ID: 830984
Sample Name: #Ud83d#Udce7 Tax Statements-2-121_076_454656_3-4(4).hTm
Cookbook: defaultwindowshtmlcookbook.jbs
Time: 22:23:18
Date: 20/03/2023
Version: 37.0.0 Beryl

Table of Contents

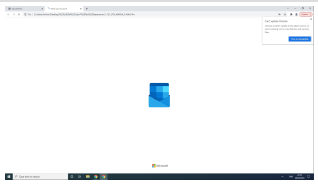
Windows Analysis Report

#Ud83d#Udce7 Tax Statements-2-121_076_454656_3-4(4).hTm

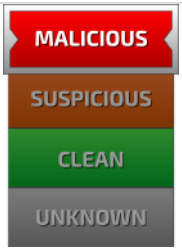
Overview

General Information

Sample Name:	#Ud83d#Udce7 Tax Statements-2-121_076_454656_3-4(4).hTm
Analysis ID:	830984
MD5:	e5497fd17c23a..
SHA1:	91f45eedfe4e0...
SHA256:	a2148a5596c5...
Infos:	



Detection



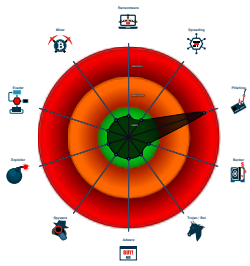
HTMLPhisher, ReCaptcha Phish

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

Signatures

- Yara detected HtmlPhish48
- Yara detected Recaptcha Phish
- Phishing site detected (based on fav…
- HTML document with suspicious title
- HTML document with suspicious na…
- JA3 SSL client fingerprint seen in co…
- Yara signature match
- IP address seen in connection with …

Classification



Process Tree

- **System is w10x64native**
- chrome.exe (PID: 1016 cmdline: C:\Program Files\Google\Chrome\Application\chrome.exe" --start-maximized "about:blank MD5: 464953824E644F10FFDC9E093FD18F94)
  - chrome.exe (PID: 8132 cmdline: "C:\Program Files\Google\Chrome\Application\chrome.exe" --type=utility --utility-sub-type=network.mojom.NetworkService --field-trial-handle=1700,18324760747851478443,7253911549642704679,131072 --disable-features=OptimizationGuideModelDownloading,OptimizationHints,OptimizationHintsFetching,OptimizationTargetPrediction --lang=en-US --service-sandbox-type=none --mojo-platform-channel-handle=1996 /prefetch:8 MD5: 464953824E644F10FFDC9E093FD18F94)
- chrome.exe (PID: 4464 cmdline: C:\Program Files\Google\Chrome\Application\chrome.exe" "C:\Users\user\Desktop\#Ud83d#Udce7 Tax Statements-2-121_076_454656_3-4(4).hTm MD5: 464953824E644F10FFDC9E093FD18F94)
- **cleanup**

Malware Configuration

No configs have been found

Yara Signatures

Initial Sample

Source	Rule	Description	Author	Strings
#Ud83d#Udce7 Tax Statements-2-121_076_454656_3-4(4).hTm	JoeSecurity_HtmlPhish_48	Yara detected HtmlPhish_48	Joe Security	

HTML

Source	Rule	Description	Author	Strings
06536.0.pages.csv	JoeSecurity_HtmlPhish_48	Yara detected HtmlPhish_48	Joe Security	
59354.1.pages.csv	JoeSecurity_ReCaptchaPhish	Yara detected Recaptcha Phish	Joe Security	

Source	Rule	Description	Author	Strings
60877.2.pages.csv	SUSP_obfuscated_JS_obfuscatorio	Detects JS obfuscation done by the js obfuscator (often malicious)	@imp0rtp3	• 0x13e1:$c5: return!![] • 0x140c:$c5: return!![] • 0x145f:$c5: return!![] • 0x149e:$c5: return!![] • 0x105c:$c8: while(!![]) • 0x107a:$d1: parseInt(_0x50c519(0xb2))/0x1*(parseInt(_0x50c519(0xb9))/0x2)+-parseInt(_0x50c519(0xbb))/0x3*(parseInt(_0x50c519(0xb5))/0x4)+parseInt(_0x50c519(0xb4))/0x5*(-parseInt(_0x50c519(0xbd))/0x6)+- • 0x1099:$d1: parseInt(_0x50c519(0xb9))/0x2)+-parseInt(_0x50c519(0xbb))/0x3*(parseInt(_0x50c519(0xb5))/0x4)+parseInt(_0x50c519(0xb4))/0x5*(-parseInt(_0x50c519(0xbd))/0x6)+-parseInt(_0x50c519(0xb8))/0x7+ • 0x10b9:$d1: parseInt(_0x50c519(0xbb))/0x3*(parseInt(_0x50c519(0xb5))/0x4)+parseInt(_0x50c519(0xb4))/0x5*(-parseInt(_0x50c519(0xbd))/0x6)+-parseInt(_0x50c519(0xb8))/0x7+parseInt(_0x50c519(0xb1))/0x8*(- • 0x10d8:$d1: parseInt(_0x50c519(0xb5))/0x4)+parseInt(_0x50c519(0xb4))/0x5*(-parseInt(_0x50c519(0xbd))/0x6)+-parseInt(_0x50c519(0xb8))/0x7+parseInt(_0x50c519(0xb1))/0x8*(-parseInt(_0x50c519(0xbf))/0x9)+- • 0x10f7:$d1: parseInt(_0x50c519(0xb4))/0x5*(-parseInt(_0x50c519(0xbd))/0x6)+-parseInt(_0x50c519(0xb8))/0x7+parseInt(_0x50c519(0xb1))/0x8*(-parseInt(_0x50c519(0xbf))/0x9)+-parseInt(_0x50c519(0xba))/0xa*(• 0x1117:$d1: parseInt(_0x50c519(0xbd))/0x6)+-parseInt(_0x50c519(0xb8))/0x7+parseInt(_0x50c519(0xb1))/0x8*(-parseInt(_0x50c519(0xbf))/0x9)+-parseInt(_0x50c519(0xba))/0xa*(parseInt(_0x50c519(0xb3))/0xb)+
60877.2.pages.csv	JoeSecurity_ReCaptchaPhish	Yara detected Recaptcha Phish	Joe Security	
06787.3.pages.csv	JoeSecurity_ReCaptchaPhish	Yara detected Recaptcha Phish	Joe Security	
Click to see the 5 entries				

Sigma Signatures

No Sigma rule has matched

Snort Signatures

No Snort rule has matched

Joe Sandbox Signatures

Phishing

Yara detected HtmlPhish48

Yara detected Recaptcha Phish

Phishing site detected (based on favicon image match)

System Summary

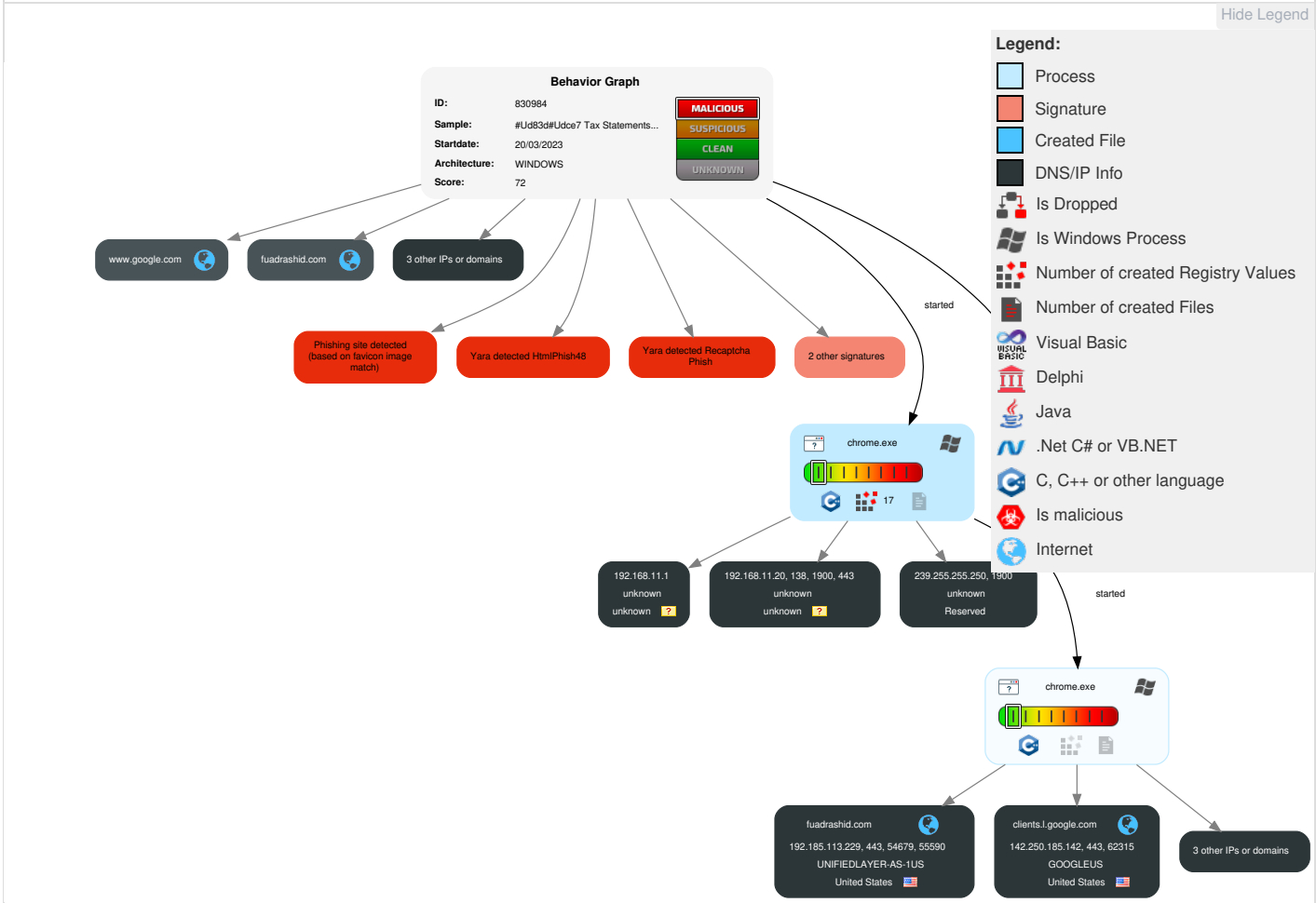
HTML document with suspicious title

HTML document with suspicious name

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	1 Process Injection	1 Process Injection	OS Credential Dumping	1 Network Service Scanning	Remote Services	Data from Local System	Exfiltration Over Other Network Medium	1 Encrypted Channel	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	Application Window Discovery	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	3 Non-Application Layer Protocol	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	Query Registry	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	4 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)	Binary Padding	NTDS	System Network Configuration Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	1 Ingress Tool Transfer	SIM Card Swap		Carrier Billing Fraud

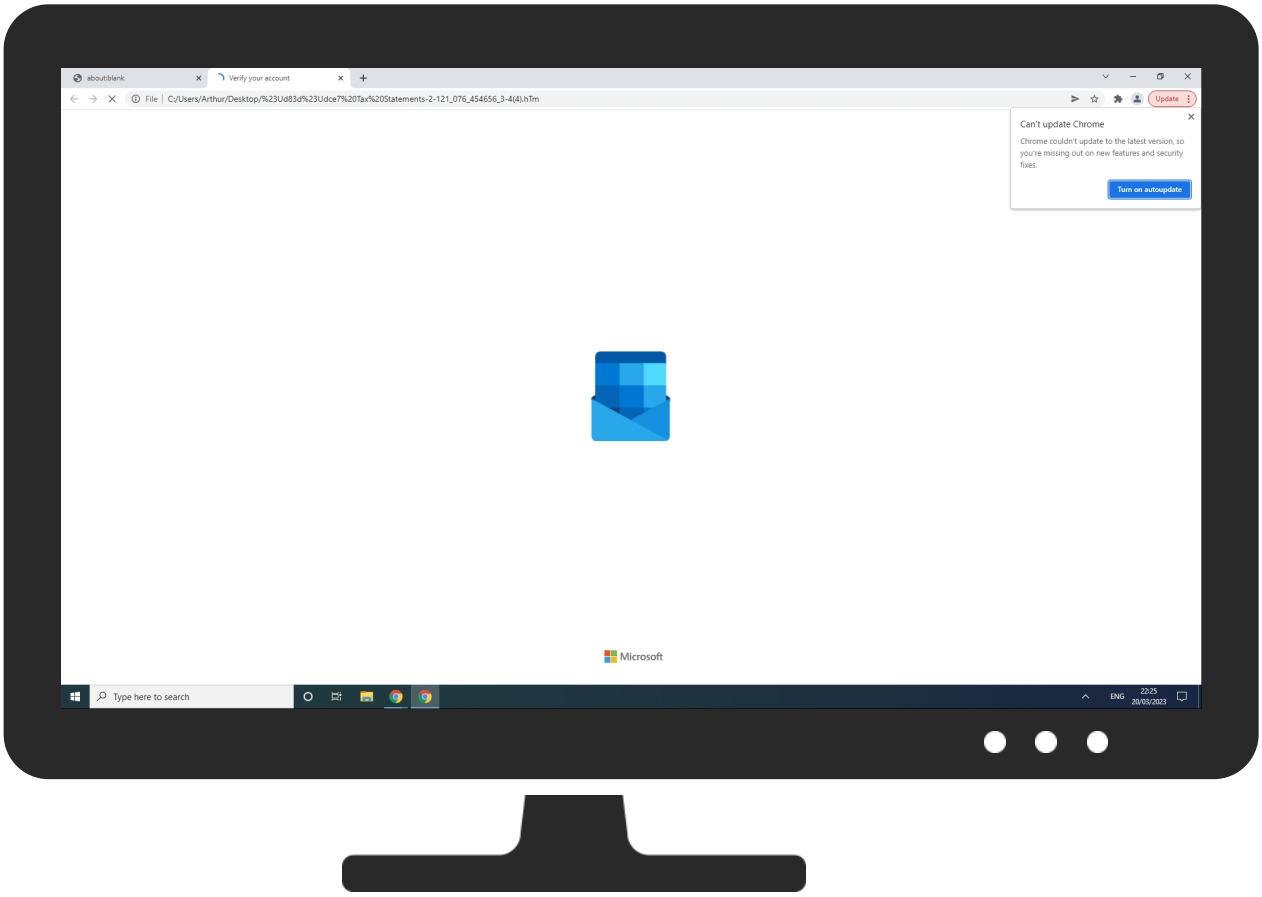
Behavior Graph



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

Source	Detection	Scanner	Label	Link
http:// https://fuadrashid.com/su35/gtl/9d3844dcadd00b46e3c10b77a0a8252475737486084017052035732 70e089c75a6b105a2f85776e2cdd4528476e3084017052035a93c9f185932557fd997ff3a4ba3e0e124e9a338084017052035b5c58094f8174d1bce72ba953e424e3130f4df0b084017052035/capt	0%	Avira URL Cloud	safe	
http://https://fuadrashid.com/su35/gtl/	0%	Avira URL Cloud	safe	

Source	Detection	Scanner	Label	Link
http://https://fuadrashid.com/su35/gtl/9d3844dcadd00b46e3c10b77a0a8252475737486084017052035732 70e089c75a6b105a2f85776e2cdd4528476e3084017052035a93c9f185932557fd997ff3a4ba3e0e124e9a338084017052035b5c58094f8174d1bce72ba953e424e3130f4df0b084017052035/gUNkRyOTOnTErUDeoDOLI	0%	Avira URL Cloud	safe	
http://https://fuadrashid.com/su35/gtl/	1%	Virustotal		Browse

Domains and IPs

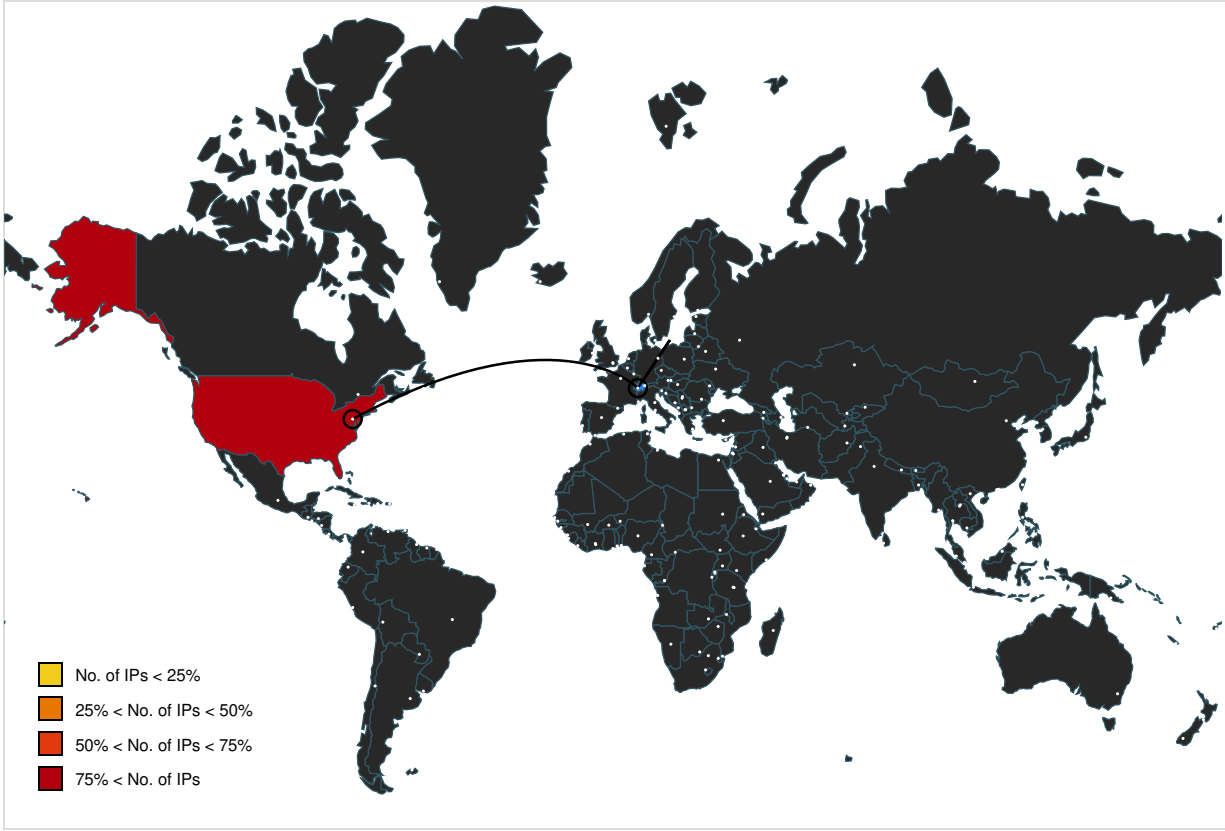
Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
accounts.google.com	142.250.185.77	true	false		high
www.google.com	142.250.185.196	true	false		high
clients.l.google.com	142.250.185.142	true	false		high
fuadrashid.com	192.185.113.229	true	false		unknown
clients2.google.com	unknown	unknown	false		high

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://https://www.google.com/recaptcha/api2/anchor?ar=1&k=%0A6Lcf2-EhAAAAAAb4lCjGZLljSQMQ9lL7LxhkWGBN&co=aHR0cHM6Ly9mdWFkcmFzaGlkLmNvbTo0NDM.&hl=en&v=Trd6gj1dhC_fx0ma_AWHc1me&size=normal&cb=eys0y7domytm	false		high
http://https://www.google.com/recaptcha/api2/anchor?ar=1&k=%0A6Lcf2-EhAAAAAAb4lCjGZLljSQMQ9lL7LxhkWGBN&co=aHR0cHM6Ly9mdWFkcmFzaGlkLmNvbTo0NDM.&hl=en&v=Trd6gj1dhC_fx0ma_AWHc1me&size=normal&cb=eys0y7domytm	false		high
http://https://fuadrashid.com/su35/gtl/	false	• 1%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://fuadrashid.com/su35/gtl/9d3844dcadd00b46e3c10b77a0a8252475737486084017052035732 70e089c75a6b105a2f85776e2cdd4528476e3084017052035a93c9f185932557fd997ff3a4ba3e0e124e9a338084017052035b5c58094f8174d1bce72ba953e424e3130f4df0b084017052035/gUNkRyOTOnTErUDeoDOLI	false	• Avira URL Cloud: safe	unknown
http://https://www.google.com/recaptcha/api.js	false		high
http://https://fuadrashid.com/su35/gtl/9d3844dcadd00b46e3c10b77a0a8252475737486084017052035732 70e089c75a6b105a2f85776e2cdd4528476e3084017052035a93c9f185932557fd997ff3a4ba3e0e124e9a338084017052035b5c58094f8174d1bce72ba953e424e3130f4df0b084017052035/gUNkRyOTOnTErUDeoDOLI#lkohanski@alkegen.com	false		unknown
http://https://accounts.google.com/ListAccounts?gpsia=1&source=ChromiumBrowser&json=standard	false		high
http://https://clients2.google.com/service/update2/crx?os=win&arch=x64&os_arch=x86_64&nacl_arch=x86-64&prod=chromecrx&prodchannel=&prodversion=94.0.4606.61&lang=en-US&acceptformat=crx3&x=id%3Dnmmhkkegccagdldgiimedpiccmgmieda%26v%3D0.0.0.0%26installedby%3Dother%26uc%26ping%3Dr%253D-1%2526e%253D1	false		high
http://https://fuadrashid.com/su35/gtl/9d3844dcadd00b46e3c10b77a0a8252475737486084017052035732 70e089c75a6b105a2f85776e2cdd4528476e3084017052035a93c9f185932557fd997ff3a4ba3e0e124e9a338084017052035b5c58094f8174d1bce72ba953e424e3130f4df0b084017052035/capt	false	• Avira URL Cloud: safe	unknown
http://https://www.google.com/recaptcha/api2/webworker.js?hl=en&v=Trd6gj1dhC_fx0ma_AWHc1me	false		high
http://https://www.google.com/recaptcha/api2/bframe?hl=en&v=Trd6gj1dhC_fx0ma_AWHc1me&k=6Lcf2-EhAAAAAAb4lCjGZLljSQMQ9lL7LxhkWGBN	false		high
http://https://www.google.com/recaptcha/api2/bframe?hl=en&v=Trd6gj1dhC_fx0ma_AWHc1me&k=6Lcf2-EhAAAAAAb4lCjGZLljSQMQ9lL7LxhkWGBN	false		high
file:///C:/Users/user/Desktop/%23Ud83d%23Udce7%20Tax%20Statements-2-121_076_454656_3-4(4).hTm	true		low

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
142.250.185.77	accounts.google.com	United States		15169	GOOGLEUS	false
239.255.255.250	unknown	Reserved		unknown	unknown	false
142.250.185.196	www.google.com	United States		15169	GOOGLEUS	false
142.250.185.142	clients.l.google.com	United States		15169	GOOGLEUS	false
192.185.113.229	fuadrashid.com	United States		46606	UNIFIEDLAYER-AS-1US	false

Private

IP
192.168.11.1
192.168.11.20
127.0.0.1

General Information

Joe Sandbox Version:	37.0.0 Beryl
Analysis ID:	830984
Start date and time:	2023-03-20 22:23:18 +01:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 7m 14s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	defaultwindowshtmlcookbook.jbs
Analysis system description:	Windows 10 64 bit 20H2 Native **physical Machine for testing VM-aware malware** (Office 2019, IE 11, Chrome 93, Firefox 91, Adobe Reader DC 21, Java 8 Update 301
Number of analysed new started processes analysed:	8
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
Sample file name:	#Ud83d#Udce7 Tax Statements-2-121_076_454656_3-4(4).hTm
Detection:	MAL
Classification:	mal72.phis.winHTM@45/0@4/8
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: .hTm

Warnings

- Exclude process from analysis (whitelisted): dllhost.exe, CompPkgSrv.exe, WMIADAP.exe, backgroundTaskHost.exe, UsoClient.exe
- TCP Packets have been reduced to 100
- Excluded IPs from analysis (whitelisted): 52.242.101.226, 13.85.23.206, 52.242.97.97, 40.127.169.103, 142.250.185.227, 34.104.35.123, 142.250.185.163, 142.250.186.138, 216.58.212.138, 142.250.186.42, 172.217.16.202, 142.250.184.234, 142.250.185.234, 142.250.185.106, 142.250.74.202, 142.250.185.138, 142.250.185.170, 142.250.185.74, 142.250.181.234, 172.217.18.106, 172.217.23.106, 142.250.186.170, 142.250.185.202, 142.250.186.99, 13.107.4.50, 142.250.184.227
- Excluded domains from analysis (whitelisted): client.wns.windows.com, content-autofill.googleapis.com, slscr.update.microsoft.com, fonts.gstatic.com, ctldl.windowsupdate.com, clientservices.googleapis.com, wdcp.microsoft.com, fe3cr.delivery.mp.microsoft.com, wdcpalt.microsoft.com, fe3.delivery.mp.microsoft.com, edgedl.me.gvt1.com, login.live.com, glb.cws.prod.dcat.dsp.trafficmanager.net, sls.update.microsoft.com, update.googleapis.com, www.gstatic.com, glb.sls.prod.dcat.dsp.trafficmanager.net
- Not all processes where analyzed, report is missing behavior information
- Report size getting too big, too many NtSetInformationFile calls found.
- Report size getting too big, too many NtWriteVirtualMemory 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

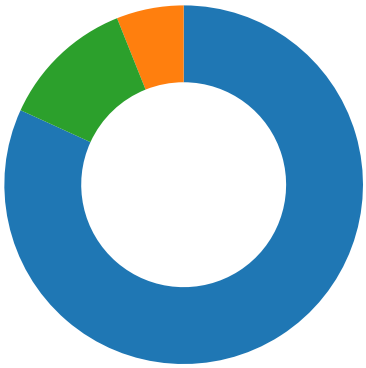
Static File Info

General

File type:	HTML document, ASCII text, with very long lines (56961), with no line terminators
Entropy (8bit):	5.425861574870474
TrID:	• HyperText Markup Language (11501/1) 33.82% • HyperText Markup Language (11501/1) 33.82% • HyperText Markup Language (11001/1) 32.35%
File name:	#Ud83d#Udce7 Tax Statements-2-121_076_454656_3-4(4).hTm
File size:	56961
MD5:	e5497fd17c23a351fd4f964d04f63871
SHA1:	91f45eedfe4e06860d0c825fe4dde6f6671f4b88
SHA256:	a2148a5596c580189823a73f156ce8e05c3b61ef1a8255f7a35ca65d9d3098cd
SHA512:	74362b0ee120af03ac05e537ca41c42fdc0aa78ebe5c12edfbf92651f2628cd7d7a0d3d88e2ca6b510381001576799a430a86e9afa183a80127c08946e74298f
SSDEEP:	384:kLwbj9WiOKqzl5tIOhmkHUBq7MQewOvufRm7BE5FTN03ozhB+WB:kwGlffhmvl6OvuZWSB
TLSH:	8A43E7FA2258D9FDB31C3630FBA52C180FDAF493659741A8DBC16A7DDD070C468AC16A
File Content Preview:	<html id="63c02758b56b08b5d84682f9dc889ec601cdf1b83c2afda9158542959a5d32416edd5e16a76a34c86726814878a3130a20a4d4c6e6f45dbc9648c820" data-63c02758b56b08b5d84682f9dc889ec601cdf1b83c2afda9158542959a5d32416edd5e16a76a34c86726814878a3130a20a4d4c6e6f45dbc9648c8

Network Behavior

Network Port Distribution



Total Packets: 66

- 1900 undefined
- 53 (DNS)
- 443 (HTTPS)

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Mar 20, 2023 22:25:12.070832968 CET	49798	443	192.168.11.20	40.113.103.199
Mar 20, 2023 22:25:12.070981026 CET	443	49798	40.113.103.199	192.168.11.20
Mar 20, 2023 22:25:12.071325064 CET	49798	443	192.168.11.20	40.113.103.199
Mar 20, 2023 22:25:12.072556019 CET	49798	443	192.168.11.20	40.113.103.199
Mar 20, 2023 22:25:12.072650909 CET	443	49798	40.113.103.199	192.168.11.20
Mar 20, 2023 22:25:12.183177948 CET	443	49798	40.113.103.199	192.168.11.20
Mar 20, 2023 22:25:12.183594942 CET	49798	443	192.168.11.20	40.113.103.199
Mar 20, 2023 22:25:12.187401056 CET	49798	443	192.168.11.20	40.113.103.199
Mar 20, 2023 22:25:12.187452078 CET	443	49798	40.113.103.199	192.168.11.20
Mar 20, 2023 22:25:12.188213110 CET	443	49798	40.113.103.199	192.168.11.20
Mar 20, 2023 22:25:12.192061901 CET	49798	443	192.168.11.20	40.113.103.199
Mar 20, 2023 22:25:12.192137003 CET	49798	443	192.168.11.20	40.113.103.199
Mar 20, 2023 22:25:12.192164898 CET	443	49798	40.113.103.199	192.168.11.20

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Mar 20, 2023 22:25:12.192461014 CET	49798	443	192.168.11.20	40.113.103.199
Mar 20, 2023 22:25:12.217365026 CET	443	49798	40.113.103.199	192.168.11.20
Mar 20, 2023 22:25:12.217773914 CET	443	49798	40.113.103.199	192.168.11.20
Mar 20, 2023 22:25:12.217983961 CET	49798	443	192.168.11.20	40.113.103.199
Mar 20, 2023 22:25:12.219639063 CET	49798	443	192.168.11.20	40.113.103.199
Mar 20, 2023 22:25:12.219640017 CET	49798	443	192.168.11.20	40.113.103.199
Mar 20, 2023 22:25:12.219737053 CET	443	49798	40.113.103.199	192.168.11.20
Mar 20, 2023 22:25:16.255217075 CET	49799	443	192.168.11.20	40.113.103.199
Mar 20, 2023 22:25:16.255367994 CET	443	49799	40.113.103.199	192.168.11.20
Mar 20, 2023 22:25:16.255620956 CET	49799	443	192.168.11.20	40.113.103.199
Mar 20, 2023 22:25:16.256016016 CET	49799	443	192.168.11.20	40.113.103.199
Mar 20, 2023 22:25:16.256107092 CET	443	49799	40.113.103.199	192.168.11.20
Mar 20, 2023 22:25:16.346580029 CET	443	49799	40.113.103.199	192.168.11.20
Mar 20, 2023 22:25:16.346906900 CET	49799	443	192.168.11.20	40.113.103.199
Mar 20, 2023 22:25:16.348265886 CET	49799	443	192.168.11.20	40.113.103.199
Mar 20, 2023 22:25:16.348314047 CET	443	49799	40.113.103.199	192.168.11.20
Mar 20, 2023 22:25:16.349461079 CET	443	49799	40.113.103.199	192.168.11.20
Mar 20, 2023 22:25:16.350948095 CET	49799	443	192.168.11.20	40.113.103.199
Mar 20, 2023 22:25:16.350948095 CET	49799	443	192.168.11.20	40.113.103.199
Mar 20, 2023 22:25:16.351069927 CET	443	49799	40.113.103.199	192.168.11.20
Mar 20, 2023 22:25:16.351089954 CET	49799	443	192.168.11.20	40.113.103.199
Mar 20, 2023 22:25:16.370872021 CET	443	49799	40.113.103.199	192.168.11.20
Mar 20, 2023 22:25:16.371225119 CET	443	49799	40.113.103.199	192.168.11.20
Mar 20, 2023 22:25:16.371345997 CET	49799	443	192.168.11.20	40.113.103.199
Mar 20, 2023 22:25:16.371345997 CET	49799	443	192.168.11.20	40.113.103.199
Mar 20, 2023 22:25:16.371484995 CET	443	49799	40.113.103.199	192.168.11.20
Mar 20, 2023 22:25:16.371525049 CET	49799	443	192.168.11.20	40.113.103.199
Mar 20, 2023 22:25:19.345463037 CET	49800	443	192.168.11.20	40.126.32.134
Mar 20, 2023 22:25:19.345602036 CET	443	49800	40.126.32.134	192.168.11.20
Mar 20, 2023 22:25:19.345813990 CET	49800	443	192.168.11.20	40.126.32.134
Mar 20, 2023 22:25:19.345932007 CET	49800	443	192.168.11.20	40.126.32.134
Mar 20, 2023 22:25:19.345973969 CET	443	49800	40.126.32.134	192.168.11.20
Mar 20, 2023 22:25:19.426796913 CET	443	49800	40.126.32.134	192.168.11.20
Mar 20, 2023 22:25:19.427050114 CET	49800	443	192.168.11.20	40.126.32.134
Mar 20, 2023 22:25:19.436054945 CET	49800	443	192.168.11.20	40.126.32.134
Mar 20, 2023 22:25:19.436090946 CET	443	49800	40.126.32.134	192.168.11.20
Mar 20, 2023 22:25:19.436619997 CET	443	49800	40.126.32.134	192.168.11.20
Mar 20, 2023 22:25:19.437078953 CET	49800	443	192.168.11.20	40.126.32.134
Mar 20, 2023 22:25:19.437078953 CET	49800	443	192.168.11.20	40.126.32.134
Mar 20, 2023 22:25:19.437130928 CET	49800	443	192.168.11.20	40.126.32.134
Mar 20, 2023 22:25:19.437196970 CET	443	49800	40.126.32.134	192.168.11.20
Mar 20, 2023 22:25:19.570770025 CET	443	49800	40.126.32.134	192.168.11.20
Mar 20, 2023 22:25:19.570858002 CET	443	49800	40.126.32.134	192.168.11.20
Mar 20, 2023 22:25:19.571094036 CET	49800	443	192.168.11.20	40.126.32.134
Mar 20, 2023 22:25:19.571182966 CET	443	49800	40.126.32.134	192.168.11.20
Mar 20, 2023 22:25:19.571244955 CET	443	49800	40.126.32.134	192.168.11.20
Mar 20, 2023 22:25:19.571399927 CET	49800	443	192.168.11.20	40.126.32.134
Mar 20, 2023 22:25:19.571399927 CET	49800	443	192.168.11.20	40.126.32.134
Mar 20, 2023 22:25:19.571502924 CET	49800	443	192.168.11.20	40.126.32.134
Mar 20, 2023 22:25:19.571553946 CET	443	49800	40.126.32.134	192.168.11.20
Mar 20, 2023 22:25:19.578614950 CET	49801	443	192.168.11.20	40.126.32.134
Mar 20, 2023 22:25:19.578757048 CET	443	49801	40.126.32.134	192.168.11.20
Mar 20, 2023 22:25:19.578969002 CET	49801	443	192.168.11.20	40.126.32.134
Mar 20, 2023 22:25:19.579085112 CET	49801	443	192.168.11.20	40.126.32.134
Mar 20, 2023 22:25:19.579128027 CET	443	49801	40.126.32.134	192.168.11.20
Mar 20, 2023 22:25:19.668971062 CET	443	49801	40.126.32.134	192.168.11.20
Mar 20, 2023 22:25:19.669231892 CET	49801	443	192.168.11.20	40.126.32.134
Mar 20, 2023 22:25:19.670562029 CET	49801	443	192.168.11.20	40.126.32.134
Mar 20, 2023 22:25:19.670639038 CET	443	49801	40.126.32.134	192.168.11.20

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Mar 20, 2023 22:25:19.671761036 CET	443	49801	40.126.32.134	192.168.11.20
Mar 20, 2023 22:25:19.672322035 CET	49801	443	192.168.11.20	40.126.32.134
Mar 20, 2023 22:25:19.672322989 CET	49801	443	192.168.11.20	40.126.32.134
Mar 20, 2023 22:25:19.672427893 CET	49801	443	192.168.11.20	40.126.32.134
Mar 20, 2023 22:25:19.672491074 CET	443	49801	40.126.32.134	192.168.11.20
Mar 20, 2023 22:25:20.100641012 CET	443	49801	40.126.32.134	192.168.11.20
Mar 20, 2023 22:25:20.100652933 CET	443	49801	40.126.32.134	192.168.11.20
Mar 20, 2023 22:25:20.100708961 CET	443	49801	40.126.32.134	192.168.11.20
Mar 20, 2023 22:25:20.100749969 CET	443	49801	40.126.32.134	192.168.11.20
Mar 20, 2023 22:25:20.100918055 CET	49801	443	192.168.11.20	40.126.32.134
Mar 20, 2023 22:25:20.101097107 CET	49801	443	192.168.11.20	40.126.32.134
Mar 20, 2023 22:25:20.101097107 CET	49801	443	192.168.11.20	40.126.32.134
Mar 20, 2023 22:25:20.101097107 CET	49801	443	192.168.11.20	40.126.32.134
Mar 20, 2023 22:25:20.116763115 CET	49802	443	192.168.11.20	40.126.32.134
Mar 20, 2023 22:25:20.116780996 CET	443	49802	40.126.32.134	192.168.11.20
Mar 20, 2023 22:25:20.116933107 CET	49802	443	192.168.11.20	40.126.32.134
Mar 20, 2023 22:25:20.117106915 CET	49802	443	192.168.11.20	40.126.32.134
Mar 20, 2023 22:25:20.117120028 CET	443	49802	40.126.32.134	192.168.11.20
Mar 20, 2023 22:25:20.181145906 CET	443	49802	40.126.32.134	192.168.11.20
Mar 20, 2023 22:25:20.181385994 CET	49802	443	192.168.11.20	40.126.32.134
Mar 20, 2023 22:25:20.182734966 CET	49802	443	192.168.11.20	40.126.32.134
Mar 20, 2023 22:25:20.182744026 CET	443	49802	40.126.32.134	192.168.11.20
Mar 20, 2023 22:25:20.182936907 CET	443	49802	40.126.32.134	192.168.11.20
Mar 20, 2023 22:25:20.183368921 CET	49802	443	192.168.11.20	40.126.32.134
Mar 20, 2023 22:25:20.183368921 CET	49802	443	192.168.11.20	40.126.32.134
Mar 20, 2023 22:25:20.183387995 CET	49802	443	192.168.11.20	40.126.32.134
Mar 20, 2023 22:25:20.183396101 CET	443	49802	40.126.32.134	192.168.11.20
Mar 20, 2023 22:25:20.183403015 CET	443	49802	40.126.32.134	192.168.11.20

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Mar 20, 2023 22:25:23.335058928 CET	63471	53	192.168.11.20	1.1.1.1
Mar 20, 2023 22:25:23.344261885 CET	53	63471	1.1.1.1	192.168.11.20
Mar 20, 2023 22:25:23.359338999 CET	59967	53	192.168.11.20	1.1.1.1
Mar 20, 2023 22:25:23.368237019 CET	53	59967	1.1.1.1	192.168.11.20
Mar 20, 2023 22:25:23.481443882 CET	59968	1900	192.168.11.20	239.255.255.250
Mar 20, 2023 22:25:23.722811937 CET	58020	53	192.168.11.20	1.1.1.1
Mar 20, 2023 22:25:23.833489895 CET	53	58020	1.1.1.1	192.168.11.20
Mar 20, 2023 22:25:24.483124018 CET	59968	1900	192.168.11.20	239.255.255.250
Mar 20, 2023 22:25:25.483990908 CET	59968	1900	192.168.11.20	239.255.255.250
Mar 20, 2023 22:25:26.485093117 CET	59968	1900	192.168.11.20	239.255.255.250
Mar 20, 2023 22:25:27.795646906 CET	49407	53	192.168.11.20	1.1.1.1
Mar 20, 2023 22:25:27.805130959 CET	53	49407	1.1.1.1	192.168.11.20
Mar 20, 2023 22:25:34.434989929 CET	138	138	192.168.11.20	192.168.11.255
Mar 20, 2023 22:27:23.332777977 CET	60784	1900	192.168.11.20	239.255.255.250
Mar 20, 2023 22:27:24.339056969 CET	60784	1900	192.168.11.20	239.255.255.250
Mar 20, 2023 22:27:25.348400116 CET	60784	1900	192.168.11.20	239.255.255.250
Mar 20, 2023 22:27:26.359318972 CET	60784	1900	192.168.11.20	239.255.255.250

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class	DNS over HTTPS
Mar 20, 2023 22:25:23.335058928 CET	192.168.11.20	1.1.1.1	0x3b2a	Standard query (0)	accounts.google.com	A (IP address)	IN (0x0001)	false
Mar 20, 2023 22:25:23.359338999 CET	192.168.11.20	1.1.1.1	0x3517	Standard query (0)	clients2.google.com	A (IP address)	IN (0x0001)	false
Mar 20, 2023 22:25:23.722811937 CET	192.168.11.20	1.1.1.1	0xc874	Standard query (0)	fuadrashid.com	A (IP address)	IN (0x0001)	false

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class	DNS over HTTPS
Mar 20, 2023 22:25:27.795646906 CET	192.168.11.20	1.1.1.1	0x6907	Standard query (0)	www.google.com	A (IP address)	IN (0x0001)	false

DNS Answers

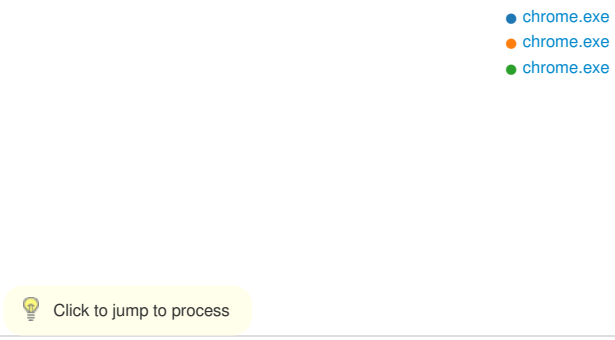
Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Mar 20, 2023 22:25:23.344261885 CET	1.1.1.1	192.168.11.20	0x3b2a	No error (0)	accounts.google.com		142.250.185.77	A (IP address)	IN (0x0001)	false
Mar 20, 2023 22:25:23.368237019 CET	1.1.1.1	192.168.11.20	0x3517	No error (0)	clients2.google.com	clients.l.google.com		CNAME (Canonical name)	IN (0x0001)	false
Mar 20, 2023 22:25:23.368237019 CET	1.1.1.1	192.168.11.20	0x3517	No error (0)	clients.l.google.com		142.250.185.142	A (IP address)	IN (0x0001)	false
Mar 20, 2023 22:25:23.833489895 CET	1.1.1.1	192.168.11.20	0xc874	No error (0)	fuadrashid.com		192.185.113.229	A (IP address)	IN (0x0001)	false
Mar 20, 2023 22:25:27.805130959 CET	1.1.1.1	192.168.11.20	0x6907	No error (0)	www.google.com		142.250.185.196	A (IP address)	IN (0x0001)	false

HTTP Request Dependency Graph

- login.live.com
- clients2.google.com
- accounts.google.com
- fuadrashid.com
- https:
  - www.google.com

Statistics

Behavior



System Behavior

Analysis Process: chrome.exe PID: **1016**, Parent PID: **7652**

General

Target ID:	0
Start time:	22:25:21
Start date:	20/03/2023
Path:	C:\Program Files\Google\Chrome\Application\chrome.exe
Wow64 process (32bit):	false
Commandline:	C:\Program Files\Google\Chrome\Application\chrome.exe" --start-maximized "about:blank
Imagebase:	0x7ff71cb20000
File size:	2509656 bytes
MD5 hash:	464953824E644F10FFDC9E093FD18F94
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities

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

File Path	Completion	Count	Source Address	Symbol

Old File Path	New File Path	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

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol

Analysis Process: chrome.exe PID: **8132**, Parent PID: **1016**

General

Target ID:	1
Start time:	22:25:22
Start date:	20/03/2023
Path:	C:\Program Files\Google\Chrome\Application\chrome.exe
Wow64 process (32bit):	false
Commandline:	"C:\Program Files\Google\Chrome\Application\chrome.exe" --type=utility --utility-sub-type=network.mojom.NetworkService --field-trial-handle=1700,18324760747851478443,7253911549642704679,131072 --disable-features=OptimizationGuideModelDownloading,OptimizationHints,OptimizationHintsFetching,OptimizationTargetPrediction --lang=en-US --service-sandbox-type=none --mojo-platform-channel-handle=1996 /prefetch:8
Imagebase:	0x7ff71cb20000
File size:	2509656 bytes
MD5 hash:	464953824E644F10FFDC9E093FD18F94
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities

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

File Path	Completion	Count	Source Address	Symbol

Old File Path	New File Path	Completion	Count	Source Address	Symbol

Analysis Process: chrome.exe PID: **4464**, Parent PID: **7652**

General

Target ID:	3
Start time:	22:25:22
Start date:	20/03/2023
Path:	C:\Program Files\Google\Chrome\Application\chrome.exe
Wow64 process (32bit):	false
Commandline:	C:\Program Files\Google\Chrome\Application\chrome.exe" "C:\Users\user\Desktop\#Ud83d#Udce7 Tax Statements-2-121_076_454656_3-4(4).hTm
Imagebase:	0x7ff71cb20000
File size:	2509656 bytes
MD5 hash:	464953824E644F10FFDC9E093FD18F94
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

Registry Activities

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

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol

Disassembly

No disassembly