

JOeSandbox Cloud BASIC



ID: 715071

Sample Name: PUMP

mt310143121.vbs

Cookbook: default.jbs

Time: 15:54:58

Date: 03/10/2022

Version: 36.0.0 Rainbow Opal

Table of Contents

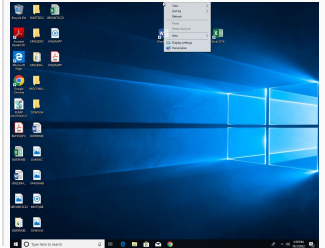
Table of Contents	2
Windows Analysis Report PUMP mt310143121.vbs	3
Overview	3
General Information	3
Detection	3
Signatures	3
Classification	3
Process Tree	3
Malware Configuration	3
Yara Signatures	3
Memory Dumps	3
Sigma Signatures	3
Snort Signatures	4
Joe Sandbox Signatures	4
System Summary	4
Data Obfuscation	4
Anti Debugging	4
Mitre Att&ck Matrix	4
Behavior Graph	4
Screenshots	5
Thumbnails	5
Antivirus, Machine Learning and Genetic Malware Detection	6
Initial Sample	6
Dropped Files	6
Unpacked PE Files	6
Domains	6
URLs	6
Domains and IPs	7
Contacted Domains	7
World Map of Contacted IPs	7
General Information	7
Warnings	7
Simulations	7
Behavior and APIs	7
Joe Sandbox View / Context	8
IPs	8
Domains	8
ASNs	8
JA3 Fingerprints	8
Dropped Files	8
Created / dropped Files	8
Static File Info	8
General	8
File Icon	8
Network Behavior	8
Statistics	9
System Behavior	9
Analysis Process: wscript.exePID: 5580, Parent PID: 3452	9
General	9
File Activities	9
Registry Activities	9
Disassembly	9

Windows Analysis Report

PUMP mt310143121.vbs

Overview

General Information

Sample Name:	PUMP mt310143121.vbs
Analysis ID:	715071
MD5:	41ad96654d44ef..
SHA1:	20dae7bc9d6dc2..
SHA256:	28bf271ec1576c...
Tags:	GuLoader vbs
Infos:	YARA
	

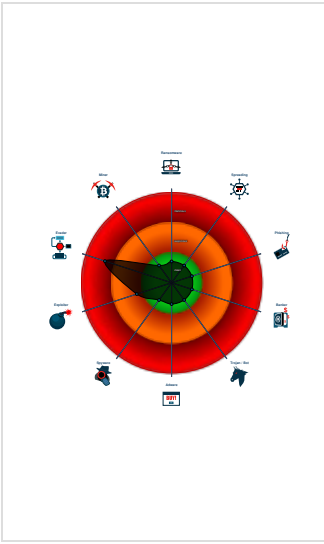
Detection

	
Score:	56
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

VBScript performs obfuscated calls...
Found potential dummy code loops ...
Potential malicious VBS script foun...
Yara signature match
Java / VBScript file with very long s...
Program does not show much activi...
Found WSH timer for Javascript or V...
Abnormal high CPU Usage

Classification



Process Tree

System is w10x64
wscript.exe (PID: 5580 cmdline: C:\Windows\System32\WScript.exe "C:\Users\user\Desktop\PUMP mt310143121.vbs" MD5: 9A68ADD12EB50DDE7586782C3EB9FF9C)
cleanup

Malware Configuration

No configs have been found

Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
00000000.00000003.248640699.00000222676D000.0000004.00000020.00020000.00000000.sdmp	SUSP_LNK_SuspiciousCommands	Detects LNK file with suspicious content	Florian Roth	<ul style="list-style-type: none">0xbb54:\$s12: Wscript.Shell

Sigma Signatures

No Sigma rule has matched

Snort Signatures

 No Snort rule has matched

Joe Sandbox Signatures

System Summary



Potential malicious VBS script found (suspicious strings)

Data Obfuscation










VBScript performs obfuscated calls to suspicious functions

Anti Debugging

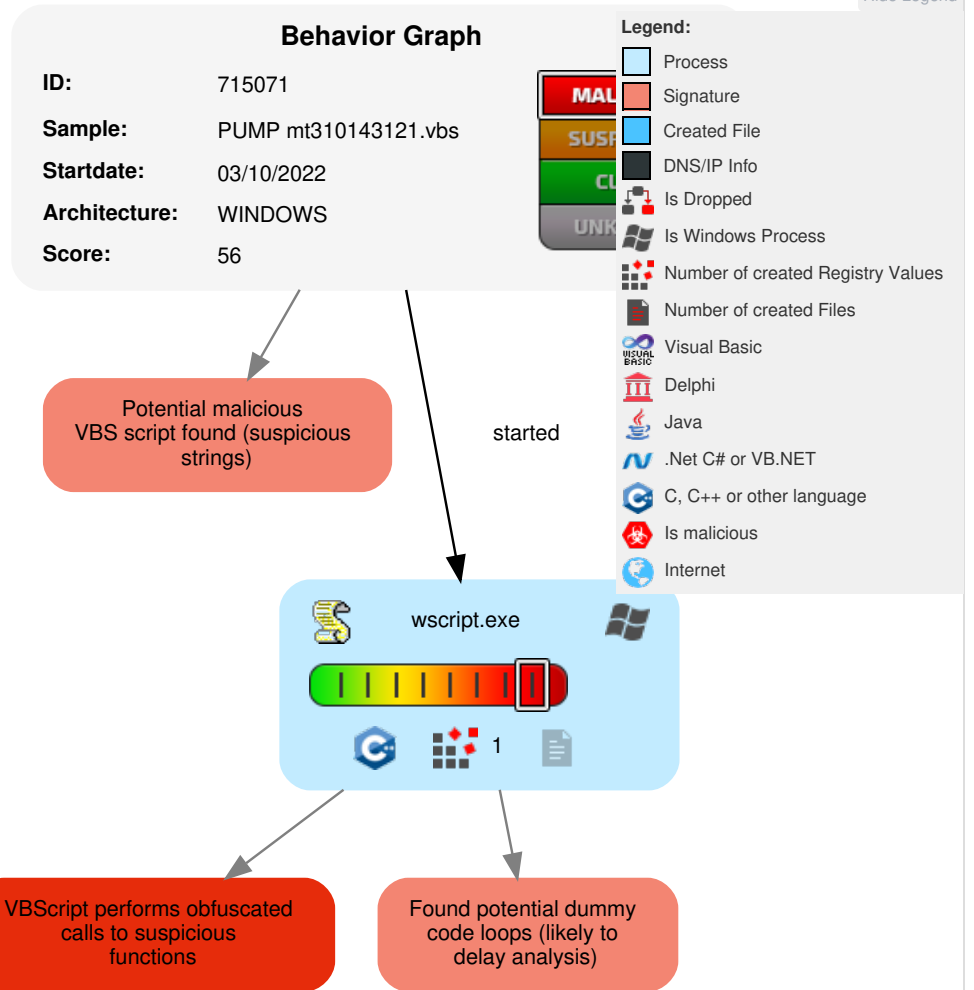


Found potential dummy code loops (likely to delay analysis)

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	 Scripting	Path Interception	Path Interception	 Virtualization/Sandbox Evasion	OS Credential Dumping	 Security Software 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	 Scripting	LSASS Memory	 Virtualization/Sandbox Evasion	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	 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

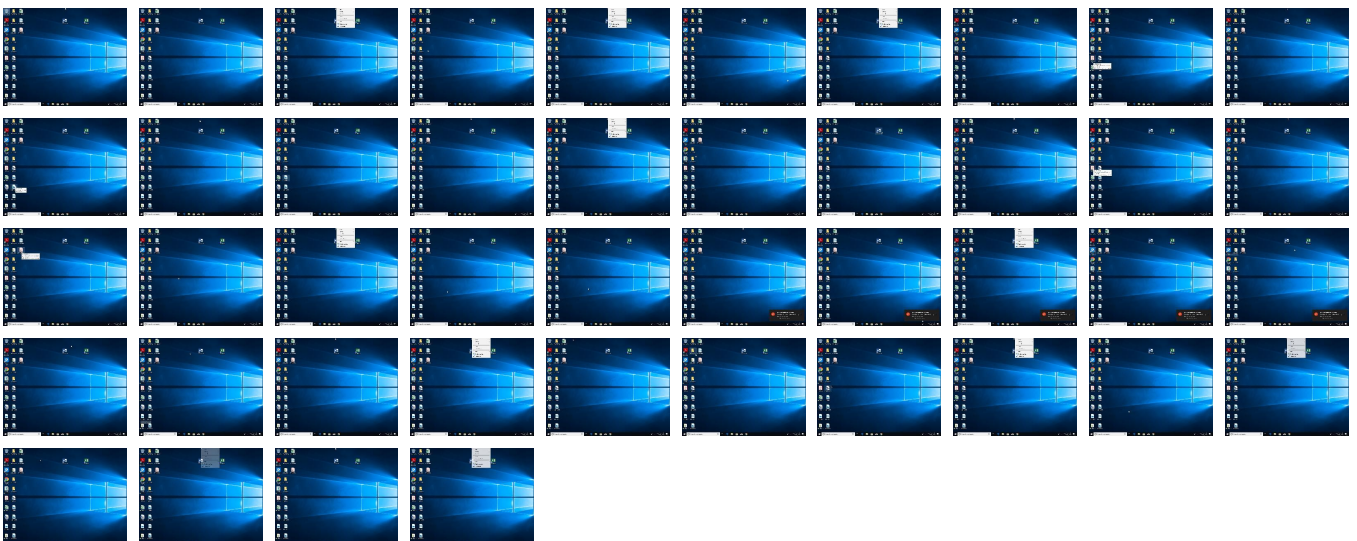
Behavior Graph



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
PUMP mt310143121.vbs	2%	ReversingLabs		


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:	715071
Start date and time:	2022-10-03 15:54:58 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 6m 46s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	PUMP mt310143121.vbs
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:	13
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:	<ul style="list-style-type: none">• HCA enabled• EGA enabled• HDC enabled• AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal56.evad.winVBS@1/0@0/0
EGA Information:	Failed
HDC Information:	Failed
HCA Information:	<ul style="list-style-type: none">• Successful, ratio: 100%• Number of executed functions: 0• Number of non-executed functions: 0
Cookbook Comments:	<ul style="list-style-type: none">• Found application associated with file extension: .vbs• Override analysis time to 240s for JS/VBS files not yet terminated

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, WMIADAP.exe, SgrmBroker.exe, conhost.exe, svchost.exe
- Excluded domains from analysis (whitelisted): fs.microsoft.com
- Not all processes where analyzed, report is missing behavior information
- Report size getting too big, too many NtAllocateVirtualMemory calls found.
- Report size getting too big, too many NtProtectVirtualMemory calls found.
- VT rate limit hit for: PUMP mt310143121.vbs

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:	ASCII text, with CRLF line terminators
Entropy (8bit):	5.150359651157965
TrID:	<ul style="list-style-type: none">Visual Basic Script (13500/0) 100.00%
File name:	PUMP mt310143121.vbs
File size:	517402
MD5:	41ad96654d44ef375097eeeb83818cf7
SHA1:	20dae7bc9d6dc2c5f947de3f871d617fb36e6edc
SHA256:	28bf271ec1576c0e7d1b2a243de952bb70c25711cdc9c2d4494002a3e2f346ca
SHA512:	e0e756b9ccc37a1fee30ff1145bf9c3b28e441bfe7c1fa47face7afd4a4db6acdf6b8a346e5f6149ea085ad35648bd950e7e48c57f5fc61f14ec7bfe7d0156e2
SSDEEP:	6144:GYvp0UseCb/CHsE2Nydr8HSMB3567Fk2AhcAjl4PWTO:LpCbwwq50ZAhLjVWC
TLSH:	19B4407B5423D0ACA7DEE2634C603EFD85D8F909C2E517AA223637C49913AFB5742E14
File Content Preview:	..'Heterogeneously46 UDTMTE GKKEIER Kinesertraadene EVECTIONS corrive Konfektens2 Aarsberetning Schoolteacherly SANDSTORMENE uvelkommen ..'Rimede210 Betydede229 embodier Dimeric221 Forebyggelsers Fornjelsessyges135 ..'hubristically ANTIHYPNOTIC KLANGLS B

File Icon




Icon Hash: e8d69ece869a9ec4

Network Behavior

🚫 No network behavior found

Statistics

 No statistics

System Behavior

Analysis Process: wscript.exe PID: 5580, Parent PID: 3452

General	
Target ID:	0
Start time:	15:55:54
Start date:	03/10/2022
Path:	C:\Windows\System32\wscript.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\WScript.exe "C:\Users\user\Desktop\PUMP mt310143121.vbs"
Imagebase:	0x7ff74fd90000
File size:	163840 bytes
MD5 hash:	9A68ADD12EB50DDE7586782C3EB9FF9C
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	<ul style="list-style-type: none">Rule: SUSP_LNK_SuspiciousCommands, Description: Detects LNK file with suspicious content, Source: 00000000.00000003.248640699.000002222676D000.00000004.00000020.00020000.00000000.sdmp, Author: Florian Roth
Reputation:	high

File Activities

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

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
-----------	--------	--------	-------	-------	------------	-------	----------------	--------

File Path	Offset	Length	Completion	Count	Source Address	Symbol
-----------	--------	--------	------------	-------	----------------	--------


Registry Activities

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

Key Path	Completion	Count	Source Address	Symbol
----------	------------	-------	----------------	--------

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
----------	------	------	------	------------	-------	----------------	--------

Disassembly

 No disassembly