









Sign in

 3CORESec / MAL-CL Public

 Notifications


 Fork


43


 Star


308


<> Code


 Issues


 Pull requests


 Actions



 Security


 Insights

MAL-CL / Descriptors / Other / Advanced IP Scanner / 





Name	Last commit message	Last commit date
 ..		
 README.md		

README.md 

Advanced IP Scanner

Table of Contents

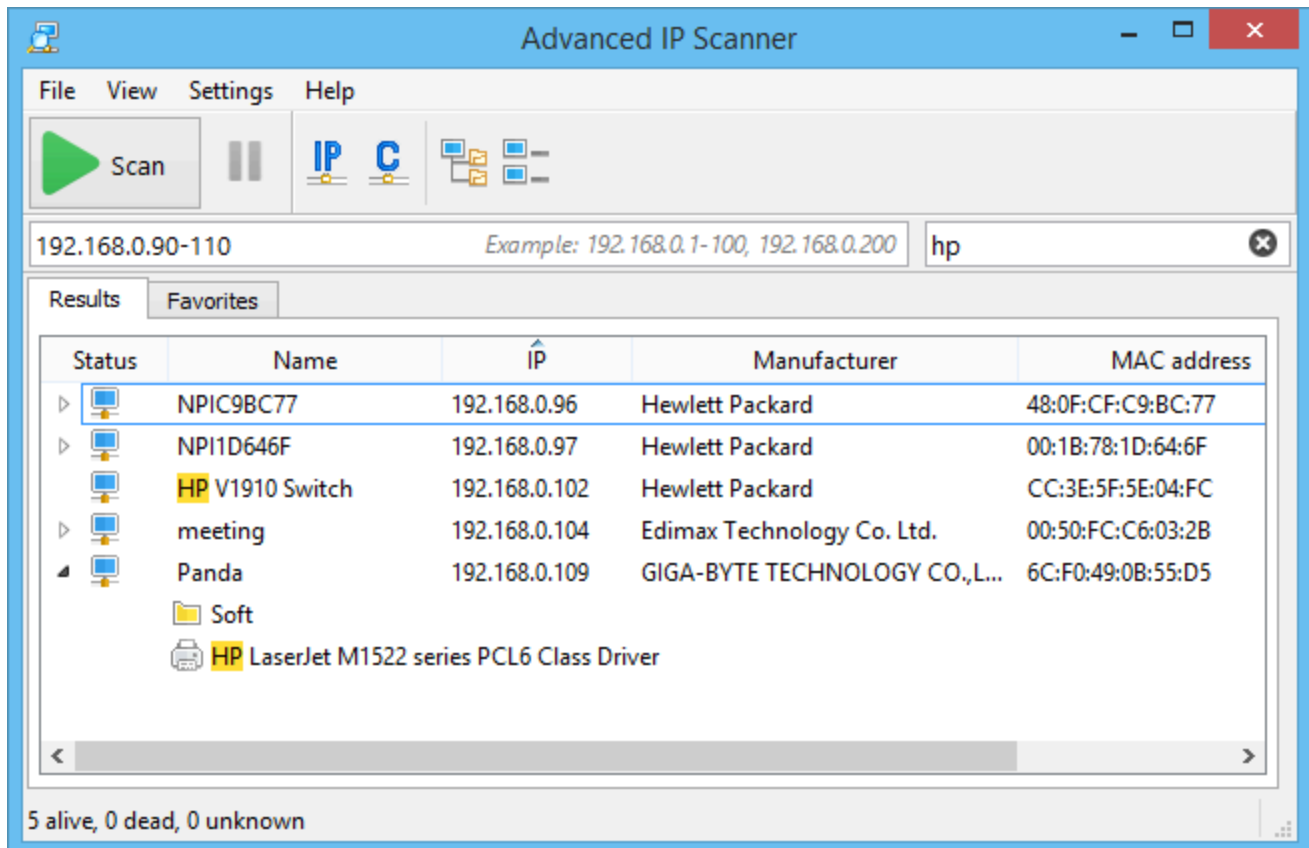
- [Advanced IP Scanner](#)
 - [Table of Contents](#)
 - [Acknowledgement\(s\)](#)
 - [Description](#)
 - [Versions History](#)
 - [File Metadata](#)
 - [Common CommandLine](#)
 - [Threat Actor Ops \(TAOps\)](#)
 - [Common Process Trees](#)

- [Default Install Location](#)
- [DFIR Artifacts](#)
- [Examples In The Wild](#)
- [Documentation](#)
- [Blogs / Reports References](#)
- [ATT&CK Techniques](#)
- [Telemetry](#)
- [Detection Validation](#)
- [Detection Rules](#)
- [LOLBAS / GTFOBins References](#)

Acknowledgement(s)

- 3CORESec - [@3CORESec](#)
- Nasreddine Bencherchali - [@nas_bench](#)

Description



Advanced IP Scanner is fast and free software for network scanning. It will allow you to quickly detect all network computers and obtain access to them. — [Advanced IP Scanner](#)

Versions History

- History for `advanced_ip_scanner.exe` :

Version	SHA1	VT
2.5.3850	1556232c5b6a998a4765a8f53d48a059cd617c59	LINK
2.5.3748	d4793c97b4a1d36cbb39b3e76a60dde182a9d7ad	LINK
2.4	a01b7f55c5edc6576d1349a0a23b781552c74244	LINK
2.3	0e840ae8efa952429c15c00776d63539c44fcef2	LINK

- History for `advanced_ip_scanner_console.exe` :
 - TBD

File Metadata

- This metadata information is based on the latest version available as of this writing (`advanced_ip_scanner.exe` - 2.5.3850).

Attribute	Value
Copyright	Copyright © 2002-2019 Famatech Corp. and its licensors. All rights reserved
Product	Advanced IP Scanner
Description	Advanced IP Scanner Setup
Original Name	/
Internal Name	/

- This metadata information is based on the latest version available as of this writing (`advanced_ip_scanner_console.exe` - 2.5.3850).
 - TBD

Common CommandLine

```
advanced_ip_scanner.exe /portable [PATH] /lng [Language]
advanced_ip_scanner_console.exe /r:[IP RANGE]
advanced_ip_scanner_console.exe /r:[IP RANGE] /v
advanced_ip_scanner_console.exe /s:ip_ranges.txt /f:scan_results.txt
```



Threat Actor Ops (TAOps)

- TBD

Common Process Trees

- TBD

Default Install Location

```
C:\Program Files (x86)\Advanced IP Scanner\
C:\Users\[user]\AppData\Local\Temp\Advanced IP Scanner 2\
C:\Users\[user]\AppData\Local\Programs\Advanced IP Scanner Portable\
```



DFIR Artifacts

- TBD

Examples In The Wild

- [ANY.RUN — ipscan25.exe](#)

Documentation

- [Advanced IP Scanner \(GUI\) — Help](#)
- Advanced IP Scanner Console Help:

Usage:

```
</r:<IP range> OR /s:<source_file>> [/f:<output_file>] [/v]
```

Description:

/r - address or range of IP addresses to scan, ex 192.168.0.1-192.168.0.255
or

/s - path to the file with IP ranges with 1 IP/IP range per line format, ex
192.168.0.1-192.168.0.128
192.168.0.155
192.168.1.10

/f - path to the file where scan results will be written

/v - show results of service scan (/v2 to show grouped)

Example:

```
advanced_ip_scanner_console.exe /r:192.168.0.1-192.168.0.255
```

```
advanced_ip_scanner_console.exe /s:ip_ranges.txt /f:scan_results.txt
```

Blogs / Reports References

- [The DFIR Report — All That for a Coinminer?](#)
- [The DFIR Report — BazarLoader and the Conti Leaks](#)
- [The DFIR Report — GoGoogle Ransomware](#)

ATT&CK Techniques

- [T1046 — Network Service Scanning](#)
- [T1135 — Network Share Discovery](#)

Telemetry

- [Security Event ID 4688 — A new process has been created](#)
- [Sysmon Event ID 1 — Process creation](#)
- [PsSetCreateProcessNotifyRoutine/Ex](#)

- [ETW - Microsoft-Windows-Kernel-Process - Event ID 1 - ProcessStart](#)

Detection Validation

- TBD

Detection Rules

- Sigma
 - [Advanced IP Scanner - Process Creation](#)
 - [Advanced IP Scanner - File Event](#)

LOLBAS / GTFOBins References

- None