# TTP Detail – T1095

## TTP Information

Name: Non-Application Layer Protocol

Description: Adversaries may use an OSI non-application layer protocol for communication between host and C2 server or among infected hosts within a network. The list of possible protocols is extensive.(Citation: Wikipedia OSI) Specific examples include use of network layer protocols, such as the Internet Control Message Protocol (ICMP), transport layer protocols, such as the User Datagram Protocol (UDP), session layer protocols, such as Socket Secure (SOCKS), as well as redirected/tunneled protocols, such as Serial over LAN (SOL).

ICMP communication between hosts is one example.(Citation: Cisco Synful Knock Evolution) Because ICMP is part of the Internet Protocol Suite, it is required to be implemented by all IP-compatible hosts.(Citation: Microsoft ICMP) However, it is not as commonly monitored as other Internet Protocols such as TCP or UDP and may be used by adversaries to hide communications.

In ESXi environments, adversaries may leverage the Virtual Machine Communication Interface (VMCI) for communication between guest virtual machines and the ESXi host. This traffic is similar to client-server communications on traditional network sockets but is localized to the physical machine running the ESXi host, meaning it does not traverse external networks (routers, switches). This results in communications that are invisible to external monitoring and standard networking tools like tcpdump, netstat, nmap, and Wireshark. By adding a VMCI backdoor to a compromised ESXi host, adversaries may persistently regain access from any guest VM to the compromised ESXi host’s backdoor, regardless of network segmentation or firewall rules in place.(Citation: Google Cloud Threat Intelligence VMWare ESXi Zero-Day 2023)

## Threat-Mapped Scoring

Score: 1.8

Priority: P4 - Informational (Low)

## Kill Chain Phases

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

## Malware

* Anchor
* Aria-body
* AuTo Stealer
* BUBBLEWRAP
* Bandook
* Bisonal
* COATHANGER
* Carbon
* Clambling
* Cobalt Strike
* Crimson
* Cryptoistic
* Cuckoo Stealer
* Derusbi
* Drovorub
* FakeM
* FunnyDream
* Gelsemium
* HiddenWasp
* InvisiMole
* J-magic
* KEYPLUG
* LITTLELAMB.WOOLTEA
* LookBack
* LunarMail
* MacMa
* Mafalda
* Metamorfo
* Mis-Type
* Misdat
* MoonWind
* NETEAGLE
* NETWIRE
* Nebulae
* Neo-reGeorg
* Ninja
* OSX\_OCEANLOTUS.D
* PHOREAL
* Pay2Key
* Penquin
* PingPull
* PipeMon
* PlugX
* QUIETEXIT
* QakBot
* RARSTONE
* RCSession
* RainyDay
* Reaver
* Regin
* Remsec
* RotaJakiro
* Royal
* SDBbot
* SUGARUSH
* Samurai
* Sardonic
* ShadowPad
* SnappyTCP
* SombRAT
* Spica
* StealBit
* TSCookie
* Taidoor
* Umbreon
* Uroburos
* WINDSHIELD
* WarzoneRAT
* WellMail
* Winnti for Linux
* Winnti for Windows
* ZIPLINE
* cd00r
* gh0st RAT
* metaMain
* reGeorg

## Tools

* Brute Ratel C4
* FRP
* Mythic
* QuasarRAT

## APTs (Intrusion Sets)

* APT3
* BITTER
* BackdoorDiplomacy
* Ember Bear
* FIN6
* HAFNIUM
* Metador
* PLATINUM
* ToddyCat