AIRGAP

Ransomware Vulnerability Scanner
(GoScanner)

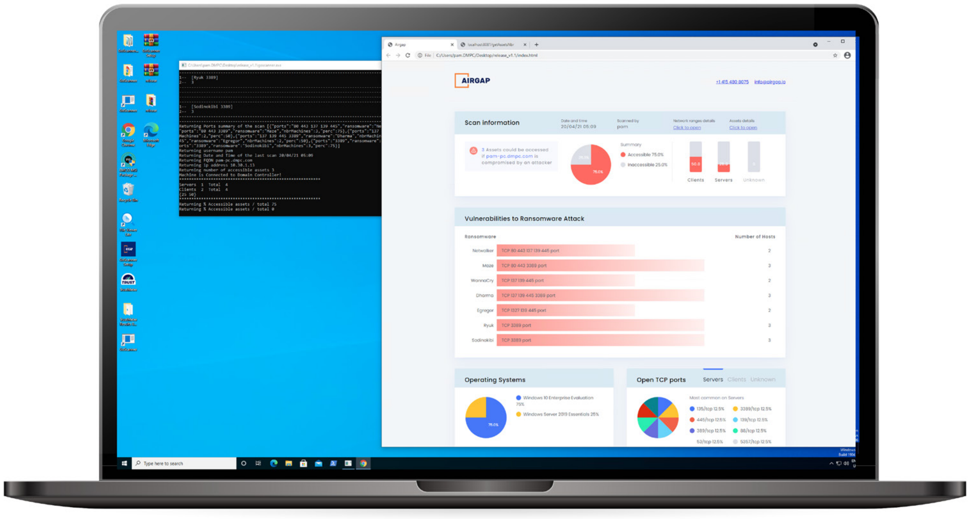
Lateral propagation of Ransomware frequently happens due to open TCP/UDP network ports on user endpoints and network servers. For example, WannaCry ransomware spreads within a network by exploiting a vulnerability in the SMP protocol (TCP/445). This port is left open on Windows client devices even if they are not sharing files with their peer devices. Security admins are frequently unaware of what network port vulnerabilities exist on their devices.

This document provides an overview of the Airgap Network Vulnerability Scanner (a.k.a GoScanner). The scanner utility is designed to be an easy-to-use application for CIOs, Security Admins and other prospective customers to run within their environment so that they can assess how vulnerable their network and endpoints are to lateral propagation threats.

The network vulnerability scanner can be downloaded and installed from the following location:

> **https://airgap-downloads.s3-us-west-1.amazonaws.com/GoScanner/GoScannerSetup.zip**

Upon installation, a desktop shortcut called "GoScanner" will be added to the desktop:



C:\Users\pam.DMPC\Desktop\release_v1.1\goscanner.exe

```
1--  [Ryuk 3389]
2--  3
------------------------------------------------------------
1--  [Sodinokibi 3389]
2--  3
------------------------------------------------------------
Returning Ports summary of the scan [{"ports":"80 443 137 139 445","ransomware":"Ne
"ports":"80 443 3389","ransomware":"Maze","nbrMachines":3,"perc":75},{"ports":"137
Machines":2,"perc":50},{"ports":"137 139 445 3389","ransomware":"Dharma","nbrMachin
45","ransomware":"Egregor","nbrMachines":2,"perc":50},{"ports":"3389","ransomware":
orts":"3389","ransomware":"Sodinokibi","nbrMachines":3,"perc":75}]
Returning username pam
Returning Date and Time of the last scan 20/04/21 05:09
Returning FQDN pam-pc.dmpc.com
Returning ip address 10.30.1.13
Returning number of accessible assets 3
Machine is Connected to Domain Controller!
**********************************************************
Servers  1  Total  4
Clients  2  Total  4
{25 50}
**********************************************************
Returning % Accessible assets / total 75
Returning % Accessible assets / total 0
```

Airgap
localhost:8081/getAssetsNbr
File | C:/Users/pam.DMPC/Desktop/release_v1.1/index.html
AIRGAP
+1 415 480 8075
info@airgap.io

Scan information

Date and time: 20/04/21 05:09

Scanned by: pam

Network ranges details: Click to open

Assets details: Click to open

3 Assets could be accessed if pam-pc.dmpc.com is compromised by an attacker

Summary: Accessible 75.0%, Inaccessible 25.0%

Vulnerabilities to Ransomware Attack

Ransomware		Number of Hosts
Netwalker	TCP 80 443 137 139 445 port	2
Maze	TCP 80 443 3389 port	3
WannaCry	TCP 137 139 445 port	2
Dharma	TCP 137 139 445 3389 port	3
Egregor	TCP 1327 139 445 port	2
Ryuk	TCP 3389 port	3
Sodinokibi	TCP 3389 port	3

Operating Systems

Windows 10 Enterprise Evaluation 75%
Windows Server 2019 Essentials 25%
75.0%

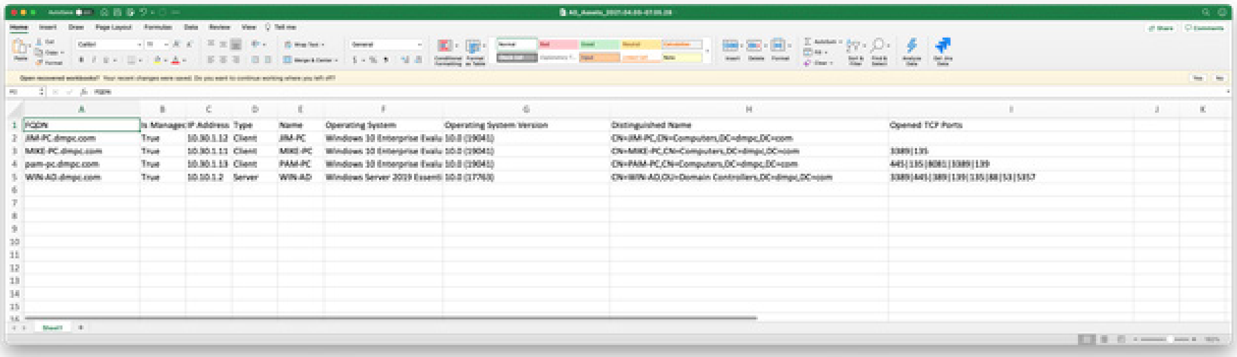
Open TCP ports

The user can simply double-click on this shortcut icon to launch this utility. This utility will then scan the network neighborhood and show the result in a browser as shown below:

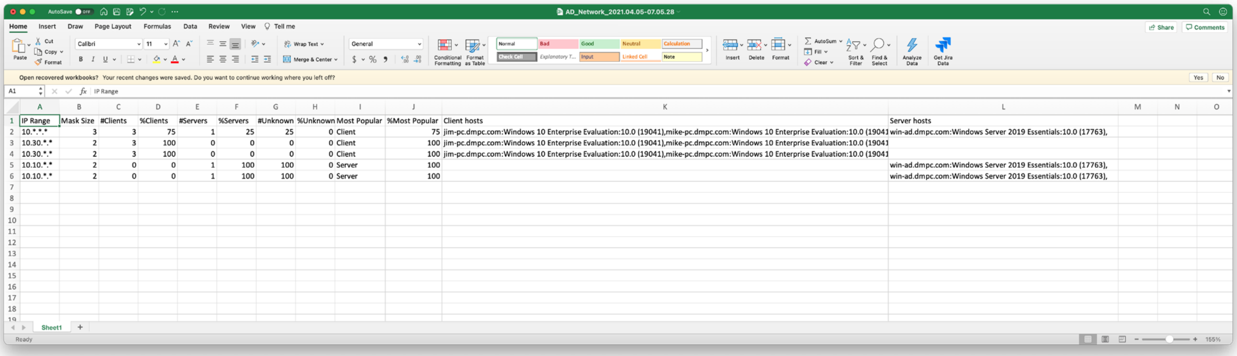
This HTML page provides the following information:

Scan Information

This provides a scan summary, including links to launch more detailed spreadsheets on the network assets and vulne rable ports on them. Network assets on the local network and those registered with Microsoft Active Directory are scanned.



FQDN	Is Managed	IP Address	Type	Name	Operating System	Operating System Version	Distinguished Name	Opened TCP Ports
JIM-PC.dmpc.com	True	10.30.1.12	Client	JIM-PC	Windows 10 Enterprise Evalu	10.0 (19041)	CN=JIM-PC,CN=Computers,DC=dmpc,DC=com	
MIKE-PC.dmpc.com	True	10.30.1.11	Client	MIKE-PC	Windows 10 Enterprise Evalu	10.0 (19041)	CN=MIKE-PC,CN=Computers,DC=dmpc,DC=com	3389|135
pam-pc.dmpc.com	True	10.30.1.13	Client	PAM-PC	Windows 10 Enterprise Evalu	10.0 (19041)	CN=PAM-PC,CN=Computers,DC=dmpc,DC=com	445|135|8081|3389|139
WIN-AD.dmpc.com	True	10.10.1.2	Server	WIN-AD	Windows Server 2019 Essenti	10.0 (17763)	CN=WIN-AD,OU=Domain Controllers,DC=dmpc,DC=com	3389|445|389|139|135|88|53|5357



AD_Network_2021.04.05-07.05.28

Open recovered workbooks? Your recent changes were saved. Do you want to continue working where you left off?

IP Range	Mask Size	#Clients	%Clients	#Servers	%Servers	#Unknown	%Unknown	Most Popular	%Most Popular	Client hosts	Server hosts
10.*.*.*	3	3	75	1	25	25	0	Client	75	jim-pc.dmpc.com:Windows 10 Enterprise Evaluation:10.0 (19041),mike-pc.dmpc.com:Windows 10 Enterprise Evaluation:10.0 (19041	win-ad.dmpc.com:Windows Server 2019 Essentials:10.0 (17763),
10.30.*.*	2	3	100	0	0	0	0	Client	100	jim-pc.dmpc.com:Windows 10 Enterprise Evaluation:10.0 (19041),mike-pc.dmpc.com:Windows 10 Enterprise Evaluation:10.0 (19041	
10.30.*.*	2	3	100	0	0	0	0	Client	100	jim-pc.dmpc.com:Windows 10 Enterprise Evaluation:10.0 (19041),mike-pc.dmpc.com:Windows 10 Enterprise Evaluation:10.0 (19041	
10.10.*.*	2	0	0	1	100	100	0	Server	100		win-ad.dmpc.com:Windows Server 2019 Essentials:10.0 (17763),
10.10.*.*	2	0	0	1	100	100	0	Server	100		win-ad.dmpc.com:Windows Server 2019 Essentials:10.0 (17763),

Assets Accessibility

This section provides a pie chart of accessible and inaccessible assets on the network. If a network asset has any open TCP ports which are vulnerable to lateral attack, then it is classified as an accessible asset. Assets are grouped into clients and servers. This grouping is based on the operating system versions they are running. The most common open TCP ports on these assets are shown alongside.

Accordion Table

that groups the network assets by their network IP prefixes, operating systems, and opened ports.

- **IP Ranges Layout:** This groups clients and server assets by their IP prefixes
- **Operating Systems:** This groups clients and server assets by their Operating Systems
- **Opened Ports:** This groups clients and server assets by the open ports.

Next Steps

After running the utility, the customer would have an idea of what assets on their network are vulnerable to lateral propagation of ransomware.

About Airgap

Ransomware threat is growing rapidly. While there are a whole bunch of security companies that are trying to prevent ransomware from getting into your network, Airgap's "Zero Trust Isolation Platform" protects your organization even if your perimeter is breached or if you have unpatched vulnerable servers inside your data center. Additionally, Airgap's "Ransomware Kill Switch" is the most potent ransomware response for the IT organization. Airgap can be deployed in minutes without any agents, forklift upgrades, or design changes. The company is founded by highly experienced cybersecurity experts and the solution is trusted by large enterprises and service providers. For more details, check out https://airgap.io