ID: 794650
Sample Name: 25jan. Required documents.lnk
Cookbook: defaultwindowsinteractivecookbook.jbs
Time: 19:46:32
Date: 30/01/2023
Version: 36.0.0 Rainbow Opal

Table of Contents

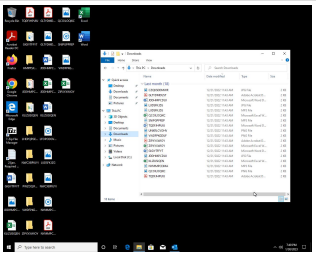
Windows Analysis Report

25jan. Required documents.lnk

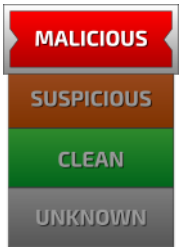
Overview

General Information

Sample Name:	25jan. Required documents.lnk
Analysis ID:	794650
MD5:	42d501d938b5…
SHA1:	476e42f9e316d..
SHA256:	1e6c697fe3b10..
Infos:	



Detection

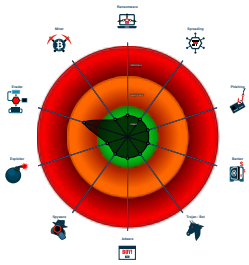


Score:	60
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Windows shortcut file (LNK) starts b…
- Multi AV Scanner detection for subm…
- Windows shortcut file (LNK) contain…
- Sample execution stops while proce…
- Uses taskkill to terminate processes
- Program does not show much activi…
- Creates a process in suspended mo…
- Enables debug privileges

Classification



Process Tree

- **System is w10x64_ra**
- cmd.exe (PID: 6496 cmdline: "C:\Windows\System32\cmd.exe" /c cd project && registry.exe registry.py & taskkill /F /IM cmd.exe MD5: 9D59442313565C2E0860B88BF32B2277)
  - conhost.exe (PID: 6504 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: C5E9B1D1103EDCEA2E408E9497A5A88F)
  - taskkill.exe (PID: 6588 cmdline: taskkill /F /IM cmd.exe MD5: 3BBEE3AC757CA54F33710DF8FB9D47A7)
- **cleanup**

Malware Configuration

No configs have been found

Yara Signatures

No yara matches

Sigma Signatures

No Sigma rule has matched

Snort Signatures

No Snort rule has matched

Joe Sandbox Signatures

AV Detection

Multi AV Scanner detection for submitted file

System Summary

Windows shortcut file (LNK) contains suspicious command line arguments

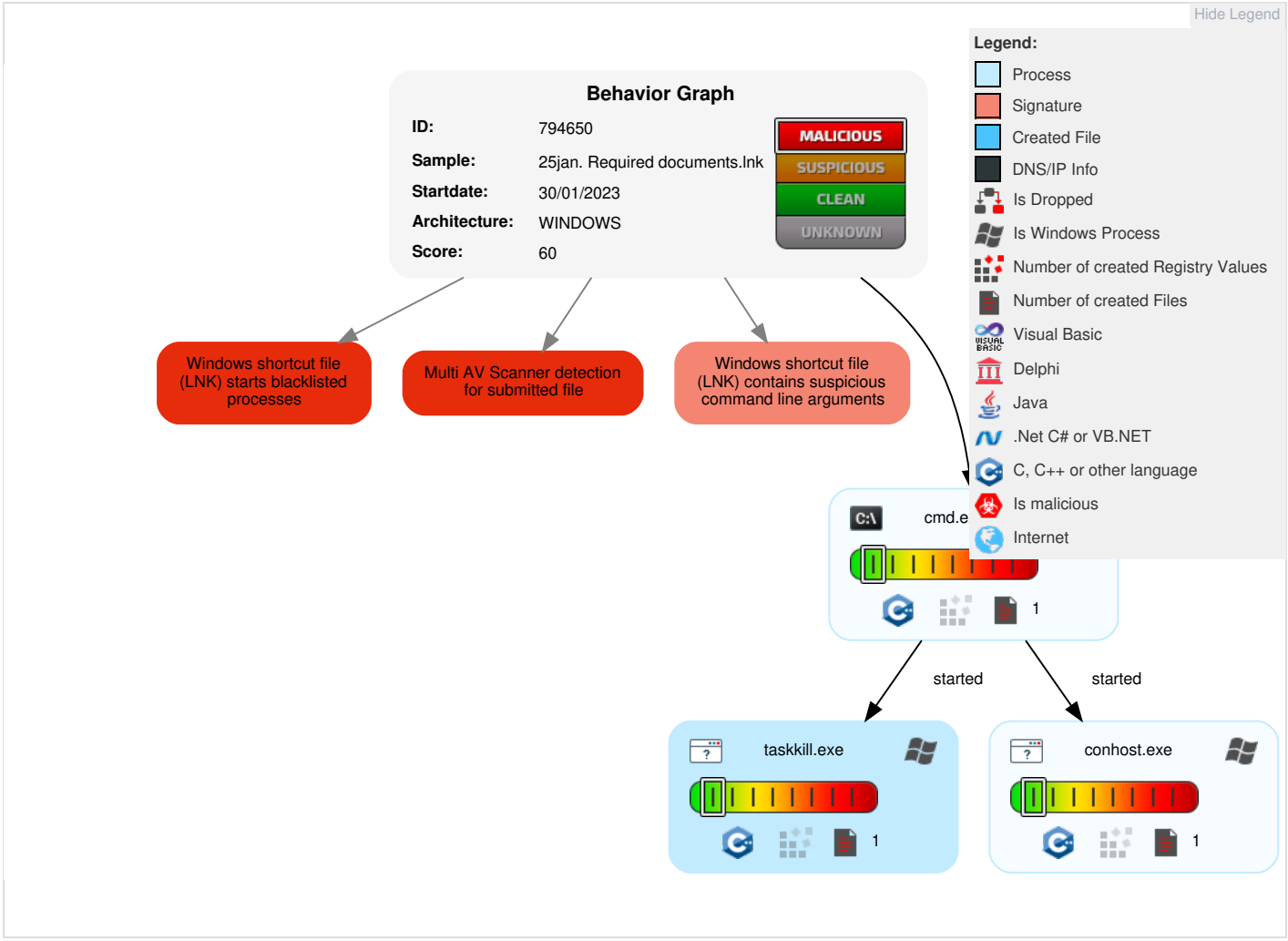
Persistence and Installation Behavior

Windows shortcut file (LNK) starts blacklisted processes

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	1 Windows Management Instrumentation	Path Interception	1 1 Process Injection	1 Disable or Modify Tools	OS Credential Dumping	1 Process Discovery	Remote Services	Data from Local System	Exfiltration Over Other Network Medium	Data Obfuscation	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	1 1 Process Injection	LSASS Memory	1 File and Directory Discovery	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Junk Data	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Obfuscated Files or Information	Security Account Manager	1 System Information Discovery	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Steganography	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data

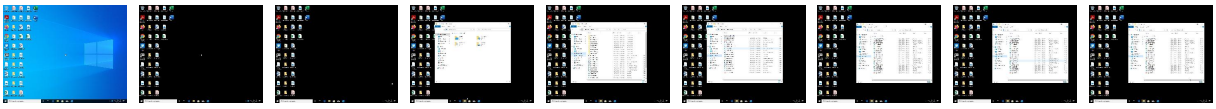
Behavior Graph

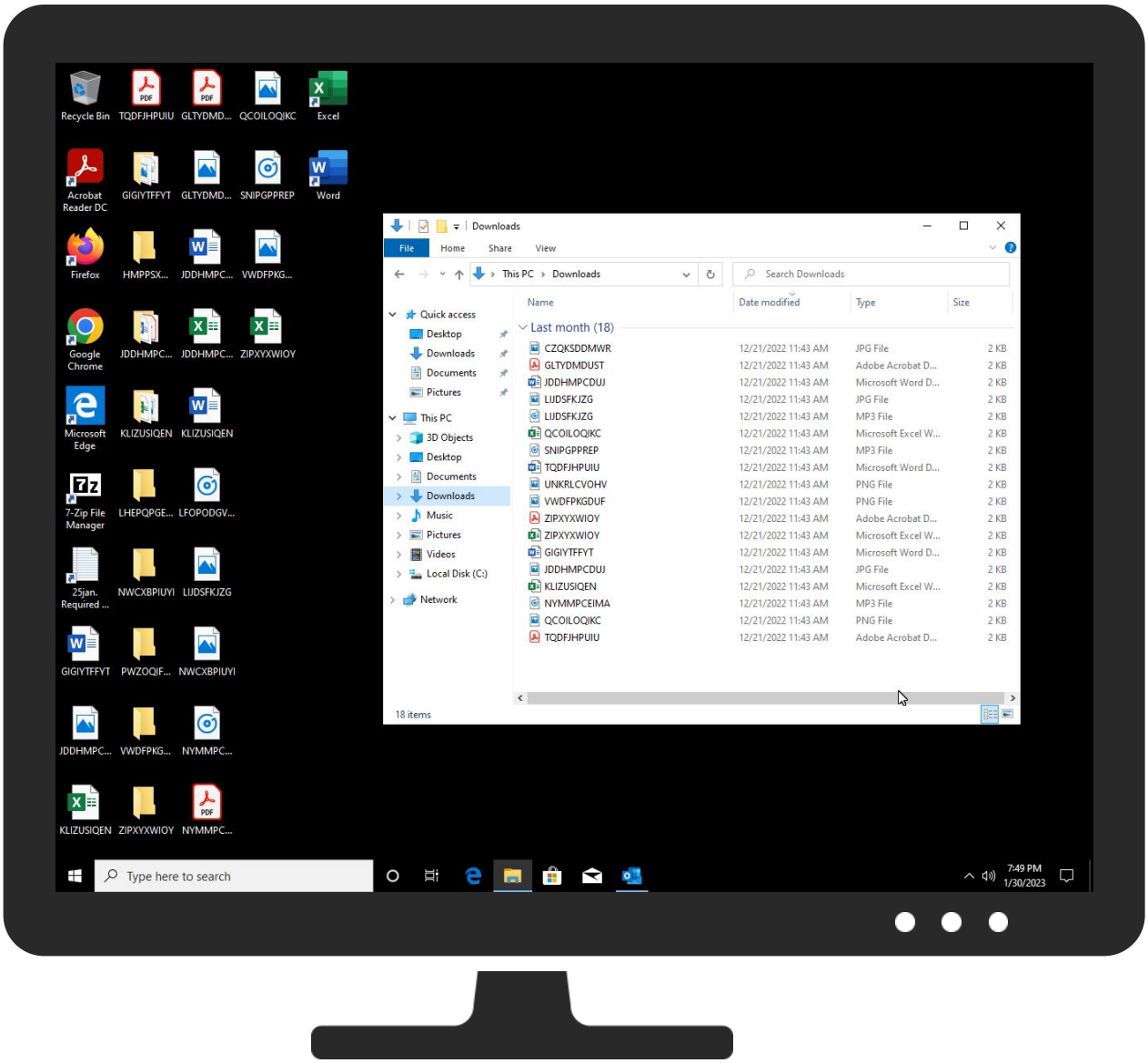


Screenshots

Thumbnails

This section contains all screenshots as thumbnails, including those not shown in the slideshow.





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

Unpacked PE 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

No contacted IP infos

General Information

Joe Sandbox Version:	36.0.0 Rainbow Opal
Analysis ID:	794650
Start date and time:	2023-01-30 19:46:32 +01:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 3m 49s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	defaultwindowsinteractivecookbook.jbs
Analysis system description:	Windows 10 64 bit version 1909 (MS Office 2019, IE 11, Chrome 104, Firefox 88, Adobe Reader DC 21, Java 8 u291, 7-Zip)
Number of analysed new started processes analysed:	9
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Sample file name:	25jan. Required documents.lnk
Detection:	MAL
Classification:	mal60.winLNK@4/0@0/0
EGA Information:	Failed
HDC Information:	Failed
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .lnk

Warnings

- Exclude process from analysis (whitelisted): dllhost.exe, rundll32.exe, WMIADAP.exe, SIHClient.exe, svchost.exe
- Excluded IPs from analysis (whitelisted): 20.190.159.75, 40.126.31.73, 20.190.159.73, 20.190.159.4, 20.190.159.2, 40.126.31.71, 40.126.31.69, 20.190.159.23
- Excluded domains from analysis (whitelisted): prda.aadg.msidentity.com, slscr.update.microsoft.com, login.live.com, ctldl.windowsupdate.com, www.tm.a.prd.aadg.akadns.net, login.msa.msidentity.com, www.tm.lg.prod.aadmsa.trafficmanager.net
- Not all processes where analyzed, report is missing behavior information

Simulations

Behavior and APIs

No simulations

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.>.....

File Icon

Icon Hash:	74f0e4e4e4e9e1ed

Static Windows Shortcut Info

General

Relative Path:	..\..\..\Windows\System32\cmd.exe
Command Line Argument:	/c cd project && registry.exe registry.py & taskkill /F /IM cmd.exe
Icon location:	%SystemRoot%\system32\imageres.dll

Network Behavior

Report size exceeds maximum size, go to the download page of this report and download PCAP to see all network behavior.

Statistics

Behavior

System Behavior

Analysis Process: cmd.exe PID: **6496**, Parent PID: **3840**

General

Target ID:	0
Start time:	19:47:07
Start date:	30/01/2023
Path:	C:\Windows\System32\cmd.exe
Wow64 process (32bit):	false
Commandline:	"C:\Windows\System32\cmd.exe" /c cd project && registry.exe registry.py & taskkill /F /IM cmd.exe
Imagebase:	0x7ff7f3020000
File size:	280064 bytes
MD5 hash:	9D59442313565C2E0860B88BF32B2277
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: conhost.exe PID: **6504**, Parent PID: **6496**

General

Target ID:	1
Start time:	19:47:07
Start date:	30/01/2023
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7603a0000
File size:	885760 bytes
MD5 hash:	C5E9B1D1103EDCEA2E408E9497A5A88F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: taskkill.exe PID: **6588**, Parent PID: **6496**

General

Target ID:	3
Start time:	19:47:07
Start date:	30/01/2023
Path:	C:\Windows\System32\taskkill.exe
Wow64 process (32bit):	false
Commandline:	taskkill /F /IM cmd.exe
Imagebase:	0x7ff6c79d0000
File size:	95744 bytes
MD5 hash:	3BBEE3AC757CA54F33710DF8FB9D47A7
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Disassembly

No disassembly