











The server team has noticed a significant network performance degradation on some of their older devices attached to the network in the 10.0.0.0/16 network. After ruling out external DDoS attacks, the security team suspects something might be going on internally

All traffic originating from within the local network is by default allowed by all hosts. There is also unrestricted use of Powershell and other applications in the environment. It's possible someone is either downloading large files or doing some kind of port scanning against hosts in the local network.

Timeline Summary and Findings:

When querying logs for any successful or failed connections on the network level within the last 24 hours there was something suspicious found. (Each DeviceName and its corresponding LocalIP is their actual IP within the network) The RemoteIP 10.0.0.5 which is a private IP within our network has repeatedly tried connectivity within the local network from different devices.

```
DeviceNetworkEvents
| where ActionType == "ConnectionFailed"
| summarize ConnectionCount = count() by DeviceName, ActionType, LocalIP, RemoteIP
| order by ConnectionCount
```










<input type="checkbox"/>	DeviceName	ActionType	LocalIP	RemoteIP	ConnectionCount
<input type="checkbox"/>	>  spartanuser-th-	ConnectionFailed	(ip) 10.0.0.234	(ip) 10.0.0.5	66
<input type="checkbox"/>	>  edr	ConnectionFailed	(ip) 10.1.1.22	(ip) 10.0.0.5	23
<input type="checkbox"/>	>  edr-andres	ConnectionFailed	(ip) 10.1.0.151	(ip) 10.0.0.5	23
<input type="checkbox"/>	>  cyber-bunny	ConnectionFailed	(ip) 10.1.0.143	(ip) 10.0.0.5	23
<input type="checkbox"/>	>  windows-vul	ConnectionFailed	(ip) 10.0.0.104	(ip) 10.0.0.5	23
<input type="checkbox"/>	>  windows-target...	ConnectionFailed	(ip) 10.0.0.5	(ip) 10.0.0.5	23
<input type="checkbox"/>	>  winsb.youngsb...	ConnectionFailed	(ip) 10.0.0.209	(ip) 10.0.0.5	23
<input type="checkbox"/>	>  kel-99	ConnectionFailed	(ip) 10.0.0.78	(ip) 10.0.0.5	23
<input type="checkbox"/>	>  villainmach20	ConnectionFailed	(ip) 10.0.0.36	(ip) 10.0.0.5	23
<input type="checkbox"/>	>  toobz-windows	ConnectionFailed	(ip) 10.0.0.161	(ip) 10.0.0.5	22

I also see here IP address 10.0.0.5 belongs to device name "windows-target" due to its LocalIP being 10.0.0.5. We see here it has a ConnectionFailed count of 23 against its own self.

Now that I have an idea of which device is causing some anomalies, we will look into exactly the number of times 10.0.0.5 has a ConnectionFailed attempt against itself and others by running...







```
let IPInQuestion = "10.0.0.5";
DeviceNetworkEvents
| where ActionType == "ConnectionFailed"
| where LocalIP == IPInQuestion
```

```
| summarize FailedConnectionsAttempts = count() by DeviceName, ActionType,
LocalIP, RemoteIP
| order by FailedConnectionsAttempts desc
```

<input type="checkbox"/>	DeviceName	ActionType	LocalIP	RemoteIP	FailedConnectionsAttempts
<input type="checkbox"/>	>  windows-target...	ConnectionFailed	(local) 10.0.0.5	(local) 10.0.0.5	23
<input type="checkbox"/>	>  windows-target...	ConnectionFailed	(local) 10.0.0.5	(local) 146.75.30.172	1
<input type="checkbox"/>	>  windows-target...	ConnectionFailed	(local) 10.0.0.5	(local) 23.53.11.74	1
<input type="checkbox"/>	>  windows-target...	ConnectionFailed	(local) 10.0.0.5	(local) 23.54.127.164	1
<input type="checkbox"/>	>  windows-target...	ConnectionFailed	(local) 10.0.0.5	(local) 92.38.145.145	1
<input type="checkbox"/>	>  windows-target...	ConnectionFailed	(local) 10.0.0.5	(local) 135.233.45.222	1
<input type="checkbox"/>	>  windows-target...	ConnectionFailed	(local) 10.0.0.5	(local) 168.63.129.16	1
<input type="checkbox"/>	>  windows-target...	ConnectionFailed	(local) 10.0.0.5	(local) 169.254.169.254	1
<input type="checkbox"/>	>  windows-target...	ConnectionFailed	(local) 10.0.0.5	(local) 199.232.90.172	1

Looking through other devices on the Local network querying their LocalIP it found that other devices on the network are also repeating failed connections among other private IP's within the network. This indicates its not only "windows-target" 10.0.0.5 with suspicious anomalies but also "edr-andres" whose LocalIP is 10.1.0.151. The major difference is no ConnectionFailed towards itself.

```
let IPInQuestion = "10.1.0.151";
DeviceNetworkEvents
| where ActionType == "ConnectionFailed"
| where LocalIP == IPInQuestion
| summarize FailedConnectionsAttempts = count() by DeviceName, ActionType,
LocalIP, RemoteIP
| order by FailedConnectionsAttempts desc
```

<input type="checkbox"/>	DeviceName	ActionType	LocalIP	RemoteIP	FailedConnectionsAttempts
<input type="checkbox"/>	>  edr-andres	ConnectionFailed	(local) 10.1.0.151	(local) 10.0.0.5	23
<input type="checkbox"/>	>  edr-andres	ConnectionFailed	(local) 10.1.0.151	(local) 103.11.9.33	1
<input type="checkbox"/>	>  edr-andres	ConnectionFailed	(local) 10.1.0.151	(local) 199.232.90.172	1
<input type="checkbox"/>	>  edr-andres	ConnectionFailed	(local) 10.1.0.151	(local) 23.218.217.140	1
<input type="checkbox"/>	>  edr-andres	ConnectionFailed	(local) 10.1.0.151	(local) 23.218.217.149	1
<input type="checkbox"/>	>  edr-andres	ConnectionFailed	(local) 10.1.0.151	(local) 146.75.30.172	1

When running a query against 10.0.0.5 for its general amount of "ConnectionFailed" ActionType I notice the amount of targeted RemotePorts.

```
let IPInQuestion = "10.0.0.5";
DeviceNetworkEvents
| where ActionType == "ConnectionFailed"
| where LocalIP == IPInQuestion
| order by Timestamp desc
```

<input type="checkbox"/>	Timestamp	DeviceId	DeviceName	ActionType	RemoteIP	RemotePort
<input type="checkbox"/>	> Sep 24, 2025 1:33:...	b1856ac7473b0cbc4...	windows-target-1	ConnectionFailed	(no) 199.232.90.172	80
<input type="checkbox"/>	> Sep 24, 2025 1:32:...	b1856ac7473b0cbc4...	windows-target-1	ConnectionFailed	(no) 23.53.11.13	80
<input type="checkbox"/>	> Sep 24, 2025 8:40:...	b1856ac7473b0cbc4...	windows-target-1	ConnectionFailed	(no) 10.0.0.5	8443
<input type="checkbox"/>	> Sep 24, 2025 8:40:...	b1856ac7473b0cbc4...	windows-target-1	ConnectionFailed	(no) 10.0.0.5	8080
<input type="checkbox"/>	> Sep 24, 2025 8:40:...	b1856ac7473b0cbc4...	windows-target-1	ConnectionFailed	(no) 10.0.0.5	5900
<input type="checkbox"/>	> Sep 24, 2025 8:39:...	b1856ac7473b0cbc4...	windows-target-1	ConnectionFailed	(no) 10.0.0.5	3306
<input type="checkbox"/>	> Sep 24, 2025 8:39:...	b1856ac7473b0cbc4...	windows-target-1	ConnectionFailed	(no) 10.0.0.5	995
<input type="checkbox"/>	> Sep 24, 2025 8:39:...	b1856ac7473b0cbc4...	windows-target-1	ConnectionFailed	(no) 10.0.0.5	993
<input type="checkbox"/>	> Sep 24, 2025 8:39:...	b1856ac7473b0cbc4...	windows-target-1	ConnectionFailed	(no) 10.0.0.5	587
<input type="checkbox"/>	> Sep 24, 2025 8:39:...	b1856ac7473b0cbc4...	windows-target-1	ConnectionFailed	(no) 10.0.0.5	465
<input type="checkbox"/>	> Sep 24, 2025 8:39:...	b1856ac7473b0cbc4...	windows-target-1	ConnectionFailed	(no) 10.0.0.5	443
<input type="checkbox"/>	> Sep 24, 2025 8:39:...	b1856ac7473b0cbc4...	windows-target-1	ConnectionFailed	(no) 10.0.0.5	194
<input type="checkbox"/>	> Sep 24, 2025 8:38:...	b1856ac7473b0cbc4...	windows-target-1	ConnectionFailed	(no) 10.0.0.5	161
<input type="checkbox"/>	> Sep 24, 2025 8:38:...	b1856ac7473b0cbc4...	windows-target-1	ConnectionFailed	(no) 10.0.0.5	143
<input type="checkbox"/>	> Sep 24, 2025 8:38:...	b1856ac7473b0cbc4...	windows-target-1	ConnectionFailed	(no) 10.0.0.5	138
<input type="checkbox"/>	> Sep 24, 2025 8:38:...	b1856ac7473b0cbc4...	windows-target-1	ConnectionFailed	(no) 10.0.0.5	137
<input type="checkbox"/>	> Sep 24, 2025 8:38:...	b1856ac7473b0cbc4...	windows-target-1	ConnectionFailed	(no) 10.0.0.5	123
<input type="checkbox"/>	> Sep 24, 2025 8:38:...	b1856ac7473b0cbc4...	windows-target-1	ConnectionFailed	(no) 10.0.0.5	110
<input type="checkbox"/>	> Sep 24, 2025 8:38:...	b1856ac7473b0cbc4...	windows-target-1	ConnectionFailed	(no) 10.0.0.5	80
<input type="checkbox"/>	> Sep 24, 2025 8:38:...	b1856ac7473b0cbc4...	windows-target-1	ConnectionFailed	(no) 10.0.0.5	69
<input type="checkbox"/>	> Sep 24, 2025 8:37:...	b1856ac7473b0cbc4...	windows-target-1	ConnectionFailed	(no) 10.0.0.5	53

This goes to show 10.0.0.5 ran a port scan against itself and 10.1.0.151 device ran a port scan towards 10.0.0.5.

Summary:

10.0.0.5 has been the target of choice by other devices within the private network (even among itself) to perform a port scan.

When deciding to look through process events I found exactly the process which executed the port scan on “edr-andres” towards “windows-target-1”. I ran the following query specifying a timeframe in which I noticed the portscan first began and ended.

```
let VMName = "edr-andres";
let specificTime = datetime(2025-09-24T19:16:44.6737007Z);
DeviceProcessEvents
| where Timestamp between ((specificTime - 10m) .. (specificTime + 10m))
| where DeviceName == VMName
| order by Timestamp desc
| project Timestamp, FileName, InitiatingProcessCommandLine
```

<input type="checkbox"/>	Timestamp	FileName	InitiatingProcessCommandLine
<input type="checkbox"/>	> Sep 24, 2025 3:19:...	conhost.exe	"FindVolume.exe" /label "Temporary Storage"
<input type="checkbox"/>	> Sep 24, 2025 3:19:...	FindVolume.exe	WaAppAgent.exe
<input type="checkbox"/>	> Sep 24, 2025 3:17:...	dllhost.exe	svchost.exe -k DcomLaunch -p
<input type="checkbox"/>	> Sep 24, 2025 3:16:...	conhost.exe	BfeToolWin8.exe
<input type="checkbox"/>	> Sep 24, 2025 3:16:...	BfeToolWin8.exe	WindowsAzureGuestAgent.exe
<input checked="" type="checkbox"/>	> Sep 24, 2025 3:16:...	powershell.exe	"cmd.exe" /c powershell.exe -ExecutionPolicy Bypass -File C:\programdata\portscan.ps1
<input type="checkbox"/>	> Sep 24, 2025 3:16:...	cmd.exe	powershell.exe

Here you see a powershell executable named "portscan.ps1" and lines up with the timing of when the portscan first began.

Logging into device "edr-andres" I quickly found the portscan powershell file under C:\programdata

To identify exactly who ran this executable I can find the AccountName associated with this device the moment this powershell file was run but I was only presented with "system" which is unusual behavior. As a result we cant directly disable this "system" account.

Remediation:

- Isolate the device in Microsoft XDR
 - Investigate why and how this portscan executed
 - Run malware scan
 - Re-image device
-

MITRE ATT&CK Framework Related TTPs:

- Tactic: **Reconnaissance (TA0043)** Technique: Network Service scanning T1046
- Tactic: **Execution (TA0002)** Technique: Powershell executing T1059.001
- Tactic: **Privilege Escalation (TA0004)** Technique: Access to local accounts T1078.003
- Tactic: **Discovery (TA0007)** Technique: Network connection discovery T1049
- Tactic: **Lateral Movement (TA0008)** Technique: Potential remote services T1021