ATT&CK® for Containers now available!

Jen Burns · Follow
Published in MITRE-Engenuity · 5 min read · Apr 29, 2021

Written by Jen Burns, Chris Ante, and Matt Bajzek

We're excited to announce the official release of ATT&CK for Containers! This release marks the culmination of a Center for Threat-Informed Defense (Center) research project sponsored by Citigroup, JPMorgan Chase, and Microsoft that investigated the viability of adding container-related techniques into ATT&CK. This investigation led to developing a draft of an ATT&CK for Containers matrix, which we contributed to ATT&CK. Our contribution was accepted and is now live in ATT&CK version 9.0! We want to give a special thank you to the community for all of your feedback and help in developing this content. Creating ATT&CK for Containers has been a fun journey for us, with a lot of new faces and names along the way. You'll notice a lot of new contributors in ATT&CK with this release, which is in part a testament to how many folks helped us scope and create this new platform in ATT&CK!

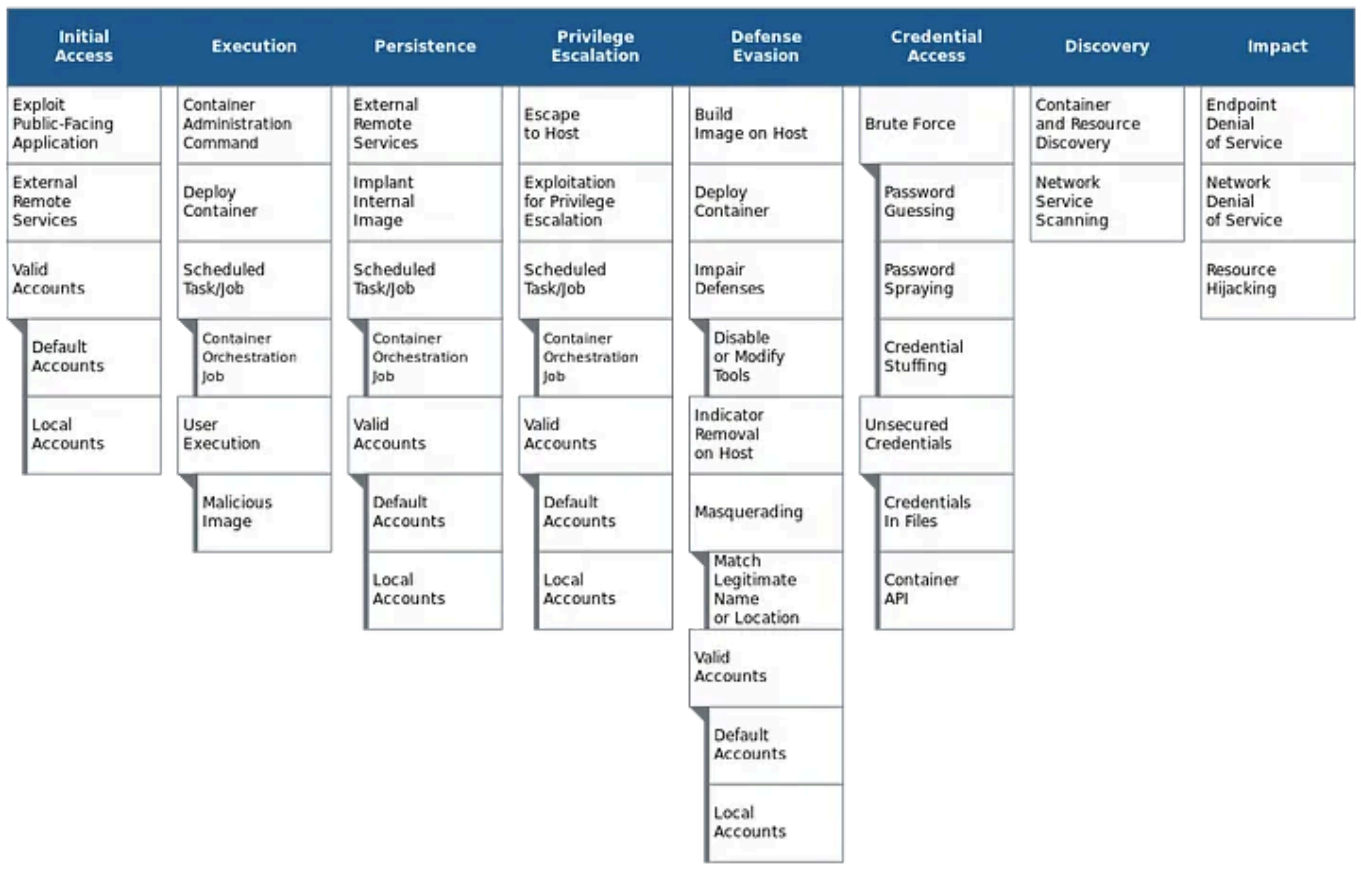

Figure 1: ATT&CK for Containers visualized in the ATT&CK Navigator

Why did container-related techniques get added to ATT&CK?

We talked about how we created ATT&CK for Containers in a previous blog post, and we recommend checking that out to learn more about our process. As a refresher on scope of ATT&CK for Containers, despite what the ATT&CK Twitter account mentioned on April 1st, it actually covers orchestration-level (e.g. Kubernetes) *and* container-level (e.g. Docker) adversary behaviors in a single Containers platform in ATT&CK.

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 to include container-related techniques in ATT&CK.

What's new from our previous blogs?

You may also notice that the current Containers matrix in ATT&CK has expanded and changed a bit from the first draft we presented in February. This is also thanks to some excellent contributions we received from the community. Here are the changes we made since releasing that first draft of ATT&CK for Containers:

Container Administration Command (T1609): We heard from you that the original name, "Container Service", wasn't great, particularly since Service is overloaded and already a concept used in Kubernetes. We decided to change the name to hopefully clarify what this term means in the ATT&CK context.

Valid Accounts: Default Accounts (T1078.001): We found that the default service account in Kubernetes fit more cleanly into this technique than Valid Accounts (T1078), so we added this sub-technique to the Containers matrix.

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.

Indicator Removal on Host (T1070): We decided that this technique may apply to an adversary deleting artifacts at the container orchestration layer, so we added it to the Containers matrix.

Network Service Scanning (T1046): We added this technique to the Containers matrix to map the behavior of adversaries scanning for services like the kubelet within a Kubernetes network.

What about malware?

We also decided to map a set of malware related to containers (Kinsing (S0599), Doki (S0600), Hildegard (S0601)) into ATT&CK. We hope the corresponding procedure examples will help clarify the scope of some of the new ATT&CK techniques and give the community a better idea of the abstraction level of techniques with the Containers matrix when compared to Linux and IaaS.

And data sources?

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:

Figure 2: Visualization of the Container data source

This graphic displays APIs that may be parsed out of Docker Daemon logs as events, but any log source that may contain information on the execution of these data components apply. We used a similar approach for the Cluster and Pod data sources.

What's next?

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.

About the Center for Threat-Informed Defense

The Center is a non-profit, privately funded research and development organization operated by MITRE Engenuity. The Center's mission is to advance the state of the art and the state of the practice in threat-informed defense globally. Comprised of participant organizations from around the globe with highly sophisticated security teams, the Center builds on MITRE ATT&CK®, an important foundation for threat-informed defense used by security teams and vendors in their enterprise security operations. Because the Center operates for the public good, outputs of its research and development are available publicly and for the benefit of all.

Mitre Attack | Containers | Cloud | Kubernetes | Threat Informed Defense