# TTP Detail – T1205

## TTP Information

Name: Traffic Signaling

Description: Adversaries may use traffic signaling to hide open ports or other malicious functionality used for persistence or command and control. Traffic signaling involves the use of a magic value or sequence that must be sent to a system to trigger a special response, such as opening a closed port or executing a malicious task. This may take the form of sending a series of packets with certain characteristics before a port will be opened that the adversary can use for command and control. Usually this series of packets consists of attempted connections to a predefined sequence of closed ports (i.e. [Port Knocking](https://attack.mitre.org/techniques/T1205/001)), but can involve unusual flags, specific strings, or other unique characteristics. After the sequence is completed, opening a port may be accomplished by the host-based firewall, but could also be implemented by custom software.

Adversaries may also communicate with an already open port, but the service listening on that port will only respond to commands or trigger other malicious functionality if passed the appropriate magic value(s).

The observation of the signal packets to trigger the communication can be conducted through different methods. One means, originally implemented by Cd00r (Citation: Hartrell cd00r 2002), is to use the libpcap libraries to sniff for the packets in question. Another method leverages raw sockets, which enables the malware to use ports that are already open for use by other programs.

On network devices, adversaries may use crafted packets to enable [Network Device Authentication](https://attack.mitre.org/techniques/T1556/004) for standard services offered by the device such as telnet. Such signaling may also be used to open a closed service port such as telnet, or to trigger module modification of malware implants on the device, adding, removing, or changing malicious capabilities. Adversaries may use crafted packets to attempt to connect to one or more (open or closed) ports, but may also attempt to connect to a router interface, broadcast, and network address IP on the same port in order to achieve their goals and objectives.(Citation: Cisco Synful Knock Evolution)(Citation: Mandiant - Synful Knock)(Citation: Cisco Blog Legacy Device Attacks) To enable this traffic signaling on embedded devices, adversaries must first achieve and leverage [Patch System Image](https://attack.mitre.org/techniques/T1601/001) due to the monolithic nature of the architecture.

Adversaries may also use the Wake-on-LAN feature to turn on powered off systems. Wake-on-LAN is a hardware feature that allows a powered down system to be powered on, or woken up, by sending a magic packet to it. Once the system is powered on, it may become a target for lateral movement.(Citation: Bleeping Computer - Ryuk WoL)(Citation: AMD Magic Packet)

## Threat-Mapped Scoring

Score: 0.0

Priority: Unclassified

## Kill Chain Phases

**•** mitre-attack: defense-evasion

**•** mitre-attack: persistence

**•** mitre-attack: command-and-control

## Malware

* BUSHWALK
* Chaos
* J-magic
* Kobalos
* Pandora
* Penquin
* Ryuk
* SYNful Knock
* TRANSLATEXT
* Umbreon
* Uroburos
* Winnti for Linux
* ZIPLINE

## APTs (Intrusion Sets)

* Kimsuky