ID: 635365
Sample Name: NEW SUBMISSION- LORENCE OJWANG - 11771 SE 71ST CT Belleview FL 34420.msg
Cookbook: default.jbs
Time: 20:25:51
Date: 27/05/2022
Version: 34.0.0 Boulder Opal

Table of Contents

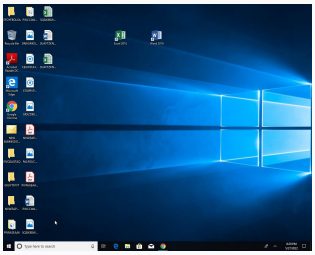
Windows Analysis Report

NEW SUBMISSION- LORENCE OJWANG - 11771 SE 71ST CT Belleview FL 34420.msg

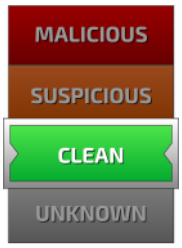
Overview

General Information

Sample Name:	NEW SUBMISSION- LORENCE OJWANG - 11771 SE 71ST CT Belleview FL 34420.msg
Analysis ID:	635365
MD5:	e1ed623777312c..
SHA1:	679cc175bebbe6..
SHA256:	f71454303497feb.



Detection

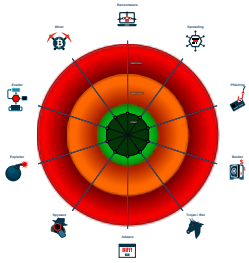


Score:	0
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

Program does not show much activi…

Classification



Process Tree

- **System is w10x64**
- OUTLOOK.EXE (PID: 3960 cmdline: C:\Program Files (x86)\Microsoft Office\Office16\OUTLOOK.EXE" /f "C:\Users\user\Desktop\NEW SUBMISSION- LORENCE OJWANG - 11771 SE 71ST CT Belleview FL 34420.msg MD5: 7DD935BA9B57D9D7EFF63C67653E70B5)
- **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

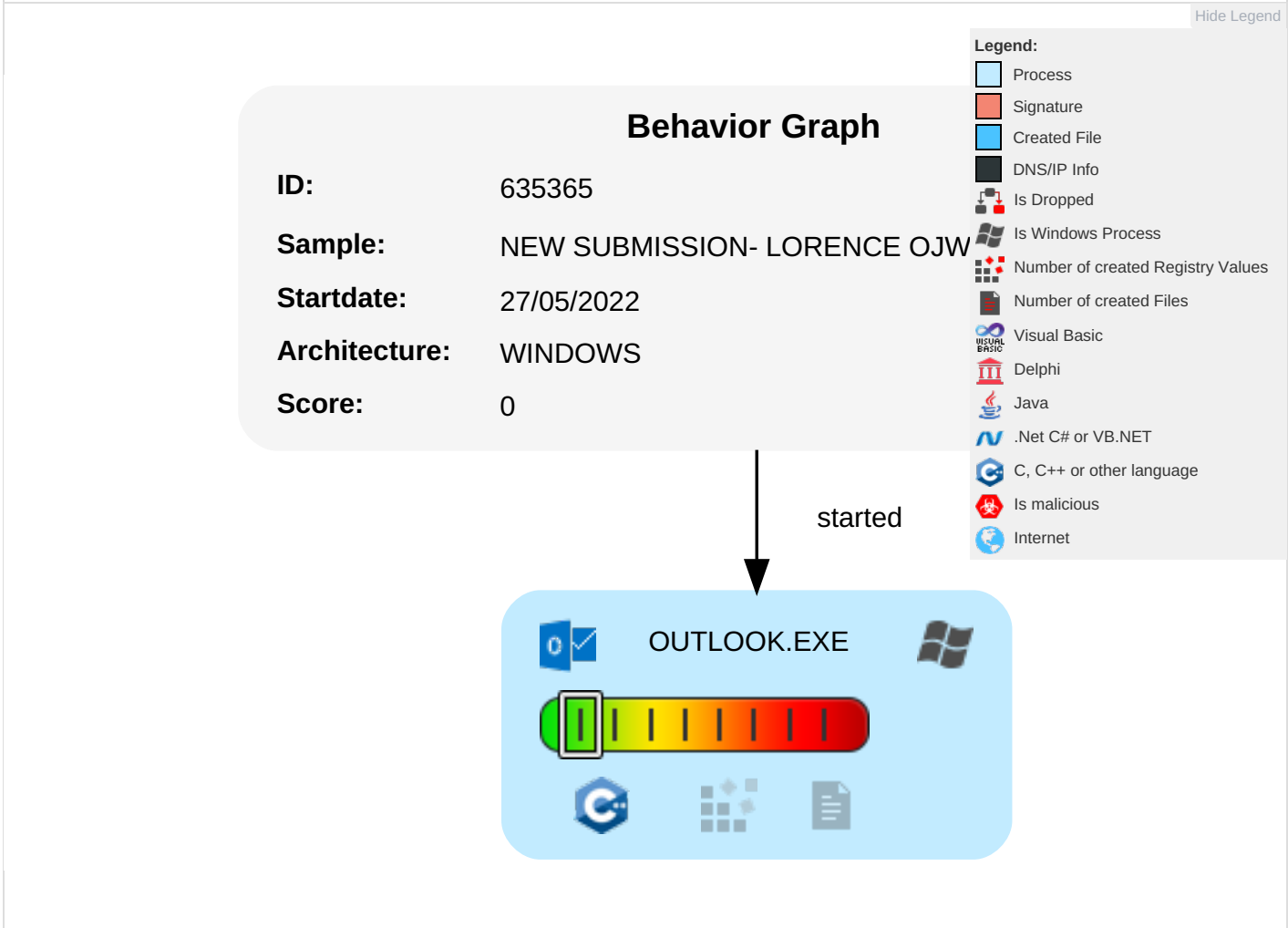
Joe Sandbox Signatures

There are no malicious signatures, click here to show all signatures.

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	Direct Volume Access	OS Credential Dumping	1 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

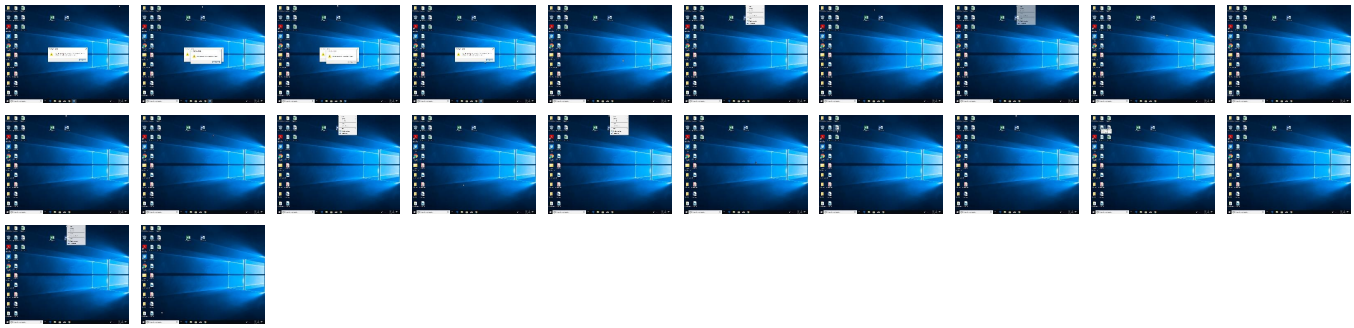
Behavior Graph



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

No Antivirus matches

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:	34.0.0 Boulder Opal
Analysis ID:	635365
Start date and time: 27/05/202220:25:51	2022-05-27 20:25:51 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 4m 26s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	NEW SUBMISSION- LORENCE OJWANG - 11771 SE 71ST CT Belleview FL 34420.msg
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:	20
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:	CLEAN
Classification:	clean0.winMSG@1/0@0/0
Cookbook Comments:	• Found application associated with file extension: .msg • Adjust boot time • Enable AMSI

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, BackgroundTransferHost.exe, WMIADAP.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, svchost.exe, wuapihost.exe
- Excluded domains from analysis (whitelisted): ris.api.iris.microsoft.com, client.wns.windows.com, fs.microsoft.com, login.live.com, sls.update.microsoft.com, displaycatalog.mp.micr

osoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, arc.msn.com
- 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:	CDFV2 Microsoft Outlook Message
Entropy (8bit):	7.965363509632674
TrID:	• Outlook Message (71009/1) 58.92% • Outlook Form Template (41509/1) 34.44% • Generic OLE2 / Multistream Compound File (8008/1) 6.64%
File name:	NEW SUBMISSION- LORENCE OJWANG - 11771 SE 71ST CT Belleview FL 34420.msg
File size:	6936576
MD5:	e1ed623777312c43f2f12e40bec26164
SHA1:	679cc175bebbe66a7b986610750c41e07eb16f57
SHA256:	f71454303497feb403523e385de4110da9d310b6d140f999c3c1c1e095ae2bb3
SHA512:	d7982e0e150f836616ef9a5214242182c3dba1606da83d5b7b9d4c10c2dc98b14b2c77a4bfbe35772ffa444d67bc4a3ad3dc9a713fe86bc50cb7cad847c98a2d
SSDEEP:	196608:RQV+q+yL5HVs70jA49XgXeSFuLEQty+8NHL7Qu:Ri3FVG0jA49BwuLEQtMH4u
TLSH:	7266F10B8D948783D56D83F57D530F9C1F162B5EE8923AEB10660ECF7A61A231D8E11E

File Content Preview:	.....>.....j.....R...S...T...U...V...W...X...Y...Z...[...\...]...^..._...y...z... {...|...}...~.....

File Icon

Icon Hash:	bac0f992edfcdf00

Network Behavior

No network behavior found

Statistics

No statistics

System Behavior

Analysis Process: OUTLOOK.EXE PID: 3960, Parent PID: 5944

General	
Target ID:	0
Start time:	20:27:10
Start date:	27/05/2022
Path:	C:\Program Files (x86)\Microsoft Office\Office16\OUTLOOK.EXE
Wow64 process (32bit):	true
Commandline:	C:\Program Files (x86)\Microsoft Office\Office16\OUTLOOK.EXE" /f "C:\Users\user\Desktop\NEW SUBMISSION- LORENCE OJWANG - 11771 SE 71ST CT Belleview FL 34420.msg
Imagebase:	0xee0000
File size:	23291112 bytes
MD5 hash:	7DD935BA9B57D9D7EFF63C67653E70B5
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

Disassembly

No disassembly