ID: 736949
Sample Name: CONTRACT_REVISED-SHIPMENT-DOCUMENTS_EXPORTS_REFERENCE-QT63637-02993900299348.exe
Cookbook: default.jbs
Time: 12:30:06
Date: 03/11/2022
Version: 36.0.0 Rainbow Opal

Table of Contents

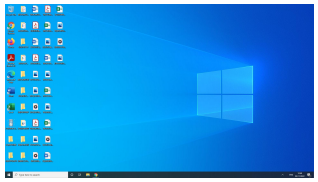
Windows Analysis Report

CONTRACT_REVISED-SHIPMENT-DOCUMENTS_EXPORTS_REFERENCE-QT63637-02993900299348.exe

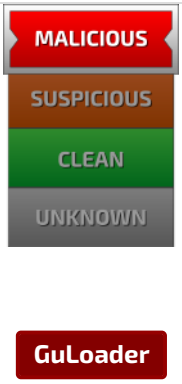
Overview

General Information

Sample Name:	CONTRACT_REVISED-SHIPMENT-DOCUMENTS_EXPORTS_REFERENCE-QT63637-02993900299348.exe
Analysis ID:	736949
MD5:	045f22ce9be3d3..
SHA1:	91b74e75d55c33..
SHA256:	e05ec32c2edc10..
Infos:	



Detection



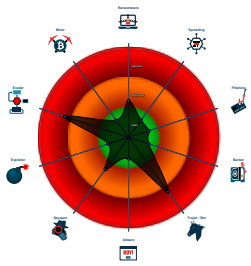
GuLoader

Score:	64
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Yara detected GuLoader
- Initial sample is a PE file and has a…
- Tries to detect Any.run
- Executable has a suspicious name …
- Tries to detect sandboxes and other…
- Uses 32bit PE files
- Found a high number of Window / U…
- Queries the volume information (nam…
- Drops PE files
- Tries to load missing DLLs
- Contains functionality to read the PE…
- Contains functionality to shutdown /…

Classification



Process Tree

- **System is w10x64native**
- CONTRACT_REVISED-SHIPMENT-DOCUMENTS_EXPORTS_REFERENCE-QT63637-02993900299348.exe (PID: 4848 cmdline: C:\Users\user\Desktop\CONTRACT_REVISED-SHIPMENT-DOCUMENTS_EXPORTS_REFERENCE-QT63637-02993900299348.exe MD5: 045F22CE9BE3D33B07A00780EE66FCFD)
  - dllhost.exe (PID: 2364 cmdline: C:\Windows\system32\DllHost.exe /Processid:{AB8902B4-09CA-4BB6-B78D-A8F59079A8D5} MD5: 08EB78E5BE019DF044C26B14703BD1FA)
  - backgroundTaskHost.exe (PID: 4408 cmdline: "C:\WINDOWS\system32\backgroundTaskHost.exe" -ServerName:App.AppXmtcan0h2tfbfy7k9kn8hbxb6dmzz1zh0.mca MD5: DA7063B17DBB8BBB3015351016868006)
  - dllhost.exe (PID: 4508 cmdline: C:\Windows\system32\DllHost.exe /Processid:{AB8902B4-09CA-4BB6-B78D-A8F59079A8D5} MD5: 08EB78E5BE019DF044C26B14703BD1FA)
  - BackgroundTransferHost.exe (PID: 4480 cmdline: "BackgroundTransferHost.exe" -ServerName:BackgroundTransferHost.1 MD5: C5D813D92E83CDE3FECD9343933E3421)
  - BackgroundTransferHost.exe (PID: 5560 cmdline: "BackgroundTransferHost.exe" -ServerName:BackgroundTransferHost.1 MD5: C5D813D92E83CDE3FECD9343933E3421)
  - ieinstal.exe (PID: 5400 cmdline: C:\Users\user\Desktop\CONTRACT_REVISED-SHIPMENT-DOCUMENTS_EXPORTS_REFERENCE-QT63637-02993900299348.exe MD5: 7871873BABCEA94FBA13900B561C7C55)
  - ieinstal.exe (PID: 1820 cmdline: C:\Users\user\Desktop\CONTRACT_REVISED-SHIPMENT-DOCUMENTS_EXPORTS_REFERENCE-QT63637-02993900299348.exe MD5: 7871873BABCEA94FBA13900B561C7C55)
  - ieinstal.exe (PID: 6908 cmdline: C:\Users\user\Desktop\CONTRACT_REVISED-SHIPMENT-DOCUMENTS_EXPORTS_REFERENCE-QT63637-02993900299348.exe MD5: 7871873BABCEA94FBA13900B561C7C55)
  - ieinstal.exe (PID: 1396 cmdline: C:\Users\user\Desktop\CONTRACT_REVISED-SHIPMENT-DOCUMENTS_EXPORTS_REFERENCE-QT63637-02993900299348.exe MD5: 7871873BABCEA94FBA13900B561C7C55)
  - ieinstal.exe (PID: 4268 cmdline: C:\Users\user\Desktop\CONTRACT_REVISED-SHIPMENT-DOCUMENTS_EXPORTS_REFERENCE-QT63637-02993900299348.exe MD5: 7871873BABCEA94FBA13900B561C7C55)
  - ieinstal.exe (PID: 4772 cmdline: C:\Users\user\Desktop\CONTRACT_REVISED-SHIPMENT-DOCUMENTS_EXPORTS_REFERENCE-QT63637-02993900299348.exe MD5: 7871873BABCEA94FBA13900B561C7C55)
  - ieinstal.exe (PID: 7620 cmdline: C:\Users\user\Desktop\CONTRACT_REVISED-SHIPMENT-DOCUMENTS_EXPORTS_REFERENCE-QT63637-02993900299348.exe MD5: 7871873BABCEA94FBA13900B561C7C55)
  - ieinstal.exe (PID: 6588 cmdline: C:\Users\user\Desktop\CONTRACT_REVISED-SHIPMENT-DOCUMENTS_EXPORTS_REFERENCE-QT63637-02993900299348.exe MD5: 7871873BABCEA94FBA13900B561C7C55)
  - ieinstal.exe (PID: 3156 cmdline: C:\Users\user\Desktop\CONTRACT_REVISED-SHIPMENT-DOCUMENTS_EXPORTS_REFERENCE-QT63637-02993900299348.exe MD5: 7871873BABCEA94FBA13900B561C7C55)
  - ieinstal.exe (PID: 5924 cmdline: C:\Users\user\Desktop\CONTRACT_REVISED-SHIPMENT-DOCUMENTS_EXPORTS_REFERENCE-QT63637-02993900299348.exe MD5: 7871873BABCEA94FBA13900B561C7C55)
  - ieinstal.exe (PID: 3988 cmdline: C:\Users\user\Desktop\CONTRACT_REVISED-SHIPMENT-DOCUMENTS_EXPORTS_REFERENCE-QT63637-02993900299348.exe MD5: 7871873BABCEA94FBA13900B561C7C55)
  - ielowutil.exe (PID: 7732 cmdline: C:\Users\user\Desktop\CONTRACT_REVISED-SHIPMENT-DOCUMENTS_EXPORTS_REFERENCE-QT63637-02993900299348.exe MD5: 650FE7460630188008BF8C8153526CEB)
  - ielowutil.exe (PID: 4760 cmdline: C:\Users\user\Desktop\CONTRACT_REVISED-SHIPMENT-DOCUMENTS_EXPORTS_REFERENCE-QT63637-02993900299348.exe

MD5: 650FE7460630188008BF8C8153526CEB)
- ielowutil.exe (PID: 7756 cmdline: C:\Users\user\Desktop\CONTRACT_REVISED-SHIPMENT-DOCUMENTS_EXPORTS_REFERENCE-QT63637-02993900299348.exe MD5: 650FE7460630188008BF8C8153526CEB)
- ielowutil.exe (PID: 4612 cmdline: C:\Users\user\Desktop\CONTRACT_REVISED-SHIPMENT-DOCUMENTS_EXPORTS_REFERENCE-QT63637-02993900299348.exe MD5: 650FE7460630188008BF8C8153526CEB)
- ielowutil.exe (PID: 3852 cmdline: C:\Users\user\Desktop\CONTRACT_REVISED-SHIPMENT-DOCUMENTS_EXPORTS_REFERENCE-QT63637-02993900299348.exe MD5: 650FE7460630188008BF8C8153526CEB)
- ielowutil.exe (PID: 6596 cmdline: C:\Users\user\Desktop\CONTRACT_REVISED-SHIPMENT-DOCUMENTS_EXPORTS_REFERENCE-QT63637-02993900299348.exe MD5: 650FE7460630188008BF8C8153526CEB)
- ielowutil.exe (PID: 6516 cmdline: C:\Users\user\Desktop\CONTRACT_REVISED-SHIPMENT-DOCUMENTS_EXPORTS_REFERENCE-QT63637-02993900299348.exe MD5: 650FE7460630188008BF8C8153526CEB)
- ielowutil.exe (PID: 7348 cmdline: C:\Users\user\Desktop\CONTRACT_REVISED-SHIPMENT-DOCUMENTS_EXPORTS_REFERENCE-QT63637-02993900299348.exe MD5: 650FE7460630188008BF8C8153526CEB)
- ielowutil.exe (PID: 7808 cmdline: C:\Users\user\Desktop\CONTRACT_REVISED-SHIPMENT-DOCUMENTS_EXPORTS_REFERENCE-QT63637-02993900299348.exe MD5: 650FE7460630188008BF8C8153526CEB)
- ielowutil.exe (PID: 7380 cmdline: C:\Users\user\Desktop\CONTRACT_REVISED-SHIPMENT-DOCUMENTS_EXPORTS_REFERENCE-QT63637-02993900299348.exe MD5: 650FE7460630188008BF8C8153526CEB)
- ExtExport.exe (PID: 5404 cmdline: C:\Users\user\Desktop\CONTRACT_REVISED-SHIPMENT-DOCUMENTS_EXPORTS_REFERENCE-QT63637-02993900299348.exe MD5: 3253FD643C51C133C3489A146781913B)
- ExtExport.exe (PID: 7588 cmdline: C:\Users\user\Desktop\CONTRACT_REVISED-SHIPMENT-DOCUMENTS_EXPORTS_REFERENCE-QT63637-02993900299348.exe MD5: 3253FD643C51C133C3489A146781913B)
- ExtExport.exe (PID: 5708 cmdline: C:\Users\user\Desktop\CONTRACT_REVISED-SHIPMENT-DOCUMENTS_EXPORTS_REFERENCE-QT63637-02993900299348.exe MD5: 3253FD643C51C133C3489A146781913B)
- ExtExport.exe (PID: 8104 cmdline: C:\Users\user\Desktop\CONTRACT_REVISED-SHIPMENT-DOCUMENTS_EXPORTS_REFERENCE-QT63637-02993900299348.exe MD5: 3253FD643C51C133C3489A146781913B)
- ExtExport.exe (PID: 1160 cmdline: C:\Users\user\Desktop\CONTRACT_REVISED-SHIPMENT-DOCUMENTS_EXPORTS_REFERENCE-QT63637-02993900299348.exe MD5: 3253FD643C51C133C3489A146781913B)
- ExtExport.exe (PID: 6700 cmdline: C:\Users\user\Desktop\CONTRACT_REVISED-SHIPMENT-DOCUMENTS_EXPORTS_REFERENCE-QT63637-02993900299348.exe MD5: 3253FD643C51C133C3489A146781913B)
- ExtExport.exe (PID: 6248 cmdline: C:\Users\user\Desktop\CONTRACT_REVISED-SHIPMENT-DOCUMENTS_EXPORTS_REFERENCE-QT63637-02993900299348.exe MD5: 3253FD643C51C133C3489A146781913B)
- ExtExport.exe (PID: 5524 cmdline: C:\Users\user\Desktop\CONTRACT_REVISED-SHIPMENT-DOCUMENTS_EXPORTS_REFERENCE-QT63637-02993900299348.exe MD5: 3253FD643C51C133C3489A146781913B)
- ExtExport.exe (PID: 5904 cmdline: C:\Users\user\Desktop\CONTRACT_REVISED-SHIPMENT-DOCUMENTS_EXPORTS_REFERENCE-QT63637-02993900299348.exe MD5: 3253FD643C51C133C3489A146781913B)
- backgroundTaskHost.exe (PID: 5840 cmdline: "C:\WINDOWS\system32\backgroundTaskHost.exe" -ServerName:App.AppXmtcan0h2tfbfy7k9kn8hbxb6dmzz1zh0.mca MD5: DA7063B17DBB8BBB3015351016868006)

- **cleanup**

Malware Configuration

No configs have been found

Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
00000002.00000002.110030353777.0000000002B90000.00000040.00000800.00020000.00000000.sdmp	JoeSecurity_GuLoader_2	Yara detected GuLoader	Joe Security	

Sigma Signatures

No Sigma rule has matched

Snort Signatures

No Snort rule has matched

Joe Sandbox Signatures

System Summary

Initial sample is a PE file and has a suspicious name

Executable has a suspicious name (potential lure to open the executable)

Data Obfuscation

Yara detected GuLoader

Malware Analysis System Evasion

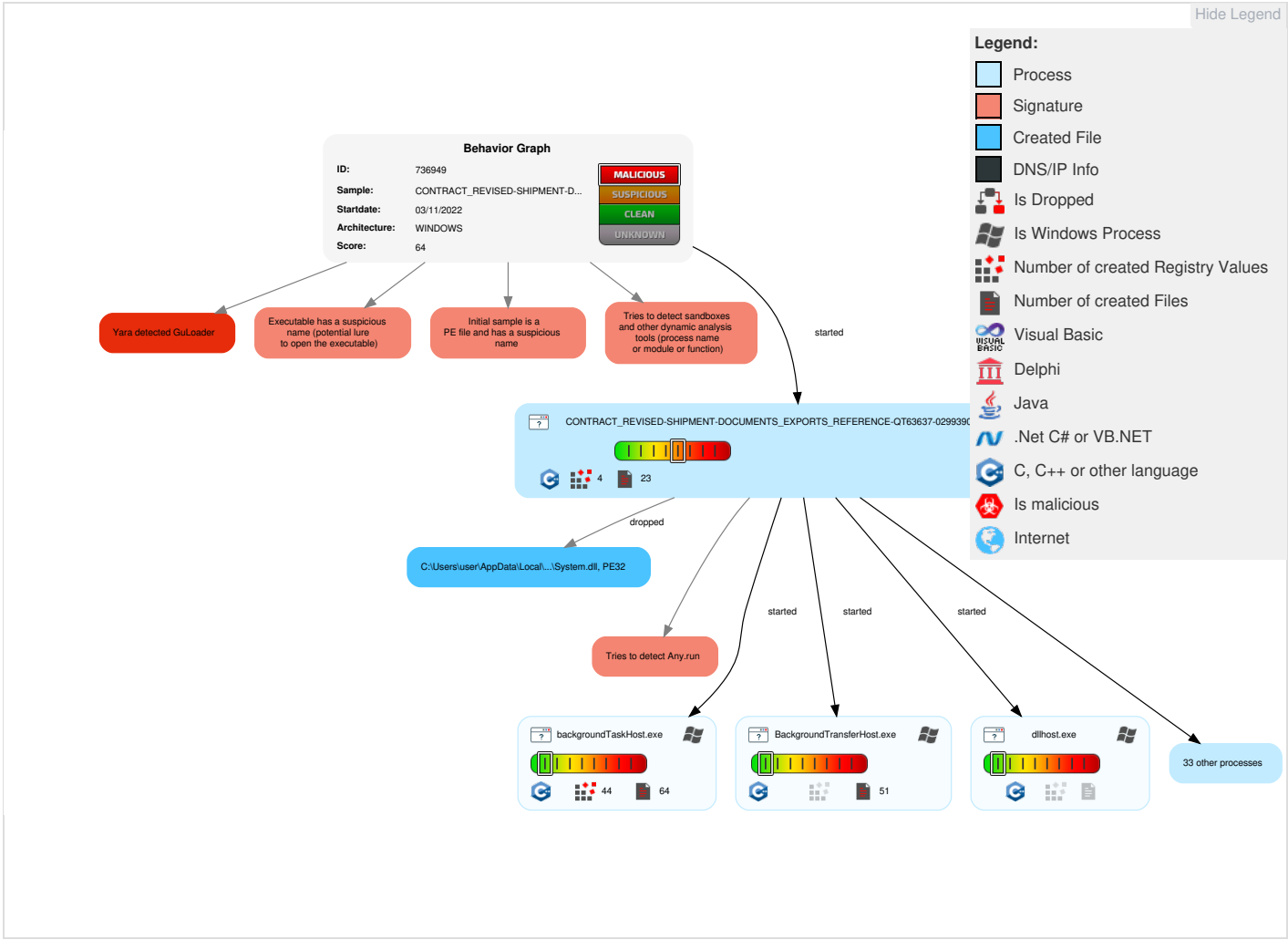
Tries to detect Any.run

Tries to detect sandboxes and other dynamic analysis tools (process name or module or function)

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	1 Native API	1 Windows Service	1 Access Token Manipulation	1 Masquerading	OS Credential Dumping	2 2 1 Security Software Discovery	Remote Services	1 Archive Collected Data	Exfiltration Over Other Network Medium	1 Encrypted Channel	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	1 System Shutdown/ Reboot
Default Accounts	Scheduled Task/Job	1 DLL Side-Loading	1 Windows Service	1 2 Virtualization/Sandbox Evasion	LSASS Memory	1 2 Virtualization/Sandbox Evasion	Remote Desktop Protocol	1 Clipboard Data	Exfiltration Over Bluetooth	Junk Data	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	1 1 Process Injection	1 Access Token Manipulation	Security Account Manager	1 Application Window Discovery	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Steganography	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	1 DLL Side-Loading	1 1 Process Injection	NTDS	3 File and Directory Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	1 Obfuscated Files or Information	LSA Secrets	1 4 System Information Discovery	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication		Manipulate App Store Rankings or Ratings
Replication Through Removable Media	Launchd	Rc.common	Rc.common	1 DLL Side-Loading	Cached Domain Credentials	System Owner/User Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service		Abuse Accessibility Features

Behavior Graph



Screenshots

Thumbnails

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

Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
CONTRACT_REVISED-SHIPMENT-DOCUMENTS_EXPORTS_REFERENCE-QT63637-02993900299348.exe	10%	ReversingLabs	Win32.Downloader.Minix	

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\nsdCB34.tmp\System.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\nsdCB34.tmp\System.dll	1%	Virustotal		Browse
C:\Users\user\AppData\Local\Temp\nsdCB34.tmp\System.dll	4%	Metadefender		Browse

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

No Antivirus matches

Domains and IPs

Contacted Domains

No contacted domains info

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://nsis.sf.net/NSIS_ErrorError	CONTRACT_REVISED-SHIPMENT-DOCUMENTS_EXPORTS_REFERENCE-QT63637-02993900299348.exe	false		high

World Map of Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	36.0.0 Rainbow Opal
Analysis ID:	736949
Start date and time:	2022-11-03 12:30:06 +01:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 13m 33s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	CONTRACT_REVISED-SHIPMENT-DOCUMENTS_EXPORTS_REFERENCE-QT63637-02993900299348.exe
Cookbook file name:	default.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
Run name:	Suspected Instruction Hammering
Number of analysed new started processes analysed:	40
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:	mal64.troj.evad.winEXE@2073/48@0/0
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 37.3% (good quality ratio 36.6%) • Quality average: 87% • Quality standard deviation: 21.2%
HCA Information:	• Successful, ratio: 97% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .exe

Warnings

- Exclude process from analysis (whitelisted): BackgroundTransferHost.exe, backgroundTaskHost.exe
- Excluded IPs from analysis (whitelisted): 20.82.210.154, 95.101.54.129, 95.101.54.113, 20.234.34.18
- Excluded domains from analysis (whitelisted): spclient.wg.spotify.com, client.wns.windows.com, asf-ris-prod-neu-azsc.northeurope.cloudapp.azure.com, ris-prod.trafficmanager.net, ctldl.windowsupdate.com, iris-de-prod-azsc-neu-b.northeurope.cloudapp.azure.com, wdcp.microsoft.com, a1449.dscg2.akamai.net, arc.msn.com, ris.api.iris.microsoft.com, wdcpalt.microsoft.com, login.live.com, arc.trafficmanager.net, img-prod-cms-rt-microsoft-com.akamaized.net
- Report size exceeded maximum capacity and may have missing behavior information.
- Report size getting too big, too many NtAllocateVirtualMemory calls found.
- Report size getting too big, too many NtWriteVirtualMemory calls found.

Simulations

Behavior and APIs

Time	Type	Description
12:31:58	API Interceptor	1x Sleep call for process: CONTRACT_REVISED-SHIPMENT-DOCUMENTS_EXPORTS_REFERENCE-QT63637-02993900299348.exe modified
12:31:58	API Interceptor	2x Sleep call for process: dllhost.exe modified

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\Packages\Microsoft.Windows.ContentDeliveryManager_cw5n1h2txyewy\AC\BackgroundTransferApi\0f40a9a4-7ba9-4798-b98b-f18214009bbd.e7219a3a-5edb-4393-8e4b-a78a641e7e36.down_meta

Process:	C:\Windows\System32\BackgroundTransferHost.exe
File Type:	data
Category:	dropped
Size (bytes):	1224
Entropy (8bit):	3.6100919570774668
Encrypted:	false
SSDEEP:	24:LLVR2mRie/km6wrHXpjgWzgxjX+vUVieQBQT1+InEysafxOc2CpX3QAbbW0VB:LLD2mRiOxzXpjPgVX+v8iTBkZ7rfeIXj
MD5:	D0E6F8A432143B3A4D4B296D928643DB
SHA1:	1C5ABADDDD94750B8E62B9C12F8671404833EB6C
SHA-256:	5B3A44CF2FF858861F73F129D818DED5CE7AD498B568CCB015DF4FA4E716DDE4
SHA-512:	275C970EDA97E19E1324CEA8AF28BFCF7BAC6B1BD6234297A5B7EAB274BF692C1748AAEA8C256B7B9F1EE186D95C2EE4D9E15CC21976E7F766DF41A03A43227F
Malicious:	false
Preview:	h.t.t.p.s.:.//.i.m.g.-.p.r.o.d.-.c.m.s.-.r.t.-.m.i.c.r.o.s.o.f.t.-.c.o.m...a.k.a.m.a.i.z.e.d...n.e.t./.c.m.s./.a.p.i./.a.m./.i.m.a.g.e.F.i.l.e.D.a.t.a./.R.W.E.y.I.E.?.v.e.r.=.7.b.e.a...L.a.s.t.-.M.o.d.i.f.i.e.d.:. .F.r.i.,. .1.6. .S.e.p. .2.0.2.2. .0.0.:.4.2.:.4.4. .G.M.T...C.o.n.t.e.n.t.-.T.y.p.e.:. .i.m.a.g.e./.j.p.e.g...A.c.c.e.s.s.-.C.o.n.t.r.o.l.-.A.l.l.o.w.-.O.r.i.g.i.n.:. .*...C.o.n.t.e.n.t.-.L.o.c.a.t.i.o.n.:. .h.t.t.p.s.:.//.i.m.a.g.e...p.r.o.d...c.m.s...r.t...m.i.c.r.o.s.o.f.t...c.o.m./.c.m.s./.a.p.i./.a.m./.i.m.a.g.e.F.i.l.e.D.a.t.a./.R.W.E.y.I.E.?.v.e.r.=.7.b.e.a...X.-.S.o.u.r.c.e.-.L.e.n.g.t.h.:. .4.5.6.2.4.2...X.-.D.a.t.a.c.e.n.t.e.r.:. .n.o.r.t.h.e.u...X.-.A.c.t.i.v.i.t.y.I.d.:. .c.8.f.5.3.a.8.b.-.1.7.5.c.-.4.d.c.b.-.8.c.3.f.-.8.8.8.1.8.9.d.f.4.d.0.9...T.i.m.i.n.g.-.A.l.l.o.w.-.O.r.i.g.i.n.:. .*...X.-.F.r.a.m.e.-.O.p.t.i.o.n.s.:. .D.E.N.Y...X.-.R.e.s.i.z.e.r.V.e.r.s.i.o.n.:. .1...0...C.o.n.t.e.n.t.-.L.e.n.g.t.h.:. .4.5.6.2.4.2...C.a.c.h.e.-.C.o.n.t.r.o.l.:. .p.u.b.l.i.

C:\Users\user\AppData\Local\Packages\Microsoft.Windows.ContentDeliveryManager_cw5n1h2txyewy\AC\BackgroundTransferApi\0f40a9a4-7ba9-4798-b98b-f18214009bbd.up_meta_secure

Process:	C:\Windows\System32\BackgroundTransferHost.exe
File Type:	data
Category:	dropped
Size (bytes):	502
Entropy (8bit):	7.293651679671136
Encrypted:	false
SSDEEP:	12:QU6NKGS32dZvsN6KbJst2vsU/YbX2JXngFJ3zfBro:QUfpKe6KbJst2R/YbXuXMB8
MD5:	C23766093AE0D9E3CBC24D662874023B
SHA1:	86C9C96A3518CED83CCAC3108CEA1207C40EF5E0
SHA-256:	EC59F368FF841989E4ACCCDBC7D3343EDDE3BDA92352C46F86D3A8E5DDE2102E
SHA-512:	F3DEAF9C47C3BB8977DD8862FF5DCC05FCA8CA12AB661228D0FE3369BB098AA0AC01945B66DBFEA02B7094BC05217223A1E447EBCBC64BB731CCAB12492B4FC6
Malicious:	false
Preview:	.....z..O.....A.n.N...U.s.....f..... .....!b4:o7.K(.Z..k,...B~...ltn..... ...##.$.....6..V.C.*CKA....t[.X.s .....<...`.=.S.A0{.F.....U.h@..p.".+....R...j..pO.x...Jj....e.=...mI.pk=..O1b.#.....0. Z.`}...wl8..\....m..@k..4.$q.is.....e.....l_"b@...wz.$a...8.....%...].y.....`.....2..aw....K....Ns...X..1Yj4.....U;k.`.j.....6...}.d..;r5..vQ[....m.6..E....X.....O>E].}5..@...=~....)hgS.}.~.v..v4X.r?.....j..7..R..3'..y....:....oL.Pr.N.

C:\Users\user\AppData\Local\Packages\Microsoft.Windows.ContentDeliveryManager_cw5n1h2txyewy\AC\BackgroundTransferApi\3843bffb-4eef-4da1-af04-618c0facc656.down_data

Process:	C:\Windows\System32\BackgroundTransferHost.exe
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 96x96, segment length 16, baseline, precision 8, 1920x1080, components 3
Category:	dropped
Size (bytes):	456242
Entropy (8bit):	7.901591558066316
Encrypted:	false
SSDEEP:	6144:NFYwf2vzmMr8881AQEGZ4TduN7vx9M8W5l31cRdZBFTZk9Rb/fnGk1+tG8:MwOvzm08T1AQlqAM8W/31ct/ZmRafL
MD5:	475D42621D87B431D87BA232216E25B8
SHA1:	9F44DC4AE1ED0D3473198B1C9DE2D4C8D813C79C
SHA-256:	562619314F336727FE5DFD3428B45C1ECF913C8E9ED90EFEAE18C6992F8B5A85
SHA-512:	9BC8BDD2BE82CAB886571EA2A9A2968069927B7E578FE38879A587A4D3B6DEC189AD01E4FCD8D3804889624C4AD7DE7B5EC497194F0CAC920B8A42636D754D5D
Malicious:	false
Preview:	......JFIF.....`.`.....C.....C.....8...."..........}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....?..JM...J.....r=..&.J,2-..jJ)..4.*V.m.;..R.vPU.....6.P]..T....#=..6.].]1..6...I..W1.._..EM...1IS.I..dU.h.....;..m.).iX...IO.F...).j]....{i*Z(*.T.6.J.r-.m.h.d.d>]!...6.a..3mN.B.h.JH.m%K...H|.m'.R.t.)..v.T.).]..DT.j]....#....M.m.wd^^i.UO.....JO..e.R...I....M.@..|.n.....6Ryuc....+.l..].)......3%.]+.1..J.....F.,>b-..-.Xw"....6Qa...t.6.6..9.v.yu/.N.J...

C:\Users\user\AppData\Local\Packages\Microsoft.Windows.ContentDeliveryManager_cw5n1h2txyewy\AC\BackgroundTransferApi\3843bffb-4eef-4da1-af04-618c0facc656.e7219a3a-5edb-4393-8e4b-a78a641e7e36.down_meta

Process:	C:\Windows\System32\BackgroundTransferHost.exe
File Type:	data
Category:	dropped
Size (bytes):	1224
Entropy (8bit):	3.6100919570774668
Encrypted:	false
SSDEEP:	24:LLVR2mRie/km6wrHXpjgWzgxjX+vUVieQBQT1+InEysafxOc2CpX3QAbbW0VB:LLD2mRiOxzXpjPgVX+v8iTBkZ7rfeIXj
MD5:	D0E6F8A432143B3A4D4B296D928643DB
SHA1:	1C5ABADDDD94750B8E62B9C12F8671404833EB6C
SHA-256:	5B3A44CF2FF858861F73F129D818DED5CE7AD498B568CCB015DF4FA4E716DDE4
SHA-512:	275C970EDA97E19E1324CEA8AF28BFCF7BAC6B1BD6234297A5B7EAB274BF692C1748AAEA8C256B7B9F1EE186D95C2EE4D9E15CC21976E7F766DF41A03A43227F
Malicious:	false
Preview:	h.t.t.p.s.:.//.i.m.g.-.p.r.o.d.-.c.m.s.-.r.t.-.m.i.c.r.o.s.o.f.t.-.c.o.m...a.k.a.m.a.i.z.e.d...n.e.t./.c.m.s./.a.p.i./.a.m./.i.m.a.g.e.F.i.l.e.D.a.t.a./.R.W.E.y.I.E.?.v.e.r.=.7.b.e.a...L.a.s.t.-.M.o.d.i.f.i.e.d.:. .F.r.i.,. .1.6. .S.e.p. .2.0.2.2. .0.0.:.4.2.:.4.4. .G.M.T...C.o.n.t.e.n.t.-.T.y.p.e.:. .i.m.a.g.e./.j.p.e.g...A.c.c.e.s.s.-.C.o.n.t.r.o.l.-.A.l.l.o.w.-.O.r.i.g.i.n.:. .*...C.o.n.t.e.n.t.-.L.o.c.a.t.i.o.n.:. .h.t.t.p.s.:.//.i.m.a.g.e...p.r.o.d...c.m.s...r.t...m.i.c.r.o.s.o.f.t...c.o.m./.c.m.s./.a.p.i./.a.m./.i.m.a.g.e.F.i.l.e.D.a.t.a./.R.W.E.y.I.E.?.v.e.r.=.7.b.e.a...X.-.S.o.u.r.c.e.-.L.e.n.g.t.h.:. .4.5.6.2.4.2...X.-.D.a.t.a.c.e.n.t.e.r.:. .n.o.r.t.h.e.u...X.-.A.c.t.i.v.i.t.y.I.d.:. .c.8.f.5.3.a.8.b.-.1.7.5.c.-.4.d.c.b.-.8.c.3.f.-.8.8.8.1.8.9.d.f.4.d.0.9...T.i.m.i.n.g.-.A.l.l.o.w.-.O.r.i.g.i.n.:. .*...X.-.F.r.a.m.e.-.O.p.t.i.o.n.s.:. .D.E.N.Y...X.-.R.e.s.i.z.e.r.V.e.r.s.i.o.n.:. .1...0...C.o.n.t.e.n.t.-.L.e.n.g.t.h.:. .4.5.6.2.4.2...C.a.c.h.e.-.C.o.n.t.r.o.l.:. .p.u.b.l.i.

C:\Users\user\AppData\Local\Packages\Microsoft.Windows.ContentDeliveryManager_cw5n1h2txyewy\AC\BackgroundTransferApi\3843bffb-4eef-4da1-af04-618c0facc656.up_meta_secure

Process:	C:\Windows\System32\backgroundTaskHost.exe
File Type:	data
Category:	dropped
Size (bytes):	502
Entropy (8bit):	7.293651679671136
Encrypted:	false
SSDEEP:	12:QU6NKGS32dZvsN6KbJst2vsU/YbX2JXngFJ3zfBro:QUfpKe6KbJst2R/YbXuXMB8
MD5:	C23766093AE0D9E3CBC24D662874023B
SHA1:	86C9C96A3518CED83CCAC3108CEA1207C40EF5E0
SHA-256:	EC59F368FF841989E4ACCCDBC7D3343EDDE3BDA92352C46F86D3A8E5DDE2102E
SHA-512:	F3DEAF9C47C3BB8977DD8862FF5DCC05FCA8CA12AB661228D0FE3369BB098AA0AC01945B66DBFEA02B7094BC05217223A1E447EBCBC64BB731CCAB12492B4FC6
Malicious:	false
Preview:	.....z..O.....A.n.N...U.s.....f..... .....!b4:o7.K(.Z..k,...B~...ltn..... ...##.$.....6..V.C.*CKA....t[.X.s .....<...`.=.S.A0{.F.....U.h@..p.".+....R...j..pO.x...Jj....e.=...mI.pk=..O1b.#.....0. Z.`}...wl8..\....m..@k..4.$q.is.....e.....l_"b@...wz.$a...8.....%...].y.....`.....2..aw....K....Ns...X..1Yj4.....U;k.`.j.....6...}.d..;r5..vQ[....m.6..E....X.....O>E].}5..@...=~....)hgS.}.~.v..v4X.r?.....j..7..R..3'..y....:....oL.Pr.N.

C:\Users\user\AppData\Local\Packages\Microsoft.Windows.ContentDeliveryManager_cw5n1h2txyewy\AC\BackgroundTransferApi\4aa5b1fb-1301-4194-8203-1cbb67304ae7.down_data

Process:	C:\Windows\System32\BackgroundTransferHost.exe
File Type:	JPEG image data, Exif standard: [TIFF image data, big-endian, direntries=7, orientation=upper-left, xresolution=98, yresolution=106, resolutionunit=2, software=Adobe Photoshop 21.1 (Windows), datetime=2021:11:11 06:55:38]
Category:	dropped
Size (bytes):	1654488
Entropy (8bit):	6.926504673655095
Encrypted:	false
SSDEEP:	24576:1k44jNiVr4qVhre8lekiZaSEKBcf/prV/RRJGoGaEqKEHisGpp7quKRDR7ripxi6:H4jNiVr4qXlZvKV9pp7qPRDNripY6
MD5:	3C36C820F3E016E8A3A63C34BA7BEF07
SHA1:	AF2A7EBB7A6D6C1815190C24EF732B2089115331
SHA-256:	F62AFA107BBFE2FEAEF84AB87277D31DFE1AAABF61400F241FDD50C45AB19D7F
SHA-512:	1074A8603B932052ED17825E83403D5F4EC3CD8CC7DB94BC4F262146DDA054640CBFB126FD728AB35C8B2B20285BC71CFE20BB3DEB3BDF8CC4B2877595B9486
Malicious:	false
Preview:	.....Exif..MM.*.....b.....j.(.....1.....r.2.....i.....'.....'.Adobe Photoshop 21.1 (Windows).2021:11:11 06:55:38.....8.....".....*.(.....2.....H.....H.....Adobe_CM.....Adobe.d.....Z..".....?.....3.....!.1.AQa."q.2.....B#$.R.b34r..C.%.S...cs5....&D.TdE.t6..U.e...u..F'.....Vfv.....7GWgw.....5.....!1..AQaq"..2.....B#.R..3$b.r..CS.cs4.%.....&5..D.T..dEU6te....u..F.....Vfv.....'7GWgw.....?..(..].1.....}S.... ..4mp#...w..[..`.[.P.=..g.w.U{.....{..?..<..l..`..:._..d.T.k.q.m...;..1.....@..A1..5w.kZCk...*`....~.*...$9.{..

C:\Users\user\AppData\Local\Packages\Microsoft.Windows.ContentDeliveryManager_cw5n1h2txyewy\AC\BackgroundTransferApi\4aa5b1fb-1301-4194-8203-1cbb67304ae7.e160842f-d7d2-487c-becb-ff7f735e3216.down_meta

Process:	C:\Windows\System32\BackgroundTransferHost.exe
File Type:	data
Category:	dropped
Size (bytes):	1230
Entropy (8bit):	3.6235419859275795
Encrypted:	false
SSDEEP:	24:LLVR2mRiwhXpjgWzgxjX+vUViwjAw2BKsDB1+euEsafxOc2CpX3KsDmbFJruZVB:LLD2mRicXpjPgVX+v8iZvBKQDbrfeIXp
MD5:	3B52759DDB62950FDD73FFE0E7B8A307
SHA1:	356FCD01F5AC95FDEBE645B7EBBA5F6346DDB2B6
SHA-256:	DF771B4E1E0AE7DB1CF36B0DCA500EFF0E6562BFC5F58BF38A04A0E35E9720E0
SHA-512:	68720AEA626BB0CEB4D04823CF9ADE719DC2FF8B83372451AECA3E587DCB5BE00CD7BE38B4965EAE035AD13DB519CE92495E311AD134FC633DDB60171CF0DABB
Malicious:	false
Preview:	h.t.t.p.s.:.//./.i.m.g.-.p.r.o.d.-.c.m.s.-.r.t.-.m.i.c.r.o.s.o.f.t.-.c.o.m...a.k.a.m.a.i.z.e.d...n.e.t./.c.m.s./.a.p.i./.a.m./.i.m.a.g.e.F.i.l.e.D.a.t.a./.R.E.4.Y.z.Z.S.?.v.e.r.=.7.b.4.6...C.o.n.t.e.n.t.-.T.y.p.e.:. .i.m.a.g.e./.j.p.e.g...A.c.c.e.s.s.-.C.o.n.t.r.o.l.-.A.l.l.o.w.-.O.r.i.g.i.n.:. .*...C.o.n.t.e.n.t.-.L.o.c.a.t.i.o.n.:. .h.t.t.p.s.:.//./.i.m.a.g.e...p.r.o.d...c.m.s...r.t...m.i.c.r.o.s.o.f.t...c.o.m./.c.m.s./.a.p.i./.a.m./.i.m.a.g.e.F.i.l.e.D.a.t.a./.R.E.4.Y.z.Z.S.?.v.e.r.=.7.b.4.6...L.a.s.t.-.M.o.d.i.f.i.e.d.:. .M.o.n.,. .0.3. .O.c.t. .2.0.2.2. .1.0.:.0.5.:.3.4. .G.M.T...X.-.S.o.u.r.c.e.-.L.e.n.g.t.h.:. .1.6.5.4.4.8.8...X.-.D.a.t.a.c.e.n.t.e.r.:. .n.o.r.t.h.e.u...X.-.A.c.t.i.v.i.t.y.I.d.:. .f.f.9.4.b.8.f.d.-.1.6.c.b.-.4.a.3.6.-.8.2.b.1.-.e.5.9.8.3.4.4.5.9.0.8.f...T.i.m.i.n.g.-.A.l.l.o.w.-.O.r.i.g.i.n.:. .*...X.-.F.r.a.m.e.-.O.p.t.i.o.n.s.:. .D.E.N.Y...X.-.R.e.s.i.z.e.r.V.e.r.s.i.o.n.:. .1...0...C.o.n.t.e.n.t.-.L.e.n.g.t.h.:. .1.6.5.4.4.8.8...C.a.c.h.e.-.C.o.n.t.r.o.l.:. .p.

C:\Users\user\AppData\Local\Packages\Microsoft.Windows.ContentDeliveryManager_cw5n1h2txyewy\AC\BackgroundTransferApi\4aa5b1fb-1301-4194-8203-1cbb67304ae7.up_meta_secure

Process:	C:\Windows\System32\backgroundTaskHost.exe
File Type:	data
Category:	dropped
Size (bytes):	502
Entropy (8bit):	7.269805200963284
Encrypted:	false
SSDEEP:	12:QU6N355QkpCJrX5hNwLBB5EwCM3Aa9Tg3gyT+UXT:QUq55e/wLB3E5+9TygpUD
MD5:	66D3F7A7F2F4C9A353D053B070431446
SHA1:	628EACB479271620DBF593D6A4395D43465F99B9
SHA-256:	5BE78EBC19D0A5BC10354FC64EB6C2CB7C8FB9763A84B6FB3B5ED201D97C2986
SHA-512:	E5B2D8BAAAAF73DFF1F7A35C3FDB9717C1ECC2F0CA2DBC25619A76E935B1A996DC836EBB23945F9A61CDAB35435D6BDFC2A3C825CB3037381A32F9E890FA5CF5
Malicious:	false
Preview:	.....z..O.....A.n.N...U.s.....f..... .....A$Hur..<..`...3.gMl..... ...3H..lr.B..Z.{..}...(q...@.6$pH. ...(._r..|.....o&..L..Fyg....g.8.....#m.My.|u.$..0..`...o[.....<p..!..Ce.n.8..q.....f.|i.XA.OSV....#d.<vG+HJ.....<.?.:Lt...4.}I. .A...&)...<.....V_a>.~.3.....J..q...U...+.E..1..t.l.Q.>O..[b.. G+.....r+..*w..R.+..G..V.4...[..<T.em.../.[.....iC..hj.G..Z.(.U...@.....ER C.(..`.....&3.X7.....h.@q.nSQ.)_.b1..h..._GB..+.{..)

C:\Users\user\AppData\Local\Packages\Microsoft.Windows.ContentDeliveryManager_cw5n1h2txyewy\AC\BackgroundTransferApi\585053d0-ba98-49e5-b1a4-c6f5d9974c26.efb8d39c-14d5-4f68-9688-1978db758a90.down_meta

Process:	C:\Windows\System32\BackgroundTransferHost.exe
File Type:	data
Category:	dropped
Size (bytes):	1230
Entropy (8bit):	3.593729487352936
Encrypted:	false
SSDEEP:	24:LLVR2mRiwsXpjgWzgxjX+vUViwiAw2BKO1+0+YsafxOc2CpX3KPbGwaVB:LLD2mRixXpjPgVX+v8iUvBKEN3rfeIXJ
MD5:	C3787AE54DB8F9B354295299F9C92DCB
SHA1:	D6E0FC5E90A6D1388BA4B400BA0E8EC042E79D5E
SHA-256:	26950ED11A16146199E0E0BF4F217FAC2992CFD4DDB41C01EED158F5114F4E6B
SHA-512:	5C85EA904FF3257C0A61A7A93183B6741BA61358450433346DC81DB41AB9EE64B6D25F3FFC90A2332E000212F0C56376FDDE713640A2C598E16297AE77D95098
Malicious:	false
Preview:	h.t.t.p.s.:.//./.i.m.g.-.p.r.o.d.-.c.m.s.-.r.t.-.m.i.c.r.o.s.o.f.t.-.c.o.m...a.k.a.m.a.i.z.e.d...n.e.t./.c.m.s./.a.p.i./.a.m./.i.m.a.g.e.F.i.l.e.D.a.t.a./.R.E.4.Y.s.j.y.?.v.e.r.=.4.a.0.6...C.o.n.t.e.n.t.-.T.y.p.e.:. .i.m.a.g.e./.j.p.e.g...A.c.c.e.s.s.-.C.o.n.t.r.o.l.-.A.l.l.o.w.-.O.r.i.g.i.n.:. .*...C.o.n.t.e.n.t.-.L.o.c.a.t.i.o.n.:. .h.t.t.p.s.:.//./.i.m.a.g.e...p.r.o.d...c.m.s...r.t...m.i.c.r.o.s.o.f.t...c.o.m./.c.m.s./.a.p.i./.a.m./.i.m.a.g.e.F.i.l.e.D.a.t.a./.R.E.4.Y.s.j.y.?.v.e.r.=.4.a.0.6...L.a.s.t.-.M.o.d.i.f.i.e.d.:. .M.o.n.,. .0.3. .O.c.t. .2.0.2.2. .1.0.:.0.5.:.3.4. .G.M.T...X.-.S.o.u.r.c.e.-.L.e.n.g.t.h.:. .1.8.2.9.9.9.4...X.-.D.a.t.a.c.e.n.t.e.r.:. .n.o.r.t.h.e.u...X.-.A.c.t.i.v.i.t.y.I.d.:. .0.a.a.6.c.f.7.0.-.b.9.6.6.-.4.9.9.0.-.a.b.1.0.-.e.a.4.b.a.6.e.8.9.0.0.4...T.i.m.i.n.g.-.A.l.l.o.w.-.O.r.i.g.i.n.:. .*...X.-.F.r.a.m.e.-.O.p.t.i.o.n.s.:. .D.E.N.Y...X.-.R.e.s.i.z.e.r.V.e.r.s.i.o.n.:. .1...0...C.o.n.t.e.n.t.-.L.e.n.g.t.h.:. .1.8.2.9.9.9.4...C.a.c.h.e.-.C.o.n.t.r.o.l.:. .p.

C:\Users\user\AppData\Local\Packages\Microsoft.Windows.ContentDeliveryManager_cw5n1h2txyewy\AC\BackgroundTransferApi\585053d0-ba98-49e5-b1a4-c6f5d9974c26.up_meta_secure

Process:	C:\Windows\System32\BackgroundTransferHost.exe
File Type:	data
Category:	dropped
Size (bytes):	502
Entropy (8bit):	7.2558971277972875
Encrypted:	false
SSDEEP:	12:QU6Nk8GuvaljuYNBPw+bWPcbcSegEgEEyzaYRdJn:QUX8Gui9XDdCPcbcrXEy2YRL
MD5:	CED4A764244AD6D3539993F812F02670
SHA1:	D1D3631ED7D56CF12174B61E468B177B98A40B47
SHA-256:	37047289C039B71534073052EE7985D242B2DAB4C28030F056E262A61F9C6123
SHA-512:	27E8BA27F01FA8BB6354C840250E3605746F46884C3130D953EE6AF183D87D369F5D6CBCBDF32A150275EB7B209B4146A5EF6876E04F3B8D79ECC58BF8A3523
Malicious:	false
Preview:	.....z..O.....A.n.N...U.s.....f..... .....N.I.V=J.QMj.&..28a..... .....x....6.....H..y.... ....O..Y#=.z...=3.....ZQ...[SB<_...(..``..m..x..:...MW..]JPm[..A..9|.f..U.>.....L.4.7..hc.K..L.s3...}..jc[h..F....."?W....G-`...7.O:..%=..L4.2..`.....1..j=.<f.h.l..8qf.>...f.7.o..3..*..r..+|.....N...K.....1ys.B..s...T..%....M:r.J...i..V@.'.T.(.. ..;.D..P&.0:.#qW}.....k.P..o..@....:...O..(l..W.wf.r....Cf...L.A.M.+06..A$e.....T+|.:.}0qx~K..

C:\Users\user\AppData\Local\Packages\Microsoft.Windows.ContentDeliveryManager_cw5n1h2txyewy\AC\BackgroundTransferApi\8086b025-ce16-4435-9cc3-d2a0f33fe026.down_data

Process:	C:\Windows\System32\BackgroundTransferHost.exe
File Type:	JPEG image data, Exif standard: [TIFF image data, big-endian, direntries=7, orientation=upper-left, xresolution=98, yresolution=106, resolutionunit=2, software=Adobe Photoshop 21.1 (Windows), datetime=2021:11:11 06:54:34]
Category:	dropped
Size (bytes):	1829994
Entropy (8bit):	7.092403290156545
Encrypted:	false
SSDEEP:	24576:LdC81bzA4GeD+kaZRfEyfcA/ir2/R0JGSUmfyttS6dSTeuErzQP/Lg40bw2Rf02b:LdC81bz/Dq39STvErQ/05d0k
MD5:	4FB1CD4A9C7B4165BF8CD730F367600C
SHA1:	1FD8481802A3512CC65105B600C9339784A31E10
SHA-256:	E60B827FEE4A3A7FF6033C3F244AE04D5A51D7E581936BE750F2EABE4F72E2A0
SHA-512:	C3D101D94A75EFE81C7E8AB1F45654271A67048A6439C2C202589038519D24B62A98F77EA267AE320ED2FC9AFBB7D6C4AE4B079C19AA05E4F7D7BA7A87C79E 1
Malicious:	false
Preview:	......Exif..MM.*.....b.....j.(.....1.....r.2.....i.....'.....'.Adobe Photoshop 21.1 (Windows).2021:11:11 06:54:34.....8.. .....".....*.(.....2.....H.....H.....Adobe_CM.....Adobe.d..... .....Z...."..... ?.....3.....!.1.AQa."q.2.....B#$.R.b34r..C.%.S...cs5....&D.TdE.t6..U.e...u..F'.....Vfv.....7GWg w.....5.....!1..AQaq"..2.....B#.R..3$b.r..CS.cs4.%.....&5..D.T..dEU6te....u..F.....Vfv.....'7GWgw.....?...n.fx..w.V..^N[..k .u....T.y._M.=..$..k.G..gV...i. .4..j.)..k..a~.~.K.2....:..-wc..[....(....X....&y.<...pu..C@..>.J.....k.8.....@..xdx...:.V..X

C:\Users\user\AppData\Local\Packages\Microsoft.Windows.ContentDeliveryManager_cw5n1h2txyewy\AC\BackgroundTransferApi\8086b025-ce16-4435-9cc3-d2a0f33fe026.efb8d39c-14d5-4f68-9688-1978db758a90.down_meta

Process:	C:\Windows\System32\BackgroundTransferHost.exe
File Type:	data
Category:	dropped
Size (bytes):	1230
Entropy (8bit):	3.593729487352936
Encrypted:	false
SSDEEP:	24:LLVR2mRiwsXpjgWzgxjX+vUViwiAw2BKO1+0+YsafxOc2CpX3KPbGwaVB:LLD2mRixXpjPgVX+v8iUvBKEN3rfeIXJ
MD5:	C3787AE54DB8F9B354295299F9C92DCB
SHA1:	D6E0FC5E90A6D1388BA4B400BA0E8EC042E79D5E
SHA-256:	26950ED11A16146199E0E0BF4F217FAC2992CFD4DDB41C01EED158F5114F4E6B
SHA-512:	5C85EA904FF3257C0A61A7A93183B6741BA61358450433346DC81DB41AB9EE64B6D25F3FFC90A2332E000212F0C56376FDDE713640A2C598E16297AE77D95098
Malicious:	false
Preview:	h.t.t.p.s.:.//.i.m.g.-.p.r.o.d.-.c.m.s.-.r.t.-.m.i.c.r.o.s.o.f.t.-.c.o.m...a.k.a.m.a.i.z.e.d...n.e.t./.c.m.s./.a.p.i./.a.m./.i.m.a.g.e.F.i.l.e.D.a.t.a./.R.E.4.Y.s.j.y.?.v.e.r.=.4.a.0.6...C. o.n.t.e.n.t.-.T.y.p.e.:. .i.m.a.g.e./.j.p.e.g...A.c.c.e.s.s.-.C.o.n.t.r.o.l.-.A.l.l.o.w.-.O.r.i.g.i.n.:. .*...C.o.n.t.e.n.t.-.L.o.c.a.t.i.o.n.:. .h.t.t.p.s.:.//.i.m.a.g.e...p.r.o.d...c.m.s...r.t...m. i.c.r.o.s.o.f.t...c.o.m./.c.m.s./.a.p.i./.a.m./.i.m.a.g.e.F.i.l.e.D.a.t.a./.R.E.4.Y.s.j.y.?.v.e.r.=.4.a.0.6...L.a.s.t.-.M.o.d.i.f.i.e.d.:. .M.o.n.,. .0.3. .O.c.t. .2.0.2.2. .1.0.:.0.5.:.3.4. .G.M.T...X.-.S.o.u.r.c.e.-.L.e.n.g.t.h.:. .1.8.2.9.9.9.4...X.-.D.a.t.a.c.e.n.t.e.r.:. .n.o.r.t.h.e.u...X.-.A.c.t.i.v.i.t.y.I.d.:. .0.a.a.6.c.f.7.0.-.b.9.6.6.-.4.9.9.0.-.a.b.1.0.-.e.a.4.b.a. 6.e.8.9.0.0.4...T.i.m.i.n.g.-.A.l.l.o.w.-.O.r.i.g.i.n.:. .*...X.-.F.r.a.m.e.-.O.p.t.i.o.n.s.:. .D.E.N.Y...X.-.R.e.s.i.z.e.r.V.e.r.s.i.o.n.:. .1...0...C.o.n.t.e.n.t.-.L.e.n.g.t.h.:. .1.8.2.9. 9.9.4...C.a.c.h.e.-.C.o.n.t.r.o.l.:. .p.

C:\Users\user\AppData\Local\Packages\Microsoft.Windows.ContentDeliveryManager_cw5n1h2txyewy\AC\BackgroundTransferApi\8086b025-ce16-4435-9cc3-d2a0f33fe026.up_meta_secure

Process:	C:\Windows\System32\backgroundTaskHost.exe
File Type:	data
Category:	dropped
Size (bytes):	502
Entropy (8bit):	7.2558971277972875
Encrypted:	false
SSDEEP:	12:QU6Nk8GuvaljuYNBPw+bWPcbcSegEgEEyzaYRdJn:QUX8Gui9XDdCPcbcrXEy2YRL
MD5:	CED4A764244AD6D3539993F812F02670
SHA1:	D1D3631ED7D56CF12174B61E468B177B98A40B47
SHA-256:	37047289C039B71534073052EE7985D242B2DAB4C28030F056E262A61F9C6123
SHA-512:	27E8BA27F01FA8BB6354C840250E3605746F46884C3130D953EE6AF183D87D369F5D6CBCBDF32A150275EB7B209B4146A5EF6876E04F3B8D79ECC58BF8A3523
Malicious:	false
Preview:	.....z..O.....A.n.N...U.s.....f..... .....N.I.V=J.QMj.&..28a..... .....x....6.....H..y.... ....O..Y#=.z...=3.....ZQ...[SB<_...(..``..m..x...:...MW..]JPm[..A..9|.f..U. >.....L.4.7..hc.K..L.s3...}..jc[h..F....."?W....G-`...7.O:..%=..L4.2..`.....1..j=.<f.h.l..8qf.>...f.7.o..3..*..r..+|.....N...K.....1ys.B..s...T..%....M:r.J...i..V@.'.T.(.. ..;.D..P&.0:.#qW}.....k.P.. o..@....:..O..(l..W.wf.r....Cf...L.A.M.+06..A$e.....T+|.:.}0qx~K..

C:\Users\user\AppData\Local\Packages\Microsoft.Windows.ContentDeliveryManager_cw5n1h2txyewy\AC\BackgroundTransferApi\8d48d2a6-6a56-420d-bb18-5dfe26c1259c.c22ac765-aa10-4c35-8f7c-a01d4239152c.down_meta

Process:	C:\Windows\System32\BackgroundTransferHost.exe

File Type:	data
Category:	dropped
Size (bytes):	1224
Entropy (8bit):	3.615198547271788
Encrypted:	false
SSDEEP:	24:LLVR2mRi5WXpjgWzgxjX+vUVi5u5Bzup1+Zb0IWsafxOc2CpX3zuObB0VB:LLD2mRiEXpjPgVX+v8iM5BqLlb0JrfeR
MD5:	FCE9B615BD0A241DCDB86B117046C824
SHA1:	DA1C473288C318B53360BEA6BFD49A8A95430247
SHA-256:	17B032A7A4C60F0AD0A3C229C7A85C175D02CBA73BF036B0E6A5317BB4A9AFED
SHA-512:	4769E86FFA24DA5ADA5349F28C09623BF0C26BF01F0BD072753EFE147521832A5C5278898C7218AF9DEDD723A293974065F572754C2C0804F9C1CBCF974C9CC
Malicious:	false
Preview:	h.t.t.p.s.:.//./.i.m.g.-.p.r.o.d.-.c.m.s.-.r.t.-.m.i.c.r.o.s.o.f.t.-.c.o.m...a.k.a.m.a.i.z.e.d...n.e.t./.c.m.s./.a.p.i./.a.m./.i.m.a.g.e.F.i.l.e.D.a.t.a./.R.W.E.D.K.u.?.v.e.r.=.7.7.3.7...C.o.n.t.e.n.t.-.T.y.p.e.:. .i.m.a.g.e./.j.p.e.g...A.c.c.e.s.s.-.C.o.n.t.r.o.l.-.A.l.l.o.w.-.O.r.i.g.i.n.:. .*...C.o.n.t.e.n.t.-.L.o.c.a.t.i.o.n.:. .h.t.t.p.s.:.//./.i.m.a.g.e...p.r.o.d...c.m.s...r.t...m.i.c.r.o.s.o.f.t...c.o.m./.c.m.s./.a.p.i./.a.m./.i.m.a.g.e.F.i.l.e.D.a.t.a./.R.W.E.D.K.u.?.v.e.r.=.7.7.3.7...L.a.s.t.-.M.o.d.i.f.i.e.d.:. .S.a.t.,. .1.7. .S.e.p. .2.0.2.2. .1.2.:.4.2.:.3.5. .G.M.T...X.-.S.o.u.r.c.e.-.L.e.n.g.t.h.:. .3.9.7.6.4.0...X.-.D.a.t.a.c.e.n.t.e.r.:. .n.o.r.t.h.e.u...X.-.A.c.t.i.v.i.t.y.I.d.:. .0.f.b.f.8.5.c.1.-.3.a.5.a.-.4.e.4.4.-.8.a.9.f.-.4.c.5.9.9.1.5.9.c.1.5.f...T.i.m.i.n.g.-.A.l.l.o.w.-.O.r.i.g.i.n.:. .*...X.-.F.r.a.m.e.-.O.p.t.i.o.n.s.:. .D.E.N.Y...X.-.R.e.s.i.z.e.r.V.e.r.s.i.o.n.:. .1...0...C.o.n.t.e.n.t.-.L.e.n.g.t.h.:. .3.9.7.6.4.0...C.a.c.h.e.-.C.o.n.t.r.o.l.:. .p.u.b.l.i.

C:\Users\user\AppData\Local\Packages\Microsoft.Windows.ContentDeliveryManager_cw5n1h2txyewy\AC\BackgroundTransferApi\8d48d2a6-6a56-420d-bb18-5dfe26c1259c.up_meta_secure

Process:	C:\Windows\System32\BackgroundTransferHost.exe
File Type:	data
Category:	dropped
Size (bytes):	502
Entropy (8bit):	7.2992415773292185
Encrypted:	false
SSDEEP:	12:QU6N7/eJekA9YsweveCA8PPC+0LxaRGrbyaYwpPfU:QUmOek6Pr2CA8LwQwr9Yw2
MD5:	53C3609CC7AF4DBA67354111D16094BA
SHA1:	C644F7C4E9547328C64A8F3BEFD70A5169F44AAA
SHA-256:	71214DDCE705BF07EC16F43A468E46D6A80F220B0BFA7AECA19C704C365A3F47
SHA-512:	BB8CC703C91A3AD283F403385EC4816CAD73ABFE85CA826C290A3C12044B9468FF9537F80A64CB1F27EE0FB8FB55B5ADF22DA5E20D96AAFFE1653912A817FDD2
Malicious:	false
Preview:	.....z..O.....A.n.N...U.s.....f..... .....].g..g.....O..Gso../..0..... ...2.....eA..2..X/...j^..d.....;. ...O!..n.`.5rFL..o?+..c.&..xg.0|.pk...Q..(t. ....P..X.....,)....H4.QFi;.I.....&....T..x.K._..S..c..Fc#...`.^.....f... +t..QS...v.a.B.t.E...wL9....Z.a(.&(.5 8 .T+1....p.d..'.....{..;y..[..nd...H.~...@.h.T/.I'J.!..@.....C...#P...L*&s.z/Y..c.n. }..o....[.\.....X...].....@.....>l<.0p..}bE...`.t....[L.t. ...T-.Oh3..{V..pP.n+.[._..

C:\Users\user\AppData\Local\Packages\Microsoft.Windows.ContentDeliveryManager_cw5n1h2txyewy\AC\BackgroundTransferApi\aa790838-db48-4eec-9b8a-be8242eb173a.56802ae0-e7ec-49c1-9ab4-e41cf1ffbd66.down_meta

Process:	C:\Windows\System32\BackgroundTransferHost.exe
File Type:	data
Category:	dropped
Size (bytes):	1232
Entropy (8bit):	3.609594899197458
Encrypted:	false
SSDEEP:	24:LLVR2mRiwsL8DWzgx71+gbMVmsafxOc2CpXpjjX+vUViwZBKPX3KUbNbCVB:LLD2mRi18kgvT7rfeIXpjjX+v8iUBKPm
MD5:	94D6269766C4BDEB60E83DEFEA9C4AE8
SHA1:	383EC055E6A59CC3C6B3C8994AA2E4947154D684
SHA-256:	4CD83D88ED67ED332238C8F97C9A6EF86D3A08722846A3CE4CF9C41C6C3FD41D
SHA-512:	6478BFE17F0EE86564D2A775B2EDE3920DFA4C403706B585B8BE107FCA1A31E79A9CFE15464A5E693D3AAB931276119C7D0F380A990CCC504B438DD6FF6171EF
Malicious:	false
Preview:	h.t.t.p.s.:.//./.i.m.g.-.p.r.o.d.-.c.m.s.-.r.t.-.m.i.c.r.o.s.o.f.t.-.c.o.m...a.k.a.m.a.i.z.e.d...n.e.t./.c.m.s./.a.p.i./.a.m./.i.m.a.g.e.F.i.l.e.D.a.t.a./.R.E.4.X.J.8.e.?.v.e.r.=.9.9.3.f...L.a.s.t.-.M.o.d.i.f.i.e.d.:. .W.e.d.,. .2.8. .S.e.p. .2.0.2.2. .0.8.:.0.2.:.1.5. .G.M.T...A.c.c.e.s.s.-.C.o.n.t.r.o.l.-.A.l.l.o.w.-.O.r.i.g.i.n.:. .*...X.-.D.a.t.a.c.e.n.t.e.r.:. .n.o.r.t.h.e.u...X.-.A.c.t.i.v.i.t.y.I.d.:. .9.3.9.a.c.f.2.3.-.1.5.7.8.-.4.6.8.3.-.9.c.d.8.-.8.4.4.3.e.1.e.f.f.f.7.7...T.i.m.i.n.g.-.A.l.l.o.w.-.O.r.i.g.i.n.:. .*...X.-.F.r.a.m.e.-.O.p.t.i.o.n.s.:. .D.E.N.Y...X.-.R.e.s.i.z.e.r.V.e.r.s.i.o.n.:. .1...0...C.o.n.t.e.n.t.-.T.y.p.e.:. .i.m.a.g.e./.j.p.e.g...C.o.n.t.e.n.t.-.L.o.c.a.t.i.o.n.:. .h.t.t.p.s.:.//./.i.m.a.g.e...p.r.o.d...c.m.s...r.t...m.i.c.r.o.s.o.f.t...c.o.m./.c.m.s./.a.p.i./.a.m./.i.m.a.g.e.F.i.l.e.D.a.t.a./.R.E.4.X.J.8.e.?.v.e.r.=.9.9.3.f...X.-.S.o.u.r.c.e.-.L.e.n.g.t.h.:. .1.6.5.2.5.9.5...C.o.n.t.e.n.t.-.L.e.n.g.t.h.:. .1.6.5.2.5.9.5...C.a.c.h.e.-.C.o.n.t.r.o.l.:. .p.

C:\Users\user\AppData\Local\Packages\Microsoft.Windows.ContentDeliveryManager_cw5n1h2txyewy\AC\BackgroundTransferApi\aa790838-db48-4eec-9b8a-be8242eb173a.down_data

Process:	C:\Windows\System32\BackgroundTransferHost.exe

File Type:	JPEG image data, Exif standard: [TIFF image data, big-endian, direntries=7, orientation=upper-left, xresolution=98, yresolution=106, resolutionunit=2, software=Adobe Photoshop 23.2 (Windows), datetime=2022:03:03 09:46:40]
Category:	dropped
Size (bytes):	1652595
Entropy (8bit):	6.7587223054274475
Encrypted:	false
SSDEEP:	24576:d4jNiVr4qVKKSPh75tPWCwK6RinQe53HN/R0JyN2e8Fu06VSshmuOZxtELH9GpmO:d4jNiVr4qo9t5+eFSxtEhamzKj
MD5:	A2EBF8AC1E98A85396D4976E14C07BB0
SHA1:	EB25BA46DEDCB9A54A83DA926B0417EDB08D8F49
SHA-256:	9815B6989D443E6C57C6497EF9439227871E1CDBBF31EF505E2C1CB0C8A647C9
SHA-512:	A7CB9B8BDE6DD85E78DA613FBB34F9ECB32A5A74022567FA344EE4331C55021AADC89685E57446514E28FD179FAF2DD9EC9DF61AA8EDCEDADCEAE7CB0047 66D4
Malicious:	false
Preview:	......Exif..MM.*.....b.....j.(.....1.....r.2.....i.....'.....'.Adobe Photoshop 23.2 (Windows).2022:03:03 09:46:40.....8..... ....."....."....*.(.....2.....f.....H.....H.....Adobe_CM.....Adobe.d..... .....Z..".....?.....3.....!.1.AQa."q.2.....B#$.R.b34r..C.%.S...cs5....&D.TdE.t6..U.e...u..F'.....Vfv.....7GWg w.....5.....!1..AQaq"..2.....B#.R..3$b.r..CS.cs4.%.....&5..D.T..dEU6te....u..F.....Vfv.....'7GWgw.....?..gH....s<..x..4..I...1.6...Z..[V.1.c.xw...S.og..... ...0...k2..e.Y.c.7.]..-.....!.~B.Y.n...O.....w.op.p.?..D..T....8..G.X.....$..f.....U..-.y

C:\Users\user\AppData\Local\Packages\Microsoft.Windows.ContentDeliveryManager_cw5n1h2txyewy\AC\BackgroundTransferApi\aa790838-db48-4eec-9b8a-be8242eb173a.up_meta_secure

Process:	C:\Windows\System32\backgroundTaskHost.exe
File Type:	data
Category:	dropped
Size (bytes):	502
Entropy (8bit):	7.299771858446448
Encrypted:	false
SSDEEP:	12:QU6N7L/A0a05huwq4BTpdY2edfHXmdRoi382teGlWI+:QUx0a0buwqQe2pdRooqOh+
MD5:	A24D374427AF1AB4862B64045D7109EE
SHA1:	550395453ADD226347182AB61A969BA3A479A519
SHA-256:	7128CF988FD86A99BA691E032E09D1737F689E8A90A438D8A3B08A98FA79D255
SHA-512:	398146F31EAB10DC4C889B52786ADA00D1B6ECE2ECDD661299D73A672551C8DACDBE487AE0C20535CC10A2770A1EB4D37A7A51A9C5089707FECBFDA727EAE C13
Malicious:	false
Preview:	.....z..O.....A.n.N...U.s.....f..... ....N.N..pqp..f.Yf['..2U..C...{..... ....@....e.TN...+....90.....y... .....Cd..?.f..YjBX...W.<?.....[Sv$.D.*S....e...}1.+^...R..&z.e.<f.<\.. ,|./t....i.....q.....g.....L...Q.~..WW.).1!SP.j...<".....F".~`)Y"..\H....!..f.....P.f.d..R>...r.....mVq.'.y..%.6.iW.4.Y...L~f..sp.....e5..d.RI.:....ko5.....2..O5..5...c..C.lf...W.1...h..KW.tV.. ....C@...~..>..2...3.*.. E./...y.q.k..%}F...$(.A..D..P...k...D.UKP.$.[

C:\Users\user\AppData\Local\Packages\Microsoft.Windows.ContentDeliveryManager_cw5n1h2txyewy\AC\BackgroundTransferApi\b554ff5d-428f-46a5-8fa9-db35cc2cdf59.e160842f-d7d2-487c-becb-ff7f735e3216.down_meta

Process:	C:\Windows\System32\BackgroundTransferHost.exe
File Type:	data
Category:	dropped
Size (bytes):	1230
Entropy (8bit):	3.6235419859275795
Encrypted:	false
SSDEEP:	24:LLVR2mRiwhXpjgWzgxjX+vUViwjAw2BKsDB1+euEsafxOc2CpX3KsDmbFJruZVB:LLD2mRicXpjPgVX+v8iZvBKQDbrfeIXp
MD5:	3B52759DDB62950FDD73FFE0E7B8A307
SHA1:	356FCD01F5AC95FDEBE645B7EBBA5F6346DDB2B6
SHA-256:	DF771B4E1E0AE7DB1CF36B0DCA500EFF0E6562BFC5F58BF38A04A0E35E9720E0
SHA-512:	68720AEA626BB0CEB4D04823CF9ADE719DC2FF8B83372451AECA3E587DCB5BE00CD7BE38B4965EAE035AD13DB519CE92495E311AD134FC633DDB60171CF0E ABB
Malicious:	false
Preview:	h.t.t.p.s.:.//.i.m.g.-.p.r.o.d.-.c.m.s.-.r.t.-.m.i.c.r.o.s.o.f.t.-.c.o.m...a.k.a.m.a.i.z.e.d...n.e.t./.c.m.s./.a.p.i./.a.m./.i.m.a.g.e.F.i.l.e.D.a.t.a./.R.E.4.Y.z.Z.S.?.v.e.r.=.7.b.4.6...C. o.n.t.e.n.t.-.T.y.p.e.:. .i.m.a.g.e./.j.p.e.g...A.c.c.e.s.s.-.C.o.n.t.r.o.l.-.A.l.l.o.w.-.O.r.i.g.i.n.:. .*...C.o.n.t.e.n.t.-.L.o.c.a.t.i.o.n.:. .h.t.t.p.s.:.//.i.m.a.g.e...p.r.o.d...c.m.s...r.t...m. i.c.r.o.s.o.f.t...c.o.m./.c.m.s./.a.p.i./.a.m./.i.m.a.g.e.F.i.l.e.D.a.t.a./.R.E.4.Y.z.Z.S.?.v.e.r.=.7.b.4.6...L.a.s.t.-.M.o.d.i.f.i.e.d.:. .M.o.n.,. .0.3. .O.c.t. .2.0.2.2. .1.0.:.0.5.:.3.4. .G.M.T...X.-.S.o.u.r.c.e.-.L.e.n.g.t.h.:. .1.6.5.4.4.8.8...X.-.D.a.t.a.c.e.n.t.e.r.:. .n.o.r.t.h.e.u...X.-.A.c.t.i.v.i.t.y.I.d.:. .f.f.9.4.b.8.f.d.-.1.6.c.b.-.4.a.3.6.-.8.2.b.1.-.e.5.9.8.3. 4.4.5.9.0.8.f...T.i.m.i.n.g.-.A.l.l.o.w.-.O.r.i.g.i.n.:. .*...X.-.F.r.a.m.e.-.O.p.t.i.o.n.s.:. .D.E.N.Y...X.-.R.e.s.i.z.e.r.V.e.r.s.i.o.n.:. .1...0...C.o.n.t.e.n.t.-.L.e.n.g.t.h.:. .1.6.5.4.4.8.8...C. a.c.h.e.-.C.o.n.t.r.o.l.:. .p.

C:\Users\user\AppData\Local\Packages\Microsoft.Windows.ContentDeliveryManager_cw5n1h2txyewy\AC\BackgroundTransferApi\b554ff5d-428f-46a5-8fa9-db35cc2cdf59.up_meta_secure

Process:	C:\Windows\System32\BackgroundTransferHost.exe
File Type:	data
Category:	dropped
Size (bytes):	502
Entropy (8bit):	7.269805200963284
Encrypted:	false
SSDEEP:	12:QU6N355QkpCJrX5hNwLBB5EwCM3Aa9Tg3gyT+UXT:QUq55e/wLB3E5+9TygpUD
MD5:	66D3F7A7F2F4C9A353D053B070431446
SHA1:	628EACB479271620DBF593D6A4395D43465F99B9
SHA-256:	5BE78EBC19D0A5BC10354FC64EB6C2CB7C8FB9763A84B6FB3B5ED201D97C2986
SHA-512:	E5B2D8BAAAAF73DFF1F7A35C3FDB9717C1ECC2F0CA2DBC25619A76E935B1A996DC836EBB23945F9A61CDAB35435D6BDFC2A3C825CB3037381A32F9E890FA5CF5
Malicious:	false
Preview:	.....z..O.....A.n.N...U.s.....f..... .....A$Hur..<..`...3.gMl..... ...3H..lr.B..Z.{..}...(q...@.6$pH. ...(._r..|.....o&..L..Fyg....g.8.....#m.My.|u.$..0..`...o[.....<p..!..Ce.n.8..q.....f.|i.XA.OSV....#d.<vG+HJ.....<.?.:Lt...4.}I. .A...&)...<.....V_a>.~.3.....J..q...U...+.E..1..t.l.Q.>O..[b.. G+.....r+..*w..R.+..G..V.4...[..<T.em.../.[.....iC..hj.G..Z.(.U...@.....ER C.(..`.....&3.X7.....h.@q.nSQ.)_.b1..h..._GB..+.{..)

C:\Users\user\AppData\Local\Packages\Microsoft.Windows.ContentDeliveryManager_cw5n1h2txyewy\AC\BackgroundTransferApi\dd6a1354-220a-435c-9960-7f2e2f731c6f.5e70bb71-9767-4cfd-9295-d09782f797ca.down_meta

Process:	C:\Windows\System32\BackgroundTransferHost.exe
File Type:	data
Category:	dropped
Size (bytes):	1232
Entropy (8bit):	3.612607647376319
Encrypted:	false
SSDEEP:	24:LLVR2mRiw+XpjgWzgxjX+vUViwo4+E1BKt1+CsafxOc2CpX3Ki5bvO/QGyV7j:LLD2mRi/XpjPgVX+v8iOPBKvbrfeIX3t
MD5:	20CAF8E9934BC613D1C78271AACCC35C
SHA1:	54067DC0B9689DF0A5EEB87552B2EFD4BF51116E
SHA-256:	A7E00C64022723DA851747B3321E5078CE412B662827B9163C76ABE108B38801
SHA-512:	BA0B8AFF5B21B92F2A6F93E25ACFC53361811C0D94C5D761ADDB15FF93C07939512B9593B0EE33389E36B6D31DCCF6E7CAF2C2678B1868920BA6C3C12DF2286
Malicious:	false
Preview:	h.t.t.p.s.:.//./.i.m.g.-.p.r.o.d.-.c.m.s.-.r.t.-.m.i.c.r.o.s.o.f.t.-.c.o.m...a.k.a.m.a.i.z.e.d...n.e.t./.c.m.s./.a.p.i./.a.m./.i.m.a.g.e.F.i.l.e.D.a.t.a./.R.E.4.Y.3.X.g.?.v.e.r.=.4.b.f.1...C.o.n.t.e.n.t.-.T.y.p.e.:. .i.m.a.g.e./.j.p.e.g...A.c.c.e.s.s.-.C.o.n.t.r.o.l.-.A.l.l.o.w.-.O.r.i.g.i.n.:. .*...C.o.n.t.e.n.t.-.L.o.c.a.t.i.o.n.:. .h.t.t.p.s.:.//./.i.m.a.g.e...p.r.o.d...c.m.s...r.t...m.i.c.r.o.s.o.f.t...c.o.m./.c.m.s./.a.p.i./.a.m./.i.m.a.g.e.F.i.l.e.D.a.t.a./.R.E.4.Y.3.X.g.?.v.e.r.=.4.b.f.1...L.a.s.t.-.M.o.d.i.f.i.e.d.:. .S.u.n.,. .2.5. .S.e.p. .2.0.2.2. .1.9.:.2.9.:.0.6. .G.M.T...X.-.S.o.u.r.c.e.-.L.e.n.g.t.h.:. .1.6.7.0.3.6.6...X.-.D.a.t.a.c.e.n.t.e.r.:. .n.o.r.t.h.e.u...X.-.A.c.t.i.v.i.t.y.I.d.:. .e.0.e.4.2.d.9.4.-.7.4.2.5.-.4.a.6.5.-.b.f.b.1.-.7.4.5.a.8.1.5.0.d.1.b.d...T.i.m.i.n.g.-.A.l.l.o.w.-.O.r.i.g.i.n.:. .*...X.-.F.r.a.m.e.-.O.p.t.i.o.n.s.:. .D.E.N.Y...X.-.R.e.s.i.z.e.r.V.e.r.s.i.o.n.:. .1...0...C.o.n.t.e.n.t.-.L.e.n.g.t.h.:. .1.6.7.0.3.6.6...C.a.c.h.e.-.C.o.n.t.r.o.l.:. .p.

C:\Users\user\AppData\Local\Packages\Microsoft.Windows.ContentDeliveryManager_cw5n1h2txyewy\AC\BackgroundTransferApi\dd6a1354-220a-435c-9960-7f2e2f731c6f.up_meta_secure

Process:	C:\Windows\System32\BackgroundTransferHost.exe
File Type:	data
Category:	dropped
Size (bytes):	502
Entropy (8bit):	7.269579834552022
Encrypted:	false
SSDEEP:	12:QU6N0FTddHZsfPtwSuWawd5n41jrGNaKNtp9Rmy:QUXPHS3iSu0kFutNtp9Rmy
MD5:	07112CA1A43AB14CF7FC496AD8CCF2B9
SHA1:	34524F5C29FC1EDC0E2E4B5B3B17909791455AF7
SHA-256:	24A1BBA0E9E5E6C7C5625B18AC2F4BEBD414D1D163430C3762464913A583A6F5
SHA-512:	13795D08031352F224FD5834D21F7295FFD3A2FE55B85B298845AF40A07FE09F70BE131E3850694998C265D65624DE59423B0495843103E02A151619BD3AF49E
Malicious:	false
Preview:	.....z..O.....A.n.N...U.s.....f..... ...}..b.....^.=K.....F.|L.r..... ...g....bW8.U..E.Y.F.b.o...2. ...4{?.$6Z...l.....b.m..P..P.....D6....>]l`w.K=....P....._.Xe)....B..3.).4..\|....?\|m9U.A.$...a.gj..;)..B....!a.j..ro.4.w3.w..}A..2F.%.....!.}..<..^|r.CZ_...a.E....Z.6... .O.....J...X.Y\.P.?."(-.L.N.zX..84.v;..\Q...I._....._.....c...F...2$...D.....s.....>|...z.}....Z4Yi1..3...@.....F.O.....d..5L.UI..B.D.2.:. ....'-wxY..\I....|.....\...{.

C:\Users\user\AppData\Local\Packages\Microsoft.Windows.ContentDeliveryManager_cw5n1h2txyewy\AC\BackgroundTransferApi\e9594213-9e57-49dd-91fb-0ee2aae6c086.56802ae0-e7ec-49c1-9ab4-e41cf1ffbd66.down_meta

Process:	C:\Windows\System32\BackgroundTransferHost.exe
File Type:	data

Category:	dropped
Size (bytes):	1232
Entropy (8bit):	3.609594899197458
Encrypted:	false
SSDEEP:	24:LLVR2mRiwsL8DWzgx71+gbMVmsafxOc2CpXpjjX+vUViwZBKPX3KUbNbCVB:LLD2mRi18kgvT7rfeIXpjjX+v8iUBKPm
MD5:	94D6269766C4BDEB60E83DEFEA9C4AE8
SHA1:	383EC055E6A59CC3C6B3C8994AA2E4947154D684
SHA-256:	4CD83D88ED67ED332238C8F97C9A6EF86D3A08722846A3CE4CF9C41C6C3FD41D
SHA-512:	6478BFE17F0EE86564D2A775B2EDE3920DFA4C403706B585B8BE107FCA1A31E79A9CFE15464A5E693D3AAB931276119C7D0F380A990CCC504B438DD6FF6171E F
Malicious:	false
Preview:	h.t.t.p.s.:.//.i.m.g.-.p.r.o.d.-.c.m.s.-.r.t.-.m.i.c.r.o.s.o.f.t.-.c.o.m...a.k.a.m.a.i.z.e.d...n.e.t./.c.m.s./.a.p.i./.a.m./.i.m.a.g.e.F.i.l.e.D.a.t.a./.R.E.4.X.J.8.e.?.v.e.r.=.9.9.3.f...L.a.s.t.-.M.o.d.i.f.i.e.d.:. .W.e.d.,. .2.8. .S.e.p. .2.0.2.2. .0.8.:.0.2.:.1.5. .G.M.T...A.c.c.e.s.s.-.C.o.n.t.r.o.l.-.A.l.l.o.w.-.O.r.i.g.i.n.:. .*...X.-.D.a.t.a.c.e.n.t.e.r.:. .n.o.r.t.h.e.u...X.-.A.c.t.i.v.i.t.y.I.d.:. .9.3.9.a.c.f.2.3.-.1.5.7.8.-.4.6.8.3.-.9.c.d.8.-.8.4.4.3.e.1.e.f.f.f.7.7...T.i.m.i.n.g.-.A.l.l.o.w.-.O.r.i.g.i.n.:. .*...X.-.F.r.a.m.e.-.O.p.t.i.o.n.s.:. .D.E.N.Y...X.-.R.e.s.i.z.e.r.V.e.r.s.i.o.n.:. .1...0...C.o.n.t.e.n.t.-.T.y.p.e.:. .i.m.a.g.e./.j.p.e.g...C.o.n.t.e.n.t.-.L.o.c.a.t.i.o.n.:. .h.t.t.p.s.:.//.i.m.a.g.e...p.r.o.d...c.m.s...r.t...m.i.c.r.o.s.o.f.t...c.o.m./.c.m.s./.a.p.i./.a.m./.i.m.a.g.e.F.i.l.e.D.a.t.a./.R.E.4.X.J.8.e.?.v.e.r.=.9.9.3.f...X.-.S.o.u.r.c.e.-.L.e.n.g.t.h.:. .1.6.5.2.5.9.5...C.o.n.t.e.n.t.-.L.e.n.g.t.h.:. .1.6.5.2.5.9.5...C.a.c.h.e.-.C.o.n.t.r.o.l.:. .p.

C:\Users\user\AppData\Local\Packages\Microsoft.Windows.ContentDeliveryManager_cw5n1h2txyewy\AC\BackgroundTransferApi\e9594213-9e57-49dd-91fb-0ee2aae6c086.up_meta_secure

Process:	C:\Windows\System32\BackgroundTransferHost.exe
File Type:	data
Category:	dropped
Size (bytes):	502
Entropy (8bit):	7.299771858446448
Encrypted:	false
SSDEEP:	12:QU6N7L/A0a05huwq4BTpdY2edfHXmdRoi382teGlWI+:QUx0a0buwqQe2pdRooqOh+
MD5:	A24D374427AF1AB4862B64045D7109EE
SHA1:	550395453ADD226347182AB61A969BA3A479A519
SHA-256:	7128CF988FD86A99BA691E032E09D1737F689E8A90A438D8A3B08A98FA79D255
SHA-512:	398146F31EAB10DC4C889B52786ADA00D1B6ECE2ECDD661299D73A672551C8DACDBE487AE0C20535CC10A2770A1EB4D37A7A51A9C5089707FECBFDA727EAE C13
Malicious:	false
Preview:	.....z..O.....A.n.N...U.s.....f..... ....N.N..pqp..f.Yf['..2U..C...{..... ....@....e.TN...+....90.....y... .....Cd..?.f..YjBX...W.<?.....[Sv$.D.*S....e...}1.+^...R..&z.e.<f.<\..,|./t....i.....q.....g.....L...Q.~..WW.).1!SP.j...<".....F".~`)Y"..\H....l..f.....P.f.d..R>...r.....mVq.'.y..%.6.iW.4.Y...L~f..sp.....e5..d.Rl.:....ko5.....2..O5..5...c..C.lf...W.1...h..KW.tV.. ....C@...~..>..2...3.*.. E./...y.q.k..%}F...$(.A..D..P..k...D.UKP.$.[

C:\Users\user\AppData\Local\Packages\Microsoft.Windows.ContentDeliveryManager_cw5n1h2txyewy\AC\BackgroundTransferApi\f9e08879-735a-4e9f-beea-1482341950 53.c22ac765-aa10-4c35-8f7c-a01d4239152c.down_meta

Process:	C:\Windows\System32\BackgroundTransferHost.exe
File Type:	data
Category:	dropped
Size (bytes):	1224
Entropy (8bit):	3.615198547271788
Encrypted:	false
SSDEEP:	24:LLVR2mRi5WXpjgWzgxjX+vUVi5u5Bzup1+Zb0IWsafxOc2CpX3zuObB0VB:LLD2mRiEXpjPgVX+v8iM5BqLlb0JrfeR
MD5:	FCE9B615BD0A241DCDB86B117046C824
SHA1:	DA1C473288C318B53360BEA6BFD49A8A95430247
SHA-256:	17B032A7A4C60F0AD0A3C229C7A85C175D02CBA73BF036B0E6A5317BB4A9AFED
SHA-512:	4769E86FFA24DA5ADA5349F28C09623BF0C26BF01F0BD072753EFE147521832A5C5278898C7218AF9DEDD723A293974065F572754C2C0804F9C1CBCF974C9CC
Malicious:	false
Preview:	h.t.t.p.s.:.//.i.m.g.-.p.r.o.d.-.c.m.s.-.r.t.-.m.i.c.r.o.s.o.f.t.-.c.o.m...a.k.a.m.a.i.z.e.d...n.e.t./.c.m.s./.a.p.i./.a.m./.i.m.a.g.e.F.i.l.e.D.a.t.a./.R.W.E.D.K.u.?.v.e.r.=.7.7.3.7...C.o.n.t.e.n.t.-.T.y.p.e.:. .i.m.a.g.e./.j.p.e.g...A.c.c.e.s.s.-.C.o.n.t.r.o.l.-.A.l.l.o.w.-.O.r.i.g.i.n.:. .*...C.o.n.t.e.n.t.-.L.o.c.a.t.i.o.n.:. .h.t.t.p.s.:.//.i.m.a.g.e...p.r.o.d...c.m.s...r.t...m.i.c.r.o.s.o.f.t...c.o.m./.c.m.s./.a.p.i./.a.m./.i.m.a.g.e.F.i.l.e.D.a.t.a./.R.W.E.D.K.u.?.v.e.r.=.7.7.3.7...L.a.s.t.-.M.o.d.i.f.i.e.d.:. .S.a.t.,. .1.7. .S.e.p. .2.0.2.2. .1.2.:.4.2.:.3.5. .G.M.T...X.-.S.o.u.r.c.e.-.L.e.n.g.t.h.:. .3.9.7.6.4.0...X.-.D.a.t.a.c.e.n.t.e.r.:. .n.o.r.t.h.e.u...X.-.A.c.t.i.v.i.t.y.I.d.:. .0.f.b.f.8.5.c.1.-.3.a.5.a.-.4.e.4.4.-.8.a.9.f.-.4.c.5.9.9.1.5.9.c.1.5.f...T.i.m.i.n.g.-.A.l.l.o.w.-.O.r.i.g.i.n.:. .*...X.-.F.r.a.m.e.-.O.p.t.i.o.n.s.:. .D.E.N.Y...X.-.R.e.s.i.z.e.r.V.e.r.s.i.o.n.:. .1...0...C.o.n.t.e.n.t.-.L.e.n.g.t.h.:. .3.9.7.6.4.0...C.a.c.h.e.-.C.o.n.t.r.o.l.:. .p.u.b.l.i.

C:\Users\user\AppData\Local\Packages\Microsoft.Windows.ContentDeliveryManager_cw5n1h2txyewy\AC\BackgroundTransferApi\f9e08879-735a-4e9f-beea-1482341950 53.down_data

Process:	C:\Windows\System32\BackgroundTransferHost.exe
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 96x96, segment length 16, baseline, precision 8, 1080x1920, components 3

Category:	dropped
Size (bytes):	397640
Entropy (8bit):	7.973540203770047
Encrypted:	false
SSDEEP:	12288:OA4HfjzIA5igAwJiGDW/CXceHRU8755e/2bhC:OA4HfNA0yJs0FU+Te/2bo
MD5:	94F381B1037C31F2F07DA813CB7CDBB0
SHA1:	D3C0DD5BC4181F267D9D33A6C55E720AF4027A61
SHA-256:	E1984ABEC89E01F9CCA9982CA6A1504AC4A6F7E39825617B04F24CD61BFBB91B
SHA-512:	F61E86C8C7519C9B3B21D36430628442CDDFB0A501AB45733C3014854614FC67AD78C0D2F48164AAF5744164BECE936BB4A7CABE8C6CC45E3DB4FD6439F1AC42
Malicious:	false
Preview:	......JFIF.....`.`.....C.....C.....8.."...}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....?....R{T.%i1._.V?...06.....J...m<.M...&.J...4tZ.\i_...b..m.....N.)J..(.....m...'4.....S....i..`v..S...c.A<...F.H9.....5 OZ]...F.K...oJ|.R..I.6...'.&?*v...zM.....75@3m.EI.....F.@\m....]....KO`)0{.+...F.R..E.q.{Q..E.q.}...F.@\n.A...P+...]....h..3h..t.m..W..R.....n.JG.;...@5z....K.....M.....M..j.....q.c.....E?...;..m..i.z..P+.....\n.F>j

C:\Users\user\AppData\Local\Packages\Microsoft.Windows.ContentDeliveryManager_cw5n1h2txyewy\AC\BackgroundTransferApi\f9e08879-735a-4e9f-beea-148234195053.up_meta_secure

Process:	C:\Windows\System32\backgroundTaskHost.exe
File Type:	data
Category:	dropped
Size (bytes):	502
Entropy (8bit):	7.2992415773292185
Encrypted:	false
SSDEEP:	12:QU6N7/eJekA9YsweveCA8PPC+0LxaRGrbyaYwpPfU:QUmOek6Pr2CA8LwQwr9Yw2
MD5:	53C3609CC7AF4DBA67354111D16094BA
SHA1:	C644F7C4E9547328C64A8F3BEFD70A5169F44AAA
SHA-256:	71214DDCE705BF07EC16F43A468E46D6A80F220B0BFA7AECA19C704C365A3F47
SHA-512:	BB8CC703C91A3AD283F403385EC4816CAD73ABFE85CA826C290A3C12044B9468FF9537F80A64CB1F27EE0FB8FB55B5ADF22DA5E20D96AAFFE1653912A817FDD2
Malicious:	false
Preview:	.....z..O.....A.n.N...U.s.....f..... .....].g..g.....O..Gso../..0..... ...2.....eA..2..X/...j^..d.....;. ...O!..n.`.5rFL..o?+..c.&..xg.0|.pk...Q..(t. ....P..X.....,)....H4.QFi;.I.....&....T..x.K.._..S..c..Fc#...`.^.....f... +t..QS...v.a.B.t.E...wL9....Z.a(.&(.5 8 .T+1....p.d..'.....{..;y..[..nd...H.~...@.h.T/.l'J.!..@.....C...#P...L*&s.z/Y..c.n. }..o....[.\.....X....].....@.....>l<.0p..}bE...`.t....[L.t. ...T-.Oh3..{V..pP.n+.[._..

C:\Users\user\AppData\Local\Packages\Microsoft.Windows.ContentDeliveryManager_cw5n1h2txyewy\AC\BackgroundTransferApi\fce64348-a319-4f43-89cb-85a2ff3766b6.5e70bb71-9767-4cfd-9295-d09782f797ca.down_meta

Process:	C:\Windows\System32\BackgroundTransferHost.exe
File Type:	data
Category:	dropped
Size (bytes):	1232
Entropy (8bit):	3.612607647376319
Encrypted:	false
SSDEEP:	24:LLVR2mRiw+XpjgWzgxjX+vUViwo4+E1BKt1+CsafxOc2CpX3Ki5bvO/QGyV7j:LLD2mRi/XpjPgVX+v8iOPBKvbrfeIX3t
MD5:	20CAF8E9934BC613D1C78271AACCC35C
SHA1:	54067DC0B9689DF0A5EEB87552B2EFD4BF51116E
SHA-256:	A7E00C64022723DA851747B3321E5078CE412B662827B9163C76ABE108B38801
SHA-512:	BA0B8AFF5B21B92F2A6F93E25ACFC53361811C0D94C5D761ADDB15FF93C07939512B9593B0EE33389E36B6D31DCCF6E7CAF2C2678B1868920BA6C3C12DF2286
Malicious:	false
Preview:	h.t.t.p.s.:.//.i.m.g.-.p.r.o.d.-.c.m.s.-.r.t.-.m.i.c.r.o.s.o.f.t.-.c.o.m...a.k.a.m.a.i.z.e.d...n.e.t./.c.m.s./.a.p.i./.a.m./.i.m.a.g.e.F.i.l.e.D.a.t.a./.R.E.4.Y.3.X.g.?.v.e.r.=.4.b.f.1...C.o.n.t.e.n.t.-.T.y.p.e.:. .i.m.a.g.e./.j.p.e.g...A.c.c.e.s.s.-.C.o.n.t.r.o.l.-.A.l.l.o.w.-.O.r.i.g.i.n.:. .*...C.o.n.t.e.n.t.-.L.o.c.a.t.i.o.n.:. .h.t.t.p.s.:.//.i.m.a.g.e...p.r.o.d...c.m.s...r.t...m.i.c.r.o.s.o.f.t...c.o.m./.c.m.s./.a.p.i./.a.m./.i.m.a.g.e.F.i.l.e.D.a.t.a./.R.E.4.Y.3.X.g.?.v.e.r.=.4.b.f.1...L.a.s.t.-.M.o.d.i.f.i.e.d.:. .S.u.n.,. .2.5. .S.e.p. .2.0.2.2. .1.9.:.2.9.:.0.6. .G.M.T...X.-.S.o.u.r.c.e.-.L.e.n.g.t.h.:. .1.6.7.0.3.6.6...X.-.D.a.t.a.c.e.n.t.e.r.:. .n.o.r.t.h.e.u...X.-.A.c.t.i.v.i.t.y.I.d.:. .e.0.e.4.2.d.9.4.-.7.4.2.5.-.4.a.6.5.-.b.f.b.1.-.7.4.5.a.8.1.5.0.d.1.b.d...T.i.m.i.n.g.-.A.l.l.o.w.-.O.r.i.g.i.n.:. .*...X.-.F.r.a.m.e.-.O.p.t.i.o.n.s.:. .D.E.N.Y...X.-.R.e.s.i.z.e.r.V.e.r.s.i.o.n.:. .1...0...C.o.n.t.e.n.t.-.L.e.n.g.t.h.:. .1.6.7.0.3.6.6...C.a.c.h.e.-.C.o.n.t.r.o.l.:. .p.

C:\Users\user\AppData\Local\Packages\Microsoft.Windows.ContentDeliveryManager_cw5n1h2txyewy\AC\BackgroundTransferApi\fce64348-a319-4f43-89cb-85a2ff3766b6.down_data

Process:	C:\Windows\System32\BackgroundTransferHost.exe

File Type:	JPEG image data, Exif standard: [TIFF image data, big-endian, direntries=7, orientation=upper-left, xresolution=98, yresolution=106, resolutionunit=2, software=Adobe Photoshop 23.2 (Windows), datetime=2022:03:03 09:45:32]
Category:	dropped
Size (bytes):	1670366
Entropy (8bit):	6.84484961165673
Encrypted:	false
SSDEEP:	24576:+dC81bz/KLQUBy+kzZJsxKdZC/2HO/R0JybmnI4asdAj/5Vf:+dC81bzuyusJdY7
MD5:	AFC98C94747E800CA80B6F2B6F6D0E99
SHA1:	7A2D652D3FBEBAEAC38E68B0EF2704B56AAA3656
SHA-256:	DCF5BB4FBC695E62BA816F65037F27BE9538EEFBED455085DEF9F0C286F0D46D
SHA-512:	B51478D385F934CE7ACE2B602CE5CE929B9091246144B26AE46AC753EA5CE72DB2100C9028A4E70DAA81E9EC3CCC158E1AFEAC8EDD81AF4D11C1DB123F5E 63F
Malicious:	false
Preview:	......Exif..MM.*.....b.....j.(.....1.....r.2.....i.....'.....'.Adobe Photoshop 23.2 (Windows).2022:03:03 09:45:32.....8.. .....".....*.(.....2.....H.....H.....Adobe_CM.....Adobe.d..... .....Z....".....?.....3.....!.1.AQa."q.2.....B#$.R.b34r..C.%.S...cs5....&D.TdE.t6..U.e...u..F'.....Vfv.....7GWg w.....5.....!1..AQaq"..2.....B#.R..3$b.r..CS.cs4.%.....&5..D.T..dEU6te....u..F.....Vfv.....'7GWgw.....?.....n..<.....5c;.....}..5...f7....$.&....[N.+.v.- %...]..Oe..I.....O[.ja.N....ub\.c....Yf5....<.....d.@sA..Lo.....c(....UT...|.w....i.....

C:\Users\user\AppData\Local\Packages\Microsoft.Windows.ContentDeliveryManager_cw5n1h2txyewy\AC\BackgroundTransferApi\fce64348-a319-4f43-89cb-85a2ff3766b6.up_meta_secure

Process:	C:\Windows\System32\backgroundTaskHost.exe
File Type:	data
Category:	dropped
Size (bytes):	502
Entropy (8bit):	7.269579834552022
Encrypted:	false
SSDEEP:	12:QU6N0FTddHZsfPtwSuWawd5n41jrGNaKNtp9Rmy:QUXPHS3iSu0kFutNtp9Rmy
MD5:	07112CA1A43AB14CF7FC496AD8CCF2B9
SHA1:	34524F5C29FC1EDC0E2E4B5B3B17909791455AF7
SHA-256:	24A1BBA0E9E5E6C7C5625B18AC2F4BEBD414D1D163430C3762464913A583A6F5
SHA-512:	13795D08031352F224FD5834D21F7295FFD3A2FE55B85B298845AF40A07FE09F70BE131E3850694998C265D65624DE59423B0495843103E02A151619BD3AF49E
Malicious:	false
Preview:	.....z..O.....A.n.N...U.s.....f..... ...}..b.....^.=K.....F.|L.r..... ...g....bW8.U..E.Y.F.b.o...2. ...4{?.$6Z...l.....b.m..P..P.....D6....>]l`w.K=....P....._.Xe)....B..3.).4. .\|....?\|m9U.A.$...a.gj..;.)..B....!a.j..ro.4.w3.w..}A..2F.%.....!.}..<..^|r.CZ_...a.E....Z.6... .O.....J...X.Y\.P.?."(-.L.N.zX..84.v;..\Q...I._...._.....c...F...2$...D.....s.....>|...z.}....Z4Yi1..3 ...@.....F.O.....d..5L.UI..B.D.2.:. ....'-wxY..\l....|.....\...{.

C:\Users\user\AppData\Local\Packages\Microsoft.Windows.ContentDeliveryManager_cw5n1h2txyewy\LocalState\ContentManagementSDK\Creatives\338387\1667478730 (copy)

Process:	C:\Windows\System32\backgroundTaskHost.exe
File Type:	Unicode text, UTF-16, little-endian text, with very long lines (25333), with no line terminators
Category:	dropped
Size (bytes):	50668
Entropy (8bit):	3.8628690863148045
Encrypted:	false
SSDEEP:	384:LqkpwmyvKwm7t3wmCC6lOaYoCGvgLbuLixSgLldfPOaY3NEoDJjmoKxo9029OaYO:AmQmamCC6mTMes5ldfFOtdz902XX
MD5:	3776917BCA6DD986576E21239AE97F3C
SHA1:	4F08609AF6856B66A9BAF1E6D1C2D0EAA3AB1310
SHA-256:	2B612E3F467B50610CD1BF5A3F0719728388821FBAB925CBA5DFF61B1474E0C8
SHA-512:	2D86E8358C0AE28EE5A467128E581209D65187C878B86517ECF85FB071CCA4E0308EDE6521CD8097F6A43CC150E92C9E8F5D6474BF170D5D049E11985999631A
Malicious:	false
Preview:	..{.".b.a.t.c.h.r.s.p.".:.{.".v.e.r.".:.".1...0.".,.".i.t.e.m.s.".:.[.{.".i.t.e.m.".:.".{.\.".f.\.".:.\.".r.a.f.\.".,.\.".v.\.".:.\.".1...0.\.",.,\.".r.d.r.\.".:.[.{.\.".c.\.".:.\.".C.D.M.\.",.,\.".u.\.".:.\.".S.u.b.s.c. r.i.b.e.d.C.o.n.t.e.n.t.\.".}.],.,\.".a.d.\.".:.{.\.".c.l.a.s.s.\.".:.\.".c.o.n.t.e.n.t.\.".,.\.".c.o.l.l.e.c.t.i.o.n.s.\.".:.[.],.,\.".n.a.m.e.\.".:.\.".L.o.c.k.S.c.r.e.e.n.\.",.,\.".p.r.o.p.e.r.t.y.M.a.n.i.f. e.s.t.\.".:.{.\.".l.a.n.d.s.c.a.p.e.I.m.a.g.e.\.".:.{.\.".t.y.p.e.\.".:.\.".i.m.a.g.e.\.".},.,\.".p.o.r.t.r.a.i.t.I.m.a.g.e.\.".:.{.\.".t.y.p.e.\.".:.\.".i.m.a.g.e.\.".},.,\.".s.h.o.w.I.m.a.g.e.O.n.S.e.c.u.r.e. L.o.c.k.\.".:.{.\.".i.s.O.p.t.i.o.n.a.l.\.".:.t.r.u.e.,.\.".t.y.p.e.\.".:.\.".b.o.o.l.e.a.n.\.".},.,\.".o.n.R.e.n.d.e.r.\.".:.{.\.".t.y.p.e.\.".:.\.".a.c.t.i.o.n.\.".}.},.,\.".p.r.o.p.e.r.t.i.e.s.\.".:.{.\.".l.a.n.d.s.c. a.p.e.I.m.a.g.e.\.".:.{.\.".f.i.l.e.S.i.z.e.\.".:.1.8.2.9.9.9.4.,.\.".h.e.i.g.h.t.\.".:.1.0.8.0.,.\.".s.h.a.2.5.6.\.".:.\.".5.g.u.C.f.+.5.K.

C:\Users\user\AppData\Local\Packages\Microsoft.Windows.ContentDeliveryManager_cw5n1h2txyewy\LocalState\ContentManagementSDK\Creatives\338387\1667478730.~tmp

Process:	C:\Windows\System32\backgroundTaskHost.exe
File Type:	Unicode text, UTF-16, little-endian text, with very long lines (25333), with no line terminators

Category:	dropped
Size (bytes):	50668
Entropy (8bit):	3.8628690863148045
Encrypted:	false
SSDEEP:	384:LqkpwmyvKwm7t3wmCC6lOaYoCGvgLbuLixSgLldfPOaY3NEoDJjmoKxo9029OaYO:AmQmamCC6mTMes5ldfFOtdz902XX
MD5:	3776917BCA6DD986576E21239AE97F3C
SHA1:	4F08609AF6856B66A9BAF1E6D1C2D0EAA3AB1310
SHA-256:	2B612E3F467B50610CD1BF5A3F0719728388821FBAB925CBA5DFF61B1474E0C8
SHA-512:	2D86E8358C0AE28EE5A467128E581209D65187C878B86517ECF85FB071CCA4E0308EDE6521CD8097F6A43CC150E92C9E8F5D6474BF170D5D049E11985999631A
Malicious:	false
Preview:	..{.".b.a.t.c.h.r.s.p.".:.{.".v.e.r.".:.".1...0.".,.".i.t.e.m.s.".:.[.{.".i.t.e.m.".:.".{.\".f.\".:.\".r.a.f.\".,.\".v.\".:.\".1...0.\".,.\".r.d.r.\".:.[.{.\".c.\".:.\".C.D.M.\".,.\".u.\".:.\".S.u.b.s.c.r.i.b.e.d.C.o.n.t.e.n.t.\".}.],.,\".a.d.\".:.{.\".c.l.a.s.s.\".:.\".c.o.n.t.e.n.t.\".,.\".c.o.l.l.e.c.t.i.o.n.s.\".:.[.],.,\".n.a.m.e.\".:.\".L.o.c.k.S.c.r.e.e.n.\".,.\".p.r.o.p.e.r.t.y.M.a.n.i.f.e.s.t.\".:.{.\".I.a.n.d.s.c.a.p.e.I.m.a.g.e.\".:.{.\".t.y.p.e.\".:.\".i.m.a.g.e.\".},.,\".p.o.r.t.r.a.i.t.I.m.a.g.e.\".:.{.\".t.y.p.e.\".:.\".i.m.a.g.e.\".},.,\".s.h.o.w.I.m.a.g.e.O.n.S.e.c.u.r.e.L.o.c.k.\".:.{.\".i.s.O.p.t.i.o.n.a.l.\".:.t.r.u.e.,.\".t.y.p.e.\".:.\".b.o.o.l.e.a.n.\".},.,\".o.n.R.e.n.d.e.r.\".:.{.\".t.y.p.e.\".:.\".a.c.t.i.o.n.\".}.},.,\".p.r.o.p.e.r.t.i.e.s.\".:.{.\".I.a.n.d.s.c.a.p.e.I.m.a.g.e.\".:.{.\".f.i.l.e.S.i.z.e.\".:.1.8.2.9.9.9.4.,.\".h.e.i.g.h.t.\".:.1.0.8.0.,.\".s.h.a.2.5.6.\".:.\".5.g.u.C.f.+.5.K.

C:\Users\user\AppData\Local\Packages\Microsoft.Windows.ContentDeliveryManager_cw5n1h2txyewy\LocalState\ContentManagementSDK\Creatives\338388\eventbeacons.dat (copy)

Process:	C:\Windows\System32\backgroundTaskHost.exe
File Type:	ASCII text, with very long lines (601), with CRLF line terminators
Category:	dropped
Size (bytes):	1206
Entropy (8bit):	5.375635149442958
Encrypted:	false
SSDEEP:	24:2AsfLWhHyUwHqbwB6wwTasfjuAsfLWhHyUwHqbwB6wwTasfjf:psTsyTWHa8uAsTsyTWHa8f
MD5:	6027FD964E3D12F5E55E7F303D62DB64
SHA1:	4584C8EEE83AFC96C0EE6FEF5D24CF79D4AED6C2
SHA-256:	2278FBCA6F5DD52C49BC652BCF24AFC0FAF0643046437E975B24B69FE3C0E0C9
SHA-512:	DB496C3FF495F6BB7447AE273AB7B2E02388163CF6ABFC94643833DBFFF4765B207539587DAC2EC681C099469AD19B74B564C57A2834FBF6F3CDF602559ACB42
Malicious:	false
Preview:	http://https://ris.api.iris.microsoft.com/v1/a/impression?CID=128000000000402926&ion=GB&lang=EN-US%2CEN-GB&oem=&devFam=WINDOWS.DESKTOP&ossku=PROFESSIONAL&cmdVer=10.0.19041.1023&mo=&cap=&EID=&&PID=400089837&UIT=P-&TargetID=700129702&AN=810648797&PG=PC000P0FR5.0000000IRT&REQASID=A673BE2E1D34470DB597AE0CE296C629&UNID=338388&ASID=96bc58feee9343f4adb4276226731ce3&PERSID=A8E1006BB917B201DA028024D9D24847&GLOBALDEVICEID=6825809749837015&LOCALID=w:B4DB5D29-CE1F-133C-E940-0BE8A7B2FF54&DS_EVTID=7d047d8fca6a4380a636a3f3e6e776c5&DEVOSVER=10.0.19042.1165&REQT=20221103T113138&TIME=20221103T123210Z&ARCRAS=&CLR=CDM..https://ris.api.iris.microsoft.com/v1/a/impression?CID=128000000000402926&ion=GB&lang=EN-US%2CEN-GB&oem=&devFam=WINDOWS.DESKTOP&ossku=PROFESSIONAL&cmdVer=10.0.19041.1023&mo=&cap=&EID=&&PID=400089837&UIT=P-&TargetID=700129702&AN=810648797&PG=PC000P0FR5.0000000IRT&REQASID=A673BE2E1D34470DB597AE0CE296C629&UNID=338388&ASID=96bc58feee9343f4adb4276226731ce3&PERSID=A8E1006BB917B201DA028024D9D24847&

C:\Users\user\AppData\Local\Packages\Microsoft.Windows.ContentDeliveryManager_cw5n1h2txyewy\LocalState\ContentManagementSDK\Creatives\338388\eventbeacons.dat.~tmp

Process:	C:\Windows\System32\backgroundTaskHost.exe
File Type:	ASCII text, with very long lines (601), with CRLF line terminators
Category:	dropped
Size (bytes):	1206
Entropy (8bit):	5.375635149442958
Encrypted:	false
SSDEEP:	24:2AsfLWhHyUwHqbwB6wwTasfjuAsfLWhHyUwHqbwB6wwTasfjf:psTsyTWHa8uAsTsyTWHa8f
MD5:	6027FD964E3D12F5E55E7F303D62DB64
SHA1:	4584C8EEE83AFC96C0EE6FEF5D24CF79D4AED6C2
SHA-256:	2278FBCA6F5DD52C49BC652BCF24AFC0FAF0643046437E975B24B69FE3C0E0C9
SHA-512:	DB496C3FF495F6BB7447AE273AB7B2E02388163CF6ABFC94643833DBFFF4765B207539587DAC2EC681C099469AD19B74B564C57A2834FBF6F3CDF602559ACB42
Malicious:	false
Preview:	http://https://ris.api.iris.microsoft.com/v1/a/impression?CID=128000000000402926&ion=GB&lang=EN-US%2CEN-GB&oem=&devFam=WINDOWS.DESKTOP&ossku=PROFESSIONAL&cmdVer=10.0.19041.1023&mo=&cap=&EID=&&PID=400089837&UIT=P-&TargetID=700129702&AN=810648797&PG=PC000P0FR5.0000000IRT&REQASID=A673BE2E1D34470DB597AE0CE296C629&UNID=338388&ASID=96bc58feee9343f4adb4276226731ce3&PERSID=A8E1006BB917B201DA028024D9D24847&GLOBALDEVICEID=6825809749837015&LOCALID=w:B4DB5D29-CE1F-133C-E940-0BE8A7B2FF54&DS_EVTID=7d047d8fca6a4380a636a3f3e6e776c5&DEVOSVER=10.0.19042.1165&REQT=20221103T113138&TIME=20221103T123210Z&ARCRAS=&CLR=CDM..https://ris.api.iris.microsoft.com/v1/a/impression?CID=128000000000402926&ion=GB&lang=EN-US%2CEN-GB&oem=&devFam=WINDOWS.DESKTOP&ossku=PROFESSIONAL&cmdVer=10.0.19041.1023&mo=&cap=&EID=&&PID=400089837&UIT=P-&TargetID=700129702&AN=810648797&PG=PC000P0FR5.0000000IRT&REQASID=A673BE2E1D34470DB597AE0CE296C629&UNID=338388&ASID=96bc58feee9343f4adb4276226731ce3&PERSID=A8E1006BB917B201DA028024D9D24847&

C:\Users\user\AppData\Local\Packages\Microsoft.Windows.ContentDeliveryManager_cw5n1h2txyewy\LocalState\ContentManagementSDK\Creatives\338388\eventbeacons.dat~RFf6a9d0.TMP (copy)

Process:	C:\Windows\System32\backgroundTaskHost.exe
File Type:	ASCII text, with very long lines (601), with CRLF line terminators
Category:	dropped
Size (bytes):	1206
Entropy (8bit):	5.375635149442958
Encrypted:	false
SSDEEP:	24:2AsfLWhHyUwHqbwB6wwTasfjuAsfLWhHyUwHqbwB6wwTasfjf:psTsyTWHa8uAsTsyTWHa8f
MD5:	6027FD964E3D12F5E55E7F303D62DB64
SHA1:	4584C8EEE83AFC96C0EE6FEF5D24CF79D4AED6C2
SHA-256:	2278FBCA6F5DD52C49BC652BCF24AFC0FAF0643046437E975B24B69FE3C0E0C9
SHA-512:	DB496C3FF495F6BB7447AE273AB7B2E02388163CF6ABFC94643833DBFFF4765B207539587DAC2EC681C099469AD19B74B564C57A2834FBF6F3CDF602559ACB42
Malicious:	false
Preview:	http://https://ris.api.iris.microsoft.com/v1/a/impression?CID=128000000000402926&ion=GB&lang=EN-US%2CEN-GB&oem=&devFam=WINDOWS.DESKTOP&ossku=PROFESSIONAL&cmdVer=10.0.19041.1023&mo=&cap=&EID=&&PID=400089837&UIT=P-&TargetID=700129702&AN=810648797&PG=PC000P0FR5.0000000IRT&REQASID=A673BE2E1D34470DB597AE0CE296C629&UNID=338388&ASID=96bc58feee9343f4adb4276226731ce3&PERSID=A8E1006BB917B201DA028024D9D24847&GLOBALDEVICEID=6825809749837015&LOCALID=w:B4DB5D29-CE1F-133C-E940-0BE8A7B2FF54&DS_EVTID=7d047d8fca6a4380a636a3f3e6e776c5&DEVOSVER=10.0.19042.1165&REQT=20221103T113138&TIME=20221103T123210Z&ARCRAS=&CLR=CDM..https://ris.api.iris.microsoft.com/v1/a/impression?CID=128000000000402926&ion=GB&lang=EN-US%2CEN-GB&oem=&devFam=WINDOWS.DESKTOP&ossku=PROFESSIONAL&cmdVer=10.0.19041.1023&mo=&cap=&EID=&&PID=400089837&UIT=P-&TargetID=700129702&AN=810648797&PG=PC000P0FR5.0000000IRT&REQASID=A673BE2E1D34470DB597AE0CE296C629&UNID=338388&ASID=96bc58feee9343f4adb4276226731ce3&PERSID=A8E1006BB917B201DA028024D9D24847&

C:\Users\user\AppData\Local\Packages\Microsoft.Windows.ContentDeliveryManager_cw5n1h2txyewy\LocalState\ContentManagementSDK\Creatives\338388\imprbeacons.dat (copy)

Process:	C:\Windows\System32\backgroundTaskHost.exe
File Type:	ASCII text, with very long lines (1749), with CRLF line terminators
Category:	dropped
Size (bytes):	1751
Entropy (8bit):	5.187469039060151
Encrypted:	false
SSDEEP:	24:28/SgQwCqjJNwB6wwTaseehjhcwhwBMDjkoDUfsLNKomN5rrxZT12KfUNiYsiIj:xx/nJ9HagNLfYsBiLTfUwSa
MD5:	2C93AB13CC18A0981DCBA4DE3AD6CA1C
SHA1:	7029805FC58E10ACC1D0F114FF437282FBDD9155
SHA-256:	35FA3451B626296266258496D5CF9E341CE8175EE37426C21C39434D85A68944
SHA-512:	ECD887D87FD377FC5D3A37D1CDCDF77EBE9172ECE58D26442E95A36F1682A2780A41F7CC9ACE1D23959E070DEC2F4FA070FCA361A7302568F7C2E672BA00E66
Malicious:	false
Preview:	http://https://arc.msn.com/v3/Delivery/Events/Impression=&PID=400089837&TID=700129702&CID=128000000000402926&BID=810648797&PG=PC000P0FR5.0000000IRT&TPID=400089837&REQASID=A673BE2E1D34470DB597AE0CE296C629&ASID=96bc58feee9343f4adb4276226731ce3&TIME=20221103T123210Z&SLOT=1&REQT=20221103T113138&MA_Score=2&PERSID=A8E1006BB917B201DA028024D9D24847&GLOBALDEVICEID=6825809749837015&LOCALID=w:B4DB5D29-CE1F-133C-E940-0BE8A7B2FF54&DS_EVTID=7d047d8fca6a4380a636a3f3e6e776c5&BCNT=1&PG=PC000P0FR5.0000000IRT&UNID=338388&MAP_TID=1EF5E8B5-9E46-4080-B9ED-081BF922B225&NCT=1&PN=DA63DF93-3DBC-42AE-A505-B34988683AC7&ASID=A673BE2E1D34470DB597AE0CE296C629&REQASID=A673BE2E1D34470DB597AE0CE296C629&ARC=1&EMS=1&AUTH=1&LOCALE=EN-US&COUNTRY=GB&HTD=-1&LANG=1033&DEVLANG=EN&CIP=102.129.143.37&ID=A8E1006BB917B201DA028024D9D24847&OPTOUTSTATE=256&HTTPS=1&PRODID=00000000-0000-0000-0000-000000000000&DVTP=2&DEVOSVER=10.0.19042.1165&DEVOSMAJ=10&DEVOSMIN=0&DEVOSBLD=19042&DEVOSMINBLD=1165&LOD=443&LOH=24&LO=637949&RAFB=0&MARKETBASEDCOUNT

C:\Users\user\AppData\Local\Packages\Microsoft.Windows.ContentDeliveryManager_cw5n1h2txyewy\LocalState\ContentManagementSDK\Creatives\338388\imprbeacons.dat.~tmp

Process:	C:\Windows\System32\backgroundTaskHost.exe
File Type:	ASCII text, with very long lines (1749), with CRLF line terminators
Category:	dropped
Size (bytes):	1751
Entropy (8bit):	5.187469039060151
Encrypted:	false
SSDEEP:	24:28/SgQwCqjJNwB6wwTaseehjhcwhwBMDjkoDUfsLNKomN5rrxZT12KfUNiYsiIj:xx/nJ9HagNLfYsBiLTfUwSa
MD5:	2C93AB13CC18A0981DCBA4DE3AD6CA1C
SHA1:	7029805FC58E10ACC1D0F114FF437282FBDD9155

SHA-256:	35FA3451B626296266258496D5CF9E341CE8175EE37426C21C39434D85A68944
SHA-512:	ECD887D87FD377FC5D3A37D1CDCDF77EBE9172ECE58D26442E95A36F1682A2780A41F7CC9ACE1D23959E070DEC2F4FA070FCA361A7302568F7C2E672BA00E66
Malicious:	false
Preview:	http:// https://arc.msn.com/v3/Delivery/Events/Impression=&PID=400089837&TID=700129702&CID=128000000000402926&BID=810648797&PG=PC000P0FR5.0000000IRT&TPID=400089837&REQASID=A673BE2E1D34470DB597AE0CE296C629&ASID=96bc58feee9343f4adb4276226731ce3&TIME=20221103T123210Z&SLOT=1&REQT=20221103T113138&MA_Score=2&PERSID=A8E1006BB917B201DA028024D9D24847&GLOBALDEVICEID=68258097498370158LOCALID=w:B4DB5D29-CE1F-133C-E940-0BE8A7B2FF54&DS_EVTID=7d047d8fca6a4380a636a3f3e6e776c5&BCNT=1&PG=PC000P0FR5.0000000IRT&UNID=338388&MAP_TID=1EF5E8B5-9E46-4080-B9ED-081BF922B225&NCT=1&PN=DA63DF93-3DBC-42AE-A505-B34988683AC7&ASID=A673BE2E1D34470DB597AE0CE296C629&REQASID=A673BE2E1D34470DB597AE0CE296C629&ARC=1&EMS=1&AUTH=1&LOCALE=EN-US&COUNTRY=GB&HTD=-1&LANG=1033&DEVLANG=EN&CIP=102.129.143.37&ID=A8E1006BB917B201DA028024D9D24847&OPTOUTSTATE=256&HTTPS=1&PRODID=00000000-0000-0000-0000-000000000000&DVTP=2&DEVOSVER=10.0.19042.1165&DEVOSMAJ=10&DEVOSMIN=0&DEVOSBLD=19042&DEVOSMINBLD=1165&LOD=443&LOH=24&LO=637949&RAFB=0&MARKETBASEDCOUNT

C:\Users\user\AppData\Local\Packages\Microsoft.Windows.ContentDeliveryManager_cw5n1h2txyewy\LocalState\ContentManagementSDK\Creatives\88000045\1667478730 (copy)

Process:	C:\Windows\System32\backgroundTaskHost.exe
File Type:	Unicode text, UTF-16, little-endian text, with very long lines (3298), with no line terminators
Category:	dropped
Size (bytes):	6598
Entropy (8bit):	3.8115883227521836
Encrypted:	false
SSDEEP:	192:Lv44wFiEMGyoO4XD3gyeXonj4fjkwRcmtGw:L6yGBRvuNtGw
MD5:	B235E75FBC79F8026E7C60436D985965
SHA1:	DB1961A8DD30D0B3C3987A9E768ED6542CCFE798
SHA-256:	7CA22885B25318C77E3A20E6A534BEECB32F63D1FD0877E5D6AC827B45B21C34
SHA-512:	9804B766E35CA7E2F1C354908A2D84D1CFA5BB1AEB2D8E734E7457B41C22E80DC78222257BE4D9EE16AEC7CCAF365F97AEC1E5E74F934B40897FC353BB6A6D85
Malicious:	false
Preview:	..{.".b.a.t.c.h.r.s.p.".:.{.".v.e.r.".:.".1...0.".,.".i.t.e.m.s.".:.[.{.".i.t.e.m.".:.".{.\".f.\".:.\".r.a.f.\".,.\".v.\".:.\".1...0.\".,.\".r.d.r.\".:.[.{.\".c.\".:.\".C.D.M.\".,.\".u.\".:.\".S.u.b.s.c.r.i.b.e.d.C.o.n.t.e.n.t.\".}.],.\".a.d.\".:.{.\".c.l.a.s.s.\".:.\".c.o.n.t.e.n.t.\".,.\".c.o.l.l.e.c.t.i.o.n.s.\".:.[.],.\".i.t.e.m.P.r.o.p.e.r.t.y.M.a.n.i.f.e.s.t.\".:.{.\".n.o.O.p.\".:.{.\".t.y.p.e.\".:.\".a.c.t.i.o.n.\".}.},.\".i.t.e.m.s.\".:.[.{.\".p.r.o.p.e.r.t.i.e.s.\".:.{.\".n.o.O.p.\".:.{.\".e.v.e.n.t.\".:.\".n.o.n.e.\".,.\".p.a.r.a.m.e.t.e.r.s.\".:.{.},.,.\".a.c.t.i.o.n.\".:.\".n.o.O.p.\".}.},.\".t.r.a.c.k.i.n.g.\".:.{.\".e.v.e.n.t.s.\".:.[.{.\".i.d.\".:.\".i.m.p.r.e.s.s.i.o.n.\".}.],.\".p.a.r.a.m.e.t.e.r.i.z.e.d.\".:.[.{.\".u.r.i.\".:.\".h.t.t.p.s.:.\./.\./.r.i.s...a.p.i...i.r.i.s...m.i.c.r.o.s.o.f.t...c.o.m.\./.v.1.\./.a.\./.{.A.C.T.I.O.N.}.?.C.I.D.=.1.2.8.0.0.0.0.0.0.0.0.1.6.2.7.4.0.9.&.r.e.g.i.o.n.=.G.B.&.l.

C:\Users\user\AppData\Local\Packages\Microsoft.Windows.ContentDeliveryManager_cw5n1h2txyewy\LocalState\ContentManagementSDK\Creatives\88000045\1667478730.~tmp

Process:	C:\Windows\System32\backgroundTaskHost.exe
File Type:	Unicode text, UTF-16, little-endian text, with very long lines (3298), with no line terminators
Category:	dropped
Size (bytes):	6598
Entropy (8bit):	3.8115883227521836
Encrypted:	false
SSDEEP:	192:Lv44wFiEMGyoO4XD3gyeXonj4fjkwRcmtGw:L6yGBRvuNtGw
MD5:	B235E75FBC79F8026E7C60436D985965
SHA1:	DB1961A8DD30D0B3C3987A9E768ED6542CCFE798
SHA-256:	7CA22885B25318C77E3A20E6A534BEECB32F63D1FD0877E5D6AC827B45B21C34
SHA-512:	9804B766E35CA7E2F1C354908A2D84D1CFA5BB1AEB2D8E734E7457B41C22E80DC78222257BE4D9EE16AEC7CCAF365F97AEC1E5E74F934B40897FC353BB6A6D85
Malicious:	false
Preview:	..{.".b.a.t.c.h.r.s.p.".:.{.".v.e.r.".:.".1...0.".,.".i.t.e.m.s.".:.[.{.".i.t.e.m.".:.".{.\".f.\".:.\".r.a.f.\".,.\".v.\".:.\".1...0.\".,.\".r.d.r.\".:.[.{.\".c.\".:.\".C.D.M.\".,.\".u.\".:.\".S.u.b.s.c.r.i.b.e.d.C.o.n.t.e.n.t.\".}.],.\".a.d.\".:.{.\".c.l.a.s.s.\".:.\".c.o.n.t.e.n.t.\".,.\".c.o.l.l.e.c.t.i.o.n.s.\".:.[.],.\".i.t.e.m.P.r.o.p.e.r.t.y.M.a.n.i.f.e.s.t.\".:.{.\".n.o.O.p.\".:.{.\".t.y.p.e.\".:.\".a.c.t.i.o.n.\".}.},.\".i.t.e.m.s.\".:.[.{.\".p.r.o.p.e.r.t.i.e.s.\".:.{.\".n.o.O.p.\".:.{.\".e.v.e.n.t.\".:.\".n.o.n.e.\".,.\".p.a.r.a.m.e.t.e.r.s.\".:.{.},.,.\".a.c.t.i.o.n.\".:.\".n.o.O.p.\".}.},.\".t.r.a.c.k.i.n.g.\".:.{.\".e.v.e.n.t.s.\".:.[.{.\".i.d.\".:.\".i.m.p.r.e.s.s.i.o.n.\".}.],.\".p.a.r.a.m.e.t.e.r.i.z.e.d.\".:.[.{.\".u.r.i.\".:.\".h.t.t.p.s.:.\./.\./.r.i.s...a.p.i...i.r.i.s...m.i.c.r.o.s.o.f.t...c.o.m.\./.v.1.\./.a.\./.{.A.C.T.I.O.N.}.?.C.I.D.=.1.2.8.0.0.0.0.0.0.0.0.1.6.2.7.4.0.9.&.r.e.g.i.o.n.=.G.B.&.l.

C:\Users\user\AppData\Local\Packages\Microsoft.Windows.ContentDeliveryManager_cw5n1h2txyewy\LocalState\TargetedContentCache\v3\280815\9dbf5cda030a4e60a261641156804856_1 (copy)

Process:	C:\Windows\System32\backgroundTaskHost.exe
File Type:	JSON data
Category:	dropped
Size (bytes):	1765

Entropy (8bit):	5.589251299472814
Encrypted:	false
SSDEEP:	48:YrLtp5jEi8kLsPSVZGcuDieRHFzkwhSgNPUV:Ev5gjshZGDZuGSgNPUV
MD5:	F3F1CC40AF34CBC0A78B3408B31631F0
SHA1:	E613A2B2B79CACAF7B274EC0F7C401CD0D7BB80C
SHA-256:	29A9061FAA1C52D4E50476DC7ED84401E14FAE066935F91C97B0825F351CE2E5
SHA-512:	34ED34EDB12439BCDD00905651856652159B083151EE12CEE05AB291C76AB82CECE43F4BEEB2D0EE0C9E962FDFA044D9BE82580FA8BC57492731F082BA9B6337
Malicious:	false
Preview:	{"class":"content","collections":[],"itemPropertyManifest":{"noOp":{"type":"action"}},"items":[{"properties":{"noOp":{"event":"none","parameters":{"ctx.action":"noOp","ctx.containerPath":"//item[0]","ctx.contentId":"9dbf5cda030a4e60a261641156804856","ctx.creativeId":"1667478696`128000000001627409`0`9dbf5cda030a4e60a261641156804856`604800`280815`137271744000000000","ctx.cv":"vMqjYPUZwU+dfMfc.0","ctx.expiration":"137271744000000000","ctx.placementId":"SubscribedContent-280815","noOp":"//item[0]/property[noOp]"},"action":"noOp"}},"tracking":{"events":[{"id":"//item[0]?eventName=impression","name":"impression"}],"parameterized":[{"uri":"https://ris.api.iris.microsoft.com/v1/a/{ACTION}?CID=128000000001627409&region=GB&lang=EN-US%2CEN-GB&oem=&devFam=WINDOWS.DESKTOP&ossku=PROFESSIONAL&cmdVer=10.0.19041.1023&mo=&cap=&EID={EID}&&PID=425116123&UIT=P-&TargetID=700333390&AN=57390238&PG=PC000P0FR5.000000000INM&REQASID=BC595D179AA34712BB1EB30ACBBCDBC0&UNID=280815&ID=A8E1006BB917B201DA028024D9D24847&AS

C:\Users\user\AppData\Local\Packages\Microsoft.Windows.ContentDeliveryManager_cw5n1h2txyewy\LocalState\TargetedContentCache\v3\280815\9dbf5cda030a4e60a261641156804856_1.~tmp

Process:	C:\Windows\System32\backgroundTaskHost.exe
File Type:	JSON data
Category:	dropped
Size (bytes):	1765
Entropy (8bit):	5.589251299472814
Encrypted:	false
SSDEEP:	48:YrLtp5jEi8kLsPSVZGcuDieRHFzkwhSgNPUV:Ev5gjshZGDZuGSgNPUV
MD5:	F3F1CC40AF34CBC0A78B3408B31631F0
SHA1:	E613A2B2B79CACAF7B274EC0F7C401CD0D7BB80C
SHA-256:	29A9061FAA1C52D4E50476DC7ED84401E14FAE066935F91C97B0825F351CE2E5
SHA-512:	34ED34EDB12439BCDD00905651856652159B083151EE12CEE05AB291C76AB82CECE43F4BEEB2D0EE0C9E962FDFA044D9BE82580FA8BC57492731F082BA9B6337
Malicious:	false
Preview:	{"class":"content","collections":[],"itemPropertyManifest":{"noOp":{"type":"action"}},"items":[{"properties":{"noOp":{"event":"none","parameters":{"ctx.action":"noOp","ctx.containerPath":"//item[0]","ctx.contentId":"9dbf5cda030a4e60a261641156804856","ctx.creativeId":"1667478696`128000000001627409`0`9dbf5cda030a4e60a261641156804856`604800`280815`137271744000000000","ctx.cv":"vMqjYPUZwU+dfMfc.0","ctx.expiration":"137271744000000000","ctx.placementId":"SubscribedContent-280815","noOp":"//item[0]/property[noOp]"},"action":"noOp"}},"tracking":{"events":[{"id":"//item[0]?eventName=impression","name":"impression"}],"parameterized":[{"uri":"https://ris.api.iris.microsoft.com/v1/a/{ACTION}?CID=128000000001627409&region=GB&lang=EN-US%2CEN-GB&oem=&devFam=WINDOWS.DESKTOP&ossku=PROFESSIONAL&cmdVer=10.0.19041.1023&mo=&cap=&EID={EID}&&PID=425116123&UIT=P-&TargetID=700333390&AN=57390238&PG=PC000P0FR5.000000000INM&REQASID=BC595D179AA34712BB1EB30ACBBCDBC0&UNID=280815&ID=A8E1006BB917B201DA028024D9D24847&AS

C:\Users\user\AppData\Local\Packages\Microsoft.Windows.ContentDeliveryManager_cw5n1h2txyewy\LocalState\TargetedContentCache\v3\338388\96bc58feee9343f4adb4276226731ce3_1 (copy)

Process:	C:\Windows\System32\backgroundTaskHost.exe
File Type:	JSON data
Category:	dropped
Size (bytes):	3399
Entropy (8bit):	5.649193848711768
Encrypted:	false
SSDEEP:	48:YrfBVUdGEFZ8Ht35cLsRkT+Ha8uDwsKkTJsuDxHaHn4FzkuLsRkT+Ha8uDCo0U/:KVySHt35EnZj88xgHnhunZjmpU/
MD5:	584C23585E9708AD7C1AEBFB8AE84ADD
SHA1:	D86FBE6C9A75624DA1E6FE8EF6352B0EB1DC22DC
SHA-256:	03E90F3EACA529DDCFB10BF15925FF410D11550D4B2B161A63FD55190E2D51DB
SHA-512:	FA7E78C8D01482BA59C91276B99FFE3AF173D3D6E97625E92C5B7D6B5E50CEF92C20D97EFCDA7A750CE38C697AECD8F5CC893912F3AAC181BCFDFFF1CDAE3E84
Malicious:	false
Preview:	{"class":"content","collections":[],"itemPropertyManifest":{"templateType":{"type":"text"},"onRender":{"type":"action"}},"items":[{"properties":{"templateType":{"text":"hidden"},"onRender":{"event":"none","parameters":{"collectionId":"Start.Suggestions","ctx.action":"addTileToCollection","ctx.containerPath":"//item[0]","ctx.contentId":"96bc58feee9343f4adb4276226731ce3","ctx.creativeId":"1667478697`128000000000402926`0`96bc58feee9343f4adb4276226731ce3`3600`338388`1372708794000000000","ctx.cv":"Qk3e8FposEiXXDUU.0","ctx.expiration":"137270879400000000","ctx.placementId":"SubscribedContent-338388","onRender":"//item[0]/property[onRender]","templateType":"hidden"},"action":"addTileToCollection"}},"tracking":{"events":[{"id":"//item[0]?eventName=impression","name":"impression"},{"id":"//item[0]?eventName=click","name":"click"},{"id":"//item[0]?eventName=install","name":"install"},{"id":"//item[0]?eventName=installComplete","name":"installComplete"},{"id":"//item[0]?eventName=dislike","name":"

C:\Users\user\AppData\Local\Packages\Microsoft.Windows.ContentDeliveryManager_cw5n1h2txyewy\LocalState\TargetedContentCache\v3\338388\96bc58feee9343f4adb4276226731ce3_1.~tmp

Process:	C:\Windows\System32\backgroundTaskHost.exe
File Type:	JSON data
Category:	dropped
Size (bytes):	3399
Entropy (8bit):	5.649193848711768
Encrypted:	false
SSDEEP:	48:YrfBVUdGEFZ8Ht35cLsRkT+Ha8uDwsKkTJsuDxHaHn4FzkuLsRkT+Ha8uDCo0U/:KVySHt35EnZj88xgHnhunZjmpU/
MD5:	584C23585E9708AD7C1AEBFB8AE84ADD
SHA1:	D86FBE6C9A75624DA1E6FE8EF6352B0EB1DC22DC
SHA-256:	03E90F3EACA529DDCFB10BF15925FF410D11550D4B2B161A63FD55190E2D51DB
SHA-512:	FA7E78C8D01482BA59C91276B99FFE3AF173D3D6E97625E92C5B7D6B5E50CEF92C20D97EFCDA7A750CE38C697AECD8F5CC893912F3AAC181BCFDFFF1CDAE3E84
Malicious:	false
Preview:	{"class":"content","collections":[],"itemPropertyManifest":{"templateType":{"type":"text"},"onRender":{"type":"action"}},"items":[{"properties":{"templateType":{"text":"hidden"},"onRender":{"event":"none","parameters":{"collectionId":"Start.Suggestions","ctx.action":"addTileToCollection","ctx.containerPath":"//item[0]","ctx.contentId":"96bc58feee9343f4adb4276226731ce3","ctx.creativeId":"1667478697`128000000000402926`0`96bc58feee9343f4adb4276226731ce3`3600`338388`1372708794000000","ctx.cv":"Qk3e8FposEiXXDUU.0","ctx.expiration":"137270879400000000","ctx.placementId":"SubscribedContent-338388","onRender":"//item[0]/property[onRender]","templateType":"hidden"},"action":"addTileToCollection"}},"tracking":{"events":[{"id":"//item[0]?eventName=impression","name":"impression"},{"id":"//item[0]?eventName=click","name":"click"},{"id":"//item[0]?eventName=install","name":"install"},{"id":"//item[0]?eventName=installComplete","name":"installComplete"},{"id":"//item[0]?eventName=dislike","name":"

C:\Users\user\AppData\Local\Packages\Microsoft.Windows.ContentDeliveryManager_cw5n1h2txyewy\LocalState\TargetedContentCache\v3\338389\03d0615dae6b45498e652e3e555b3e3d_1 (copy)

Process:	C:\Windows\System32\backgroundTaskHost.exe
File Type:	JSON data
Category:	dropped
Size (bytes):	1767
Entropy (8bit):	5.577925996504267
Encrypted:	false
SSDEEP:	48:YrLtLku8kLsPSR5NuDiemHFzkwhkKQyUs:ENkPslueuGkuUs
MD5:	F475EFAFBB0FAB970B2FA43682541384
SHA1:	A8C2A3C78EAEDCE3A3B81A2D3A3E7B26BD94AEE8
SHA-256:	633F87D55B480221AD0E76D1A5CEC296BD4115EA1770A3C2E0B8CE0EDD3B7A43
SHA-512:	6F64E07F6E630A2C753D56B16D8F8357D9C6DC3C90CB23E5BC347FC530F988D72F4759FCB91115A5020E8C7915107995C3242AC3FB0EF5A7D48F5DC2805A8EF
Malicious:	false
Preview:	{"class":"content","collections":[],"itemPropertyManifest":{"noOp":{"type":"action"}},"items":[{"properties":{"noOp":{"event":"none","parameters":{"ctx.action":"noOp","ctx.containerPath":"//item[0]","ctx.contentId":"03d0615dae6b45498e652e3e555b3e3d","ctx.creativeId":"1667478696`128000000001627409`0`03d0615dae6b45498e652e3e555b3e3d`604800`338389`137271744000000000","ctx.cv":"49s6YbKJiUGNere0.0","ctx.expiration":"137271744000000000","ctx.placementId":"SubscribedContent-338389","noOp":"//item[0]/property[noOp]"},"action":"noOp"}},"tracking":{"events":[{"id":"//item[0]?eventName=impression","name":"impression"}],"parameterized":[{"uri":"https://ris.api.iris.microsoft.com/v1/a/{ACTION}?CID=128000000001627409&region=GB&lang=EN-US%2CEN-GB&oem=&devFam=WINDOWS.DESKTOP&ossku=PROFESSIONAL&cmdVer=10.0.19041.1023&mo=&cap=&EID={EID}&&PID=425116219&UIT=P-&TargetID=700333446&AN=1262935398&PG=PC000P0FR5.0000000IRU&REQASID=75EF775624424489969BB6FE3EAA1836&UNID=338389&ID=A8E1006BB917B201DA028024D9D24847&

C:\Users\user\AppData\Local\Packages\Microsoft.Windows.ContentDeliveryManager_cw5n1h2txyewy\LocalState\TargetedContentCache\v3\338389\03d0615dae6b45498e652e3e555b3e3d_1.~tmp

Process:	C:\Windows\System32\backgroundTaskHost.exe
File Type:	JSON data
Category:	dropped
Size (bytes):	1767
Entropy (8bit):	5.577925996504267
Encrypted:	false
SSDEEP:	48:YrLtLku8kLsPSR5NuDiemHFzkwhkKQyUs:ENkPslueuGkuUs
MD5:	F475EFAFBB0FAB970B2FA43682541384
SHA1:	A8C2A3C78EAEDCE3A3B81A2D3A3E7B26BD94AEE8
SHA-256:	633F87D55B480221AD0E76D1A5CEC296BD4115EA1770A3C2E0B8CE0EDD3B7A43
SHA-512:	6F64E07F6E630A2C753D56B16D8F8357D9C6DC3C90CB23E5BC347FC530F988D72F4759FCB91115A5020E8C7915107995C3242AC3FB0EF5A7D48F5DC2805A8EF
Malicious:	false

Preview:	{"class":"content","collections":[],"itemPropertyManifest":{"noOp":{"type":"action"}},"items":[{"properties":{"noOp":{"event":"none","parameters":{"ctx.action":"noOp","ctx.containerPath":"//item[0]","ctx.contentId":"03d0615dae6b45498e652e3e555b3e3d","ctx.creativeId":"1667478696`1280000000001627409`0`03d0615dae6b45498e652e3e555b3e3d`604800`338389`137271744000000000","ctx.cv":"49s6YbKJiUGNere0.0","ctx.expiration":"137271744000000000","ctx.placementId":"SubscribedContent-338389","noOp":"//item[0]/property[noOp]"},"action":"noOp"}},"tracking":{"events":[{"id":"//item[0]?eventName=impression","name":"impression"}],"parameterized":[{"uri":"https://ris.api.iris.microsoft.com/v1/a/{ACTION}?CID=12800000000001627409&region=GB&lang=EN-US%2CEN-GB&oem=&devFam=WINDOWS.DESKTOP&ossku=PROFESSIONAL&cmdVer=10.0.19041.1023&mo=&cap=&EID={EID}&&PID=425116219&UIT=P-&TargetID=700333446&AN=1262935398&PG=PC000P0FR5.0000000IRU&REQASID=75EF775624424489969BB6FE3EAA1836&UNID=338389&ID=A8E1006BB917B201DA028024D9D24847&

C:\Users\user\AppData\Local\Temp\nsdCB34.tmp\System.dll

Process:	C:\Users\user\Desktop\CONTRACT_REVISED-SHIPMENT-DOCUMENTS_EXPORTS_REFERENCE-QT63637-02993900299348.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	12288
Entropy (8bit):	5.737556724687435
Encrypted:	false
SSDEEP:	192:MenY0qWTlt70lAj/lQ0sEWc/wtYbBH2aDybC7y+XBaIwL:M8+Qlt70Fj/lQRY/9VjjgL
MD5:	6E55A6E7C3FDBD244042EB15CB1EC739
SHA1:	070EA80E2192ABC42F358D47B276990B5FA285A9
SHA-256:	ACF90AB6F4EDC687E94AAF604D05E16E6CFB5E35873783B50C66F307A35C6506
SHA-512:	2D504B74DA38EDC967E3859733A2A9CACD885DB82F0CA69BFB66872E882707314C54238344D45945DC98BAE85772ACEEF71A741787922D640627D3C8AE8F1C3
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0% • Antivirus: Virustotal, Detection: 1%, Browse • Antivirus: Metadefender, Detection: 4%, Browse
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....qr*.5.D.5.D.5.D...J.2.D.5.E.!.D.....2.D.a0t.1.D.V1n.4.D..3@.4.D.Rich5.D.....PE..L...X..`.....!.....".....)....@.....p.....@.....B.....@..P.....`.....@..X.....text...O ....."..... ..`.rdata..c....@.....&.....@..@.data...x....P.....*.....@....reloc.....`.....,.....@..B.....

C:\Users\user\AppData\Roaming\Shoved\Factorist\dialog-warning-symbolic.symbolic.png

Process:	C:\Users\user\Desktop\CONTRACT_REVISED-SHIPMENT-DOCUMENTS_EXPORTS_REFERENCE-QT63637-02993900299348.exe
File Type:	PNG image data, 16 x 16, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	286
Entropy (8bit):	6.880810677512409
Encrypted:	false
SSDEEP:	6:6v/lhPysDQqinrW8/97kGwr/F+Elz3hsKrnLluYK/SwtNVp:6v/7ZiK817kG3Mz3ZliSoN7
MD5:	03DEC13C99CA8B2766C9B4468E0E781B
SHA1:	DA2202AF040D5494D7281FAB003C748457255CEE
SHA-256:	DEBC1949821086D01AE4A60BFFF1A73CFF47E7AB100E9028556496C254C05655
SHA-512:	566533ABC453A817570660154026D2206866073AB28CA6243C15AFF6A57C4A8B686EB7F23B4161EF4AE2A2C5C71F3DD6FD7271F4667A8C2E606D7CA19CC71FE
Malicious:	false
Preview:	.PNG.....IHDR.....a....sBIT....|.d.....IDAT8...?J.A.....A...../.%.2....<.....6...H..i..-.'Eva.qw_`.|.3.0.s.....O_2..Y=....p..N..].J.....t.Q6..y... ..u.....|.u....1.D..b...2|..H.....HS]=...~.M..$.>q.....|..wq.~vZ.|a..f..Tg.x._|....IEND.B`.

C:\Users\user\AppData\Roaming\Shoved\skrupforelskede.bin

Process:	C:\Users\user\Desktop\CONTRACT_REVISED-SHIPMENT-DOCUMENTS_EXPORTS_REFERENCE-QT63637-02993900299348.exe
File Type:	data
Category:	dropped
Size (bytes):	106887
Entropy (8bit):	7.75553468119485
Encrypted:	false
SSDEEP:	1536:bYpDSzihO1IsnBzEfH5ZR0fha22stcSuYZtL+8VdfWuZTJrBWmlRsMM:mDcgO1IeQfH5ZRXstcgKodfhrBBDM
MD5:	73A6739AA8670352F00CA22E28B2E5E3
SHA1:	14B5E6BB7FA6A534D9CCB20C19F57D82C8C8D634
SHA-256:	1E182B58911811ED9709B682EFE83DD96093AC013DA58698D2687E526E4D3B96
SHA-512:	46D0E7F0B7EC4042B66B0CF98076D9E59157B3A011A9EB2E1238D4B5B579B9B9194F257F3B6DB9191F66F135232B0D9DA85360CBC8F87B612847FAE471083971
Malicious:	false
Preview:	Tw8... .....x.q.f..a.!..P.....r...D..L.i.:....D...|..$d.....u.....<..g..b..`.....3...<....;.....^.....#.....;<._.....W<V....s.w.....5XU....F...5G*6.<Q..%-L...<...,-...C....y5.....<`.....[1.....`@.....@..m<s@.....@<L..K=L...u..W.....l.....`]h.Q..&.-.X[?S..;.c..vh..^.!....o.....ue.@....C&<..}....G/.E....N.b.Sx.k..*.0..-.V..F.....gCV....a$r".q..<2)..@^$.i ...5./.Y...z'...5)jJI..:.J.[S.....`e.D_(.yp.[?....A..6uD7+.....WHf..Vp....\g.8.;....k.9....Z.W....8D.+..+..+..+..+..+..+..+..+..+..+..~..{.q...p...9..t...G.X.e.X.\..D.V...8H.+..+..+..+..+..+..+..+..+..+..+..+..~p....W...qr..?...|.]q,..t.2.....!0I.V...q.C..I..A-.'R..*.....pf...'..q.%.....V.!>...4.....,;c.....5\%\q/.]..Y.....W..p.a...%.?. &...`.u/E..R.]h.h.b....~p...5P..|V....m.W.~....n.`.....&.I5v..E.a.q..E..?.....U.....Uz...~p.e...~p..U.i..(.c..`.....5...a.|V.....@|N.....|.X..V..h.a... &

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive
Entropy (8bit):	7.688048037898308
TrID:	• Win32 Executable (generic) a (10002005/4) 99.96% • Generic Win/DOS Executable (2004/3) 0.02% • DOS Executable Generic (2002/1) 0.02% • Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00%
File name:	CONTRACT_REVISED-SHIPMENT-DOCUMENTS_EXPORTS_REFERENCE-QT63637-02993900299348.exe
File size:	236896
MD5:	045f22ce9be3d33b07a00780ee66fcfd
SHA1:	91b74e75d55c33d8d82b10bed51ca7d3ad80147c
SHA256:	e05ec32c2edc10b6917a3cbcac9d823cb37db908cc51f3ec459800992e2b8b37
SHA512:	c363c64fe3b52d615601810b577168be5b3339ba6bde011ae0c76bbee76718782f8b737b0c9f6d82d34197045ce1c35389cba26622349bb2c0c77f62ed29d063
SSDEEP:	6144:vT4DtMeWIPR0PVPCespE0s67yIMYxrzWJougaEzEk:vTpeZ00SI18ogC
TLSH:	2134014177B5C463ED564A30C813A7F2A9B97C11D9E89F4707423E8EBC76382DA1A32D
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....1...Pf..Pf..Pf.*_9..Pf..Pg.LPf.*_;..Pf..sV..Pf..V`..Pf.Rich.Pf.....PE..L...P..`.....h.....

File Icon

Icon Hash:	879b931b3bb3b393

Static PE Info

General

Entrypoint:	0x4034c5
Entrypoint Section:	.text
Digitally signed:	true
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	RELOCS_STRIPPED, EXECUTABLE_IMAGE, LINE_NUMS_STRIPPED, LOCAL_SYMS_STRIPPED, 32BIT_MACHINE
DLL Characteristics:	DYNAMIC_BASE, NX_COMPAT, NO_SEH, TERMINAL_SERVER_AWARE
Time Stamp:	0x60FC9250 [Sat Jul 24 22:21:04 2021 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	6e7f9a29f2c85394521a08b9f31f6275

Authenticode Signature

Signature Valid:	**false**
Signature Issuer:	OU="Squatterism Autodialing ", E=Wirestitched@Longobardian.No, O=driftier, L=West Tarbert, S=Scotland, C=GB
Signature Validation Error:	**A certificate chain processed, but terminated in a root certificate which is not trusted by the trust provider**
Error Number:	-2146762487
Not Before, Not After	• 17/07/2022 17:44:12 16/07/2025 17:44:12
Subject Chain	• OU="Squatterism Autodialing ", E=Wirestitched@Longobardian.No, O=driftier, L=West Tarbert, S=Scotland, C=GB
Version:	3
Thumbprint MD5:	CE0B0A248006454637FB21369D393B35
Thumbprint SHA-1:	FDB8159D5CAE5E96B90D0300979493249FE76435
Thumbprint SHA-256:	67AA1334C6C443A496FCD527B5F1A30A2CA661AC20D33E7BCCADEF6982D2575C

Serial:	33616A6CE5467077

Entrypoint Preview
Instruction
sub esp, 000002D4h
push ebx
push esi
push edi
push 00000020h
pop edi
xor ebx, ebx
push 00008001h
mov dword ptr [esp+14h], ebx
mov dword ptr [esp+10h], 0040A2E0h
mov dword ptr [esp+1Ch], ebx
call dword ptr [004080CCh]
call dword ptr [004080D0h]
and eax, BFFFFFFFh
cmp ax, 00000006h
mov dword ptr [00434F0Ch], eax
je 00007FF0B0CBF363h
push ebx
call 00007FF0B0CC2651h
cmp eax, ebx
je 00007FF0B0CBF359h
push 00000C00h
call eax
mov esi, 004082B0h
push esi
call 00007FF0B0CC25CBh
push esi
call dword ptr [00408154h]
lea esi, dword ptr [esi+eax+01h]
cmp byte ptr [esi], 00000000h
jne 00007FF0B0CBF33Ch
push 0000000Bh
call 00007FF0B0CC2624h
push 00000009h
call 00007FF0B0CC261Dh
push 00000007h
mov dword ptr [00434F04h], eax
call 00007FF0B0CC2611h
cmp eax, ebx
je 00007FF0B0CBF361h
push 0000001Eh
call eax
test eax, eax
je 00007FF0B0CBF359h
or byte ptr [00434F0Fh], 00000040h
push ebp
call dword ptr [00408038h]
push ebx
call dword ptr [00408298h]
mov dword ptr [00434FD8h], eax
push ebx
lea eax, dword ptr [esp+34h]
push 000002B4h
push eax
push ebx
push 0042B228h

Instruction
call dword ptr [0040818Ch]
push 0040A2C8h

Rich Headers

Programming Language:	• [EXP] VC++ 6.0 SP5 build 8804

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x8610	0xa0	.rdata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x7e000	0x147e8	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x37ca8	0x20b8	.ndata
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x8000	0x2b0	.rdata
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x6793	0x6800	False	0.6720628004807693	data	6.495258513279076	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
.rdata	0x8000	0x14a4	0x1600	False	0.4385653409090909	data	5.01371465125838	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0xa000	0x2b018	0x600	False	0.5240885416666666	data	4.155579717739458	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.ndata	0x36000	0x48000	0x0	False	0	empty	0.0	IMAGE_SCN_CNT_UNINITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.rsrc	0x7e000	0x147e8	0x14800	False	0.8290658346036586	data	7.314494987254223	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_BITMAP	0x7e4f0	0x368	Device independent bitmap graphic, 96 x 16 x 4, image size 768	English	United States
RT_ICON	0x7e858	0x820b	PNG image data, 256 x 256, 8-bit/color RGBA, non-interlaced	English	United States
RT_ICON	0x86a68	0x39ac	PNG image data, 256 x 256, 8-bit colormap, non-interlaced	English	United States
RT_ICON	0x8a418	0x25a8	Device independent bitmap graphic, 48 x 96 x 32, image size 9600	English	United States
RT_ICON	0x8c9c0	0x14fa	PNG image data, 256 x 256, 4-bit colormap, non-interlaced	English	United States
RT_ICON	0x8dec0	0x10a8	Device independent bitmap graphic, 32 x 64 x 32, image size 4224	English	United States
RT_ICON	0x8ef68	0xea8	Device independent bitmap graphic, 48 x 96 x 8, image size 2304	English	United States
RT_ICON	0x8fe10	0x8a8	Device independent bitmap graphic, 32 x 64 x 8, image size 1024	English	United States
RT_ICON	0x906b8	0x668	Device independent bitmap graphic, 48 x 96 x 4, image size 1152	English	United States

Name	RVA	Size	Type	Language	Country
RT_ICON	0x90d20	0x568	Device independent bitmap graphic, 16 x 32 x 8, image size 256	English	United States
RT_ICON	0x91288	0x468	Device independent bitmap graphic, 16 x 32 x 32, image size 1088	English	United States
RT_ICON	0x916f0	0x2e8	Device independent bitmap graphic, 32 x 64 x 4, image size 512	English	United States
RT_ICON	0x919d8	0x128	Device independent bitmap graphic, 16 x 32 x 4, image size 128	English	United States
RT_DIALOG	0x91b00	0x144	data	English	United States
RT_DIALOG	0x91c48	0x13c	data	English	United States
RT_DIALOG	0x91d88	0x100	data	English	United States
RT_DIALOG	0x91e88	0x11c	data	English	United States
RT_DIALOG	0x91fa8	0xc4	data	English	United States
RT_DIALOG	0x92070	0xb6	data	English	United States
RT_DIALOG	0x92128	0x60	data	English	United States
RT_GROUP_ICON	0x92188	0xae	data	English	United States
RT_VERSION	0x92238	0x270	data	English	United States
RT_MANIFEST	0x924a8	0x33e	XML 1.0 document, ASCII text, with very long lines (830), with no line terminators	English	United States

Imports

DLL	Import
ADVAPI32.dll	RegCreateKeyExW, RegEnumKeyW, RegQueryValueExW, RegSetValueExW, RegCloseKey, RegDeleteValueW, RegDeleteKeyW, AdjustTokenPrivileges, LookupPrivilegeValueW, OpenProcessToken, SetFileSecurityW, RegOpenKeyExW, RegEnumValueW
SHELL32.dll	SHGetSpecialFolderLocation, SHFileOperationW, SHBrowseForFolderW, SHGetPathFromIDListW, ShellExecuteExW, SHGetFileInfoW
ole32.dll	OleInitialize, OleUninitialize, CoCreateInstance, IIDFromString, CoTaskMemFree
COMCTL32.dll	ImageList_Create, ImageList_Destroy, ImageList_AddMasked
USER32.dll	GetClientRect, EndPaint, DrawTextW, IsWindowEnabled, DispatchMessageW, wsprintfA, CharNextA, CharPrevW, MessageBoxIndirectW, GetDlgItemTextW, SetDlgItemTextW, GetSystemMetrics, FillRect, AppendMenuW, TrackPopupMenu, OpenClipboard, SetClipboardData, CloseClipboard, IsWindowVisible, CallWindowProcW, GetMessagePos, CheckDlgButton, LoadCursorW, SetCursor, GetWindowLongW, GetSysColor, SetWindowPos, PeekMessageW, SetClassLongW, GetSystemMenu, EnableMenuItem, GetWindowRect, ScreenToClient, EndDialog, RegisterClassW, SystemParametersInfoW, CreateWindowExW, GetClassInfoW, DialogBoxParamW, CharNextW, ExitWindowsEx, DestroyWindow, CreateDialogParamW, SetTimer, SetWindowTextW, PostQuitMessage, SetForegroundWindow, ShowWindow, wsprintfW, SendMessageTimeoutW, FindWindowExW, IsWindow, GetDlgItem, SetWindowLongW, LoadImageW, GetDC, ReleaseDC, EnableWindow, InvalidateRect, SendMessageW, DefWindowProcW, BeginPaint, EmptyClipboard, CreatePopupMenu
GDI32.dll	SetBkMode, SetBkColor, GetDeviceCaps, CreateFontIndirectW, CreateBrushIndirect, DeleteObject, SetTextColor, SelectObject
KERNEL32.dll	GetExitCodeProcess, WaitForSingleObject, GetModuleHandleA, GetProcAddress, GetSystemDirectoryW, lstrcatW, Sleep, lstrcpyA, WriteFile, GetTempFileNameW, CreateFileW, lstrcmpiA, RemoveDirectoryW, CreateProcessW, CreateDirectoryW, GetLastError, CreateThread, GlobalLock, GlobalUnlock, GetDiskFreeSpaceW, WideCharToMultiByte, lstrcpynW, lstrlenW, SetErrorMode, GetVersion, GetCommandLineW, GetTempPathW, GetWindowsDirectoryW, SetEnvironmentVariableW, ExitProcess, CopyFileW, GetCurrentProcess, GetModuleFileNameW, GetFileSize, GetTickCount, MulDiv, SetFileAttributesW, GetFileAttributesW, SetCurrentDirectoryW, MoveFileW, GetFullPathNameW, GetShortPathNameW, SearchPathW, CompareFileTime, SetFileTime, CloseHandle, lstrcmpiW, lstrcmpW, ExpandEnvironmentStringsW, GlobalFree, GlobalAlloc, GetModuleHandleW, LoadLibraryExW, MoveFileExW, FreeLibrary, WritePrivateProfileStringW, GetPrivateProfileStringW, lstrlenA, MultiByteToWideChar, ReadFile, SetFilePointer, FindClose, FindNextFileW, FindFirstFileW, DeleteFileW

Possible Origin

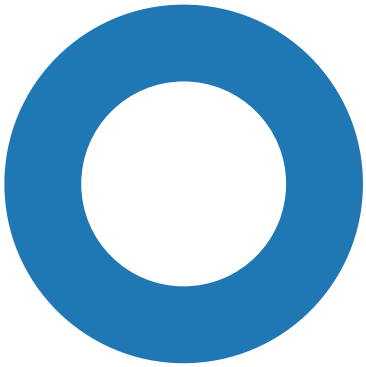
Language of compilation system	Country where language is spoken	Map
English	United States	

Network Behavior

No network behavior found

Statistics

Behavior



- CONTRACT_REVISED-SHIPMENT..
- dllhost.exe
- backgroundTaskHost.exe
- dllhost.exe
- BackgroundTransferHost.exe
- BackgroundTransferHost.exe
- ieinstal.exe
- ieinstal.exe
- ieinstal.exe
- ieinstal.exe
- ieinstal.exe
- ieinstal.exe
- ieinstal.exe
- ieinstal.exe
- ieinstal.exe
- ieinstal.exe
- ielowutil.exe
- ielowutil.exe
- ielowutil.exe
- ielowutil.exe
- ielowutil.exe
- ielowutil.exe
- ielowutil.exe
- ielowutil.exe
- ielowutil.exe
- ielowutil.exe
- ExtExport.exe
- ExtExport.exe
- ExtExport.exe
- ExtExport.exe
- ExtExport.exe
- ExtExport.exe
- ExtExport.exe
- ExtExport.exe
- ExtExport.exe
- backgroundTaskHost.exe

Click to jump to process

System Behavior

Analysis Process: CONTRACT_REVISED-SHIPMENT-DOCUMENTS_EXPORTS_REFERENCE-QT63637-02993900299348.exe

PID: **4848**, Parent PID: **4788**

General

Target ID:	2
Start time:	12:31:58
Start date:	03/11/2022
Path:	C:\Users\user\Desktop\CONTRACT_REVISED-SHIPMENT-DOCUMENTS_EXPORTS_REFERENCE-QT63637-02993900299348.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\CONTRACT_REVISED-SHIPMENT-DOCUMENTS_EXPORTS_REFERENCE-QT63637-02993900299348.exe
Imagebase:	0x400000
File size:	236896 bytes
MD5 hash:	045F22CE9BE3D33B07A00780EE66FCFD
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_GuLoader_2, Description: Yara detected GuLoader, Source: 00000002.00000002.110030353777.0000000002B90000.00000040.00000800.00020000.00000000.sdmp, Author: Joe Security
Reputation:	low

File Activities

Registry Activities

Analysis Process: dllhost.exe PID: **2364**, Parent PID: **812**

General

Target ID:	3
Start time:	12:31:58
Start date:	03/11/2022
Path:	C:\Windows\System32\dllhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\DllHost.exe /Processid:{AB8902B4-09CA-4BB6-B78D-A8F59079A8D5}
Imagebase:	0x7ff612890000
File size:	21312 bytes
MD5 hash:	08EB78E5BE019DF044C26B14703BD1FA
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	moderate

Analysis Process: backgroundTaskHost.exe PID: **4408**, Parent PID: **812**

General

Target ID:	4
Start time:	12:32:09
Start date:	03/11/2022
Path:	C:\Windows\System32\backgroundTaskHost.exe
Wow64 process (32bit):	false
Commandline:	"C:\WINDOWS\system32\backgroundTaskHost.exe" -ServerName:App.AppXmtcan0h2tfbfy7k9kn8hbxb6dmzz1zh0.mca
Imagebase:	0x7ff618d70000
File size:	19776 bytes
MD5 hash:	DA7063B17DBB8BBB3015351016868006
Has elevated privileges:	false
Has administrator privileges:	false
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	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

File Path	Offset	Length	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: dllhost.exe PID: **4508**, Parent PID: **812**

General	
Target ID:	5
Start time:	12:32:10
Start date:	03/11/2022
Path:	C:\Windows\System32\dllhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\DllHost.exe /Processid:{AB8902B4-09CA-4BB6-B78D-A8F59079A8D5}
Imagebase:	0x7ff612890000
File size:	21312 bytes
MD5 hash:	08EB78E5BE019DF044C26B14703BD1FA
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	moderate

Analysis Process: BackgroundTransferHost.exe PID: **4480**, Parent PID: **812**

General	
Target ID:	7
Start time:	12:32:11
Start date:	03/11/2022
Path:	C:\Windows\System32\BackgroundTransferHost.exe
Wow64 process (32bit):	false
Commandline:	"BackgroundTransferHost.exe" -ServerName:BackgroundTransferHost.1
Imagebase:	0x7ff609480000
File size:	37376 bytes
MD5 hash:	C5D813D92E83CDE3FECD9343933E3421
Has elevated privileges:	false
Has administrator privileges:	false
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	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

Analysis Process: BackgroundTransferHost.exe PID: **5560**, Parent PID: **812**

General	
Target ID:	8
Start time:	12:32:14
Start date:	03/11/2022
Path:	C:\Windows\System32\BackgroundTransferHost.exe
Wow64 process (32bit):	false

Commandline:	"BackgroundTransferHost.exe" -ServerName:BackgroundTransferHost.1
Imagebase:	0x7ff609480000
File size:	37376 bytes
MD5 hash:	C5D813D92E83CDE3FECD9343933E3421
Has elevated privileges:	false
Has administrator privileges:	false
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

Analysis Process: ieinstal.exe PID: 5400, Parent PID: 4848

General

Target ID:	9
Start time:	12:32:28
Start date:	03/11/2022
Path:	C:\Program Files (x86)\Internet Explorer\ieinstal.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\Desktop\CONTRACT_REVISED-SHIPMENT-DOCUMENTS_EXPORTS_REFERENCE-QT63637-02993900299348.exe
Imagebase:	0x570000
File size:	480256 bytes
MD5 hash:	7871873BABCEA94FBA13900B561C7C55
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: ieinstal.exe PID: 1820, Parent PID: 4848

General

Target ID:	10
Start time:	12:32:29
Start date:	03/11/2022
Path:	C:\Program Files (x86)\Internet Explorer\ieinstal.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\Desktop\CONTRACT_REVISED-SHIPMENT-DOCUMENTS_EXPORTS_REFERENCE-QT63637-02993900299348.exe
Imagebase:	0x570000
File size:	480256 bytes
MD5 hash:	7871873BABCEA94FBA13900B561C7C55
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: ieinstal.exe PID: 6908, Parent PID: 4848

General

Target ID:	11
Start time:	12:32:29
Start date:	03/11/2022
Path:	C:\Program Files (x86)\Internet Explorer\ieinstal.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\Desktop\CONTRACT_REVISED-SHIPMENT-DOCUMENTS_EXPORTS_REFERENCE-QT63637-02993900299348.exe
Imagebase:	0x570000

File size:	480256 bytes
MD5 hash:	7871873BABCEA94FBA13900B561C7C55
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: ieinstal.exe PID: **1396**, Parent PID: **4848**

General	
Target ID:	12
Start time:	12:32:29
Start date:	03/11/2022
Path:	C:\Program Files (x86)\Internet Explorer\ieinstal.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\Desktop\CONTRACT_REVISED-SHIPMENT-DOCUMENTS_EXPORTS_REFERENCE-QT63637-02993900299348.exe
Imagebase:	0x570000
File size:	480256 bytes
MD5 hash:	7871873BABCEA94FBA13900B561C7C55
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: ieinstal.exe PID: **4268**, Parent PID: **4848**

General	
Target ID:	13
Start time:	12:32:29
Start date:	03/11/2022
Path:	C:\Program Files (x86)\Internet Explorer\ieinstal.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\Desktop\CONTRACT_REVISED-SHIPMENT-DOCUMENTS_EXPORTS_REFERENCE-QT63637-02993900299348.exe
Imagebase:	0x570000
File size:	480256 bytes
MD5 hash:	7871873BABCEA94FBA13900B561C7C55
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: ieinstal.exe PID: **4772**, Parent PID: **4848**

General	
Target ID:	14
Start time:	12:32:30
Start date:	03/11/2022
Path:	C:\Program Files (x86)\Internet Explorer\ieinstal.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\Desktop\CONTRACT_REVISED-SHIPMENT-DOCUMENTS_EXPORTS_REFERENCE-QT63637-02993900299348.exe
Imagebase:	0x570000
File size:	480256 bytes
MD5 hash:	7871873BABCEA94FBA13900B561C7C55
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: ieinstal.exe PID: **7620**, Parent PID: **4848**

General	
Target ID:	15
Start time:	12:32:30
Start date:	03/11/2022
Path:	C:\Program Files (x86)\Internet Explorer\ieinstal.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\Desktop\CONTRACT_REVISED-SHIPMENT-DOCUMENTS_EXPORTS_REFERENCE-QT63637-02993900299348.exe
Imagebase:	0x570000
File size:	480256 bytes
MD5 hash:	7871873BABCEA94FBA13900B561C7C55
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: ieinstal.exe PID: **6588**, Parent PID: **4848**

General	
Target ID:	16
Start time:	12:32:30
Start date:	03/11/2022
Path:	C:\Program Files (x86)\Internet Explorer\ieinstal.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\Desktop\CONTRACT_REVISED-SHIPMENT-DOCUMENTS_EXPORTS_REFERENCE-QT63637-02993900299348.exe
Imagebase:	0x570000
File size:	480256 bytes
MD5 hash:	7871873BABCEA94FBA13900B561C7C55
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: ieinstal.exe PID: **3156**, Parent PID: **4848**

General	
Target ID:	17
Start time:	12:32:31
Start date:	03/11/2022
Path:	C:\Program Files (x86)\Internet Explorer\ieinstal.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\Desktop\CONTRACT_REVISED-SHIPMENT-DOCUMENTS_EXPORTS_REFERENCE-QT63637-02993900299348.exe
Imagebase:	0x570000
File size:	480256 bytes
MD5 hash:	7871873BABCEA94FBA13900B561C7C55
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: ieinstal.exe PID: **5924**, Parent PID: **4848**

General	
Target ID:	18
Start time:	12:32:31
Start date:	03/11/2022
Path:	C:\Program Files (x86)\Internet Explorer\ieinstal.exe
Wow64 process (32bit):	false

Commandline:	C:\Users\user\Desktop\CONTRACT_REVISED-SHIPMENT-DOCUMENTS_EXPORTS_REFERENCE-QT63637-02993900299348.exe
Imagebase:	0x570000
File size:	480256 bytes
MD5 hash:	7871873BABCEA94FBA13900B561C7C55
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: ieinstal.exe PID: **3988**, Parent PID: **4848**

General	
Target ID:	19
Start time:	12:32:31
Start date:	03/11/2022
Path:	C:\Program Files (x86)\Internet Explorer\ieinstal.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\Desktop\CONTRACT_REVISED-SHIPMENT-DOCUMENTS_EXPORTS_REFERENCE-QT63637-02993900299348.exe
Imagebase:	0x570000
File size:	480256 bytes
MD5 hash:	7871873BABCEA94FBA13900B561C7C55
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: ielowutil.exe PID: **7732**, Parent PID: **4848**

General	
Target ID:	20
Start time:	12:32:31
Start date:	03/11/2022
Path:	C:\Program Files (x86)\Internet Explorer\ielowutil.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\Desktop\CONTRACT_REVISED-SHIPMENT-DOCUMENTS_EXPORTS_REFERENCE-QT63637-02993900299348.exe
Imagebase:	0x520000
File size:	221696 bytes
MD5 hash:	650FE7460630188008BF8C8153526CEB
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: ielowutil.exe PID: **4760**, Parent PID: **4848**

General	
Target ID:	21
Start time:	12:32:32
Start date:	03/11/2022
Path:	C:\Program Files (x86)\Internet Explorer\ielowutil.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\Desktop\CONTRACT_REVISED-SHIPMENT-DOCUMENTS_EXPORTS_REFERENCE-QT63637-02993900299348.exe
Imagebase:	0x520000
File size:	221696 bytes
MD5 hash:	650FE7460630188008BF8C8153526CEB
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: ielowutil.exe PID: **7756**, Parent PID: **4848**

General	
Target ID:	22
Start time:	12:32:32
Start date:	03/11/2022
Path:	C:\Program Files (x86)\Internet Explorer\ielowutil.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\Desktop\CONTRACT_REVISED-SHIPMENT-DOCUMENTS_EXPORTS_REFERENCE-QT63637-02993900299348.exe
Imagebase:	0x520000
File size:	221696 bytes
MD5 hash:	650FE7460630188008BF8C8153526CEB
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: ielowutil.exe PID: **4612**, Parent PID: **4848**

General	
Target ID:	23
Start time:	12:32:32
Start date:	03/11/2022
Path:	C:\Program Files (x86)\Internet Explorer\ielowutil.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\Desktop\CONTRACT_REVISED-SHIPMENT-DOCUMENTS_EXPORTS_REFERENCE-QT63637-02993900299348.exe
Imagebase:	0x520000
File size:	221696 bytes
MD5 hash:	650FE7460630188008BF8C8153526CEB
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: ielowutil.exe PID: **3852**, Parent PID: **4848**

General	
Target ID:	24
Start time:	12:32:33
Start date:	03/11/2022
Path:	C:\Program Files (x86)\Internet Explorer\ielowutil.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\Desktop\CONTRACT_REVISED-SHIPMENT-DOCUMENTS_EXPORTS_REFERENCE-QT63637-02993900299348.exe
Imagebase:	0x520000
File size:	221696 bytes
MD5 hash:	650FE7460630188008BF8C8153526CEB
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: ielowutil.exe PID: **6596**, Parent PID: **4848**

General	
Target ID:	25
Start time:	12:32:33
Start date:	03/11/2022
Path:	C:\Program Files (x86)\Internet Explorer\ielowutil.exe

Wow64 process (32bit):	false
Commandline:	C:\Users\user\Desktop\CONTRACT_REVISED-SHIPMENT-DOCUMENTS_EXPORTS_REFERENCE-QT63637-02993900299348.exe
Imagebase:	0x520000
File size:	221696 bytes
MD5 hash:	650FE7460630188008BF8C8153526CEB
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: ielowutil.exe PID: **6516**, Parent PID: **4848**

General

Target ID:	26
Start time:	12:32:33
Start date:	03/11/2022
Path:	C:\Program Files (x86)\Internet Explorer\ielowutil.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\Desktop\CONTRACT_REVISED-SHIPMENT-DOCUMENTS_EXPORTS_REFERENCE-QT63637-02993900299348.exe
Imagebase:	0x520000
File size:	221696 bytes
MD5 hash:	650FE7460630188008BF8C8153526CEB
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: ielowutil.exe PID: **7348**, Parent PID: **4848**

General

Target ID:	27
Start time:	12:32:34
Start date:	03/11/2022
Path:	C:\Program Files (x86)\Internet Explorer\ielowutil.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\Desktop\CONTRACT_REVISED-SHIPMENT-DOCUMENTS_EXPORTS_REFERENCE-QT63637-02993900299348.exe
Imagebase:	0x520000
File size:	221696 bytes
MD5 hash:	650FE7460630188008BF8C8153526CEB
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: ielowutil.exe PID: **7808**, Parent PID: **4848**

General

Target ID:	28
Start time:	12:32:34
Start date:	03/11/2022
Path:	C:\Program Files (x86)\Internet Explorer\ielowutil.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\Desktop\CONTRACT_REVISED-SHIPMENT-DOCUMENTS_EXPORTS_REFERENCE-QT63637-02993900299348.exe
Imagebase:	0x520000
File size:	221696 bytes
MD5 hash:	650FE7460630188008BF8C8153526CEB
Has elevated privileges:	true
Has administrator privileges:	true

Programmed in:	C, C++ or other language

Analysis Process: ielowutil.exe PID: **7380**, Parent PID: **4848**

General	
Target ID:	29
Start time:	12:32:34
Start date:	03/11/2022
Path:	C:\Program Files (x86)\Internet Explorer\ielowutil.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\Desktop\CONTRACT_REVISED-SHIPMENT-DOCUMENTS_EXPORTS_REFERENCE-QT63637-02993900299348.exe
Imagebase:	0x520000
File size:	221696 bytes
MD5 hash:	650FE7460630188008BF8C8153526CEB
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: ExtExport.exe PID: **5404**, Parent PID: **4848**

General	
Target ID:	30
Start time:	12:32:35
Start date:	03/11/2022
Path:	C:\Program Files (x86)\Internet Explorer\ExtExport.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\Desktop\CONTRACT_REVISED-SHIPMENT-DOCUMENTS_EXPORTS_REFERENCE-QT63637-02993900299348.exe
Imagebase:	0x610000
File size:	45056 bytes
MD5 hash:	3253FD643C51C133C3489A146781913B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: ExtExport.exe PID: **7588**, Parent PID: **4848**

General	
Target ID:	31
Start time:	12:32:35
Start date:	03/11/2022
Path:	C:\Program Files (x86)\Internet Explorer\ExtExport.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\Desktop\CONTRACT_REVISED-SHIPMENT-DOCUMENTS_EXPORTS_REFERENCE-QT63637-02993900299348.exe
Imagebase:	0x610000
File size:	45056 bytes
MD5 hash:	3253FD643C51C133C3489A146781913B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: ExtExport.exe PID: **5708**, Parent PID: **4848**

General	
Target ID:	32
Start time:	12:32:35

Start date:	03/11/2022
Path:	C:\Program Files (x86)\Internet Explorer\ExtExport.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\Desktop\CONTRACT_REVISED-SHIPMENT-DOCUMENTS_EXPORTS_REFERENCE-QT63637-02993900299348.exe
Imagebase:	0x610000
File size:	45056 bytes
MD5 hash:	3253FD643C51C133C3489A146781913B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: ExtExport.exe PID: **8104**, Parent PID: **4848**

General	
Target ID:	33
Start time:	12:32:36
Start date:	03/11/2022
Path:	C:\Program Files (x86)\Internet Explorer\ExtExport.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\Desktop\CONTRACT_REVISED-SHIPMENT-DOCUMENTS_EXPORTS_REFERENCE-QT63637-02993900299348.exe
Imagebase:	0x610000
File size:	45056 bytes
MD5 hash:	3253FD643C51C133C3489A146781913B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: ExtExport.exe PID: **1160**, Parent PID: **4848**

General	
Target ID:	34
Start time:	12:32:36
Start date:	03/11/2022
Path:	C:\Program Files (x86)\Internet Explorer\ExtExport.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\Desktop\CONTRACT_REVISED-SHIPMENT-DOCUMENTS_EXPORTS_REFERENCE-QT63637-02993900299348.exe
Imagebase:	0x610000
File size:	45056 bytes
MD5 hash:	3253FD643C51C133C3489A146781913B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: ExtExport.exe PID: **6700**, Parent PID: **4848**

General	
Target ID:	35
Start time:	12:32:36
Start date:	03/11/2022
Path:	C:\Program Files (x86)\Internet Explorer\ExtExport.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\Desktop\CONTRACT_REVISED-SHIPMENT-DOCUMENTS_EXPORTS_REFERENCE-QT63637-02993900299348.exe
Imagebase:	0x610000
File size:	45056 bytes
MD5 hash:	3253FD643C51C133C3489A146781913B
Has elevated privileges:	true

Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: ExtExport.exe PID: **6248**, Parent PID: **4848**

General	
Target ID:	36
Start time:	12:32:36
Start date:	03/11/2022
Path:	C:\Program Files (x86)\Internet Explorer\ExtExport.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\Desktop\CONTRACT_REVISED-SHIPMENT-DOCUMENTS_EXPORTS_REFERENCE-QT63637-02993900299348.exe
Imagebase:	0x610000
File size:	45056 bytes
MD5 hash:	3253FD643C51C133C3489A146781913B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: ExtExport.exe PID: **5524**, Parent PID: **4848**

General	
Target ID:	37
Start time:	12:32:36
Start date:	03/11/2022
Path:	C:\Program Files (x86)\Internet Explorer\ExtExport.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\Desktop\CONTRACT_REVISED-SHIPMENT-DOCUMENTS_EXPORTS_REFERENCE-QT63637-02993900299348.exe
Imagebase:	0x610000
File size:	45056 bytes
MD5 hash:	3253FD643C51C133C3489A146781913B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: ExtExport.exe PID: **5904**, Parent PID: **4848**

General	
Target ID:	38
Start time:	12:32:37
Start date:	03/11/2022
Path:	C:\Program Files (x86)\Internet Explorer\ExtExport.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\Desktop\CONTRACT_REVISED-SHIPMENT-DOCUMENTS_EXPORTS_REFERENCE-QT63637-02993900299348.exe
Imagebase:	0x610000
File size:	45056 bytes
MD5 hash:	3253FD643C51C133C3489A146781913B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: backgroundTaskHost.exe PID: **5840**, Parent PID: **812**

General	
Target ID:	39

Start time:	12:32:37
Start date:	03/11/2022
Path:	C:\Windows\System32\backgroundTaskHost.exe
Wow64 process (32bit):	false
Commandline:	"C:\WINDOWS\system32\backgroundTaskHost.exe" -ServerName:App.AppXmtcan0h2tfbfy7k9kn8hbxb6dmzz1zh0.mca
Imagebase:	0x7ff618d70000
File size:	19776 bytes
MD5 hash:	DA7063B17DBB8BBB3015351016868006
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Disassembly

No disassembly