

OUTPUT:

Process Explorer:

Process Explorer - Sysinternals: www.sysinternals.com [EXPAT\Expat] (Administrator)

File Options View Process Find Users Help

Process	CPU	Private Bytes	Working Set	PID	Description	Company Name
ABService.exe	< 0.01	29,340 K	22,540 K	4216	AOMEI Backupper Schedule...	AOMEI International Netw...
amdfendrar.exe		3,836 K	8,012 K	2084	AMD Crash Defender Service	Advanced Micro Devices, ...
ApplicationFrameHost.exe		9,384 K	29,984 K	68	Application Frame Host	Microsoft Corporation
atiecbox.exe		2,856 K	12,932 K	2628	AMD External Events Client ...	AMD
atiesrv.exe		1,428 K	6,532 K	2112	AMD External Events Servic...	AMD
atmgr.exe	< 0.01	52,160 K	72,640 K	10096	Cisco Webex Service	Cisco Webex LLC
audiodg.exe		9,908 K	15,916 K	2592	Windows Audio Device Grap...	Microsoft Corporation
CCleaner64.exe	< 0.01	20,392 K	33,188 K	9944	CCleaner	Pirform Software Ltd
ChromaCam_SystemTray.exe		16,684 K	24,160 K	10752	ChromaCamSystemTray	Personify, Inc.
ciscowebestart.exe	< 0.01	6,912 K	21,308 K	10028	Webex	Cisco Webex LLC
ClassicStartMenu.exe		3,200 K	12,772 K	1656	Classic Start Menu	IvoSoft
cmd.exe		2,304 K	4,376 K	8320	Windows Command Processor	Microsoft Corporation
cmw_srv.exe	< 0.01	95,736 K	126,180 K	4372	Hss.Service.Application	Pango Inc.
CompPkgSrv.exe		1,704 K	9,056 K	5816	Component Package Suppor...	Microsoft Corporation
conhost.exe	< 0.01	6,656 K	2,292 K	2540	Console Window Host	Microsoft Corporation
conhost.exe		6,212 K	10,860 K	6724	Console Window Host	Microsoft Corporation
conhost.exe		6,340 K	11,232 K	6372	Console Window Host	Microsoft Corporation
conhost.exe		6,336 K	11,220 K	7852	Console Window Host	Microsoft Corporation
conhost.exe		6,996 K	16,692 K	6764	Console Window Host	Microsoft Corporation
csrss.exe		1,908 K	5,456 K	644	Client Server Runtime Process	Microsoft Corporation
csrss.exe	< 0.01	7,052 K	5,884 K	788	Client Server Runtime Process	Microsoft Corporation
ctfmon.exe		5,724 K	28,748 K	4368	CTF Loader	Microsoft Corporation
DbxSvc.exe		3,380 K	8,444 K	4264	Dropbox Service	Dropbox, Inc.
dllhost.exe		3,128 K	10,956 K	6992	COM Surrogate	Microsoft Corporation
dllhost.exe		5,544 K	14,696 K	8820	COM Surrogate	Microsoft Corporation
DriverUpdate.exe	< 0.01	59,504 K	1,364 K	9628	Driver Booster Driver Update	IObit
Dropbox.exe	< 0.01	318,596 K	405,304 K	10992	Dropbox	Dropbox, Inc.
Dropbox.exe		2,688 K	9,960 K	11012	Dropbox	Dropbox, Inc.
Dropbox.exe		2,448 K	9,296 K	11040	Dropbox	Dropbox, Inc.
Dropbox.exe		3,160 K	12,680 K	11092	Dropbox	Dropbox, Inc.
Dropbox Update.exe		2,112 K	4,536 K	4996	Dropbox Update	Dropbox, Inc.
dwm.exe	0.75	98,388 K	92,524 K	1204	Desktop Window Manager	Microsoft Corporation
E_YATIUNE.EXE		4,608 K	11,712 K	9368	EPSON Status Monitor 3	Seiko Epson Corporation
EEventManager.exe	< 0.01	3,532 K	15,408 K	10840	Epson Event Manager	Seiko Epson Corporation
EPPCCMON.EXE		2,028 K	9,008 K	6692	Epson Printer Connection Ch...	Seiko Epson Corporation
escsvc64.exe		1,388 K	6,640 K	4348	Epson Scanner Service (64bit)	Seiko Epson Corporation
explorer.exe	< 0.01	95,012 K	185,300 K	2024	Windows Explorer	Microsoft Corporation
firefox.exe	0.38	320,812 K	13,568 K	11904	Firefox	Mozilla Corporation
firefox.exe	0.38	292,024 K	9,972 K	1576	Firefox	Mozilla Corporation
firefox.exe	0.38	227,372 K	5,824 K	11684	Firefox	Mozilla Corporation
firefox.exe		47,148 K	160 K	5988	Firefox	Mozilla Corporation

•

Process Explorer - Sysinternals: www.sysinternals.com [AWC\Administrator] (Administrator)

File Options View Process Find Users Help

Run At Logon
 Verify Image Signatures
 VirusTotal.com
 Always On Top
 Replace Task Manager
 Hide When Minimized
 Allow Only One Instance
 Confirm Kill
 Tray Icons
 Configure Symbols...
 Configure Colors...
 Difference Highlight Duration...
 Font...
 Theme

Process	Private Bytes	Working Set	PID	Description	Company Name
smartscreen.exe	2,232 K	67,876 K	100		
WmiPrvSE.exe	60 K	8 K	0		
smss.exe	40 K	128 K	4		
csrss.exe	0 K	0 K	n/a	Hardware Interrupts and DPCs	
csrss.exe	1,064 K	1,232 K	308		
csrss.exe	1,948 K	6,284 K	424		
wininit.exe	2,112 K	6,908 K	492		
services.exe	1,324 K	6,984 K	540		
svchost.exe	5,732 K	14,144 K	624		
svchost.exe	6,964 K	23,384 K	840	Host Process for Windows S...	Microsoft Corporation
TextInputHost.exe	10,208 K	43,384 K	4736		Microsoft Corporation
StartMenuExperienceHost.exe	14,072 K	56,356 K	2912		Microsoft Corporation
RuntimeBroker.exe	3,696 K	21,448 K	4224	Runtime Broker	Microsoft Corporation
RuntimeBroker.exe	6,920 K	23,848 K	5296	Runtime Broker	Microsoft Corporation
SearchApp.exe	30,976 K	44,452 K	5840	Search application	Microsoft Corporation
ShellExperienceHost.exe	13,100 K	46,052 K	6432	Windows Shell Experience H...	Microsoft Corporation
RuntimeBroker.exe	4,956 K	22,632 K	7116	Runtime Broker	Microsoft Corporation
RuntimeBroker.exe	2,256 K	16,856 K	2720	Runtime Broker	Microsoft Corporation
dllhost.exe	3,152 K	12,704 K	8492	COM Surrogate	Microsoft Corporation
smartscreen.exe	8,020 K	23,496 K	5016	Windows Defender SmartScr...	Microsoft Corporation
WmiPrvSE.exe	2,388 K	9,060 K	8076	WMI Provider Host	Microsoft Corporation
svchost.exe	6,568 K	13,136 K	904	Host Process for Windows S...	Microsoft Corporation
svchost.exe	2,532 K	10,664 K	960	Host Process for Windows S...	Microsoft Corporation
svchost.exe	3,820 K	12,308 K	372	Host Process for Windows S...	Microsoft Corporation
svchost.exe	1,912 K	9,960 K	676	Host Process for Windows S...	Microsoft Corporation
svchost.exe	3,600 K	7,872 K	1112	Host Process for Windows S...	Microsoft Corporation
svchost.exe	1,196 K	5,436 K	1120	Host Process for Windows S...	Microsoft Corporation

Process	CPU	Private Bytes	Working Set	PID	Description	Company Name	Verified Signer
Registry		2,236 K	67,876 K	100			
System Idle Process	55.56	60 K	8 K	0			
System	2.78	40 K	128 K	4			
Interrupts	1.39	0 K	0 K	n/a	Hardware Interrupts and DPCs		
smss.exe		1,064 K	1,232 K	308			
csrss.exe	< 0.01	1,948 K	6,276 K	424			
csrss.exe	< 0.01	2,112 K	6,908 K	492			
wininit.exe		1,324 K	6,984 K	540			
services.exe	< 0.01	5,660 K	14,096 K	624			
svchost.exe		6,908 K	23,368 K	840	Host Process for Windows S...	Microsoft Corporation	(Verified) Microsoft...
TextInputHost.exe		10,208 K	43,376 K	4736		Microsoft Corporation	(Verified) Microsoft...
StartMenuExperienceHost.exe		14,072 K	56,356 K	2912		Microsoft Corporation	(Verified) Microsoft...
RuntimeBroker.exe		3,696 K	21,448 K	4224	Runtime Broker	Microsoft Corporation	(Verified) Microsoft...
RuntimeBroker.exe		6,920 K	23,848 K	5296	Runtime Broker	Microsoft Corporation	(Verified) Microsoft...
SearchApp.exe	Susp...	30,976 K	44,452 K	5840	Search application	Microsoft Corporation	(Verified) Microsoft...
ShellExperienceHost.exe	Susp...	13,100 K	46,052 K	6432	Windows Shell Experience H...	Microsoft Corporation	(Verified) Microsoft...
RuntimeBroker.exe		4,956 K	22,632 K	7116	Runtime Broker	Microsoft Corporation	(Verified) Microsoft...
RuntimeBroker.exe		2,256 K	16,856 K	2720	Runtime Broker	Microsoft Corporation	(Verified) Microsoft...
dllhost.exe		3,152 K	12,704 K	8492	COM Surrogate	Microsoft Corporation	(Verified) Microsoft...
smartscreen.exe		8,020 K	23,472 K	5016	Windows Defender SmartScr...	Microsoft Corporation	(Verified) Microsoft...
WmiPrvSE.exe		2,220 K	9,032 K	8076	WMI Provider Host	Microsoft Corporation	(Verified) Microsoft...
svchost.exe		6,516 K	13,084 K	904	Host Process for Windows S...	Microsoft Corporation	(Verified) Microsoft...
svchost.exe		2,592 K	10,684 K	960	Host Process for Windows S...	Microsoft Corporation	(Verified) Microsoft...
svchost.exe		3,976 K	12,408 K	372	Host Process for Windows S...	Microsoft Corporation	(Verified) Microsoft...
svchost.exe		1,912 K	9,960 K	676	Host Process for Windows S...	Microsoft Corporation	(Verified) Microsoft...
svchost.exe		3,548 K	7,852 K	1112	Host Process for Windows S...	Microsoft Corporation	(Verified) Microsoft...
svchost.exe		1,196 K	5,436 K	1120	Host Process for Windows S...	Microsoft Corporation	(Verified) Microsoft...
svchost.exe		1,608 K	12,072 K	1128	Host Process for Windows S...	Microsoft Corporation	(Verified) Microsoft...
svchost.exe	< 0.01	16,244 K	21,204 K	1136	Host Process for Windows S...	Microsoft Corporation	(Verified) Microsoft...
svchost.exe		1,524 K	7,212 K	1144	Host Process for Windows S...	Microsoft Corporation	(Verified) Microsoft...
svchost.exe		3,076 K	10,116 K	1240	Host Process for Windows S...	Microsoft Corporation	(Verified) Microsoft...
svchost.exe		1,896 K	7,736 K	1248	Host Process for Windows S...	Microsoft Corporation	(Verified) Microsoft...

- Run any malware:

Process Explorer - Sysinternals: www.sysinternals.com [EXPAT,Expat] (Administrator)

File Options View Process Find Users Help

<Filter by name>

Process	CPU	Private Bytes	Working Set	PID	Description	Company Name	Verified Signer	VirusTotal	Command Line
conhost.exe		6,212 K	10,860 K	6724	Console Window Host	Microsoft Corporation	(Verified) Microsoft Windows	0/73	\\??C:\WINDOW...
conhost.exe		6,340 K	11,232 K	6372	Console Window Host	Microsoft Corporation	(Verified) Microsoft Windows	0/73	\\??C:\WINDOW...
conhost.exe		6,304 K	11,204 K	7852	Console Window Host	Microsoft Corporation	(Verified) Microsoft Windows	0/73	\\??C:\WINDOW...
conhost.exe		6,996 K	16,716 K	6764	Console Window Host	Microsoft Corporation	(Verified) Microsoft Windows	0/73	\\??C:\WINDOW...
csrss.exe		1,912 K	5,460 K	644	Client Server Runtime Process	Microsoft Corporation	(Verified) Microsoft Windows Publisher	0/71	%SystemRoot%\s...
csrss.exe		7,056 K	5,892 K	788	Client Server Runtime Process	Microsoft Corporation	(Verified) Microsoft Windows Publisher	0/71	%SystemRoot%\s...
ctfmon.exe		5,728 K	28,764 K	4368	CTF Loader	Microsoft Corporation	(Verified) Microsoft Windows	0/72	"ctfmon.exe"
DiaSvc.exe		3,380 K	8,444 K	4264	Dropbox Service	Dropbox, Inc.	(Verified) Dropbox, Inc.	0/23	C:\WINDOWS\sy...
dlhst.exe		3,128 K	10,956 K	6992	COM Surrogate	Microsoft Corporation	(Verified) Microsoft Windows	0/23	C:\WINDOWS\S...
dlhst.exe		5,544 K	14,696 K	8820	COM Surrogate	Microsoft Corporation	(Verified) Microsoft Windows	0/23	C:\WINDOWS\S...
DriverUpdate.exe	< 0.01	59,504 K	1,328 K	9628	Driver Booster Driver Update	IObit	(Verified) IObit CO., LTD	1/23	"C:\Program Files...
Dropbox.exe	< 0.01	318,648 K	405,020 K	10992	Dropbox	Dropbox, Inc.	(Verified) Dropbox, Inc.	0/23	"C:\Program Files...
Dropbox.exe		2,688 K	9,960 K	11012	Dropbox	Dropbox, Inc.	(Verified) Dropbox, Inc.	0/23	"C:\Program Files...
Dropbox.exe		2,448 K	9,296 K	11040	Dropbox	Dropbox, Inc.	(Verified) Dropbox, Inc.	0/23	"C:\Program Files...
Dropbox.exe		3,164 K	12,680 K	11092	Dropbox	Dropbox, Inc.	(Verified) Dropbox, Inc.	0/23	"C:\Program Files...
DropboxUpdate.exe		2,112 K	4,536 K	4996	Dropbox Update	Dropbox, Inc.	(Verified) Dropbox, Inc.	0/23	"C:\Program Files...
dwm.exe	1.51	98,396 K	92,692 K	1204	Desktop Window Manager	Microsoft Corporation	(Verified) Microsoft Windows	0/23	"dwm.exe"
E_YATIUNE.EXE		4,608 K	11,712 K	9368	EPSON Status Monitor 3	Seiko Epson Corporation	(Verified) SEIKO EPSON CORPORATION	0/74	"C:\Windows\Sys...
EEventManager.exe	< 0.01	3,532 K	15,408 K	10840	Epson Event Manager	Seiko Epson Corporation	(No signature was present in the subject) Seiko Epson Corporation	0/70	"C:\Program Files...
EPCCMON.EXE		2,108 K	8,992 K	6692	Epson Printer Connection Ch...	Seiko Epson Corporation	(Verified) SEIKO EPSON CORPORATION	0/73	"C:\Program Files...
escsvc64.exe		1,388 K	6,640 K	4348	Epson Scanner Service (64bt)	Seiko Epson Corporation	(Verified) SEIKO EPSON CORPORATION	0/72	C:\WINDOWS\sy...
explorer.exe	< 0.01	94,768 K	185,356 K	2024	Windows Explorer	Microsoft Corporation	(Verified) Microsoft Windows	0/72	C:\WINDOWS\E...
firefox.exe	< 0.01	302,100 K	20,212 K	11904	Firefox	Mozilla Corporation	(Verified) Mozilla Corporation	0/72	"C:\Program Files...
firefox.exe	< 0.01	292,136 K	10,096 K	1576	Firefox	Mozilla Corporation	(Verified) Mozilla Corporation	0/72	"C:\Program Files...
firefox.exe	< 0.01	223,824 K	13,108 K	11684	Firefox	Mozilla Corporation	(Verified) Mozilla Corporation	0/72	"C:\Program Files...
firefox.exe		47,124 K	3,420 K	5988	Firefox	Mozilla Corporation	(Verified) Mozilla Corporation	0/72	"C:\Program Files...
firefox.exe		32,320 K	16 K	7708	Firefox	Mozilla Corporation	(Verified) Mozilla Corporation	0/72	"C:\Program Files...
firefox.exe	< 0.01	760,284 K	26,204 K	8080	Firefox	Mozilla Corporation	(Verified) Mozilla Corporation	0/72	"C:\Program Files...
firefox.exe	< 0.01	85,804 K	15,324 K	10356	Firefox	Mozilla Corporation	(Verified) Mozilla Corporation	0/72	"C:\Program Files...
firefox.exe		27,420 K	16 K	11928	Firefox	Mozilla Corporation	(Verified) Mozilla Corporation	0/72	"C:\Program Files...
Firemin_X64.exe	1.13	33,076 K	38,204 K	10956	Firemin	Rizonesoft	(Verified) Open Source Developer Detick Payne	4/74	"C:\Program Files...
fontdrvhost.exe		6,400 K	12,704 K	780	Usemode Font Driver Host	Microsoft Corporation	(Verified) Microsoft Windows	0/23	"fontdrvhost.exe"
fontdrvhost.exe		1,744 K	4,424 K	776	Usemode Font Driver Host	Microsoft Corporation	(Verified) Microsoft Windows	0/23	"fontdrvhost.exe"
FontReaderUpdateService.exe	< 0.01	1,532 K	7,740 K	4384	Font Reader Update Service	Font Software Inc.	(Verified) FONT SOFTWARE INC.	0/74	"C:\PROGRAM FI...
GoogleCrashHandler.exe		1,812 K	1,100 K	1224	Google Crash Handler	Google LLC	(Verified) Google LLC	0/73	"C:\Program Files...
GoogleCrashHandler64.exe		1,860 K	1,040 K	1232	Google Crash Handler	Google LLC	(Verified) Google LLC	0/71	"C:\Program Files...

0/72 "C:\Program Files..."
 4/74 "C:\Program Files..."
 0/73 "fontdrvhost.exe"

- Found this Firemin_X64 malware found

firefox.exe:11904 Properties

Image Performance Performance Graph Disk and Network

GPU Graph Threads TCP/IP Security Environment Strings

☒ Resolve addresses

P...	Local Address	Remote Address	State
TCP	expat:1055	ec2-44-241-251-147.us-west-2.comput...	ESTA
TCP	expat:1388	104.16.248.249.https	ESTA
TCP	expat.ms-olap3	239.237.117.34.bc.googleusercontent...	ESTA
TCP	expat:2453	server-13-226-235-121.lax50.r.cloudfro...	ESTA
TCP	expat:2046	expat:2047	ESTA
TCP	expat:2047	expat:2046	ESTA