ANY RUN
INTERACTIVE MALWARE ANALYSIS

General Info

File name:	sample1.exe
Full analysis:	https://app.any.run/tasks/d50c6c7c-ed46-4d5b-a09d-e1ba327f8077
Verdict:	Malicious activity
Threats:	**DarkComet** DarkComet RAT is a malicious program designed to remotely control or administer a victim's computer, steal private data and spy on the victim. **Remote Access Trojan** Remote access trojans (RATs) are a type of malware that enables attackers to establish complete to partial control over infected computers. Such malicious programs often have a modular design, offering a wide range of functionalities for conducting illicit activities on compromised systems. Some of the most common features of RATs include access to the users' data, webcam, and keystrokes. This malware is often distributed through phishing emails and links.
Analysis date:	March 07, 2025 at 01:07:56
OS:	Windows 10 Professional (build: 19045, 64 bit)
Tags:	darkcomet rat
Indicators:	☣
MIME:	application/vnd.microsoft.portable-executable
File info:	PE32 executable (GUI) Intel 80386, for MS Windows, 9 sections
MD5:	C1F59C6B996C64CEF3DAEB5B04396BE7
SHA1:	6C981DCF9CCA212895A747A3ED4FEC8B681DF880
SHA256:	98B7108D6547494DA52784E3DDC3605AF499194C181312996D31CFC063D93612
SSDEEP:	12288:5zf5pMx2ueAY91N7qcESnFmBjaYMLVeb59y4DxStejtNb2iZ+8i4lbYnNvXZt:5zfMx2ug91N7LE2FmBjaZVtejZZt8n9

Software environment set and analysis options

Launch configuration

Task duration:	60 seconds	**Heavy Evasion option:**	off	**Network geolocation:**	off
Additional time used:	none	**MITM proxy:**	off	**Privacy:**	Public submission
Fakenet option:	off	**Route via Tor:**	off	**Autoconfirmation of UAC:**	on
Network:	on				

Software preset

- Internet Explorer 11.3636.19041.0
- Adobe Acrobat (64-bit) (23.001.20093)
- Adobe Flash Player 32 NPAPI (32.0.0.465)
- Adobe Flash Player 32 PPAPI (32.0.0.465)
- CCleaner (6.20)
- FileZilla 3.65.0 (3.65.0)
- Google Chrome (122.0.6261.70)
- Google Update Helper (1.3.36.51)
- Java 8 Update 271 (64-bit) (8.0.2710.9)
- Java Auto Updater (2.8.271.9)
- Microsoft Edge (122.0.2365.59)
- Microsoft Edge Update (1.3.185.17)
- Microsoft Office Professional 2019 - de-de (16.0.16026.20146)
- Microsoft Office Professional 2019 - en-us (16.0.16026.20146)
- Microsoft Office Professional 2019 - es-es (16.0.16026.20146)
- Microsoft Office Professional 2019 - it-it (16.0.16026.20146)
- Microsoft Office Professional 2019 - ja-jp (16.0.16026.20146)
- Microsoft Office Professional 2019 - ko-kr (16.0.16026.20146)
- Microsoft Office Professional 2019 - pt-br (16.0.16026.20146)
- Microsoft Office Professional 2019 - tr-tr (16.0.16026.20146)
- Microsoft Office Professionnel 2019 - fr-fr (16.0.16026.20146)
- Microsoft Office профессиональный 2019 - ru-ru (16.0.16026.20146)
- Microsoft OneNote - en-us (16.0.16026.20146)
- Microsoft Update Health Tools (3.74.0.0)
- Microsoft Visual C++ 2013 Redistributable (x64) - 12.0.30501 (12.0.30501.0)
- Microsoft Visual C++ 2013 x64 Additional Runtime - 12.0.21005 (12.0.21005)
- Microsoft Visual C++ 2013 x64 Minimum Runtime - 12.0.21005 (12.0.21005)
- Microsoft Visual C++ 2015-2022 Redistributable (x64) - 14.36.32532 (14.36.32532.0)
- Microsoft Visual C++ 2015-2022 Redistributable (x86) - 14.36.32532 (14.36.32532.0)
- Microsoft Visual C++ 2022 X64 Additional Runtime - 14.36.32532 (14.36.32532)
- Microsoft Visual C++ 2022 X64 Minimum Runtime - 14.36.32532 (14.36.32532)
- Microsoft Visual C++ 2022 X86 Additional Runtime - 14.36.32532 (14.36.32532)
- Microsoft Visual C++ 2022 X86 Minimum Runtime - 14.36.32532 (14.36.32532)
- Mozilla Firefox (x64 en-US) (123.0)
- Mozilla Maintenance Service (123.0)
- Notepad++ (64-bit x64) (7.9.1)
- Office 16 Click-to-Run Extensibility Component (16.0.15726.20202)
- Office 16 Click-to-Run Licensing Component (16.0.16026.20146)
- Office 16 Click-to-Run Localization Component (16.0.15726.20202)
- Office 16 Click-to-Run Localization Component (16.0.15928.20198)
- PowerShell 7-x64 (7.3.5.0)
- Skype version 8.104 (8.104)
- Update for Windows 10 for x64-based Systems (KB4023057) (2.59.0.0)
- Update for Windows 10 for x64-based Systems (KB4023057) (2.63.0.0)
- Update for Windows 10 for x64-based Systems (KB4480730) (2.55.0.0)
- Update for Windows 10 for x64-based Systems (KB5001716) (8.93.0.0)
- VLC media player (3.0.11)
- WinRAR 5.91 (64-bit) (5.91.0)
- Windows PC Health Check (3.6.2204.08001)

Hotfixes

- Client LanguagePack Package
- DotNetRollup
- DotNetRollup 481
- FodMetadata Package
- Foundation Package
- Hello Face Package
- InternetExplorer Optional Package
- KB5003791
- KB5011048
- KB5015684
- KB5033052
- LanguageFeatures Basic en us Package
- LanguageFeatures Handwriting en us Package
- LanguageFeatures OCR en us Package
- LanguageFeatures Speech en us Package
- LanguageFeatures TextToSpeech en us Package
- MSPaint FoD Package
- MediaPlayer Package
- Microsoft OneCore ApplicationModel Sync Desktop FOD Package
- Microsoft OneCore DirectX Database FOD Package
- NetFx3 OnDemand Package
- Notepad FoD Package
- OpenSSH Client Package
- PowerShell ISE FOD Package
- Printing PMCPPC FoD Package
- Printing WFS FoD Package
- ProfessionalEdition
- QuickAssist Package
- RollupFix
- ServicingStack
- ServicingStack 3989
- StepsRecorder Package
- TabletPCMath Package
- UserExperience Desktop Package
- WordPad FoD Package

Behavior activities

MALICIOUS

Changes the autorun value in the registry

- sample1.exe (PID: 7464)
- msdcsc.exe (PID: 7588)

Changes the login/logoff helper path in the registry

- sample1.exe (PID: 7464)

DARKCOMET mutex has been found

- msdcsc.exe (PID: 7588)
- iexplore.exe (PID: 7664)

SUSPICIOUS

Starts CMD.EXE for commands execution

- sample1.exe (PID: 7464)

Executable content was dropped or overwritten

- sample1.exe (PID: 7464)

Reads security settings of Internet Explorer

- sample1.exe (PID: 7464)

Starts itself from another location

- sample1.exe (PID: 7464)

Executing commands from a ".bat" file

- sample1.exe (PID: 7464)

Uses ATTRIB.EXE to modify file attributes

- cmd.exe (PID: 7552)
- cmd.exe (PID: 7512)

INFO

Checks supported languages

- sample1.exe (PID: 7464)
- msdcsc.exe (PID: 7588)

Reads the computer name

- sample1.exe (PID: 7464)
- msdcsc.exe (PID: 7588)

The sample compiled with english language support

- sample1.exe (PID: 7464)

Process checks computer location settings

- sample1.exe (PID: 7464)

Create files in a temporary directory

- sample1.exe (PID: 7464)

Creates files or folders in the user directory

- BackgroundTransferHost.exe (PID: 5452)

Reads security settings of Internet Explorer

- BackgroundTransferHost.exe (PID: 7172)
- BackgroundTransferHost.exe (PID: 7496)
- BackgroundTransferHost.exe (PID: 4400)
- BackgroundTransferHost.exe (PID: 5452)
- BackgroundTransferHost.exe (PID: 7300)

Reads the software policy settings

- BackgroundTransferHost.exe (PID: 5452)

Checks proxy server information

- BackgroundTransferHost.exe (PID: 5452)

Connects to unusual port

- iexplore.exe (PID: 7664)

Malware configuration

No Malware configuration.

Static information

TRiD

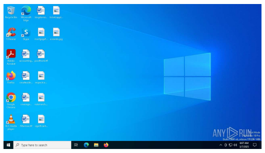
.exe	Win32 Executable Delphi generic (31.9)
.scr	Windows screen saver (29.4)
.dll	Win32 Dynamic Link Library (generic) (14.8)
.exe	Win32 Executable (generic) (10.1)
.exe	Win16/32 Executable Delphi generic (4.6)

EXIF

EXE

ProductVersion:	4, 0, 0, 0
ProductName:	Remote Service Application
OriginalFileName:	MSRSAAP.EXE
LegalCopyright:	Copyright (C) 1999
InternalName:	MSRSAAPP
FileVersion:	1, 0, 0, 1
FileDescription:	Remote Service Application
CompanyName:	Microsoft Corp.
Comments:	Remote Service Application
CharacterSet:	Unicode
LanguageCode:	English (U.S.)
FileSubtype:	-
ObjectFileType:	Executable application
FileOS:	Win32
FileFlags:	(none)
FileFlagsMask:	0x003f
ProductVersionNumber:	4.0.0.0
FileVersionNumber:	4.0.0.0
Subsystem:	Windows GUI
SubsystemVersion:	4
ImageVersion:	-
OSVersion:	4
EntryPoint:	0x9f92c
UninitializedDataSize:	-
InitializedDataSize:	88064
CodeSize:	651264
LinkerVersion:	2.25
PEType:	PE32
ImageFileCharacteristics:	Executable, No line numbers, No symbols, Bytes reversed lo, 32-bit, Bytes reversed hi
TimeStamp:	2011:10:30 20:22:14+00:00
MachineType:	Intel 386 or later, and compatibles

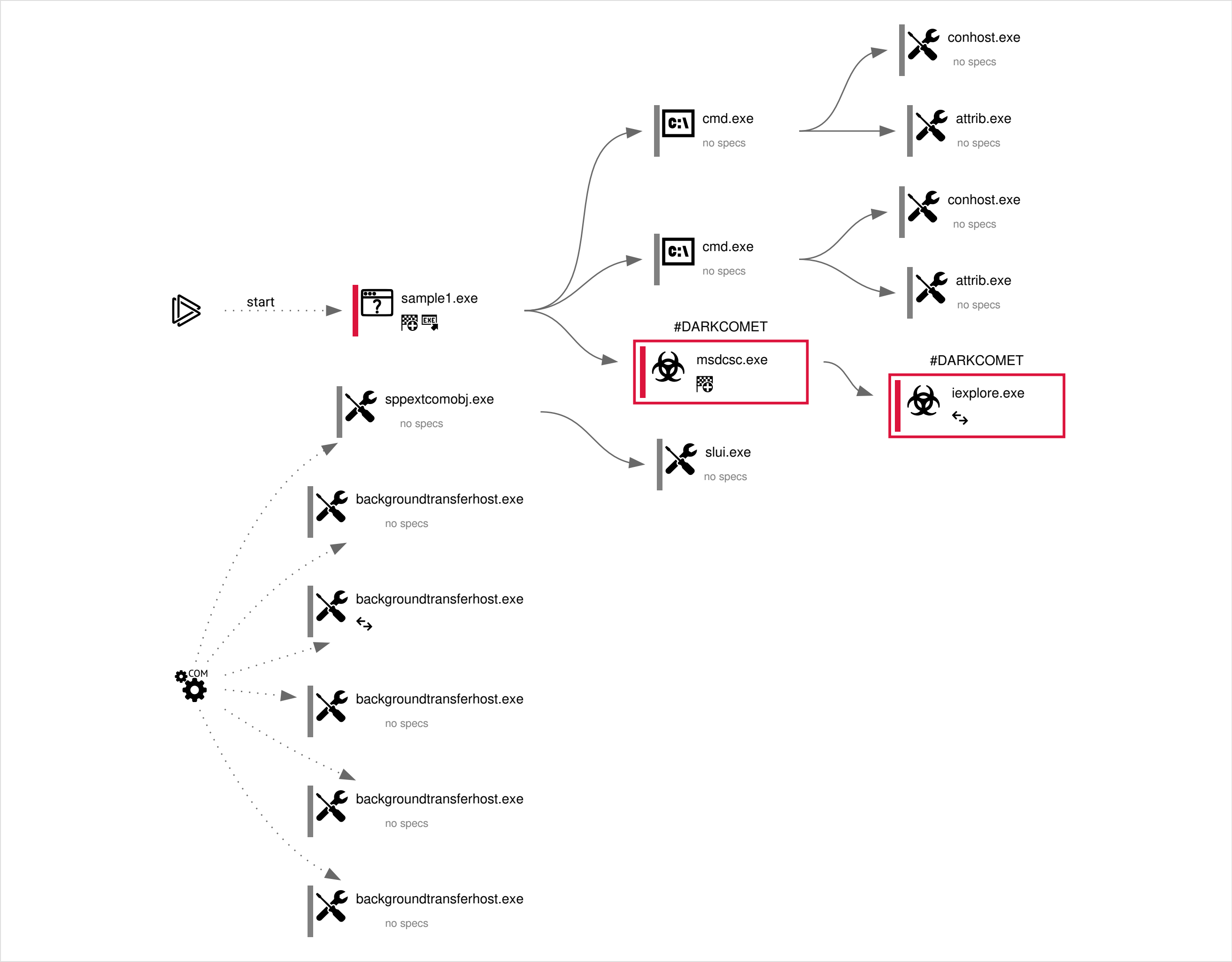
Video and screenshots



Processes

Total processes	Monitored processes	Malicious processes	Suspicious processes
148	16	3	0

Behavior graph



Specs description

- Program did not start
- Probably Tor was used
- Known threat
- Connects to the network
- Task contains several apps running
- File is detected by antivirus software
- The process has the malware config
- Low-level access to the HDD
- Behavior similar to spam
- RAM overrun
- CPU overrun
- Application downloaded the executable file
- Inspected object has suspicious PE structure
- Process was added to the startup
- Task has injected processes
- Network attacks were detected
- Process starts the services
- Actions similar to stealing personal data
- Behavior similar to exploiting the vulnerability
- Debug information is available
- Executable file was dropped
- Integrity level elevation
- System was rebooted
- Task has apps ended with an error
- Task contains an error or was rebooted

Process information

PID	CMD	Path	Indicators	Parent process
7464	"C:\Users\admin\AppData\Local\Temp\sample1.exe"	C:\Users\admin\AppData\Local\Temp\sample1.exe		explorer.exe

Information

User:	admin	**Company:**	Microsoft Corp.

PID	CMD	Path	Indicators	Parent process

Integrity Level:	MEDIUM	Description:	Remote Service Application
Exit code:	0	Version:	1, 0, 0, 1

7512	C:\WINDOWS\system32\cmd.exe /c ""C:\Users\admin\AppData\Local\Temp\tmpcmd.bat" "	C:\Windows\SysWOW64\cmd.exe	—	sample1.exe

Information

User:	admin	Company:	Microsoft Corporation
Integrity Level:	MEDIUM	Description:	Windows Command Processor
Exit code:	0	Version:	10.0.19041.3636 (WinBuild.160101.0800)

7520	\??\C:\WINDOWS\system32\conhost.exe 0xffffffff -ForceV1	C:\Windows\System32\conhost.exe	—	cmd.exe

Information

User:	admin	Company:	Microsoft Corporation
Integrity Level:	MEDIUM	Description:	Console Window Host
Exit code:	0	Version:	10.0.19041.1 (WinBuild.160101.0800)

7552	C:\WINDOWS\system32\cmd.exe /c ""C:\Users\admin\AppData\Local\Temp\tmpcmd.bat" "	C:\Windows\SysWOW64\cmd.exe	—	sample1.exe

Information

User:	admin	Company:	Microsoft Corporation
Integrity Level:	MEDIUM	Description:	Windows Command Processor
Exit code:	0	Version:	10.0.19041.3636 (WinBuild.160101.0800)

7560	\??\C:\WINDOWS\system32\conhost.exe 0xffffffff -ForceV1	C:\Windows\System32\conhost.exe	—	cmd.exe

Information

User:	admin	Company:	Microsoft Corporation
Integrity Level:	MEDIUM	Description:	Console Window Host
Exit code:	0	Version:	10.0.19041.1 (WinBuild.160101.0800)

7588	"C:\Users\admin\Documents\MSDCSC\msdcsc.exe"	C:\Users\admin\Documents\MSDCSC\msdcsc.exe	🏁 ☣	sample1.exe

Information

User:	admin	Company:	Microsoft Corp.
Integrity Level:	MEDIUM	Description:	Remote Service Application
Exit code:	0	Version:	1, 0, 0, 1

7648	attrib "C:\Users\admin\AppData\Local\Temp" +s +h	C:\Windows\SysWOW64\attrib.exe	—	cmd.exe

Information

User:	admin	Company:	Microsoft Corporation
Integrity Level:	MEDIUM	Description:	Attribute Utility
Exit code:	0	Version:	10.0.19041.1 (WinBuild.160101.0800)

7656	attrib "C:\Users\admin\AppData\Local\Temp" +s +h	C:\Windows\SysWOW64\attrib.exe	—	cmd.exe

Information

User:	admin	Company:	Microsoft Corporation
Integrity Level:	MEDIUM	Description:	Attribute Utility
Exit code:	0	Version:	10.0.19041.1 (WinBuild.160101.0800)

7664	"C:\Program Files (x86)\Internet Explorer\iexplore.exe"	C:\Program Files (x86)\Internet Explorer\iexplore.exe	☣ ⇆	msdcsc.exe

Information

User:	admin	Company:	Microsoft Corporation
Integrity Level:	MEDIUM	Description:	Internet Explorer
Version:	11.00.19041.1 (WinBuild.160101.0800)		

7792	C:\WINDOWS\system32\SppExtComObj.exe -Embedding	C:\Windows\System32\SppExtComObj.Exe	—	svchost.exe

Information

User:	NETWORK SERVICE	Company:	Microsoft Corporation
Integrity Level:	SYSTEM	Description:	KMS Connection Broker
Version:	10.0.19041.3996 (WinBuild.160101.0800)		

7824	"C:\WINDOWS\System32\SLUI.exe" RuleId=3482d82e-ca2c-4e1f-8864-da0267b484b2;Action=AutoActivate;AppId=55c92734-d682-4d71-983e-d6ec3f16059f;SkuId=4de7cb65-cdf1-4de9-8ae8-e3cce27b9f2c;NotificationInterval=1440;Trigger=TimerEvent	C:\Windows\System32\slui.exe	—	SppExtComObj.Exe

PID	CMD	Path	Indicators	Parent process

Information

User:	NETWORK SERVICE	Company:	Microsoft Corporation
Integrity Level:	SYSTEM	Description:	Windows Activation Client
Version:	10.0.19041.1 (WinBuild.160101.0800)		

7496	"BackgroundTransferHost.exe" -ServerName:BackgroundTransferHost.1	C:\Windows\System32\BackgroundTransferHost.exe	—	svchost.exe

Information

User:	admin	Company:	Microsoft Corporation
Integrity Level:	MEDIUM	Description:	Download/Upload Host
Exit code:	1	Version:	10.0.19041.3636 (WinBuild.160101.0800)

5452	"BackgroundTransferHost.exe" -ServerName:BackgroundTransferHost.1	C:\Windows\System32\BackgroundTransferHost.exe	⇆	svchost.exe

Information

User:	admin	Company:	Microsoft Corporation
Integrity Level:	MEDIUM	Description:	Download/Upload Host
Exit code:	1	Version:	10.0.19041.3636 (WinBuild.160101.0800)

4400	"BackgroundTransferHost.exe" -ServerName:BackgroundTransferHost.1	C:\Windows\System32\BackgroundTransferHost.exe	—	svchost.exe

Information

User:	admin	Company:	Microsoft Corporation
Integrity Level:	MEDIUM	Description:	Download/Upload Host
Exit code:	1	Version:	10.0.19041.3636 (WinBuild.160101.0800)

7172	"BackgroundTransferHost.exe" -ServerName:BackgroundTransferHost.1	C:\Windows\System32\BackgroundTransferHost.exe	—	svchost.exe

Information

User:	admin	Company:	Microsoft Corporation
Integrity Level:	MEDIUM	Description:	Download/Upload Host
Exit code:	1	Version:	10.0.19041.3636 (WinBuild.160101.0800)

7300	"BackgroundTransferHost.exe" -ServerName:BackgroundTransferHost.1	C:\Windows\System32\BackgroundTransferHost.exe	—	svchost.exe

Information

User:	admin	Company:	Microsoft Corporation
Integrity Level:	MEDIUM	Description:	Download/Upload Host
Exit code:	1	Version:	10.0.19041.3636 (WinBuild.160101.0800)

Registry activity

Total events	Read events	Write events	Delete events
2 720	2 695	25	0

Modification events

(PID) Process:	(7464) sample1.exe	Key:	HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
Operation:	write	Name:	MicroUpdate
Value:	C:\Users\admin\Documents\MSDCSC\msdcsc.exe		

(PID) Process:	(7464) sample1.exe	Key:	HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon
Operation:	write	Name:	UserInit
Value:	C:\Windows\system32\userinit.exe,C:\Users\admin\Documents\MSDCSC\msdcsc.exe		

(PID) Process:	(7588) msdcsc.exe	Key:	HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
Operation:	write	Name:	MicroUpdate
Value:	C:\Users\admin\Documents\MSDCSC\msdcsc.exe		

(PID) Process:	(7664) iexplore.exe	Key:	HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
Operation:	write	Name:	MicroUpdate
Value:	C:\Users\admin\Documents\MSDCSC\msdcsc.exe		

(PID) Process: (7496) BackgroundTransferHost.exe **Key:** HKEY_CLASSES_ROOT\Local Settings\Software\Microsoft\Windows\CurrentVersion\AppContainer\Storage\microsoft.windows.contentdeliverymanager_cw5n1h2txyewy\Internet Settings\Cache\Content
Operation: write **Name:** CachePrefix
Value:

(PID) Process: (7496) BackgroundTransferHost.exe **Key:** HKEY_CLASSES_ROOT\Local Settings\Software\Microsoft\Windows\CurrentVersion\AppContainer\Storage\microsoft.windows.contentdeliverymanager_cw5n1h2txyewy\Internet Settings\Cache\Cookies
Operation: write **Name:** CachePrefix
Value: Cookie:

(PID) Process: (7496) BackgroundTransferHost.exe **Key:** HKEY_CLASSES_ROOT\Local Settings\Software\Microsoft\Windows\CurrentVersion\AppContainer\Storage\microsoft.windows.contentdeliverymanager_cw5n1h2txyewy\Internet Settings\Cache\History
Operation: write **Name:** CachePrefix
Value: Visited:

(PID) Process: (5452) BackgroundTransferHost.exe **Key:** HKEY_CLASSES_ROOT\Local Settings\Software\Microsoft\Windows\CurrentVersion\AppContainer\Storage\microsoft.windows.contentdeliverymanager_cw5n1h2txyewy\Internet Settings\Cache\Content
Operation: write **Name:** CachePrefix
Value:

(PID) Process: (5452) BackgroundTransferHost.exe **Key:** HKEY_CLASSES_ROOT\Local Settings\Software\Microsoft\Windows\CurrentVersion\AppContainer\Storage\microsoft.windows.contentdeliverymanager_cw5n1h2txyewy\Internet Settings\Cache\Cookies
Operation: write **Name:** CachePrefix
Value: Cookie:

(PID) Process: (5452) BackgroundTransferHost.exe **Key:** HKEY_CLASSES_ROOT\Local Settings\Software\Microsoft\Windows\CurrentVersion\AppContainer\Storage\microsoft.windows.contentdeliverymanager_cw5n1h2txyewy\Internet Settings\Cache\History
Operation: write **Name:** CachePrefix
Value: Visited:

(PID) Process: (4400) BackgroundTransferHost.exe **Key:** HKEY_CLASSES_ROOT\Local Settings\Software\Microsoft\Windows\CurrentVersion\AppContainer\Storage\microsoft.windows.contentdeliverymanager_cw5n1h2txyewy\Internet Settings\Cache\Content
Operation: write **Name:** CachePrefix
Value:

(PID) Process: (4400) BackgroundTransferHost.exe **Key:** HKEY_CLASSES_ROOT\Local Settings\Software\Microsoft\Windows\CurrentVersion\AppContainer\Storage\microsoft.windows.contentdeliverymanager_cw5n1h2txyewy\Internet Settings\Cache\Cookies
Operation: write **Name:** CachePrefix
Value: Cookie:

(PID) Process: (4400) BackgroundTransferHost.exe **Key:** HKEY_CLASSES_ROOT\Local Settings\Software\Microsoft\Windows\CurrentVersion\AppContainer\Storage\microsoft.windows.contentdeliverymanager_cw5n1h2txyewy\Internet Settings\Cache\History
Operation: write **Name:** CachePrefix
Value: Visited:

(PID) Process: (7172) BackgroundTransferHost.exe **Key:** HKEY_CLASSES_ROOT\Local Settings\Software\Microsoft\Windows\CurrentVersion\AppContainer\Storage\microsoft.windows.contentdeliverymanager_cw5n1h2txyewy\Internet Settings\Cache\Content
Operation: write **Name:** CachePrefix
Value:

(PID) Process: (7172) BackgroundTransferHost.exe **Key:** HKEY_CLASSES_ROOT\Local Settings\Software\Microsoft\Windows\CurrentVersion\AppContainer\Storage\microsoft.windows.contentdeliverymanager_cw5n1h2txyewy\Internet Settings\Cache\Cookies
Operation: write **Name:** CachePrefix
Value: Cookie:

(PID) Process: (7172) BackgroundTransferHost.exe **Key:** HKEY_CLASSES_ROOT\Local Settings\Software\Microsoft\Windows\CurrentVersion\AppContainer\Storage\microsoft.windows.contentdeliverymanager_cw5n1h2txyewy\Internet Settings\Cache\History
Operation: write **Name:** CachePrefix
Value: Visited:

(PID) Process: (7300) BackgroundTransferHost.exe **Key:** HKEY_CLASSES_ROOT\Local Settings\Software\Microsoft\Windows\CurrentVersion\AppContainer\Storage\microsoft.windows.contentdeliverymanager_cw5n1h2txyewy\Internet Settings\Cache\Content
Operation: write **Name:** CachePrefix
Value:

(PID) Process: (7300) BackgroundTransferHost.exe **Key:** HKEY_CLASSES_ROOT\Local Settings\Software\Microsoft\Windows\CurrentVersion\AppContainer\Storage\microsoft.windows.contentdeliverymanager_cw5n1h2txyewy\Internet Settings\Cache\Cookies
Operation: write **Name:** CachePrefix
Value: Cookie:

(PID) Process: (7300) BackgroundTransferHost.exe **Key:** HKEY_CLASSES_ROOT\Local Settings\Software\Microsoft\Windows\CurrentVersion\AppContainer\Storage\microsoft.windows.contentdeliverymanager_cw5n1h2txyewy\Internet Settings\Cache\History
Operation: write **Name:** CachePrefix
Value: Visited:

Files activity

Executable files Suspicious files Text files Unknown types

1	5	2	0

Dropped files

PID	Process	Filename	Type
5452	BackgroundTransferHost.exe	C:\Users\admin\AppData\Local\Packages\Microsoft.Windows.ContentDeliveryManager_cw5n1h2txyewy\AC\BackgroundTransferApi\4380f70e-4a84-4c53-a3e0-c502b6f46f1b.down_data **MD5:** — **SHA256:** —	—
7464	sample1.exe	C:\Users\admin\Documents\MSDCSC\msdcsc.exe **MD5:** C1F59C6B996C64CEF3DAEB5B04396BE7 **SHA256:** 6D1D39E43E4817E5728567F78FF84590AA7EC99DD5C0A75E96DE0108340B69EB	executable
5452	BackgroundTransferHost.exe	C:\Users\admin\AppData\Local\Packages\Microsoft.Windows.ContentDeliveryManager_cw5n1h2txyewy\AC\BackgroundTransferApi\4380f70e-4a84-4c53-a3e0-c502b6f46f1b.31a1ac0d-8f8c-42c9-bb3c-9a762d83c9da.down_meta **MD5:** E97D2250C1632E0089BD5775EFDA2920 **SHA256:** 55C47DA2C8A0D97CA7E0DEA2DB7D9AD4DA3CC188D8EE601DC22B589C407ABBA9	binary
5452	BackgroundTransferHost.exe	C:\Users\admin\AppData\Local\Packages\Microsoft.Windows.ContentDeliveryManager_cw5n1h2txyewy\AC\BackgroundTransferApi\961147e5-ad0d-42ac-9a1e-11986abb3a7f.up_meta_secure **MD5:** 82917EB5C8B131E780450D6F9A982356 **SHA256:** 1EF69DF23BE59545933AF3B474164005450951FD081D3CC9ED02C62DF0B9B884	binary
5452	BackgroundTransferHost.exe	C:\Users\admin\AppData\Local\Packages\Microsoft.Windows.ContentDeliveryManager_cw5n1h2txyewy\AC\Microsoft\CryptnetUrlCache\MetaData\26C212D9399727259664BDFCA073966E_F9F7D6A7ECE73106D2A8C63168CDA10D **MD5:** 31C6F158304BCEC9E11CBD271D4410F2 **SHA256:** 324491D110FEAFA9CDB38FB6FD6CCF20CFC23354F4113CBAA2A4922A4139FCA6	binary
5452	BackgroundTransferHost.exe	C:\Users\admin\AppData\Local\Packages\Microsoft.Windows.ContentDeliveryManager_cw5n1h2txyewy\AC\Microsoft\CryptnetUrlCache\Content\26C212D9399727259664BDFCA073966E_F9F7D6A7ECE73106D2A8C63168CDA10D **MD5:** 38989CDC9B939CBF439472EC8FEBE5D7 **SHA256:** 05491F06DCD3C4FBB8FF3B2D2007CD4DFE1CE2B651587DF866B2657984EFB329	binary
5452	BackgroundTransferHost.exe	C:\Users\admin\AppData\Local\Packages\Microsoft.Windows.ContentDeliveryManager_cw5n1h2txyewy\AC\BackgroundTransferApi\961147e5-ad0d-42ac-9a1e-11986abb3a7f.31a1ac0d-8f8c-42c9-bb3c-9a762d83c9da.down_meta **MD5:** E97D2250C1632E0089BD5775EFDA2920 **SHA256:** 55C47DA2C8A0D97CA7E0DEA2DB7D9AD4DA3CC188D8EE601DC22B589C407ABBA9	binary
7464	sample1.exe	C:\Users\admin\AppData\Local\Temp\tmpcmd.bat **MD5:** 67D69D8BC0D3CBA42627A0DB76DA3DED **SHA256:** 0BBCB0869A4A4C6B2BE976363ECBF9C238458FDAB7E5E736F77DA94EC77FF886	text

Network activity

HTTP(S) requests	TCP/UDP connections	DNS requests	Threats
5	30	14	0

HTTP requests

PID	Process	Method	HTTP Code	IP	URL	CN	Type	Size	Reputation
6544	svchost.exe	GET	200	184.30.131.245:80	http://ocsp.digicert.com/MFEwTzBNMEswSTAJBgUrDgMCGgUABBSAUQYBMq2awn1Rh6Doh%2FsBYgFV7gQUA95QNVbRTLtm8KPiGxvDl7I90VUCEAJ0LqoXyo4hxxe7H%2Fz9DKA%3D	unknown	—	—	whitelisted
7608	SIHClient.exe	GET	200	184.30.21.171:80	http://www.microsoft.com/pkiops/crl/Microsoft%20ECC%20Update%20Secure%20Server%20CA%202.1.crl	unknown	—	—	whitelisted
7608	SIHClient.exe	GET	200	184.30.21.171:80	http://www.microsoft.com/pkiops/crl/Microsoft%20ECC%20Product%20Root%20Certificate%20Authority%202018.crl	unknown	—	—	whitelisted
5452	BackgroundTransferHost.exe	GET	200	184.30.131.245:80	http://ocsp.digicert.com/MFEwTzBNMEswSTAJBgUrDgMCGgUABBTrjrydRyt%2BApF3GSPypfHBxR5XtQQUs9tIpPmhxdiuNkHMEWNpYim8S8YCEAI5PUjXAkJafLQcAAsO18o%3D	unknown	—	—	whitelisted
8040	backgroundTaskHost.exe	GET	200	184.30.131.245:80	http://ocsp.digicert.com/MFEwTzBNMEswSTAJBgUrDgMCGgUABBQ50otx%2Fh0Ztl%2Bz8SiPI7wEWVxDlQQUTiJUIBiV5uNu5g%2F6%2BrkS7QYXjzkCEAUZZSZEml49Gjh0j13P68w%3D	unknown	—	—	whitelisted

Connections

PID	Process	IP	Domain	ASN	CN	Reputation
—	—	192.168.100.255:137	—	—	—	whitelisted
2104	svchost.exe	51.104.136.2:443	settings-win.data.microsoft.com	MICROSOFT-CORP-MSN-AS-BLOCK	IE	whitelisted
—	—	51.104.136.2:443	settings-win.data.microsoft.com	MICROSOFT-CORP-MSN-AS-BLOCK	IE	whitelisted
4	System	192.168.100.255:138	—	—	—	whitelisted
7664	iexplore.exe	10.10.15.83:1604	—	—	—	unknown

PID	Process	IP	Domain	ASN	CN	Reputation
2112	svchost.exe	20.73.194.208:443	settings-win.data.microsoft.com	MICROSOFT-CORP-MSN-AS-BLOCK	NL	whitelisted
3216	svchost.exe	40.113.103.199:443	client.wns.windows.com	MICROSOFT-CORP-MSN-AS-BLOCK	NL	whitelisted
6544	svchost.exe	20.190.160.128:443	login.live.com	MICROSOFT-CORP-MSN-AS-BLOCK	NL	whitelisted
6544	svchost.exe	184.30.131.245:80	ocsp.digicert.com	AKAMAI-AS	US	whitelisted
8040	backgroundTaskHost.exe	20.223.35.26:443	arc.msn.com	MICROSOFT-CORP-MSN-AS-BLOCK	IE	whitelisted
8040	backgroundTaskHost.exe	184.30.131.245:80	ocsp.digicert.com	AKAMAI-AS	US	whitelisted
5452	BackgroundTransferHost.exe	2.23.227.208:443	www.bing.com	Ooredoo Q.S.C.	QA	whitelisted
5452	BackgroundTransferHost.exe	184.30.131.245:80	ocsp.digicert.com	AKAMAI-AS	US	whitelisted
2104	svchost.exe	20.73.194.208:443	settings-win.data.microsoft.com	MICROSOFT-CORP-MSN-AS-BLOCK	NL	whitelisted
7608	SIHClient.exe	4.245.163.56:443	slscr.update.microsoft.com	MICROSOFT-CORP-MSN-AS-BLOCK	US	whitelisted
7608	SIHClient.exe	184.30.21.171:80	www.microsoft.com	AKAMAI-AS	DE	whitelisted
7608	SIHClient.exe	20.3.187.198:443	fe3cr.delivery.mp.microsoft.com	MICROSOFT-CORP-MSN-AS-BLOCK	US	whitelisted

DNS requests

Domain	IP	Reputation
settings-win.data.microsoft.com	51.104.136.2 20.73.194.208	whitelisted
google.com	142.250.184.206	whitelisted
client.wns.windows.com	40.113.103.199	whitelisted
login.live.com	20.190.160.128 20.190.160.4 20.190.160.64 40.126.32.68 20.190.160.20 40.126.32.133 20.190.160.132 40.126.32.138	whitelisted
ocsp.digicert.com	184.30.131.245	whitelisted
arc.msn.com	20.223.35.26	whitelisted
www.bing.com	2.23.227.208 2.23.227.215	whitelisted
slscr.update.microsoft.com	4.245.163.56	whitelisted
www.microsoft.com	184.30.21.171	whitelisted
fe3cr.delivery.mp.microsoft.com	20.3.187.198	whitelisted

Threats

No threats detected

Debug output strings

No debug info