



ID: 321424
Sample Name:
addceupr21_bubbles.exe
Cookbook: default.jbs
Time: 01:56:02
Date: 22/11/2020
Version: 31.0.0 Red Diamond

Table of Contents

Table of Contents 2
Analysis Report addceupr21_bubbles.exe 4
Overview 4
General Information 4
Detection 4
Signatures 4
Classification 4
Startup 4
Malware Configuration 4
Yara Overview 4
Sigma Overview 4
Signature Overview 4
AV Detection: 5
System Summary: 5
Mitre Att&ck Matrix 5
Behavior Graph 5
Screenshots 6
Thumbnails 6
Antivirus, Machine Learning and Genetic Malware Detection 7
Initial Sample 7
Dropped Files 7
Unpacked PE Files 7
Domains 7
URLs 7
Domains and IPs 8
Contacted Domains 8
Contacted IPs 8
General Information 8
Simulations 8
Behavior and APIs 8
Joe Sandbox View / Context 9
IPs 9
Domains 9
ASN 9
JA3 Fingerprints 9
Dropped Files 9
Created / dropped Files 9
Static File Info 9
General 9
File Icon 9
Static PE Info 10
General 10
Entrypoint Preview 10
Data Directories 10
Sections 10
Resources 11
Imports 11
Version Infos 11
Possible Origin 11
Network Behavior 11
Code Manipulations 11
Statistics 12
System Behavior 12
Analysis Process: addceupr21_bubbles.exe PID: 380 Parent PID: 5684 12
General 12
File Activities 12

Disassembly 12
Code Analysis 12

Copyright null 2020

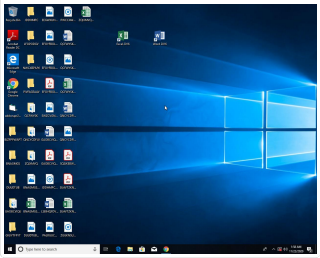
Analysis Report addceupr21_bubbles.exe

Overview

General Information

Sample Name:	addceupr21_bubbles.exe
Analysis ID:	321424
MD5:	11c2b95348f338d.
SHA1:	3346e2fe2384afd..
SHA256:	a365df50290d34a.

Most interesting Screenshot:



Detection

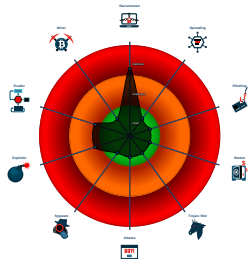


Score:	72
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Antivirus / Scanner detection for sub…
- Multi AV Scanner detection for subm…
- Potential malicious icon found
- Machine Learning detection for samp…
- PE file has a writeable .text section
- Antivirus or Machine Learning detec…
- Found inlined nop instructions (likely…
- Found large amount of non-executed…
- PE file contains an invalid checksum
- PE file contains strange resources
- Program does not show much activi…
- Sample file is different than original …

Classification



Startup

- **System is w10x64**
- addceupr21_bubbles.exe (PID: 380 cmdline: 'C:\Users\user\Desktop\addceupr21_bubbles.exe' MD5: 11C2B95348F338DB6835C23E6BE1C862)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

No yara matches

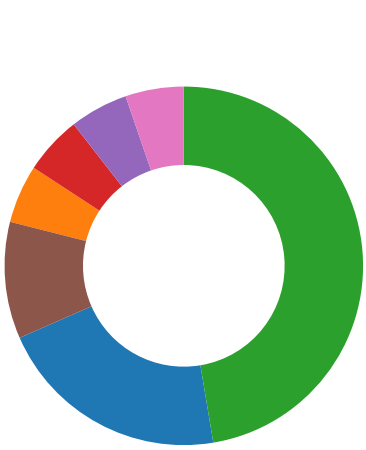
Sigma Overview

No Sigma rule has matched

Signature Overview

- AV Detection
- Software Vulnerabilities

Copyright null 2020



Click to jump to signature section

AV Detection:



Antivirus / Scanner detection for submitted sample

Multi AV Scanner detection for submitted file

Machine Learning detection for sample

System Summary:



Potential malicious icon found

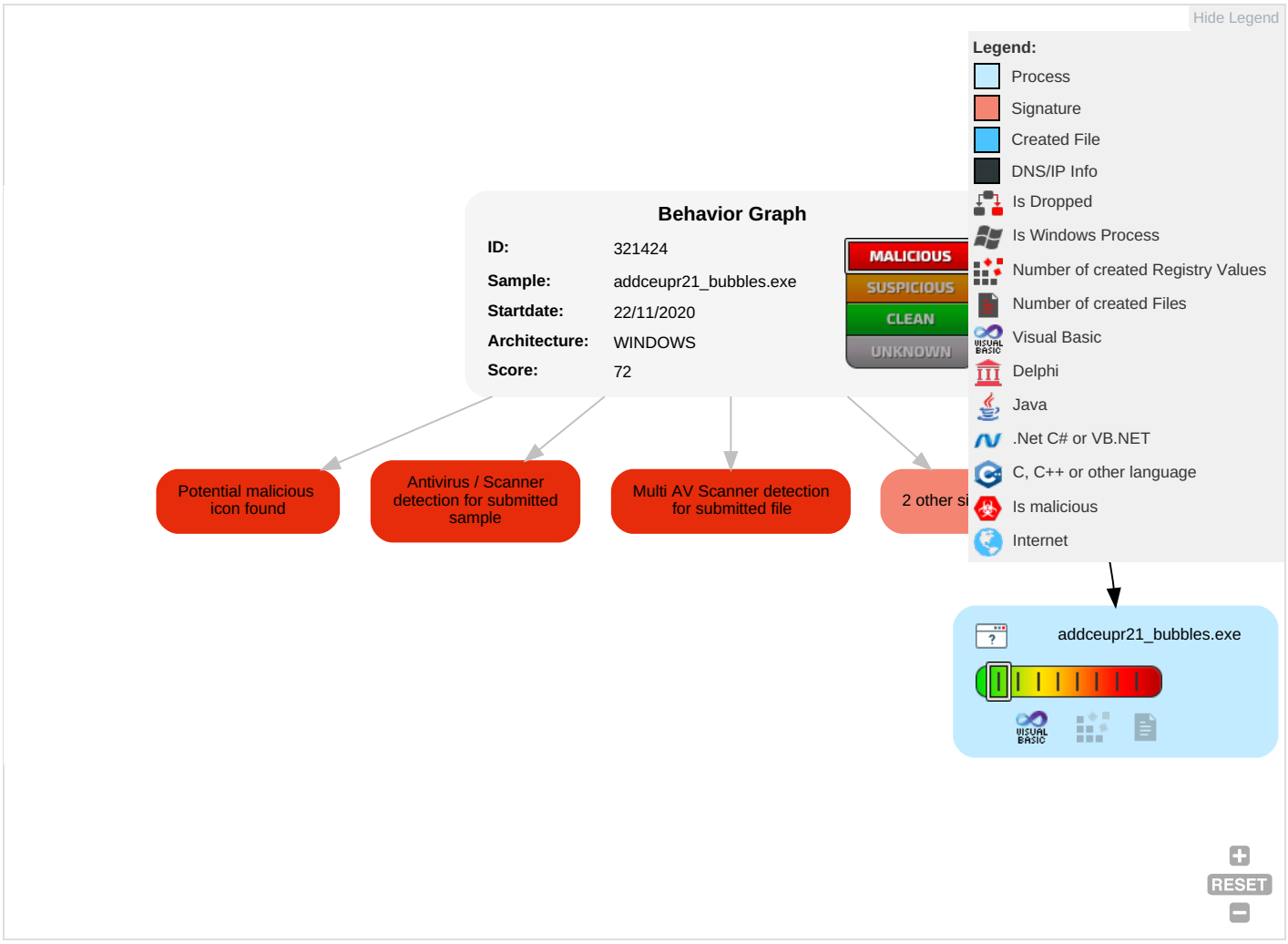
PE file has a writeable .text section

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	Software Packing 1	OS Credential Dumping	System Information Discovery 1	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	Obfuscated Files or Information 1	LSASS Memory	Application Window 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

Behavior Graph

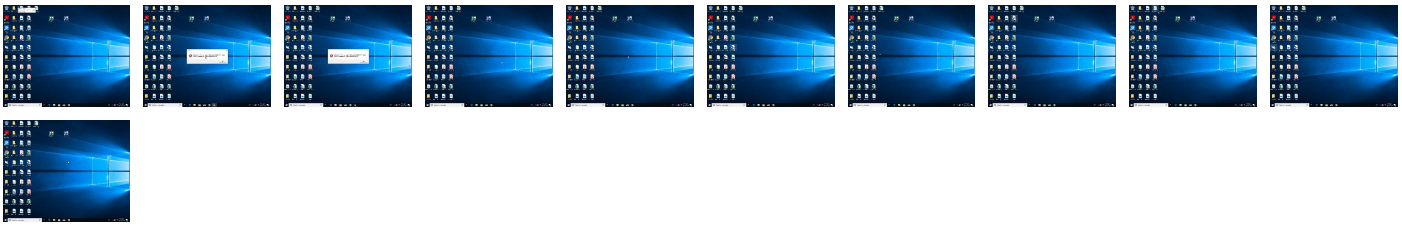
Copyright null 2020



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
addceupr21_bubbles.exe	27%	Virustotal		Browse
addceupr21_bubbles.exe	100%	Avira	TR/Dropper.Gen	
addceupr21_bubbles.exe	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
0.2.addceupr21_bubbles.exe.400000.0.unpack	100%	Avira	TR/Dropper.Gen		Download File
0.0.addceupr21_bubbles.exe.400000.0.unpack	100%	Avira	TR/Dropper.Gen		Download File

Domains

No Antivirus matches

URLs

No Antivirus matches

Copyright null 2020

Domains and IPs

Contacted Domains

No contacted domains info

Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	31.0.0 Red Diamond
Analysis ID:	321424
Start date:	22.11.2020
Start time:	01:56:02
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 4m 40s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	addceupr21_bubbles.exe
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	25
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
Detection:	MAL
Classification:	mal72.rans.winEXE@1/0@0/0
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 65% (good quality ratio 20%) • Quality average: 31.1% • Quality standard deviation: 46%
HCA Information:	Failed
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .exe
Warnings:	Show All • Exclude process from analysis (whitelisted): taskhostw.exe, MpCmdRun.exe, audiodg.exe, BackgroundTransferHost.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, svchost.exe, UsoClient.exe

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

No created / dropped files found

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows
Entropy (8bit):	4.49233828273567
TrID:	• Win32 Executable (generic) a (10002005/4) 99.15% • Win32 Executable Microsoft Visual Basic 6 (82127/2) 0.81% • Generic Win/DOS Executable (2004/3) 0.02% • DOS Executable Generic (2002/1) 0.02% • Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00%
File name:	addceupr21_bubbles.exe
File size:	53248
MD5:	11c2b95348f338db6835c23e6be1c862
SHA1:	3346e2fe2384afd22218c16c9028b56a2fed3d66
SHA256:	a365df50290d34a97ad1c02a9c1d9d39a6365720f947703 292a3a00a6575a61c
SHA512:	3e38713f66ab5e6a8a20428978f8280250a1e782a8398a 081c93e2135d6527584c0fac8a42c3a3ea14c3631e67a8 91dbf5fc8f5b51e0d781138b4eda19e681e
SSDEEP:	384:62sltQZAASik6ixk0sBZZ1XCvUARW6KMgH6/oPP D7tWBCVSVZb1HOqaVSM36:UltQZA96ck0sBx8RW6K h3D7kBBpue
File Content Preview:	MZ.....@.....!..L.!Th is program cannot be run in DOS mode....$..... ...z.....T.....Rich.....PE..L....g5<..... .....@.....

File Icon



Icon Hash:	20047c7c70f0e004

Static PE Info

General

Entrypoint:	0x401318
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	LOCAL_SYMS_STRIPPED, 32BIT_MACHINE, EXECUTABLE_IMAGE, LINE_NUMS_STRIPPED, RELOCS_STRIPPED
DLL Characteristics:	
Time Stamp:	0x3C3567D3 [Fri Jan 4 08:29:07 2002 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	9845ab130c6b0538839ca253be6d3d6e

Entrypoint Preview

Instruction
push 00401B0Ch
call 00007FF5B07B21C5h
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
xor byte ptr [eax], al
add byte ptr [eax], al
push 38000000h
add byte ptr [eax], al
add bh, bh
rcl dword ptr [edx-6Ch], 1

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x7f34	0x28	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0xa000	0x8d4	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x228	0x20	
IMAGE_DIRECTORY_ENTRY_IAT	0x1000	0x114	.text
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics

Copyright null 2020

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x8000	0x8000	False	0.298797607422	data	4.9798968159	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_SHARED, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.data	0x9000	0x1000	0x1000	False	0.223876953125	data	2.36191635208	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0xa000	0x20ac	0x3000	False	0.334309895833	data	4.39637685669	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_SHARED, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0xa7a4	0x130	data		
RT_ICON	0xa4bc	0x2e8	data		
RT_ICON	0xa394	0x128	GLS_BINARY_LSB_FIRST		
RT_GROUP_ICON	0xa364	0x30	data		
RT_VERSION	0xa150	0x214	data	English	United States

Imports

DLL	Import
MSVBVM60.DLL	EVENT_SINK_GetIDsOfNames, __vbaVarTstGt, __vbaStrI2, _CIcos, _adj_fptan, __vbaStrI4, __vbaFreeVar, __vbaLateIdCall, __vbaFreeVarList, _adj_fdiv_m64, EVENT_SINK_Invoke, __vbaNextEachVar, __vbaFreeObjList, _adj_fprem1, __vbaStrCat, __vbaHresultCheckObj, _adj_fdiv_m32, Zombie_GetTypeInfo, __vbaObjSet, _adj_fdiv_m16i, __vbaObjSetAddref, _adj_fdivr_m16i, __vbaForEachCollVar, _CIsin, __vbaVarZero, __vbaChkstk, EVENT_SINK_AddRef, __vbaVarTstEq, __vbaNextEachCollVar, __vbaVarLateMemSt, _adj_fpatan, Zombie_GetTypeInfoCount, EVENT_SINK_Release, __vbaNew, _CIsqrt, EVENT_SINK_QueryInterface, __vbaExceptHandler, _adj_fprem, _adj_fdivr_m64, __vbaLateIdStAd, __vbaFPException, __vbaVarCat, _CIlog, __vbaErrorOverflow, __vbaNew2, _adj_fdiv_m32i, _adj_fdivr_m32i, __vbaFreeStrList, _adj_fdivr_m32, _adj_fdiv_r, __vbaVerifyVarObj, __vbaVarLateMemCallLd, _CIatan, __vbaStrMove, __vbaCastObj, __vbaForEachVar, _allmul, __vbaLateIdSt, _CItan, __vbaAryUnlock, _CIexp, __vbaFreeObj, __vbaFreeStr

Version Infos

Description	Data
Translation	0x0409 0x04b0
InternalName	Bubbles
FileVersion	1.00
CompanyName	CooperVision
ProductName	Bubbles
ProductVersion	1.00
OriginalFilename	Bubbles.exe

Possible Origin

Language of compilation system	Country where language is spoken	Map
English	United States	

Network Behavior

No network behavior found

Code Manipulations

Statistics

System Behavior

Analysis Process: addceupr21_bubbles.exe PID: 380 Parent PID: 5684

General

Start time:	01:56:49
Start date:	22/11/2020
Path:	C:\Users\user\Desktop\addceupr21_bubbles.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\addceupr21_bubbles.exe'
Imagebase:	0x400000
File size:	53248 bytes
MD5 hash:	11C2B95348F338DB6835C23E6BE1C862
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Visual Basic
Reputation:	low

File Activities

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Disassembly

Code Analysis