Smart iconography on your wiki

Cindy Cicalese
Conventions are your friends

One of the best ways to make almost anything easier to grasp in a hurry is to follow the existing conventions—the widely used or standardized design patterns. For example:

- How things look. Many elements have a standardized appearance, like the icon that tells you it’s a link to a video, the search icon, and the social networking sharing options.
Iconography - key concepts

- Use icons to represent key concepts in your wiki
- Show these icons on the sidebar or menu as a legend to remind the user what they mean
- Show these icons on the title bar of pages to identify what concepts they identify with
- Show these icons in page text as needed (avoid overuse to create a distraction)
- Show these icons in search results
Example - EMA wiki

https://collaborate.mitre.org/ema
Use icons to represent key concepts in your wiki

- Capabilities
- Subcapabilities
- Behaviors
- Behavior Instances
- Obfuscation Methods
- Attributes
Show these icons on the sidebar or menu as a legend to remind the user what they mean

- example uses extension CustomNavBlocks with Vector skin
- can add icons to menus in Chameleon skin
Show these icons on the title bar of pages to identify what concepts they identify with.

**sandbox detect & evade**

**EMA ID:** ema-1233

Detects whether the malware instance is being executed inside of an instrumented sandbox environment (e.g., Cuckoo Sandbox). If so, conditional execution selects for benign execution path.

**Examples:**

- Injected DLL Testing: Testing for the name of a particular DLL that is known to be injected by a sandbox for API hooking is a common way of detecting sandbox environments. This can be achieved through the `kernel32!GetModuleHandle` API call and other means.
- Product Key/ID Testing: Checking for a particular product key/ID associated with a sandbox environment (commonly associated with the Windows host OS used in the environment) can be used to detect whether a malware instance is being executed in a particular sandbox. This can be achieved through several means, including testing for the Key/ID
Find Agent: Cuckoo uses a python agent to interact with the host guest. By listing the process and finding python.exe or pythonw.exe or by looking for an agent.py in the system, a malware can detect Cuckoo.

http://unprotect.tdgt.org/index.php/Sandbox_Evasion

Associated Attributes:
- Anti-Behavioral Analysis: targeted sandbox
- Common: applicable platform
- Common: technique

Associated Capabilities/Subcapabilities:
- Anti-Behavioral Analysis

Associated With sandbox detect & evade
- Injected DLL Testing
- Product Key/ID Testing
- Screen Resolution Testing
- Timing/Date Checks

References:

<table>
<thead>
<tr>
<th>Date</th>
<th>Malware Family</th>
<th>URL</th>
</tr>
</thead>
</table>
Show these icons in search results
Network graphing (VIKI and VikiTitleIcon)
TitleIcon

https://www.mediawiki.org/wiki/Extension:Title_ICON

- Use SMW property to specify Title Icon as the name of a File page on a page (possibly in a template) or category
- Image is scaled and displayed on the title bar and in search results
- Can use SMW to query for Title Icon to display in page text
Potential enhancements to TitleIcon

- alternate storage mechanisms:
  - Multi-content Revisions (MCR)
  - Cargo
- parser function to retrieve icons
- alternate icon types:
  - Unicode characters ([https://phabricator.wikimedia.org/T184134](https://phabricator.wikimedia.org/T184134))
  - Font Awesome icons
  - requires a non-backward compatible change to allow typed icons
- specify link target ([https://phabricator.wikimedia.org/T190822](https://phabricator.wikimedia.org/T190822))
- Title Icons for namespaces ([https://phabricator.wikimedia.org/T190824](https://phabricator.wikimedia.org/T190824))
- merge with DisplayTitle?