Contributing to ATT&CK™

You can help contribute to ATT&CK.

ATT&CK is in a constant state of development. We are always on the lookout for new information to help refine and extend what is covered. We are looking for contributions in the following areas in particular, but if you have other information you think may be useful, please reach out to us at attack@mitre.org

Techniques

We appreciate your help to let us know about what new techniques and technique variations adversaries and red teamers are using. You can start by emailing us the technique name, a brief description, and references or knowledge about how it is being used by adversaries or red teams. We suggest you take a close look at what we already have on our site, paying attention to the level of abstraction of techniques. Since we are working on adding new technique details constantly, we will deconflict what you send with what we're working on. We'll provide feedback and work with you to get the content added.

macOS and Linux

While we are looking for new techniques for Windows, macOS, and Linux, we are interested in macOS and Linux techniques in particular since there is a lack of publicly available threat intel for techniques used against those systems. This leads to gaps in the knowledge base that you can help fill.

Threat Intelligence

We map Group and Software examples on our site, and there is too much open source threat intelligence reporting for us to keep up on everything. We appreciate your help with referenced information about how Groups and Software samples use ATT&CK techniques. Threat intelligence contributions are most helpful to us when they are in the specific format we have on our website, including citing techniques and group aliases to publicly-available references. We ask that you provide the technique name, a brief description of how the technique is implemented, and the publicly-available reference.

Data Sources

We often don't have direct access to endpoint or network log data for technique use in incidents. We're always looking for partners who would be interested in sharing relevant data from logs that show how adversaries are using ATT&CK techniques beyond what appears in threat reporting.

Your Use Cases

It's always helpful for us to hear about how you're using ATT&CK in your organization. We appreciate any information you can share with us about your specific use case or application of ATT&CK, and particularly any success stories you've had as a result.

If you have contributions in these or any other areas, please email us at attack@mitre.org.

Contribution Examples

New Technique Example

Technique Name: COM, ROM, & BE GONE
Tactic: Persistence
Platform: Windows
Required Permissions: User
Data Sources: Windows API, Process monitoring, or other sources that can be used to detect this activity
Description: Component Object Model (COM) servers associated with Graphics Interchange Format (GIF) image viewers can be abused to corrupt arbitrary memory banks. Adversaries may leverage this opportunity to modify, mux, and maliciously annoy (MMA) read-only memory (ROM) regularly accessed during normal system operations.
Detection: Monitor the JIF viewers for muxing and malicious annoyance. Use event ID 423420 and 234222 to detect changes.
Mitigation: Configure the Registry key HKLM\SYSTEM\ControlSet\001\Control\WindowsJIFControl\ to 0 to disable MMA access if not needed within the environment.
Adversary Use: Here is a publicly-available reference about FUZZYSNUGGLYDUCK using this technique: (www[.]awesomeThreatReports[.]org/FUZZYSNUGGLYDUCK_NOMS _ON_ROM_VIA_COM). Additionally, our red team uses this in our operations.
Additional References: Here is a reference from the researcher who discovered this technique: (www[.]crazySmartResearcher[.]net/POC_DETECTIONS_&_MITIGATIONS_4_WHEN_COM_RAMS_ROM)

Group & Software Example

Group Name: FUZZYSNUGGLYDUCK (www[.]sourceX[.]com)
Group Alias: APT1337 (www[.]sourceY[.]com)

Description: FUZZYSNUGGLYDUCK is a Great Lakes-based threat group that has been active since at least May 2018. The group focuses on targeting the aviation sector. (www[.]sourceY[.]com)

Techniques:

- Spearphishing Attachment (T1193) – FUZZYSNUGGLYDUCK has used spearphishing email attachments containing images of stale bread to deliver malware. (www[.]sourceX[.]com)
- File and Directory Discovery (T1083) – FUZZYSNUGGLYDUCK has searched files and directories for the string *quack*. (www[.]sourceY[.]com)

Software Name: FLYINGV (www[.]sourceX[.]com) (wwwVsourceZ[.]com)

Group Association: FLYINGV has been used by FUZZYSNUGGLYDUCK. (www[.]sourceZ[.]com)
Description: FLYINGV is custom malware used by FUZZYSNUGGLYDUCK as a second-stage RAT. (www[.]sourceZ[.]com)
Platform: Windows

Techniques:

- Registry Run Keys / Start Folder (T1060) – FLYINGV has added the Registry Run key "HueyDeweyLouie" to establish persistence. (www[.]sourceX[.]com)
- File and Directory Discovery (T1083) – FLYINGV has used rundll32.exe to load its malicious dll file, estevez.dll. (www[.]sourceX[.]com)