On 2024-03-14

by Julien Houry, Incident Responder

CYBERSECURITY

Uncovering Cyber Intruders: A Forensic Deep Dive into NetScan, Angry IP Scanner, and Advanced Port Scanner

The use of network scanners with a graphical user interface has been observed in a number of former IR engagements conducted by our CSIRT.
Discover how operators use these tools to map networks and minimize detection.

Summary

Introduction

The use of network scanners with a graphical user interface (GUI) has been observed in a number of former IR engagements conducted by the CSIRT Airbus Protect.

Indeed, Ransomware and Advanced Persistent Threat (APT) operators often use tools like GUI network scanners as part of their techniques.

By using network scanners, operators can map the network, identify interesting targets and plan their attack strategy while minimizing the chances of being detected. This discovery phase is important in the case of an intrusion, as it enables the proper deployment of the subsequent steps in the cyber kill chain.

In this article, we will study three GUI-based network scanners: NetScan, Angry IP Scanner & Advanced Port Scanner, with the aim of discovering forensics artifacts. The focus will be on the type of data they generate and how to exploit this data to find out how these tools have been used on an infrastructure. This is by no means a detection approach, as is sometimes the case with NIDS.

Once these artifacts have been identified, the next step will be to effectively leverage them. To this end, we will be developing modules for Velociraptor, a tool used for digital forensics and incident response (DFIR). These modules, called Artefact by this solution, will be designed to automate the collection and the analysis of data generated by network scanners, facilitating more efficient and thorough forensics investigation at scale.

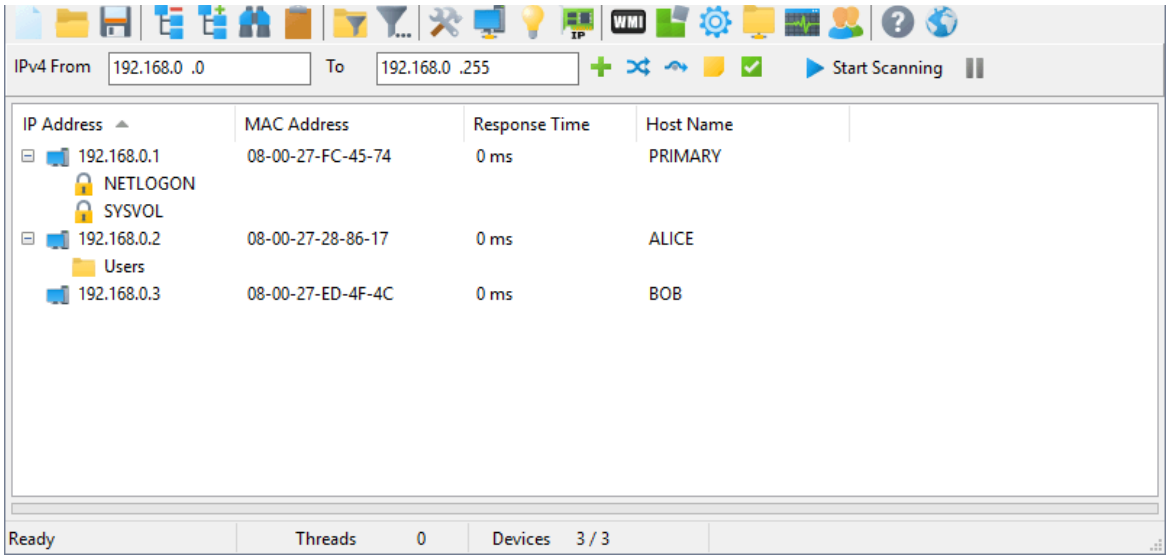
research methodology

In our approach to tracking a program's execution on a system, we use Procmon from the Sysinternals suite. We will be focusing on all the actions of a particular program. To render our analysis more precise, we specifically filter for the operations CreateFile and RegCreateKey. These filters allow to see when a program creates or opens files and when it creates registry keys.

By doing this, we get a clear picture of how the program interacts with the system, especially in terms of file and registry modifications.

SoftPerfect Network Scanner (NetScan)

SoftPerfect Network Scanner, also known as NetScan, is a multifunctional network scanning tool that detects devices and open ports on a network, identifies file shares, provides IP configuration details, integrates security features, has an intuitive graphical user interface, enables report generation and data export, supports SNMP protocol and offers scripting options for automating network scanning tasks.



Artifacts discovered

netscan.lic

This file serves as the license file used to determine whether the application has a valid purchased license or is available for free use. It is formatted as an XML file and contains information related to the program's graphical user interface language configuration and license details, including the license name. In the case of the portable version, this file is located in the current usage directory on the filesystem. For the system-installed version, it can be found in `C:UsersCURRENTUSERAppDataRoamingSoftPerfect Network Scanner`.

Here's an example of a netscan.lic content:

```
<?xml version="1.0" encoding="utf-8" standalone="yes"?>
    <network-scanner-license>
    <license/>
    <upgrade>0</upgrade>
    <language>French</language>
        <nmap/>
        <autoupdate>
        <prompt>false</prompt>
        <enabled>false</enabled>
        <lastcheck>0</lastcheck>
    </autoupdate>
```

netscan.xml

This XML file enables users to access information regarding the tool's configuration, selected scan ports, and a history of scanned IP ranges. In the case of the portable version, this file can be found in the current usage directory on the filesystem. For the system-installed version, it is located in `C:UsersCURRENTUSERAppDataRoamingSoftPerfect Network Scanner`.

Here's an example of a netscan.xml content:

```
<history>
    <item>
        <data>192.168.1.0-192.168.1.100</data>
    </item>
    <item>
        <data>192.168.1.0-192.168.1.200</data>
    </item>
    <item>
        <data>192.168.1.0-192.168.1.210</data>
    </item>
</history>
```

Velociraptor query

To locate and parse XML files on the filesystem, we employed the [glob()] plugin, which employs a global expression to search for files by name (specifically, in our case: netscan.xml & netscan.lic because these files are generated each time they are used). After identifying these files, we utilize the [parse_xml] parser to extract information from the XML files into a designated field. Additionally, we ensure that the request includes both the creation and modification timestamps.

Here are the written queries:

NetScan_lic:

```
LET netscan_lic = SELECT * FROM glob(globs='*\\**\\netscan.lic')
SELECT OSPath,Btime,Mtime, parse_xml(file=OSPath) AS ParsedXML
FROM netscan lic
```

NetScan_xml:

```
LET netscan_xml = SELECT * FROM glob(globs='*\\**\\netscan.xml')
SELECT OSPath,Btime,Mtime, parse_xml(file=OSPath) AS ParsedXML
FROM netscan xml
```

Results in Velociraptor

Angry IP Scanner

Angry IP Scanner is a lightweight, fast, and easy-to-use network scanner. It efficiently scans IP addresses and ports, with the ability to resolve hostnames, determine MAC addresses, and scan ports. It supports various data export options and is extendable via plugins.

Artifacts discovered

A registry key is created when Angry IP Scanner is used, and is located in `HKEY_USERS*SOFTWAREJavaSoftPrefsipscan`.

In this registry key, we can observe 4 subkeys of interest:

- language: Displays the language used in the GUI, may prove useful to have a possible idea of the language used by a threat actor but you need to be careful about attribution and correlate this information with a modus operandi to avoid falling into the trap of a false flag.
- last/Run/Version: Displays the version of Angry IP Scanner
- last/Version/Check: Captures the EPOCH time (in UTC +0) when the application was first started
- port/String: Displays the selected ports for scanning

Velociraptor query

This Velociraptor query is straightforward; we simply parse these sub-keys and rename the fields to enhance our comprehension of the artifacts:

- last/Run/Version as Version
- port/String as PortScanConfiguration
- last/Run/Version as FirstStarted

```
parameters:
    - name: RegistryPath
    default: HKEY_USERS\\*\\SOFTWARE\\JavaSoft\\Prefs\\ipscan
    - name: RegistryData
    type: regex
    default: .
sources:
    - precondition:
        SELECT OS FROM info() where OS = 'windows'

query: |
    SELECT Key.FileInfo.FullPath AS FullPath, Key.FileInfo.ModTime
AS ModificationTime, language, get(field="last/Run/Version",
default="Unknown") AS Version, get(field="port/String",
default="Unknown") AS PortScanConfiguration,
get(field="last/Run/Version", default="Unknown") AS FirstStarted FROM
read_reg_key(globs=RegistryPath, accessor="registry")
```

Results in Velociraptor

Advanced Port Scanner

Advanced Port Scanner is a specialized networking utility designed for scanning devices on a network, identifying open ports, and recognizing services operating on these ports. Primarily utilized by network administrators, IT experts, and security professionals, this tool plays a crucial role in evaluating a network's security.

It also features capabilities for remote computer access, supports Wake-on-LAN, and has the ability to shut down computers remotely. With its intuitive interface and availability in a portable version, it is an ideal choice for professionals managing network infrastructure and security.

Artifacts discovered

During the monitoring of executions and the execution of various IP scans using this solution, we noticed the creation of two registry keys in the following locations:

```
`\HKEY\USERS\CurrentUser\SOFTWARE\Famatech\advanced_port_scanner\`
`\HKEY\USERS\CurrentUser\SOFTWARE\Famatech\advanced_port_scanner\State
\`
```

Notably, these keys contain several subkeys of interest:

For the registry key: “advanced_port_scanner”:

- run: Displays the version of Advanced Port Scanner
- locale_timestamp: Indicates the time in EPOCH (UTC +0) at which the application was first launched
- locale: Displays the language chosen for the graphical interface, may prove useful to have an idea of the native language of a threat actor

For the registry key: “advanced_port_scannerState”:

- LastPortsUsed: Displays the last ports used in the last scan
- LastRangeUsed: Displays the last IP range used in the last scan
- IpRangesMruList: Displays all the IP ranges scanned by the tool, the first digit of each prefix in this list indicates the frequency of scans for each range
- PortsMruList: Displays all the ports that have been scanned by the tool, the first digit of each prefix in this list indicates the frequency of scans for each port
- SearchMruList: Displays all the IP addresses or hostnames that have been searched using the GUI’s “search” feature

Velociraptor query

This Velociraptor query parse the registry keys and their respectively sub-keys:

```
parameters:
    - name: RegistryPath_APS
    default:
HKEY_USERS\\*\\SOFTWARE\\Famatech\\advanced_port_scanner
    - name: RegistryPath_State
    default:
HKEY_USERS\\*\\SOFTWARE\\Famatech\\advanced_port_scanner\\State
    - name: RegistryData
    type: regex
    default: .
sources:
    - precondition:
    SELECT OS From info() where OS = 'windows'
    - name: AdvancedPortScanner
    query: |
    SELECT Key.FileInfo.FullPath AS FullPath, Key.FileInfo.ModTime
AS ModificationTime, run, locale, locale_timestamp
    FROM read_reg_key(globs=RegistryPath_APS, accessor="registry")
WHERE Key.FileInfo.FullPath =~ RegistryData
    - name: State
    query: |
    SELECT Key.FileInfo.FullPath AS FullPath, Key.FileInfo.ModTime
AS ModificationTime, LastPortsUsed, LastRangeUsed, IpRangesMruList,
PortsMruList, SearchMruList
```

Results in Velociraptor

Conclusion

This study of GUI-based network scanners can reveal unique forensic artifacts. These artifacts, including specific files and registry keys, are crucial for distinguishing between legitimate administrative actions and malicious activities.

By understanding and exploiting this data with tools such as Velociraptor, DFIR teams can detect more effectively and understand the misuse of these commonly used network management tools.

More on Cybersecurity

Cybersecurity

Digital Risk Management: A Business-Aligned Approach

Organisations today face a complex and evolving array of risks that require effective management. Some are inherently digital, while others are traditional risks amplified by technology. From cyberattacks to technical disruptions, these threats pose significant challenges for businesses, holding the power to impact operations, finances,

Cybersecurity

Airbus Protect explains: Vulnerability Management

What is vulnerability management? Vulnerability analyst Pierre Louis Gensou explains. Vulnerability management and vulnerability intelligence are crucial elements of IT security. As a vulnerability analyst, my role is to identify security flaws, assess their impact on the components we monitor, and inform customers of the associated risks. What is a vulnerability? When we say

Cybersecurity

Regulation (EU, Euratom) 2023/2841: What does it mean for EUIBAs?

What is Regulation 2023/2841? The EU cybersecurity Regulation, which came into force at the start of this year, aims to establish a comprehensive and standardised approach to cybersecurity across European Union Institutions, Bodies and Agencies (EUIBA). This ensures that all entities are well-protected against evolving cyber threats and capable of executing a coordinated incident [...]

line. To safeguard their future, organisations [...]

Read more

Read more

more