# TTP Detail – T1611

## TTP Information

Name: Escape to Host

Description: Adversaries may break out of a container or virtualized environment to gain access to the underlying host. This can allow an adversary access to other containerized or virtualized resources from the host level or to the host itself. In principle, containerized / virtualized resources should provide a clear separation of application functionality and be isolated from the host environment.(Citation: Docker Overview)

There are multiple ways an adversary may escape from a container to a host environment. Examples include creating a container configured to mount the host’s filesystem using the bind parameter, which allows the adversary to drop payloads and execute control utilities such as cron on the host; utilizing a privileged container to run commands or load a malicious kernel module on the underlying host; or abusing system calls such as `unshare` and `keyctl` to escalate privileges and steal secrets.(Citation: Docker Bind Mounts)(Citation: Trend Micro Privileged Container)(Citation: Intezer Doki July 20)(Citation: Container Escape)(Citation: Crowdstrike Kubernetes Container Escape)(Citation: Keyctl-unmask)

Additionally, an adversary may be able to exploit a compromised container with a mounted container management socket, such as `docker.sock`, to break out of the container via a [Container Administration Command](https://attack.mitre.org/techniques/T1609).(Citation: Container Escape) Adversaries may also escape via [Exploitation for Privilege Escalation](https://attack.mitre.org/techniques/T1068), such as exploiting vulnerabilities in global symbolic links in order to access the root directory of a host machine.(Citation: Windows Server Containers Are Open)

In ESXi environments, an adversary may exploit a vulnerability in order to escape from a virtual machine into the hypervisor.(Citation: Broadcom VMSA-2025-004)

Gaining access to the host may provide the adversary with the opportunity to achieve follow-on objectives, such as establishing persistence, moving laterally within the environment, accessing other containers or virtual machines running on the host, or setting up a command and control channel on the host.

## Threat-Mapped Scoring

Score: 1.8

Priority: P4 - Informational (Low)

## Kill Chain Phases

**•** mitre-attack: privilege-escalation

## Malware

* Doki
* Hildegard
* Siloscape

## Tools

* Peirates

## APTs (Intrusion Sets)

* TeamTNT