# TTP Detail – T1491.002

## TTP Information

Name: External Defacement

Description: An adversary may deface systems external to an organization in an attempt to deliver messaging, intimidate, or otherwise mislead an organization or users. [External Defacement](https://attack.mitre.org/techniques/T1491/002) may ultimately cause users to distrust the systems and to question/discredit the system’s integrity. Externally-facing websites are a common victim of defacement; often targeted by adversary and hacktivist groups in order to push a political message or spread propaganda.(Citation: FireEye Cyber Threats to Media Industries)(Citation: Kevin Mandia Statement to US Senate Committee on Intelligence)(Citation: Anonymous Hackers Deface Russian Govt Site) [External Defacement](https://attack.mitre.org/techniques/T1491/002) may be used as a catalyst to trigger events, or as a response to actions taken by an organization or government. Similarly, website defacement may also be used as setup, or a precursor, for future attacks such as [Drive-by Compromise](https://attack.mitre.org/techniques/T1189).(Citation: Trend Micro Deep Dive Into Defacement)

## Threat-Mapped Scoring

Score: 0.0

Priority: Unclassified

## Kill Chain Phases

**•** mitre-attack: impact

## APTs (Intrusion Sets)

* Ember Bear
* Sandworm Team