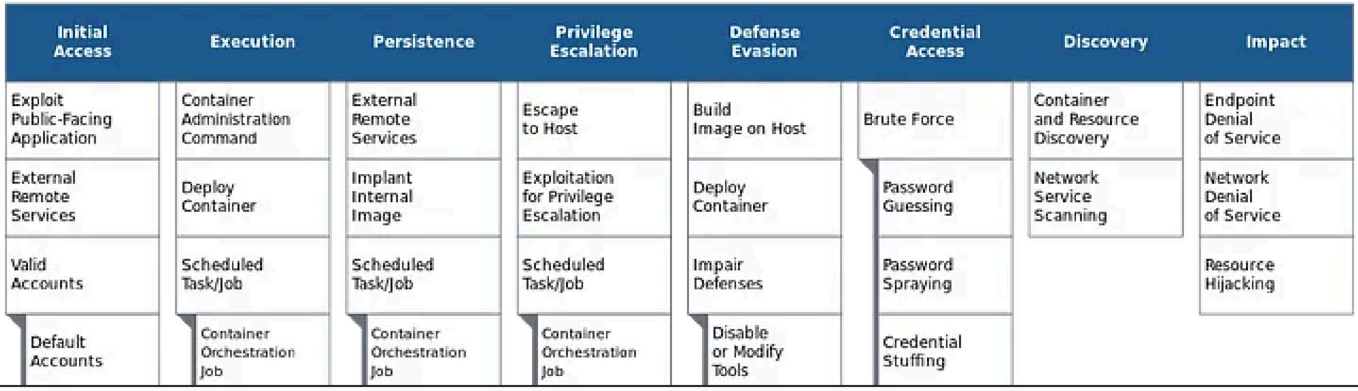
ATT&CK® for Containers now available!

Jen Burns · Follow

a testament to how many folks helped us scope and create this new platform in ATT&CK!



Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Impact
Exploit Public-Facing Application	Container Administration Command	External Remote Services	Escape to Host	Build Image on Host	Brute Force	Container and Resource Discovery	Endpoint Denial of Service
External Remote Services	Deploy Container	Implant Internal Image	Exploitation for Privilege Escalation	Deploy Container	Password Guessing	Network Service Scanning	Network Denial of Service
Valid Accounts	Scheduled Task/Job	Scheduled Task/Job	Scheduled Task/Job	Impair Defenses	Password Spraying		Resource Hijacking
Default Accounts	Container Orchestration Job	Container Orchestration Job	Container Orchestration Job	Disable or Modify Tools	Credential Stuffing		

In our previous blog post, we also mentioned a few open-ended questions that we wanted to answer before this content was included in ATT&CK. We received some excellent feedback from the community about these, including feedback on the question of **whether or not adversary activity inside containers always ultimately leads to cryptomining.** What we heard from you is that the vast majority of activity that you've observed ***does*** lead to cryptomining. However, evidence from a number of parties led us to conclude that adversaries utilizing containers for more "traditional" purposes, such as exfiltration and collection of sensitive data, is publicly under reported. Ultimately, this led the ATT&CK team to make the decision

Exploitation for Privilege Escalation (T1068): We decided that this technique applies to virtualized environments such as containers when adversaries exploit software vulnerabilities to facilitate escaping to the underlying host. We added this technique to the Containers matrix with that in mind.

Impair Defenses (T1562) and **Impair Defenses: Disable or Modify Tools (T1562.001):** We added the sub-technique in particular because we wanted to include the case where security tools related to a container deployment are disabled by an adversary.

To match the refactor of data sources in ATT&CK, we also developed a set of data sources that pertain to container techniques. Since there are strong relationships between the Containers, Cloud, and host-based platforms in ATT&CK, you'll notice that there is some overlap on data sources across these platforms as well. For many data sources specific to containers, however, we decided to build data sources similar to the way we built them for Cloud. In Cloud, we focused on the specific APIs and events that align with adversary behaviors. An example of how we translated that to Containers is the Container data source below:

With the completion of this Center project, ATT&CK for Containers will be maintained by the ATT&CK team, who would love your continuous feedback and contributions! Let the team know what you think, what could be improved, and most importantly what you see adversaries doing in the wild related to containers. Feel free to send an email at any time to attack@mitre.org.

If you have ideas for other R&D projects that the Center should consider, please email us at ctid@mitre-engenuity.org.

-- 1

Written by Jen Burns

Follow