ID: 794655
Sample Name: 25jan. Required documents.lnk
Cookbook: defaultlinuxfilecookbook.jbs
Time: 19:54:03
Date: 30/01/2023
Version: 36.0.0 Rainbow Opal

Table of Contents

Linux Analysis Report

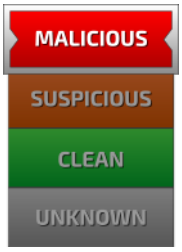
25jan. Required documents.lnk

Overview

General Information

Sample Name:	25jan. Required documents.lnk
Analysis ID:	794655
MD5:	42d501d938b5…
SHA1:	476e42f9e316d..
SHA256:	1e6c697fe3b10..
Infos:	

Detection

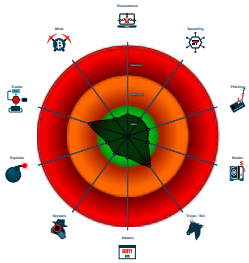


Score:	48
Range:	0 - 100
Whitelisted:	false

Signatures

- Multi AV Scanner detection for subm…
- Uses the "uname" system call to qu…
- Tries to connect to HTTP servers, b…
- Creates hidden files and/or directorie…

Classification



Analysis Advice

All HTTP servers contacted by the sample do not answer. The sample is likely an old dropper which does no longer work.

Non-zero exit code suggests an error during the execution. Lookup the error code for hints.

General Information

Joe Sandbox Version:	36.0.0 Rainbow Opal
Analysis ID:	794655
Start date and time:	2023-01-30 19:54:03 +01:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 5m 19s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	defaultlinuxfilecookbook.jbs
Analysis system description:	Ubuntu Linux 20.04 x64 (Kernel 5.4.0-72, Firefox 91.0, Evince Document Viewer 3.36.10, LibreOffice 6.4.7.2, OpenJDK 11.0.11)
Analysis Mode:	default
Sample file name:	25jan. Required documents.lnk
Detection:	MAL
Classification:	mal48.linLNK@0/0@0/0

Runtime Messages

Command:	xdg-open "/tmp/25jan. Required documents.lnk"
PID:	6234
Exit Code:	4
Exit Code Info:	
Killed:	False
Standard Output:	
Standard Error:	

Process Tree

- **system is lnxubuntu20**
  - exo-open (PID: 6246, Parent: 6234, MD5: 60a307a6a6325e2034eb5cc56bff1abd) Arguments: exo-open "/tmp/25jan. Required documents.lnk"
- **cleanup**

Yara Signatures

No yara matches

Snort Signatures

No Snort rule has matched

Joe Sandbox Signatures

AV Detection

Multi AV Scanner detection for submitted file

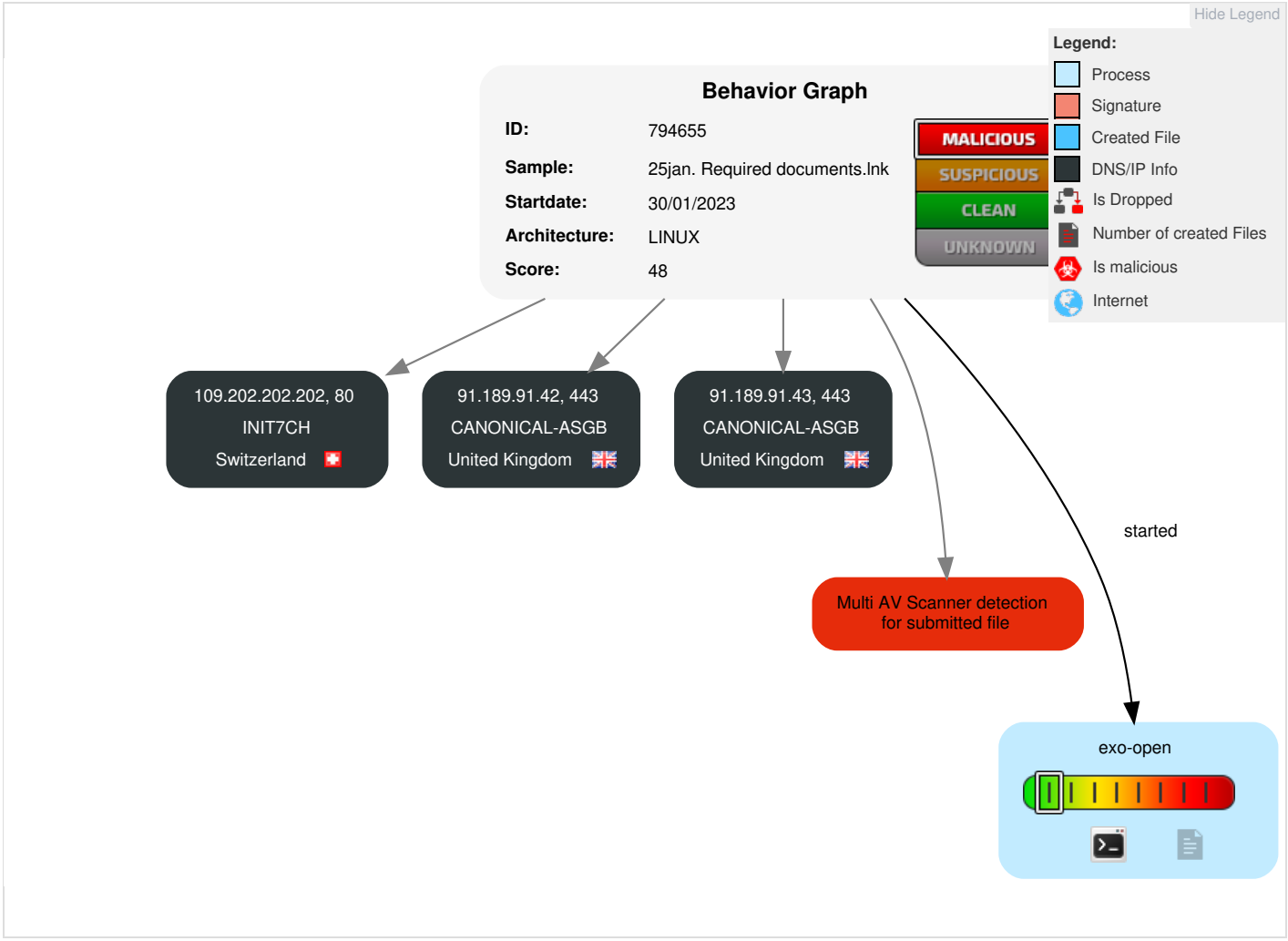
Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	Windows Management Instrumentation	Path Interception	Path Interception	1 Hidden Files and Directories	OS Credential Dumping	1 Security Software Discovery	Remote Services	Data from Local System	Exfiltration Over Other Network Medium	1 Encrypted Channel	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Rootkit	LSASS Memory	Application Window Discovery	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	1 Application Layer Protocol	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout

Malware Configuration

No configs have been found

Behavior Graph



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
25jan. Required documents.lnk	8%	Virustotal		Browse

Dropped Files

No Antivirus matches

Domains

No Antivirus matches

URLs

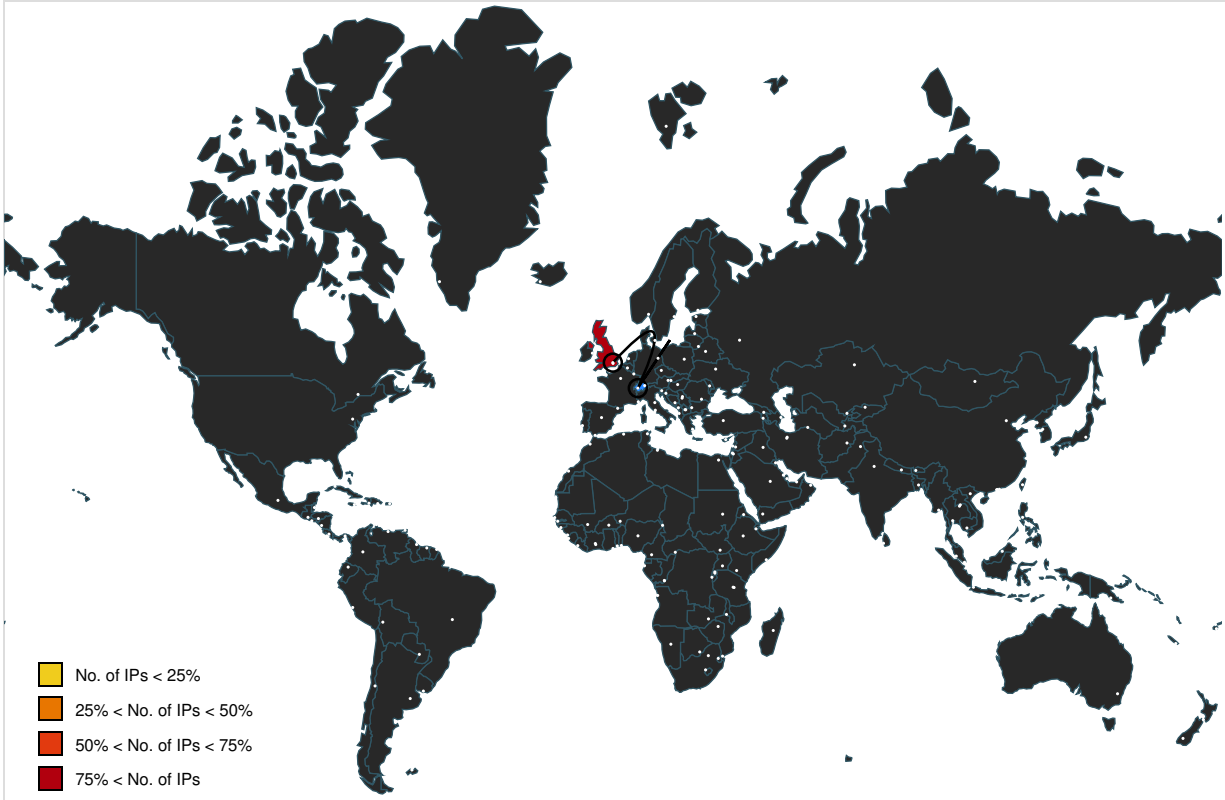
No Antivirus matches

Domains and IPs

Contacted Domains

No contacted domains info

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
109.202.202.202	unknown	Switzerland		13030	INIT7CH	false
91.189.91.43	unknown	United Kingdom		41231	CANONICAL-ASGB	false
91.189.91.42	unknown	United Kingdom		41231	CANONICAL-ASGB	false

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

No created / dropped files found

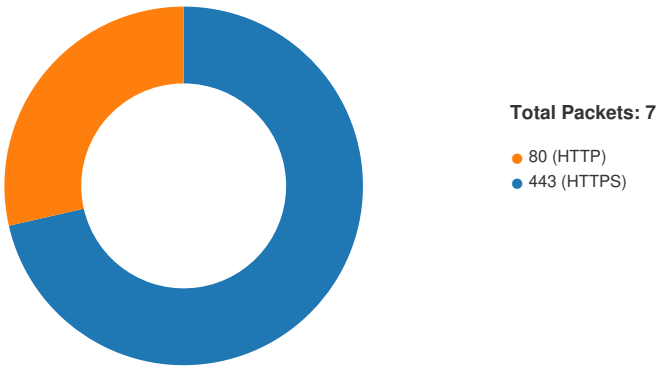
Static File Info

General

File type:	MS Windows shortcut, Item id list present, Points to a file or directory, Has Relative path, Has command line arguments, Icon number=14, Archive, ctime=Sat Jul 16 12:18:48 2016, mtime=Sat Jul 16 12:18:48 2016, atime=Sat Jul 16 12:18:48 2016, length=232960, window=hide
Entropy (8bit):	4.469401886349938
TrID:	• Windows Shortcut (20020/1) 100.00%
File name:	25jan. Required documents.lnk
File size:	1312
MD5:	42d501d938b5152accfb8541ccd302a5
SHA1:	476e42f9e316d44fbd4bf2371e2c8b5c0503eab5
SHA256:	1e6c697fe3b106fd43b6d7c96752a3618eaa04765e89bf8bc4b2e7cb8eb5034c
SHA512:	0ea012f85c749ccbb153766423c88d166eb186725b21ba1be442f3ac7d3290aa3356b80fefceff23dd010dd82e814bbd316f7e7b7a5d43e76c224c4e16f577e8
SSDEEP:	24:8vJ25BdHdaUCMbXUx+/fqiT0x4o0agFDTXD/Fom:80hH5h0OoATXjFo
TLSH:	C821870507FBA319F3B24E76043AE3458FA2F951FD63A72D5254A18C8860F08EC74B17
File Content Preview:	L.....F.... .....d.....d.....d.....5....P.O. .:i.....+00.../C:\.....V.1...../Urk..Windows.@.....H.0/Urk.....u...W.i.n.d.o.w.s.....Z.1.....)V.>..System32..B.....H.0)V.>.....

Network Behavior

Network Port Distribution



TCP Packets

System Behavior

Analysis Process: exo-open PID: 6246, Parent PID: 6234

General

Start time:	19:54:55
Start date:	30/01/2023
Path:	/usr/bin/exo-open
Arguments:	exo-open "/tmp/25jan. Required documents.lnk"
File size:	27264 bytes
MD5 hash:	60a307a6a6325e2034eb5cc56bff1abd

File Activities

File Read

Directory Enumerated

Directory Created