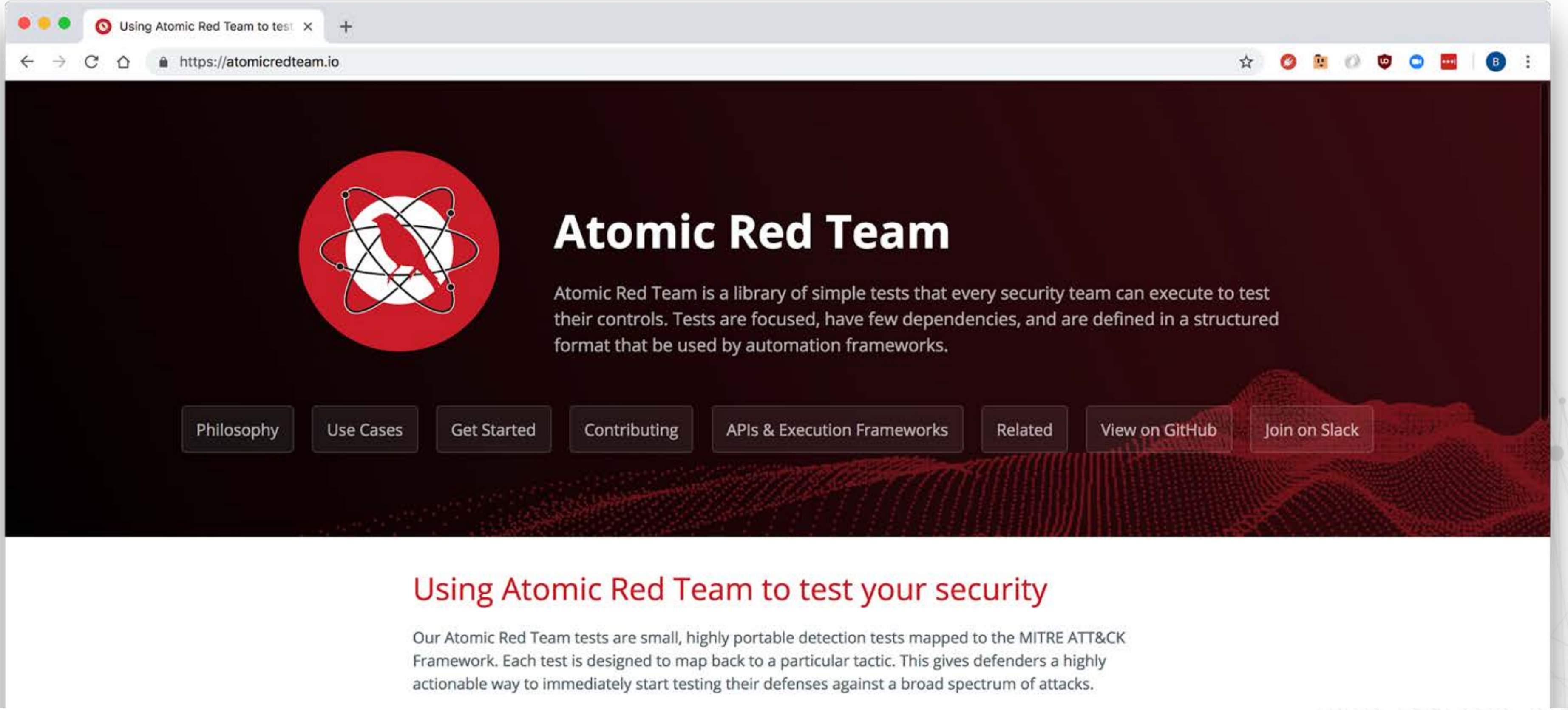


Regsvr32

Technique

ID	T1117
Tactic	Defense Evasion, Execution
Platform	Windows
Permissions Required	User, Administrator
Data Sources	Loaded DLLs, Process monitoring, Process command-line parameters, Windows Registry
Supports Remote	No
Defense Bypassed	Process whitelisting, Anti-virus
Contributors	Casey Smith

Now what?



Atomic Red Team

Atomic Red Team is a library of simple tests that every security team can execute to test their controls. Tests are focused, have few dependencies, and are defined in a structured format that be used by automation frameworks.

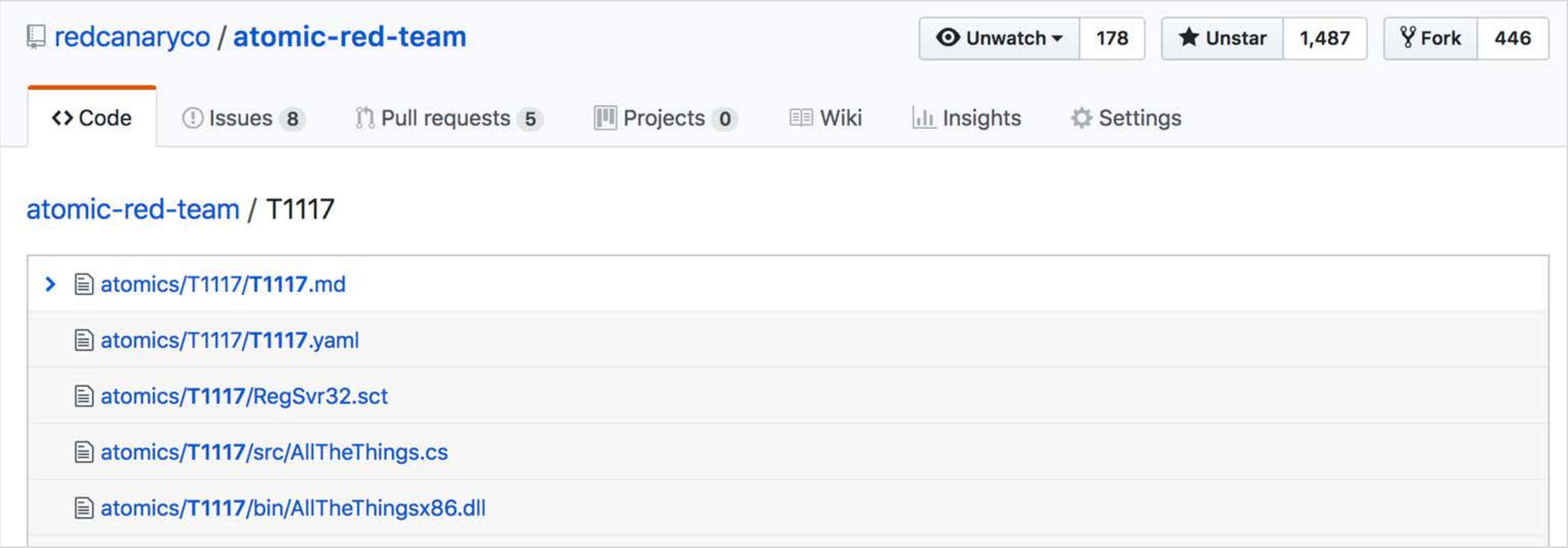
Using Atomic Red Team to test your security

Our Atomic Red Team tests are small, highly portable detection tests mapped to the MITRE ATT&CK Framework. Each test is designed to map back to a particular tactic. This gives defenders a highly actionable way to immediately start testing their defenses against a broad spectrum of attacks.

https://atomicredteam.io

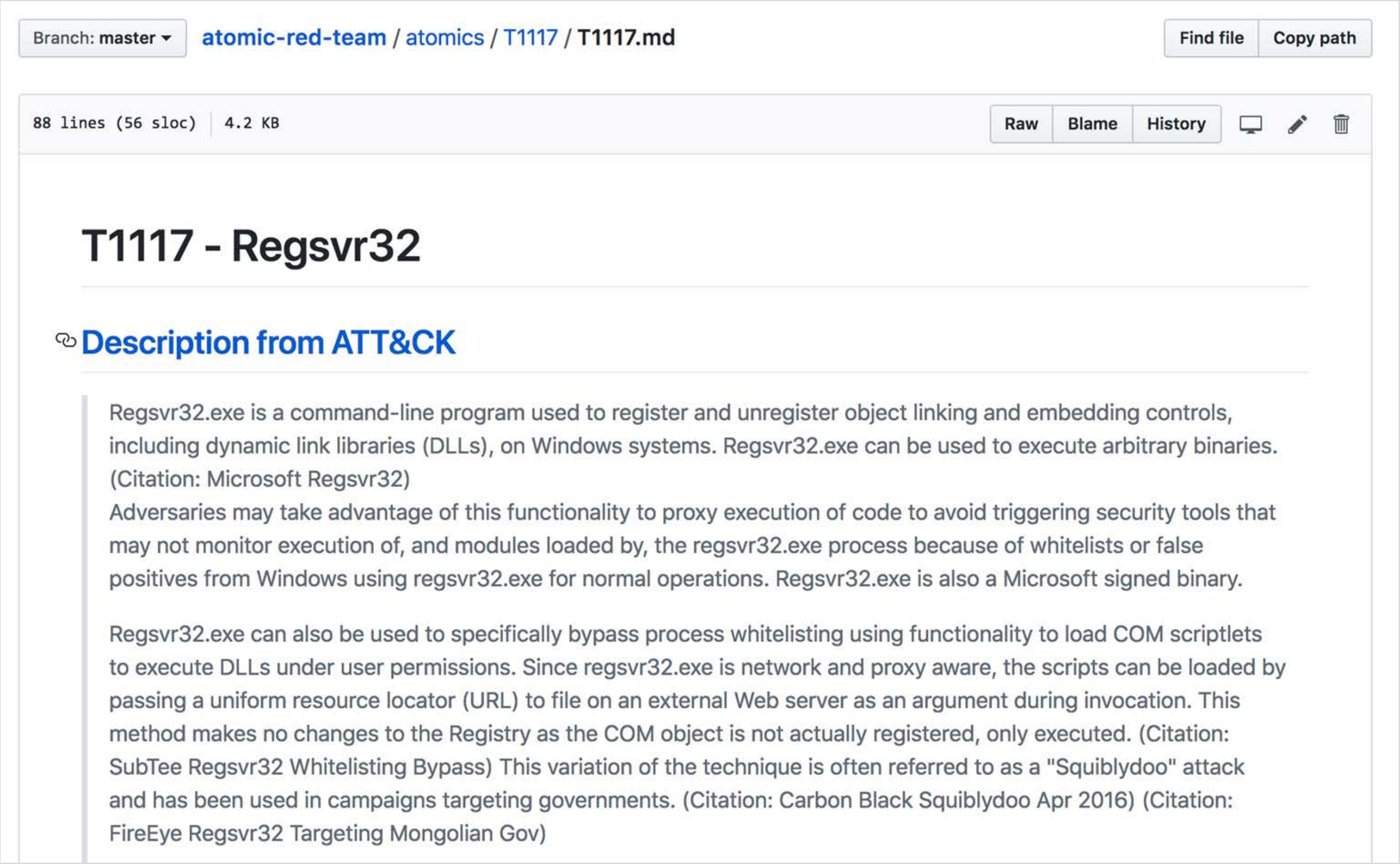
red canary

https://github.com/redcanaryco/atomic-red-team/find/master



atomic-red-team / T1117

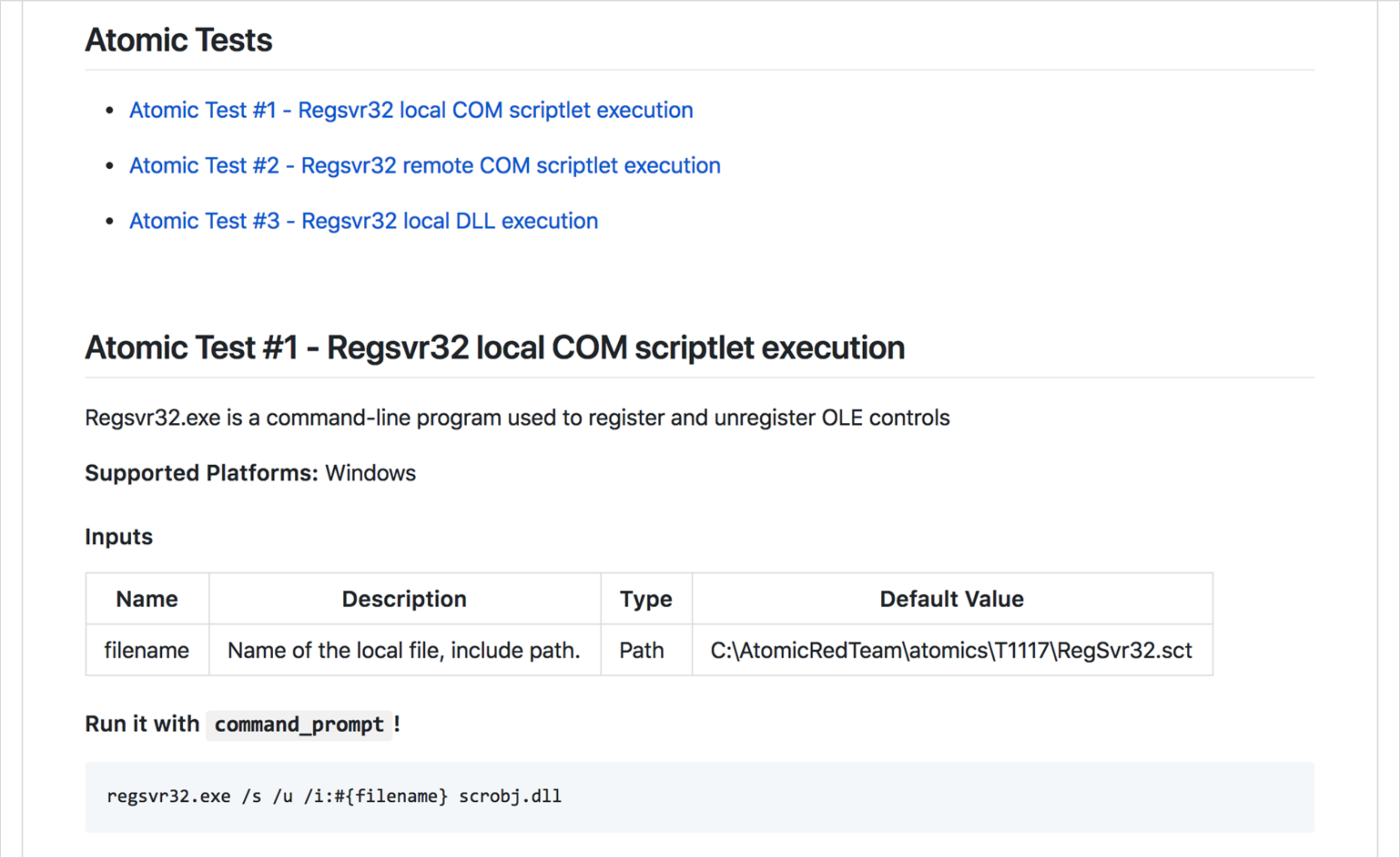
- atomics/T1117/T1117.md
- atomics/T1117/T1117.yaml
- atomics/T1117/RegSvr32.sct
- atomics/T1117/src/AllTheThings.cs
- atomics/T1117/bin/AllTheThingsx86.dll



T1117 - Regsvr32

Description from ATT&CK

> Regsvr32.exe is a command-line program used to register and unregister object linking and embedding controls, including dynamic link libraries (DLLs), on Windows systems. Regsvr32.exe can be used to execute arbitrary binaries. (Citation: Microsoft Regsvr32)
> Adversaries may take advantage of this functionality to proxy execution of code to avoid triggering security tools that may not monitor execution of, and modules loaded by, the regsvr32.exe process because of whitelists or false positives from Windows using regsvr32.exe for normal operations. Regsvr32.exe is also a Microsoft signed binary.
>
> Regsvr32.exe can also be used to specifically bypass process whitelisting using functionality to load COM scriptlets to execute DLLs under user permissions. Since regsvr32.exe is network and proxy aware, the scripts can be loaded by passing a uniform resource locator (URL) to file on an external Web server as an argument during invocation. This method makes no changes to the Registry as the COM object is not actually registered, only executed. (Citation: SubTee Regsvr32 Whitelisting Bypass) This variation of the technique is often referred to as a "Squiblydoo" attack and has been used in campaigns targeting governments. (Citation: Carbon Black Squiblydoo Apr 2016) (Citation: FireEye Regsvr32 Targeting Mongolian Gov)



Atomic Tests

- Atomic Test #1 - Regsvr32 local COM scriptlet execution
- Atomic Test #2 - Regsvr32 remote COM scriptlet execution
- Atomic Test #3 - Regsvr32 local DLL execution

Atomic Test #1 - Regsvr32 local COM scriptlet execution

Regsvr32.exe is a command-line program used to register and unregister OLE controls

Supported Platforms: Windows

Inputs

Name	Description	Type	Default Value
filename	Name of the local file, include path.	Path	C:\AtomicRedTeam\atomics\T1117\RegSvr32.sct

Run it with `command_prompt` !

```
regsvr32.exe /s /u /i:#{filename} scrobj.dll
```

How can I use Atomic Tests?

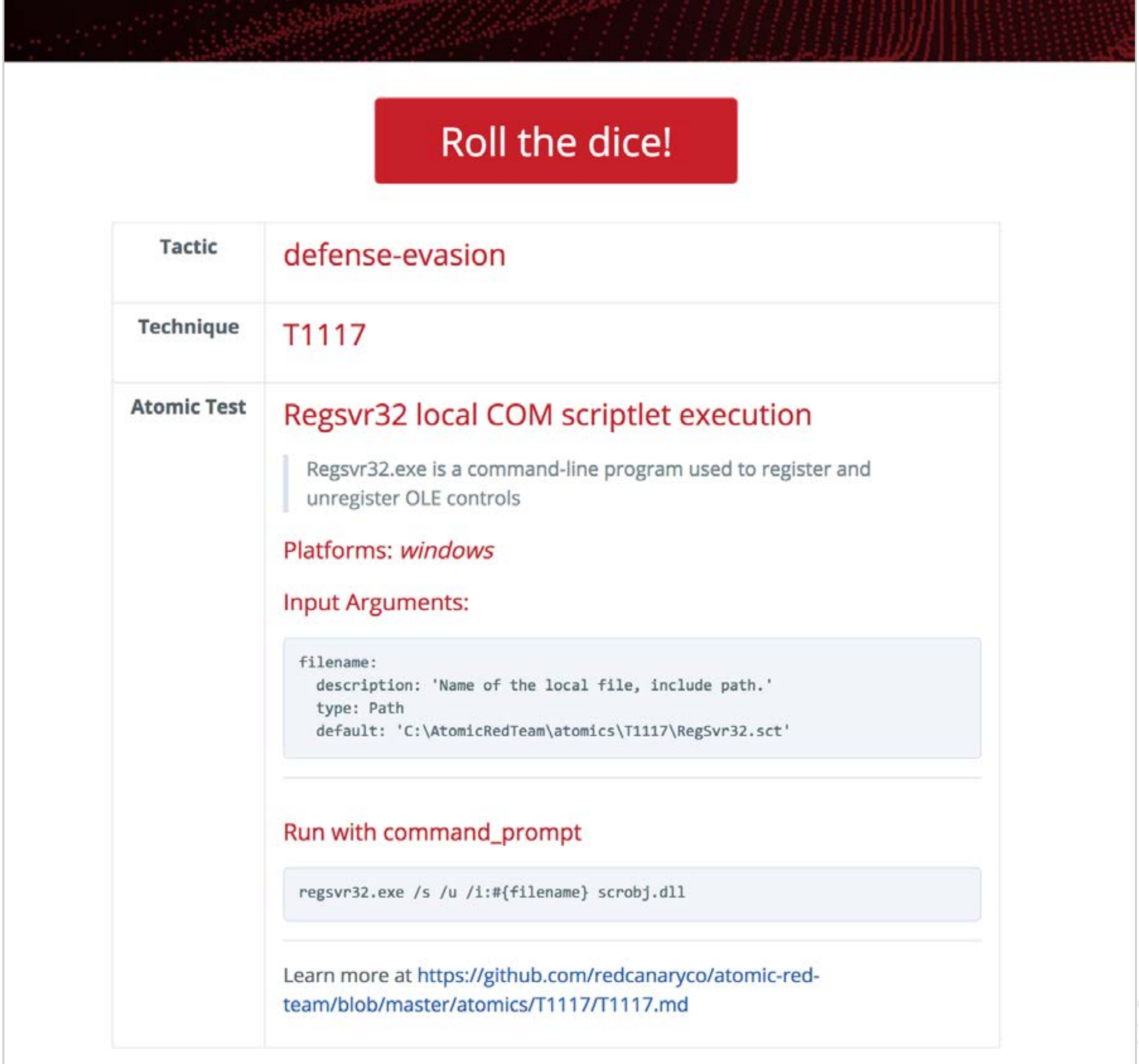
Ways to use Atomic Tests:

1) Create a recurring calendar invite

2) Know thy gaps

3) Hold your team accountable

4) Hold your partners/vendors accountable



Roll the dice!

Tactic	defense-evasion
Technique	T1117

Atomic Test	Regsvr32 local COM scriptlet execution
	Regsvr32.exe is a command-line program used to register and unregister OLE controls
	Platforms: *windows*
	Input Arguments:
	`filename:`
	`  description: 'Name of the local file, include path.'`
	`  type: Path`
	`  default: 'C:\AtomicRedTeam\atomics\T1117\RegSvr32.sct'`
	Run with command_prompt
	`regsvr32.exe /s /u /i:#{filename} scrobj.dll`
	Learn more at https://github.com/redcanaryco/atomic-red-team/blob/master/atomics/T1117/T1117.md

http://atomicredteam.io/roll-the-dice

Contribute tests to Atomic Red Team:

atomicredteam.io

Subscribe to the Red Canary blog:

redcanary.com/blog

red canary