# TTP Detail – T1190

## TTP Information

Name: Exploit Public-Facing Application

Description: Adversaries may attempt to exploit a weakness in an Internet-facing host or system to initially access a network. The weakness in the system can be a software bug, a temporary glitch, or a misconfiguration.  
  
Exploited applications are often websites/web servers, but can also include databases (like SQL), standard services (like SMB or SSH), network device administration and management protocols (like SNMP and Smart Install), and any other system with Internet-accessible open sockets.(Citation: NVD CVE-2016-6662)(Citation: CIS Multiple SMB Vulnerabilities)(Citation: US-CERT TA18-106A Network Infrastructure Devices 2018)(Citation: Cisco Blog Legacy Device Attacks)(Citation: NVD CVE-2014-7169) On ESXi infrastructure, adversaries may exploit exposed OpenSLP services; they may alternatively exploit exposed VMware vCenter servers.(Citation: Recorded Future ESXiArgs Ransomware 2023)(Citation: Ars Technica VMWare Code Execution Vulnerability 2021) Depending on the flaw being exploited, this may also involve [Exploitation for Defense Evasion](https://attack.mitre.org/techniques/T1211) or [Exploitation for Client Execution](https://attack.mitre.org/techniques/T1203).  
  
If an application is hosted on cloud-based infrastructure and/or is containerized, then exploiting it may lead to compromise of the underlying instance or container. This can allow an adversary a path to access the cloud or container APIs (e.g., via the [Cloud Instance Metadata API](https://attack.mitre.org/techniques/T1552/005)), exploit container host access via [Escape to Host](https://attack.mitre.org/techniques/T1611), or take advantage of weak identity and access management policies.  
  
Adversaries may also exploit edge network infrastructure and related appliances, specifically targeting devices that do not support robust host-based defenses.(Citation: Mandiant Fortinet Zero Day)(Citation: Wired Russia Cyberwar)  
  
For websites and databases, the OWASP top 10 and CWE top 25 highlight the most common web-based vulnerabilities.(Citation: OWASP Top 10)(Citation: CWE top 25)

## Threat-Mapped Scoring

Score: 1.8

Priority: P4 - Informational (Low)

## Kill Chain Phases

**•** mitre-attack: initial-access

## Malware

* BOLDMOVE
* COATHANGER
* Siloscape
* SoreFang
* ZxShell

## Tools

* Havij
* sqlmap

## APTs (Intrusion Sets)

* APT28
* APT29
* APT39
* APT41
* APT5
* Agrius
* Axiom
* BackdoorDiplomacy
* BlackByte
* BlackTech
* Blue Mockingbird
* Cinnamon Tempest
* Dragonfly
* Earth Lusca
* Ember Bear
* FIN13
* FIN7
* Fox Kitten
* GALLIUM
* GOLD SOUTHFIELD
* HAFNIUM
* INC Ransom
* Ke3chang
* Kimsuky
* Leviathan
* Magic Hound
* Moses Staff
* MuddyWater
* Play
* Rocke
* Salt Typhoon
* Sandworm Team
* Sea Turtle
* Threat Group-3390
* ToddyCat
* Volatile Cedar
* Volt Typhoon
* Winter Vivern
* menuPass