# TTP Detail – T1068

## TTP Information

Name: Exploitation for Privilege Escalation

Description: Adversaries may exploit software vulnerabilities in an attempt to elevate privileges. Exploitation of a software vulnerability occurs when an adversary takes advantage of a programming error in a program, service, or within the operating system software or kernel itself to execute adversary-controlled code. Security constructs such as permission levels will often hinder access to information and use of certain techniques, so adversaries will likely need to perform privilege escalation to include use of software exploitation to circumvent those restrictions.

When initially gaining access to a system, an adversary may be operating within a lower privileged process which will prevent them from accessing certain resources on the system. Vulnerabilities may exist, usually in operating system components and software commonly running at higher permissions, that can be exploited to gain higher levels of access on the system. This could enable someone to move from unprivileged or user level permissions to SYSTEM or root permissions depending on the component that is vulnerable. This could also enable an adversary to move from a virtualized environment, such as within a virtual machine or container, onto the underlying host. This may be a necessary step for an adversary compromising an endpoint system that has been properly configured and limits other privilege escalation methods.

Adversaries may bring a signed vulnerable driver onto a compromised machine so that they can exploit the vulnerability to execute code in kernel mode. This process is sometimes referred to as Bring Your Own Vulnerable Driver (BYOVD).(Citation: ESET InvisiMole June 2020)(Citation: Unit42 AcidBox June 2020) Adversaries may include the vulnerable driver with files delivered during Initial Access or download it to a compromised system via [Ingress Tool Transfer](https://attack.mitre.org/techniques/T1105) or [Lateral Tool Transfer](https://attack.mitre.org/techniques/T1570).

## Threat-Mapped Scoring

Score: 1.8

Priority: P4 - Informational (Low)

## Kill Chain Phases

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

## Malware

* BlackByte 2.0 Ransomware
* Carberp
* Cobalt Strike
* CosmicDuke
* Hildegard
* InvisiMole
* JHUHUGIT
* Pandora
* ProLock
* Remsec
* Siloscape
* Stuxnet
* Wingbird
* XCSSET
* ZeroCleare
* Zox

## Tools

* Empire
* PoshC2

## APTs (Intrusion Sets)

* APT28
* APT29
* APT32
* APT33
* BITTER
* BlackByte
* Cobalt Group
* FIN6
* FIN8
* HAFNIUM
* LAPSUS$
* MoustachedBouncer
* OilRig
* PLATINUM
* Scattered Spider
* Threat Group-3390
* Tonto Team
* Turla
* Volt Typhoon
* Whitefly
* ZIRCONIUM