

# New Resources from the Center

**Richard Struse**

**EU ATT&CK Community Workshop: June 1, 2021**

# Together, we are changing the rules of the game



*All Center R&D project outputs are made  
freely-available to the world*



# MITRE

**SOLVING PROBLEMS  
FOR A SAFER WORLD™**

Members as of April 2021

# The center by the numbers

*Advancing the state of the art and the state of  
the practice in threat-informed defense globally*



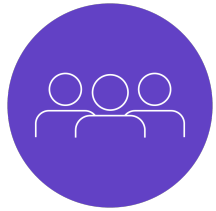
**Mission:**

**1**



**Months old:**

**18**



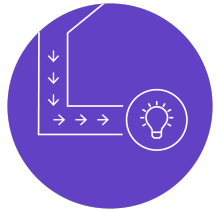
**Members:**

**25**



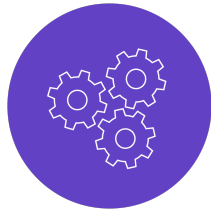
**Sponsors per project (average):**

**4**



**Ideas in pipeline:**

**35**



**Projects underway:**

**8**



**Published projects:**

**6**

# Completed Project Highlights

# Adversary Emulation Plans

## FIN6, menuPass

**Problem:** Understanding defenses from the adversary perspective is critical, but teams often lack the resources to conduct effective adversary emulation

**Solution:** Establish a library of standardized intelligence-driven adversary emulation plans that can be easily leveraged by defenders

**Impact:** Greatly reduce time & cost for defenders to test their defenses against real-world adversary TTPs

**Published:** Sep 2020, Feb 2021

Center R&D outputs  
available at:

<https://github.com/center-for-threat-informed-defense>

# Controls Mappings

**Problem:** Defenders struggle to relate large and unwieldy security control frameworks such as NIST 800-53 to TTPs in ATT&CK

**Solution:** Create a comprehensive and open, curated set of mappings between 800-53 controls and ATT&CK techniques

**Impact:** Defenders can quickly and easily focus on understanding how the controls in use in their environment relate to adversary TTPs of interest to them

**Published:** Dec 2020

© 2021 MITRE Engenuity. Approved for public release. Document # CT0024 TLP:WHITE

# Container Techniques

## Container Techniques

**Problem:** Defenders lack visibility into adversary behaviors in and against container technologies leaving their organizations exposed to emerging threats

**Solution:** Expand MITRE ATT&CK to describe adversary behaviors in and against container technologies including Docker and Kubernetes

**Impact:** Brings focus to adversary behaviors in an emergent domain leveraging the well-understood and widely adopted ATT&CK methodology

**Published:** April 2021

This project's outputs have been directly incorporated into ATT&CK

# Running Project Preview



# Upcoming Mapping Projects

## Security Mapping: Other Platforms

**Problem:** Users of various platforms lack a comprehensive view of how native security controls can help defend against real-world adversary TTPs

**Solution:** Build a scoring methodology and use it to create mappings showing how effective each security control is in defending against specific ATT&CK techniques

**Impact:** Empowers defenders with objective data on which controls are most useful in defending against the adversary TTPs they care about

**Release Date:** Beginning June 2021

- Look for the Center to release mappings for various cloud service providers and operating systems
- Will be released on GitHub

# Sightings Ecosystem

## Sightings Ecosystem

**Problem:** Defenders lack visibility into which adversary behaviors they should focus their attention on first

**Solution:** Build and operate a way for organizations to safely contribute sightings of specific ATT&CK TTPs powering analytics that give defenders a picture of what TTPs are used where and when

**Impact:** Injects real-world data and insights from that data into the decision-making process of defenders, allowing them to focus their resources on the highest-priority problems

**Release Date:** Dec 2021



A notional, data driven technique prioritization based on last 30 days. Red techniques are most frequently seen. Unmarked techniques were not seen.

- Looking for data contributors
- <https://medium.com/mitre-engenuity/tracking-adversary-footprints-e37668a0d665>
- For more information, email [ctid@mitre-engenuity.org](mailto:ctid@mitre-engenuity.org)

# ATT&CK Workbench

## ATT&CK Workbench

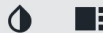
**Problem:** Defenders struggle to integrate their organization's local knowledge of adversaries and their TTPs with the public ATT&CK knowledge base

**Solution:** Build an easy-to-use open-source software tool that allows organizations to manage and extend their own local version of ATT&CK and keep it in sync with MITRE's knowledge base

**Impact:** Drastically reduces the barriers for defenders to ensure that their threat intelligence is aligned with the public ATT&CK knowledge base

**Release Date:** June 2021

- Scheduled to be released on GitHub later this month!



# ATT&CK WORKBENCH

MITRE ATT&CK® is a globally-accessible knowledge base of adversary tactics and techniques based on real-world observations.

ATT&CK Workbench is a tool designed to containerize the ATT&CK knowledge base, making ATT&CK easier to use and extend throughout the community. This application is your own customized instance of the knowledge base where you can explore, extend, and annotate ATT&CK data.

LEARN MORE ?

## Explore

MATRICES

TECHNIQUES

TACTICS

MITIGATIONS

GROUPS

SOFTWARE

ADMIN



## APT3

MODIFIED 29 MARCH 2020

ID

G0022

VERSION

1.3

CONTRIBUTORS

ASSOCIATED GROUPS

APT3<sup>[1][2][6]</sup>, Gothic Panda<sup>[4][2][6]</sup>, Pirpi<sup>[4]</sup>,  
UPS Team<sup>[1][2][6]</sup>, Buckeye<sup>[6]</sup>, Threat Group-0110<sup>[2][6]</sup>,  
TG-0110<sup>[2][6]</sup>

DESCRIPTION

APT3 is a China-based threat group that researchers have attributed to China's Ministry of State Security.<sup>[1][2]</sup> This group is responsible for the campaigns known as Operation Clandestine Fox, Operation Clandestine Wolf, and Operation Double Tap.<sup>[1][5]</sup> As of June 2015, the group appears to have shifted from targeting primarily US victims to primarily political organizations in Hong Kong.<sup>[6]</sup>

MITRE has also developed an APT3 Adversary Emulation Plan.<sup>[3]</sup>

## Techniques Used

[+ ADD A TECHNIQUE](#)☐ show deprecated

SOURCE	TYPE	TARGET	DESCRIPTION
G0022	APT3	uses T1053.005 Scheduled Task	An APT3 downloader creates persistence by creating the following scheduled task: schtasks /create /tn "mysc" /tr C:\Users\Public\test.e /sc ONLOGON /ru "System".

## NOTES



search



### Notes from IR team

1 JUNE 2021, 8:41 AM



Potential APT3 activity seen in West Coast office - contact Mary Smith for more info.



name \*

ID

version \*

0.1

☐ sub-technique?

platforms

Write

Preview

**Description** ⓘ

Description

domains

tactics



Write

Preview

**Detection** ⓘ

Detection

To sign up for updates from the Center, visit:

<https://share.hsforms.com/1fBf6rPTLT8-ROom3UUCG5w4m7ji>

# Thank you!

[www.mitre-engenuity.org/ctid](http://www.mitre-engenuity.org/ctid)



Center  
for Threat  
Informed  
Defense