Analysis Report

ID	acd277dca4b8eef93d654c6bc9ab3c32
OS	2600.xpsp.080413-2111
Started	8/11/16 18:35:54
Ended	8/11/16 18:41:46
Duration	0:05:52
Sandbox	car-work-055 (pilot-d)
Filename	sample.exe
Magic Type	PE32 executable (GUI) Intel 80386, for MS Windows
Analyzed As	exe
SHA256	2ee811948ac77d720144bd0dfa257dd46a79b1cfd774e8cc639a1101d96b6d84
SHA1	cd10b653a876d5ca58341f10cc490de464378632
MD5	e1db2ec3a8060dba3555dcc4e0f97706

Warnings

Executable Failed Integrity Check

Behavioral Indicators

Possible CyberGate Rat Detected

Severity: 100 **Confidence: 100**

CyberGate is a Remote Access Tool (RAT). It is based on SpyNet and is related to other RAT trojans (Xtreme, DarkComet). CyberGate allows an attacker to browse and manipulate files, devices and settings of the target as well as download and execute new material. It also has a wide range of media capturing abilities, such as keyloggers, screen, audio and video capture and remote enabling of webcams. It is also capable of URL redirection.

Categories	malware
Tags	trojan, host, RAT

Excessive Remote Process Code Injection Detected

Severity: 95 **Confidence: 100**

A process was detected injecting code into multiple other processes. Legitimate programs may inject code into a remote process on occasion, especially for debugging. In order to bypass Data Execution Prevention (DEP), memory allocated within a process must be marked with the flag PAGE_EXECUTE_READWRITE. Malware will often allocate memory in this way for remote processes to inject code. In this case, a process allocated a memory region in several processes with the Read/Write/Execute privileges.

Categories	evasion
Tags	memory, injection, threshold

Process ID	Process Name
1304 (seq.exe)	seq.exe

Artifact Flagged by Antivirus Service

Severity: 100 **Confidence: 95**

An antivirus service flagged an artifact as potentially malicious. Online services, such as VirusTotal, leverage a large number of antivirus engines and their data when testing a file. This oftentimes will fill in gaps left by using a single antivirus engine. However, due to false-positives, having a single antivirus engine flag a file is often insufficient to determine if the file truly is malicious. Conversely, if multiple engines detect a threat, then it is almost certain the file performs some degree of undesirable behavior.

Categories forensics
Tags file, antivirus

Artifact ID	SHA256	Path
13	2ee811948ac77d720144bd0dfa257dd46a79b1cfd774e8cc639a1101d96b6d84	\TEMP\sample.exe
26	2ee811948ac77d720144bd0dfa257dd46a79b1cfd774e8cc639a1101d96b6d84	sample.exe

.NET Process Used in Process Hollowing

Severity: 95 **Confidence: 100**

The sample contains .NET tools that are launched with invalid options. This is a sign of a process-hollowing technique used by .NET applications. In process-hollowing, a dummy process is started in a suspended state, then the existing sections of the executable in memory are overwritten with the injected code. Malware uses this technique to inject malicious code into a common program and bypass checks for odd programs in the process table.

Categories evasion
Tags process, .NET, hollowing, injection

Process ID	Process Name	Command Line
1996 (RegSvcs.exe)	RegSvcs.exe	"C:\WINDOWS\Microsoft.NET\Framework\v2.0.50727\RegSvcs.exe"
1228 (RegSvcs.exe)	RegSvcs.exe	C:\WINDOWS\Microsoft.NET\Framework\v2.0.50727\RegSvcs.exe

Excessive Suspicious Activity Detected

Severity: 90 **Confidence: 100**

The submitted sample has been observed performing a number of suspicious actions. None of the individual actions by themselves are particularly malicious, but when all behaviors are observed together they can be considered malicious. For information about the suspicious activities, refer to the other indicators triggered by this sample.

Categories compound
Tags suspicious, threshold

Registry Persistance Mechanism Refers to an Executable in a User Data Directory

Severity: 90 **Confidence: 100**

Registry keys can be used to load applications when Windows is started. Malware often uses these key locations to maintain persistence on the host. The key value will indicate where the program that will load on startup is located. If that program is located in a user data folder, it can be considered particularly suspicious.

Categories persistence
Tags process, autorun, registry

	RegKey Data	RegKey Value	

RegKey Data	Type	Name	RegKey Name
C:\Documents and Settings\Administrator\Application Data\pbt\seq.exe C:\DOCUME~1\ADMINI~1\APPLIC~1\pbt\dit.ktcs\\0	SZ	WindowsUpdaters	MACHINE\SOFTWARE\MICROSOENTVERSION\RUN
C:\Documents and Settings\Administrator\Application Data\pbt\seq.exe C:\DOCUME~1\ADMINI~1\APPLIC~1\pbt\dit.ktcs\\0	SZ	WindowsUpdaters	MACHINE\SOFTWARE\MICROSOENTVERSION\RUN

Process Hollowing Detected	Severity: 90	Confidence: 95
File Name of Executable on Disk Does Not Match Original File Name	Severity: 80	Confidence: 100
Process Sends ICMP Traffic	Severity: 70	Confidence: 90
Process Modified an Executable File	Severity: 60	Confidence: 100

Malware will modify executables on a system, to hide logs or other evidence. Also, by modifying various executables it can disable functionality in the system which may detect or hamper the operation of the malware. Lastly, it may be attempting to hide an executable, so that it appears to be a legitimate file. Please review the 'Disk Artifacts' section in order to view additional details about this file.

Categories file, persistence
Tags executable, file, process, PE

Path	Process Name	Process ID
\Documents and Settings\Administrator\Application Data\pbt\seq.exe	sample.exe	1992 (sample.exe)

Process Modified File in a User Directory	Severity: 70	Confidence: 80
Process Modified Autorun Registry Key Value	Severity: 80	Confidence: 60
Dynamic DNS Domain Detected	Severity: 50	Confidence: 60
Potential Code Injection Detected	Severity: 50	Confidence: 50
PE Resource Indicates Spanish Origin	Severity: 25	Confidence: 60
Executable Signed With Digital Certificate	Severity: 10	Confidence: 100
Executable with Encrypted Sections	Severity: 30	Confidence: 30
Executable Packed with UPX	Severity: 30	Confidence: 30
Artifact Packed with RAR	Severity: 30	Confidence: 30
DNS Response Contains Low Time to Live (TTL) Value	Severity: 35	Confidence: 20
Domain Resolves to Localhost	Severity: 25	Confidence: 25
RAT Queried Domain	Severity: 25	Confidence: 25
Executable Imported the IsDebuggerPresent Symbol	Severity: 20	Confidence: 20

HTTP Traffic

DNS Traffic

Query Type: A, Query Data: put0carad3verg4.strangled.net Stream: 4 Query: 21717

TTL: -
Timestamp: +139.096s

Query Type: A, Query Data: wins10up.16-b.it Stream: 4 Query: 21916

TTL: -
Timestamp: +84.578s

Query Type: A, Query Data: www.google.com Stream: 4 Query: 25330

TTL: -
Timestamp: +51.396s

Query Type: A, Query Data: clar0dsl.serveminecraft.net Stream: 4 Query: 35435

TTL: -
Timestamp: +148.767s

Query Type: A, Query Data: sslwin.moneyhome.biz Stream: 4 Query: 54106

TTL: -
Timestamp: +111.936s

Query Type: A, Query Data: k4l1m3r4.publicvm.com Stream: 4 Query: 56703

TTL: -
Timestamp: +57.338s

Query Type: A, Query Data: wins10up.16-b.it Stream: 10 Query: 12626

TTL: -
Timestamp: +184.942s

TCP/IP Streams

Network Stream: 0

Src. IP 0.0.0.0
Src. Port 68
Dest. IP 255.255.255.255
Dest. Port 67
Transport UDP
Artifacts 0
Packets 3
Bytes 989
Timestamp +27.268s

Network Stream: 1 (DHCP)

Src. IP 172.16.159.201
Src. Port 68
Dest. IP 172.16.1.1
Dest. Port 67
Transport UDP
Artifacts 0
Packets 2
Bytes 656
Timestamp +28.041s

Network Stream: 2

Src. IP 172.16.1.1
Src. Port 8
Dest. IP 172.16.159.201
Dest. Port 0
Transport ICMP
Artifacts 0
Packets 2
Bytes 96
Timestamp +28.056s

Network Stream: 3

Src. IP 172.16.159.201
Src. Port 1045
Dest. IP 239.255.255.250
Dest. Port 1900
Transport UDP
Artifacts 0
Packets 3
Bytes 483
Timestamp +30.225s

Network Stream: 4 (DNS)

Src. IP 172.16.159.201
Src. Port 1047
Dest. IP 172.16.1.1
Dest. Port 53
Transport UDP
Artifacts 0
Packets 12
Bytes 902
Timestamp +51.396s

Network Stream: 5

Src. IP 172.16.159.201
Src. Port 8
Dest. IP 216.58.218.132
Dest. Port 0
Transport ICMP
Artifacts 0
Packets 2
Bytes 128
Timestamp +51.426s

Network Stream: 6

Src. IP 172.16.159.201
Src. Port 1048
Dest. IP 187.189.61.165
Dest. Port 900
Transport TCP
Artifacts 0
Packets 3
Bytes 144
Timestamp +57.362s

Network Stream: 7

Src. IP 172.16.159.201

Src. Port 1049
Dest. IP 187.155.176.22
Dest. Port 900
Transport TCP
Artifacts 0
Packets 3
Bytes 144
Timestamp +84.68s

Network Stream: 8

Src. IP 172.16.159.201
Src. Port 1050
Dest. IP 187.136.81.43
Dest. Port 900
Transport TCP
Artifacts 0
Packets 3
Bytes 144
Timestamp +111.982s

Network Stream: 9

Src. IP 172.16.159.201
Src. Port 1053
Dest. IP 187.189.61.165
Dest. Port 900
Transport TCP
Artifacts 0
Packets 3
Bytes 144
Timestamp +157.603s

Network Stream: 10 (DNS)

Src. IP 172.16.159.201
Src. Port 1047
Dest. IP 172.16.1.1
Dest. Port 53
Transport UDP
Artifacts 0
Packets 2
Bytes 140
Timestamp +184.942s

Network Stream: 11

Src. IP 172.16.159.201
Src. Port 1054
Dest. IP 187.155.34.157
Dest. Port 900
Transport TCP
Artifacts 0
Packets 61
Bytes 9901
Timestamp +185.163s

Processes

Name: sample.exe

PID: 1992
Children: 1
File Actions: 21
Registry Actions: 22
Analysis Reason: Is target sample.

Name: RegSvcs.exe

Parent: 1992

PID: 904
Children: 1
File Actions: 4
Registry Actions: 22
Analysis Reason: Parent is being analyzed

Name: seq.exe

Parent: 904

PID: 1304
Children: 1
File Actions: 3
Registry Actions: 14
Analysis Reason: Parent is being analyzed

Name: RegSvcs.exe

Parent: 1304

PID: 1996
Children: 0
File Actions: 4
Registry Actions: 18
Analysis Reason: Parent is being analyzed

Name: wmiprvse.exe

PID: 452
Children: 0
File Actions: 0
Registry Actions: 0
Analysis Reason: Process activity after target sample started.

Children: 0
File Actions: 0
Registry Actions: 0
Analysis Reason: Process activity after target sample started.

Name: services.exe

PID: 660
Children: 0
File Actions: 0
Registry Actions: 0
Analysis Reason: Process activity after target sample started.

Name: unknown

PID: 672
Children: 0
File Actions: 1
Registry Actions: 0
Analysis Reason: Process activity after target sample started.

Name: svchost.exe

PID: 920
Children: 0
File Actions: 0
Registry Actions: 0
Analysis Reason: Process activity after target sample started.

Name: svchost.exe

PID: 1028
Children: 0
File Actions: 4
Registry Actions: 2
Analysis Reason: Process activity after target sample started.

Name: svchost.exe

PID: 1048
Children: 0
File Actions: 0
Registry Actions: 0
Analysis Reason: Process activity after target sample started.

Name: RegSvcs.exe

PID: 1228
Children: 0
File Actions: 1
Registry Actions: 15
Analysis Reason: Process activity after target sample started.

Name: Explorer.EXE

PID: 1400
Children: 0
File Actions: 0
Registry Actions: 0
Analysis Reason: Process activity after target sample started.

Metadata | Behavioral Indicators | Network Activity | Processes | Artifacts | Registry Activity | File Activity

Artifact 1: \Documents and Settings\Administrator...Bx\ZWcCUkGLY8aBx.dat

Src: disk
Imports: 0
Type: data
SHA256: `3b271649a94ad5be4ef46ecbb6a4e7363e8498b7e69b751737bf30df2e0d1dde`
Size: 2
Exports: 0
AV Sigs: 0
MD5: `93e00066d099c0485cfffa1359246d26`

Artifact 2: \WINDOWS\system32\config\SysEvent.Evt

Src: disk
Imports: 0
Type: data
SHA256: `b7adc757a5a3b9ab60d2d957123d371ed45837341ba9c5560d3c5851998ce6ae`
Size: 65536
Exports: 0
AV Sigs: 0

MD5 : eb0c3ecfecdbdcb345abf0cdfe9be571

Artifact 3: \Documents and Settings\Administrator...on Data\pbt\apk.docx

Modified by: 1992 (sample.exe)

Src: disk
Imports: 0
Type: ASCII text, with very long lines, with CRLF line terminators
SHA256: 236f175e24ee3e266bd8c25b7dbcd9d1a808058e6be206c6079b89a7473fb937
Size: 38827
Exports: 0
AV Sigs: 0
MD5 : 1d5cb4c34d2c4a0d3cbde8135a769752

Artifact 4: \Documents and Settings\Administrator...ion Data\pbt\ndh.ico

Modified by: 1992 (sample.exe)

Src: disk
Imports: 0
Type: ASCII text, with very long lines, with CRLF line terminators
SHA256: 68ce00ea2f152228d5f657a44ba8690ea2748231975ef90c1ed1e0e3d2e4207e
Size: 38033
Exports: 0
AV Sigs: 0
MD5 : c9792f1f6fc74691c2d390a58aa5d591

Artifact 5: \Documents and Settings\Administrator...ion Data\pbt\mke.dat

Modified by: 1992 (sample.exe)

Src: disk
Imports: 0
Type: ASCII text, with very long lines, with CRLF line terminators
SHA256: ad2d05ea9f32441472da292c783913dc4a3145710d4d9e56b7c53e5c684264ec
Size: 24066
Exports: 0
AV Sigs: 0
MD5 : 03dbc4243e20225d9bd9d6c64e4aae46

Artifact 6: \Documents and Settings\Administrator...ion Data\pbt\uhb.jpg

Modified by: 1992 (sample.exe)

Src: disk
Imports: 0
Type: ASCII text, with very long lines, with CRLF line terminators
SHA256: f8f09c225dbeda097a57158167e466329b2bd8d806f0da3494264e18f83692f7
Size: 48818
Exports: 0
AV Sigs: 0
MD5 : db93c6dc0ad50f7e881c775a5f24ee23

Artifact 7: \Documents and Settings\Administrator...ion Data\pbt\jjw.ico

Modified by: 1992 (sample.exe)

Src: disk
Imports: 0
Type: ASCII text, with very long lines, with CRLF line terminators
SHA256: ff5f97ce7f5d7246c97326aebf348d8df3ce527278e05dd225a05965872b1486
Size: 37300
Exports: 0
AV Sigs: 0
MD5 : 8af381e5cd4a7d08b2dc524bb272d849

Artifact 8: \Documents and Settings\Administrator...ion Data\pbt\dit.ktc

Modified by: 1992 (sample.exe)

Src: disk
Imports: 0
Type: ASCII text, with very long lines, with CRLF line terminators

SHA256: 6655d1a98eece7b2aed46a66729e92633ad5126d06d4c8a07e3e0d9eb2106055
Size: 406021
Exports: 0
AV Sigs: 0
MD5: 065a6e4e5c22ae26f84fa96da9bb843a

Artifact 9: \Documents and Settings\Administrator...ion Data\pbt\wsl.ppt

Modified by: 1992 (sample.exe)

Src: disk
Imports: 0
Type: ASCII text, with very long lines, with CRLF line terminators
SHA256: 1fd4e769d5c37296ed89fab18c24e7791f2826d5908d6c575da4bc97c3f12e4e
Size: 1069845
Exports: 0
AV Sigs: 0
MD5: ae20e856438e0e4aed68d3b29bb00b89

Artifact 10: \Documents and Settings\Administrator...Bx\ZWcCUkGLY8aBx.svr

Modified by: 1996 (RegSvcs.exe)

Src: disk
Imports: 0
Type: data
SHA256: 95e4f8cf64c5311a338587db944bf1c18bcbe705226b7aa81a46fb96bff0a7e5
Size: 365086
Exports: 0
AV Sigs: 0
MD5: 74b95118128f276328bd18db61c141f0

Artifact 11: \Documents and Settings\Administrator...Bx\ZWcCUkGLY8aBx.nfo

Created by: 1996 (RegSvcs.exe)

Src: disk
Imports: 0
Type: data
SHA256: b7b9c173d28df1e581f50c2eb321323afdd8bba308ae01fd23402e15b31941f3
Size: 3604
Exports: 0
AV Sigs: 0
MD5: 0097ffd3c0d7fee5deb04c5503189995

Artifact 12: \Documents and Settings\Administrator...ion Data\pbt\seq.exe

Modified by: 1992 (sample.exe)

Src: disk
Imports: 500
Type: DLL - PE32 executable (GUI) Intel 80386, for MS Windows
SHA256: fb73a819b37523126c7708a1d06f3b8825fa60c926154ab2d511ba668f49dc4b
Size: 750320
Exports: 0
AV Sigs: 0
MD5: 71d8f6d5dc35517275bc38ebcc815f9f

Artifact 13: \TEMP\sample.exe

Read by: 1992 (sample.exe)

Src: disk
Imports: 168
Type: EXE - PE32 executable (GUI) Intel 80386, for MS Windows, ...
SHA256: 2ee811948ac77d720144bd0dfa257dd46a79b1cfd774e8cc639a1101d96b6d84
Size: 1589018
Exports: 0
AV Sigs: 0

MD5 : e1db2ec3a8060dba3555dcc4e0f97706

Artifact 14: 904-RegSvcs.exe

Related to: 904 (RegSvcs.exe)

Src: memory
Imports: 500
Type: DLL - PE32 executable (GUI) Intel 80386, for MS Windows
SHA256: 01a4ec924b727a8e7d7b9a43344c51146562cc7813b018973c84cf9989066cb8
Size: 742400
Exports: 0
AV Sigs: 0
MD5 : 8423c613038d45505e9a05583a1a69e1

Artifact 15: 660-services.exe

Related to: 660 (services.exe)

Src: memory
Imports: 274
Type: DLL - PE32 executable (GUI) Intel 80386, for MS Windows
SHA256: 0377a99a8c7f6c7b043f5da283a1404846c597d0fd7214950b5d64de5eabde3a
Size: 108544
Exports: 0
AV Sigs: 0
MD5 : 504961cea9d742df793f9e558c14125d

Artifact 16: 616-winlogon.exe

Related to: 616 (winlogon.exe)

Src: memory
Imports: 159
Type: DLL - PE32 executable (GUI) Intel 80386, for MS Windows
SHA256: 0de12e51cb647c7a2a1e4001735c0c08dc40daaa7ece9ef843074d96683e2fdb
Size: 507904
Exports: 0
AV Sigs: 0
MD5 : 7e14837d88f0215117ed2d2ecb320e86

Artifact 17: 1228-RegSvcs.exe

Related to: 1228 (RegSvcs.exe)

Src: memory
Imports: 28
Type: DLL - PE32 executable (GUI) Intel 80386, for MS Windows, ...
SHA256: 2de82db1b809ea412fc563e9c06eeca44293820441c050587b7dc154be7f87b2
Size: 365056
Exports: 0
AV Sigs: 0
MD5 : 2de7c29fc36a26598db0f45e627f369f

Artifact 18: 1400-Explorer.EXE

Related to: 1400 (Explorer.EXE)

Src: memory
Imports: 500
Type: DLL - PE32 executable (GUI) Intel 80386, for MS Windows
SHA256: 46ad99320c1b0142ddf929de42fe187ee251317b95ebb63c53de433424d7bbe9
Size: 1033728
Exports: 0
AV Sigs: 0
MD5 : 95211359cd81f7efe3c848154a29b643

Artifact 19: 920-svchost.exe

Related to: 920 (svchost.exe)

Src: memory
Imports: 79
Type: DLL - PE32 executable (GUI) Intel 80386, for MS Windows

SHA256: 5d4942c54308eb195f45413fda6ae0406dd3001504bddd3f769ec239ddd35670
Size: 14336
Exports: 0
AV Sigs: 0
MD5: c45eb0c386f2ca7b80186a364b8562b3

Artifact 20: 524-smss.exe

Related to: 524 (smss.exe)

Src: memory
Imports: 52
Type: DLL - PE32 executable (native) Intel 80386, for MS Windows
SHA256: 66ae51c3eb307d0cbca93978d1ea33239f4a1863557896a189ecf372f801e4d9
Size: 50688
Exports: 0
AV Sigs: 0
MD5: fe407b76b717147caeff6eab9ffc6c93

Artifact 21: 1048-svchost.exe

Related to: 1048 (svchost.exe)

Src: memory
Imports: 79
Type: DLL - PE32 executable (GUI) Intel 80386, for MS Windows
SHA256: 75a774459b9d694ee5e1c76b4c48a91d88ed6a1b647806081342d73b9f7c35dc
Size: 14336
Exports: 0
AV Sigs: 0
MD5: a9af1a50669f672c2a6bdcc3811ac27b

Artifact 22: 592-csrss.exe

Related to: 592 (csrss.exe)

Src: memory
Imports: 12
Type: DLL - PE32 executable (native) Intel 80386, for MS Windows
SHA256: 8693aa906c6e8bcbf12f64e53a803e18e0eb562c717b6d09d91fec737c9e93b5
Size: 6144
Exports: 0
AV Sigs: 0
MD5: 9df924c7a1b9ffa0117534939471f71d

Artifact 23: 1028-svchost.exe

Related to: 1028 (svchost.exe)

Src: memory
Imports: 79
Type: DLL - PE32 executable (GUI) Intel 80386, for MS Windows
SHA256: ad5a5302cfbc769b550c1dac24e4d8fc746557a23e9d520ecec5bf73b290457c
Size: 14336
Exports: 0
AV Sigs: 0
MD5: d2f510c2b37c665efccedfd102780c9f

Artifact 24: 852-svchost.exe

Related to: 852 (svchost.exe)

Src: memory
Imports: 79
Type: DLL - PE32 executable (GUI) Intel 80386, for MS Windows
SHA256: c649b0c85a7a192083fe4a35c08a00cc9fd988d507efc65f0a8ce84e0c2bd23a
Size: 14336
Exports: 0
AV Sigs: 0
MD5: 8091101992ec47fdfd955757d9688334

Artifact 25: 1532-svchost.exe

Related to: 1532 (svchost.exe)

Src: memory
Imports: 79
Type: DLL - PE32 executable (GUI) Intel 80386, for MS Windows
SHA256: `fad97736580b566e83ca6ab12b38ec8c09bef45be8e606fac4ea230f572f9483`
Size: 14336
Exports: 0
AV Sigs: 0
MD5: `0a7400ae760cb22ea8986390fafc251c`

Artifact 26: sample.exe

Src: submitted
Imports: 168
Type: EXE - PE32 executable (GUI) Intel 80386, for MS Windows, ...
SHA256: `2ee811948ac77d720144bd0dfa257dd46a79b1cfd774e8cc639a1101d96b6d84`
Size: 1589018
Exports: 0
AV Sigs: 0
MD5: `e1db2ec3a8060dba3555dcc4e0f97706`

Registry Activity

Created Keys

Created Key	PID	Access List	Option List
USER\S-1-5-21-1202660629-583907252-1801674531-500\SOFTWARE\1996	1996 (RegSvcs.exe)	MAXIMUM_ALLOWED	REG_OPTION_NON_VOLATILE
USER\S-1-5-21-1202660629-583907252-1801674531-500\SOFTWARE\ZWcCUkGLY8aBx	1996 (RegSvcs.exe)	MAXIMUM_ALLOWED	REG_OPTION_NON_VOLATILE

Deleted Keys

Deleted Key	PID
USER\S-1-5-21-1202660629-583907252-1801674531-500\SOFTWARE\1996	1228 (RegSvcs.exe)

Modified Keys

Modified Key	PID	Value Name	Data
USER\S-1-5-21-1202660629-583907252-1801674531-500\SOFTWARE\MICROSOFT\WINDOWS\SHELLNOROAMMUICACHE	1992 (sample.exe)	C:\Documents and Settings\Administrator\Application Data\pbt\seq.exe	AutoIt v3 Scri
MACHINE\SOFTWARE\MICROSOFT\WINDOWS\CURRENTVERSION\EXPLORER\SHELL FOLDERS	1992 (sample.exe)	Common Documents	C:\Document
MACHINE\SOFTWARE\MICROSOFT\CRYPTOGRAPHY\RNG	1992 (sample.exe)	Seed	ux1TXpzfqZ7 72HKVjRf7bu
USER\S-1-5-21-1202660629-583907252-1801674531-500\SOFTWARE\MICROSOFT\WINDOWS\CURRENTVERSION\EXPLOR	1992 (sample.exe)	Cookies	C:\Document

ER\SHELL FOLDERS			
USER\S-1-5-21-1202660629-583907252-1801674531-500\SOFTWARE\MICROSOFT\WINDOWS\CURRENTVERSION\EXPLORER\MOUNTPOINTS2\{2421CC9A-3EFF-11E6-A1E7-FC8CDBFBD8A2}	1992 (sample.exe)	BaseClass	Drive
USER\S-1-5-21-1202660629-583907252-1801674531-500\SOFTWARE\MICROSOFT\WINDOWS\CURRENTVERSION\INTERNET SETTINGS\ZONEMAP	1992 (sample.exe)	IntranetName	1
MACHINE\SOFTWARE\MICROSOFT\CRYPTOGRAPHY\RNG	1992 (sample.exe)	Seed	QCeFarcNBK OQncY1YZj2
MACHINE\SOFTWARE\MICROSOFT\CRYPTOGRAPHY\RNG	1992 (sample.exe)	Seed	NgZgX+AJriy E326rcveaqI
MACHINE\SOFTWARE\MICROSOFT\CRYPTOGRAPHY\RNG	1992 (sample.exe)	Seed	tbzCXtSXFbw Yi8k47B1qjS
USER\S-1-5-21-1202660629-583907252-1801674531-500\SOFTWARE\MICROSOFT\WINDOWS\CURRENTVERSION\EXPLORER\SHELL FOLDERS	1992 (sample.exe)	Cache	C:\Document Internet Files
MACHINE\SOFTWARE\MICROSOFT\CRYPTOGRAPHY\RNG	1992 (sample.exe)	Seed	O78Am7yGH UHsXmS5Ta
USER\S-1-5-21-1202660629-583907252-1801674531-500\SOFTWARE\MICROSOFT\WINDOWS\CURRENTVERSION\EXPLORER\MOUNTPOINTS2\{1209A444-8D68-11E1-9FE0-806D6172696F}	1992 (sample.exe)	BaseClass	Drive
USER\S-1-5-21-1202660629-583907252-1801674531-500\SOFTWARE\MICROSOFT\WINDOWS\CURRENTVERSION\EXPLORER\MOUNTPOINTS2\{75EF541F-D065-11E1-AC7A-525400123456}	1992 (sample.exe)	BaseClass	Drive
MACHINE\SOFTWARE\MICROSOFT\CRYPTOGRAPHY\RNG	1992 (sample.exe)	Seed	GepOmaqIw VHvDFD2/1d
MACHINE\SOFTWARE\MICROSOFT\CRYPTOGRAPHY\RNG	1992 (sample.exe)	Seed	KPXEwZ982 dARSSBFsU
USER\S-1-5-21-1202660629-583907252-1801674531-500\SOFTWARE\MICROSOFT\WINDOWS\CURRENTVERSION\EXPLORER\MOUNTPOINTS2\{AF5E62D0-F159-11E5-A1E5-00501E3AE7B5}	1992 (sample.exe)	BaseClass	Drive
MACHINE\SOFTWARE\MICROSOFT\CRYPTOGRAPHY\RNG	1992 (sample.exe)	Seed	wZTxlNbivOn RX2NpzE9qa
USER\S-1-5-21-1202660629-583907252-1801674531-500\SOFTWARE\MICROSOFT\WINDOWS\CURRENTVERSION\EXPLORER\SHELL FOLDERS	1992 (sample.exe)	Personal	C:\Document
USER\S-1-5-21-1202660629-583907252-1801674531-500\SOFTWARE\MICROSOFT\WINDOWS\CURRENTVERSION\INTERNET SETTINGS\ZONEMAP	1992 (sample.exe)	ProxyBypass	1
USER\S-1-5-21-1202660629-583907252-1801674531-500\SOFTWARE\MICROSOFT\WINDOWS\CURRENTVERSION\INTERNET SETTINGS\ZONEMAP	1992 (sample.exe)	UNCAsIntranet	1
MACHINE\SOFTWARE\MICROSOFT\WINDOWS\CURRENTVERSION\EXPLORER\SHELL FOLDERS	1992 (sample.exe)	Common Desktop	C:\Document
USER\S-1-5-21-1202660629-583907252-1801674531-500\SOFTWARE\MICROSOFT\WINDOWS\CURRENTVERSION\EXPLORER\SHELL FOLDERS	1992 (sample.exe)	Desktop	C:\Document
MACHINE\SOFTWARE\MICROSOFT\CRYPTOGRAPHY\RNG	904 (RegSvcs.exe)	Seed	55AZ8ncknP kV8DWpVzxr
MACHINE\SOFTWARE\MICROSOFT\CRYPTOGRAPHY\RNG	904 (RegSvcs.exe)	Seed	5rAZmTHjwd IH+DEa09Je
MACHINE\SOFTWARE\MICROSOFT\CRYPTOGRAPHY\RNG	904 (RegSvcs.exe)	Seed	Sx9k1n/7Lq3 qmAQ5UVrjb
MACHINE\SOFTWARE\MICROSOFT\CRYPTOGRAPHY\RNG	904	Seed	cc3ITMp/MYC

	(RegSvcs.exe)		+pX26lPcct1
MACHINE\SOFTWARE\MICROSOFT\CRYPTOGRAPHY\RNG	904 (RegSvcs.exe)	Seed	mdbSfXLh/l0 dlgDJRbikEl
MACHINE\SOFTWARE\MICROSOFT\CRYPTOGRAPHY\RNG	904 (RegSvcs.exe)	Seed	9lj37Ct6R72 NTEl0wQp9
MACHINE\SOFTWARE\MICROSOFT\CRYPTOGRAPHY\RNG	904 (RegSvcs.exe)	Seed	vel7EQsrATj C/NKb0cR+N
USER\S-1-5-21-1202660629-583907252-1801674531-500\SOFTWARE\MICROSOFT\WINDOWS\CURRENTVERSION\EXPLORER\MOUNTPOINTS2\{2421CC9A-3EFF-11E6-A1E7-FC8CDBFBD8A2}	904 (RegSvcs.exe)	BaseClass	Drive
MACHINE\SOFTWARE\MICROSOFT\WINDOWS\CURRENTVERSION\RUN	904 (RegSvcs.exe)	WindowsUpdaters	C:\Document C:\DOCUME~
USER\S-1-5-21-1202660629-583907252-1801674531-500\SOFTWARE\MICROSOFT\WINDOWS\CURRENTVERSION\EXPLORER\SHELL FOLDERS	904 (RegSvcs.exe)	AppData	C:\Document
MACHINE\SOFTWARE\MICROSOFT\CRYPTOGRAPHY\RNG	904 (RegSvcs.exe)	Seed	V5fyq4Tnfg4 l+0aSt19ovt8
MACHINE\SOFTWARE\MICROSOFT\CRYPTOGRAPHY\RNG	904 (RegSvcs.exe)	Seed	pwE0O8K/g9 DCzYFw/sM
USER\S-1-5-21-1202660629-583907252-1801674531-500\SOFTWARE\MICROSOFT\WINDOWS\CURRENTVERSION\EXPLORER\MOUNTPOINTS2\{75EF541F-D065-11E1-AC7A-525400123456}	904 (RegSvcs.exe)	BaseClass	Drive
USER\S-1-5-21-1202660629-583907252-1801674531-500\SOFTWARE\MICROSOFT\WINDOWS\CURRENTVERSION\EXPLORER\MOUNTPOINTS2\{AF5E62D0-F159-11E5-A1E5-00501E3AE7B5}	904 (RegSvcs.exe)	BaseClass	Drive
MACHINE\SOFTWARE\MICROSOFT\CRYPTOGRAPHY\RNG	904 (RegSvcs.exe)	Seed	14uq9RIbX5 i/PUwoh/BR
MACHINE\SOFTWARE\MICROSOFT\CRYPTOGRAPHY\RNG	904 (RegSvcs.exe)	Seed	ri8/7IoGGEiF 45XyL9oan7
USER\S-1-5-21-1202660629-583907252-1801674531-500\SOFTWARE\MICROSOFT\WINDOWS\CURRENTVERSION\EXPLORER\MOUNTPOINTS2\{1209A444-8D68-11E1-9FE0-806D6172696F}	904 (RegSvcs.exe)	BaseClass	Drive
MACHINE\SOFTWARE\MICROSOFT\CRYPTOGRAPHY\RNG	904 (RegSvcs.exe)	Seed	NBAk/4nGS3 SLnj4hb1xSp
MACHINE\SOFTWARE\MICROSOFT\CRYPTOGRAPHY\RNG	904 (RegSvcs.exe)	Seed	uh7WuQXZD TOnNSubQw =
MACHINE\SOFTWARE\MICROSOFT\CRYPTOGRAPHY\RNG	904 (RegSvcs.exe)	Seed	wIxoQuWIxM PXyXc5uR7M
MACHINE\SOFTWARE\MICROSOFT\CRYPTOGRAPHY\RNG	904 (RegSvcs.exe)	Seed	xbxwxT7ErVE nrbJbq59Dfff
MACHINE\SOFTWARE\MICROSOFT\CRYPTOGRAPHY\RNG	904 (RegSvcs.exe)	Seed	ibAO23Q0k9 MCnHOAzb3
MACHINE\SOFTWARE\MICROSOFT\WINDOWS\CURRENTVERSION\RUN	1304 (seq.exe)	WindowsUpdaters	C:\Document C:\DOCUME~
MACHINE\SOFTWARE\MICROSOFT\CRYPTOGRAPHY\RNG	1304 (seq.exe)	Seed	8E7fvPBBTC F+pr5sccu9N
USER\S-1-5-21-1202660629-583907252-1801674531-500\SOFTWARE\MICROSOFT\WINDOWS\CURRENTVERSION\EXPLORER\MOUNTPOINTS2\{2421CC9A-3EFF-11E6-A1E7-FC8CDBFBD8A2}	1304 (seq.exe)	BaseClass	Drive
MACHINE\SOFTWARE\MICROSOFT\CRYPTOGRAPHY\RNG	1304 (seq.exe)	Seed	8n0QBHKO5 w/9QPtYPbU

USER\S-1-5-21-1202660629-583907252-1801674531-500\SOFTWARE\MICROSOFT\WINDOWS\CURRENTVERSION\EXPLORER\MOUNTPOINTS2\{1209A444-8D68-11E1-9FE0-806D6172696F}	1304 (seq.exe)	BaseClass	Drive
MACHINE\SOFTWARE\MICROSOFT\CRYPTOGRAPHY\RNG	1304 (seq.exe)	Seed	WXfsJ3fU9N 2a+lpjL7xRP
USER\S-1-5-21-1202660629-583907252-1801674531-500\SOFTWARE\MICROSOFT\WINDOWS\CURRENTVERSION\EXPLORER\SHELL FOLDERS	1304 (seq.exe)	AppData	C:\Document
MACHINE\SOFTWARE\MICROSOFT\CRYPTOGRAPHY\RNG	1304 (seq.exe)	Seed	Vm383IfFsLs Ke85BDgAzo
MACHINE\SOFTWARE\MICROSOFT\CRYPTOGRAPHY\RNG	1304 (seq.exe)	Seed	Xj1L0npvhY1 m/Q8xM+d3u
MACHINE\SOFTWARE\MICROSOFT\CRYPTOGRAPHY\RNG	1304 (seq.exe)	Seed	GcDWESInim 9t5xW/TY7jcc
MACHINE\SOFTWARE\MICROSOFT\CRYPTOGRAPHY\RNG	1304 (seq.exe)	Seed	kwqGB5HXkI kvR2NtgCvHt
USER\S-1-5-21-1202660629-583907252-1801674531-500\SOFTWARE\MICROSOFT\WINDOWS\CURRENTVERSION\EXPLORER\MOUNTPOINTS2\{AF5E62D0-F159-11E5-A1E5-00501E3AE7B5}	1304 (seq.exe)	BaseClass	Drive
USER\S-1-5-21-1202660629-583907252-1801674531-500\SOFTWARE\MICROSOFT\WINDOWS\CURRENTVERSION\EXPLORER\MOUNTPOINTS2\{75EF541F-D065-11E1-AC7A-525400123456}	1304 (seq.exe)	BaseClass	Drive
MACHINE\SOFTWARE\MICROSOFT\CRYPTOGRAPHY\RNG	1304 (seq.exe)	Seed	tvoSyv/Ye6Sd QBQX7c9yuc
MACHINE\SOFTWARE\MICROSOFT\CRYPTOGRAPHY\RNG	1996 (RegSvcs.exe)	Seed	ilJxTRRkPBC GpZoUh+b7\
MACHINE\SOFTWARE\MICROSOFT\CRYPTOGRAPHY\RNG	1996 (RegSvcs.exe)	Seed	qDLudn0qLc Ukhy6gRetXp
MACHINE\SOFTWARE\MICROSOFT\CRYPTOGRAPHY\RNG	1996 (RegSvcs.exe)	Seed	k4kwFf8vsSX QLj7m4ZEdf
USER\S-1-5-21-1202660629-583907252-1801674531-500\SOFTWARE\MICROSOFT\WINDOWS\CURRENTVERSION\EXPLORER\MOUNTPOINTS2\{AF5E62D0-F159-11E5-A1E5-00501E3AE7B5}	1996 (RegSvcs.exe)	BaseClass	Drive
MACHINE\SOFTWARE\MICROSOFT\CRYPTOGRAPHY\RNG	1996 (RegSvcs.exe)	Seed	b9cXVQU8NU 4obKSwZdAc
USER\S-1-5-21-1202660629-583907252-1801674531-500\SOFTWARE\1996	1996 (RegSvcs.exe)	Mutex	ZWcCUkGLY
USER\S-1-5-21-1202660629-583907252-1801674531-500\SOFTWARE\ZWCCUKGLY8ABX	1996 (RegSvcs.exe)	ServerStarted	8/11/2016 18
USER\S-1-5-21-1202660629-583907252-1801674531-500\SOFTWARE\MICROSOFT\WINDOWS\CURRENTVERSION\EXPLORER\SHELL FOLDERS	1996 (RegSvcs.exe)	AppData	C:\Document
USER\S-1-5-21-1202660629-583907252-1801674531-500\SOFTWARE\MICROSOFT\WINDOWS\CURRENTVERSION\EXPLORER\MOUNTPOINTS2\{1209A444-8D68-11E1-9FE0-806D6172696F}	1996 (RegSvcs.exe)	BaseClass	Drive
USER\S-1-5-21-1202660629-583907252-1801674531-500\SOFTWARE\MICROSOFT\WINDOWS\CURRENTVERSION\EXPLORER\MOUNTPOINTS2\{2421CC9A-3EFF-11E6-A1E7-FC8CDBFBD8A2}	1996 (RegSvcs.exe)	BaseClass	Drive
USER\S-1-5-21-1202660629-583907252-1801674531-500\SOFTWARE\MICROSOFT\WINDOWS\CURRENTVERSION\EXPLORER\MOUNTPOINTS2\{75EF541F-D065-11E1-AC7A-525400123456}	1996 (RegSvcs.exe)	BaseClass	Drive
MACHINE\SOFTWARE\MICROSOFT\CRYPTOGRAPHY\RNG	1996 (RegSvcs.exe)	Seed	q1rXZKQ+tR kq6EuR93k8

MACHINE\SOFTWARE\MICROSOFT\CRYPTOGRAPHY\RNG	1996 (RegSvcs.exe)	Seed	dIEQ/THXp+e Ky2iugti1crfA
MACHINE\SOFTWARE\MICROSOFT\CRYPTOGRAPHY\RNG	1996 (RegSvcs.exe)	Seed	wOiAf9t7Wk5 6WsUbp2yH
MACHINE\SOFTWARE\MICROSOFT\CRYPTOGRAPHY\RNG	1996 (RegSvcs.exe)	Seed	Zfb9H5Ogmc 7zNshBKuR
USER\S-1-5-21-1202660629-583907252-1801674531-500\SOFTWARE\ZWCCUKGLY8ABX	1996 (RegSvcs.exe)	InstalledServer	C:\WINDOWS
MACHINE\SYSTEM\CONTROLSET001\CONTROL\NETWORK\{4D36E972-E325-11CE-BFC1-08002BE10318}\{C20FDDB0-BD90-4E06-8D7A-87767A382393}\CONNECTION	1028 (svchost.exe)	PnpInstanceID	PCI\VEN_808 0&18
USER\S-1-5-21-1202660629-583907252-1801674531-500\SOFTWARE\MICROSOFT\WINDOWS\CURRENTVERSION\EXPLORER\SHELL FOLDERS	1028 (svchost.exe)	AppData	C:\Document
MACHINE\SOFTWARE\MICROSOFT\CRYPTOGRAPHY\RNG	1228 (RegSvcs.exe)	Seed	rT+VCQ0sqS v4BJHelwyLc
USER\S-1-5-21-1202660629-583907252-1801674531-500\SOFTWARE\MICROSOFT\WINDOWS\CURRENTVERSION\EXPLORER\MOUNTPOINTS2\{2421CC9A-3EFF-11E6-A1E7-FC8CDBFBD8A2}	1228 (RegSvcs.exe)	BaseClass	Drive
MACHINE\SOFTWARE\MICROSOFT\CRYPTOGRAPHY\RNG	1228 (RegSvcs.exe)	Seed	OaQJ/iONT3 nm2tm9QbP
USER\S-1-5-21-1202660629-583907252-1801674531-500\SOFTWARE\MICROSOFT\WINDOWS\CURRENTVERSION\EXPLORER\MOUNTPOINTS2\{1209A444-8D68-11E1-9FE0-806D6172696F}	1228 (RegSvcs.exe)	BaseClass	Drive
MACHINE\SOFTWARE\MICROSOFT\CRYPTOGRAPHY\RNG	1228 (RegSvcs.exe)	Seed	Im6hiJA6MnA Ce60E7wHb
MACHINE\SOFTWARE\MICROSOFT\CRYPTOGRAPHY\RNG	1228 (RegSvcs.exe)	Seed	Gacftl5YHIJW V9NVZ0sREx
USER\S-1-5-21-1202660629-583907252-1801674531-500\SOFTWARE\ZWCCUKGLY8ABX	1228 (RegSvcs.exe)	FirstExecution	11/08/2016 1
MACHINE\SOFTWARE\MICROSOFT\CRYPTOGRAPHY\RNG	1228 (RegSvcs.exe)	Seed	HeHVWC4IB xSoQSf9+Jvt
USER\S-1-5-21-1202660629-583907252-1801674531-500\SOFTWARE\MICROSOFT\WINDOWS\CURRENTVERSION\EXPLORER\SHELL FOLDERS	1228 (RegSvcs.exe)	AppData	C:\Document
USER\S-1-5-21-1202660629-583907252-1801674531-500\SOFTWARE\MICROSOFT\WINDOWS\CURRENTVERSION\EXPLORER\MOUNTPOINTS2\{75EF541F-D065-11E1-AC7A-525400123456}	1228 (RegSvcs.exe)	BaseClass	Drive
MACHINE\SOFTWARE\MICROSOFT\CRYPTOGRAPHY\RNG	1228 (RegSvcs.exe)	Seed	AAJjfmhtoixu xkkbXnhkz74
MACHINE\SOFTWARE\MICROSOFT\CRYPTOGRAPHY\RNG	1228 (RegSvcs.exe)	Seed	KxyID8HIhOZ RHtnt+VOBH
USER\S-1-5-21-1202660629-583907252-1801674531-500\SOFTWARE\MICROSOFT\WINDOWS\CURRENTVERSION\EXPLORER\MOUNTPOINTS2\{AF5E62D0-F159-11E5-A1E5-00501E3AE7B5}	1228 (RegSvcs.exe)	BaseClass	Drive
MACHINE\SOFTWARE\MICROSOFT\CRYPTOGRAPHY\RNG	1228 (RegSvcs.exe)	Seed	vdmnhzEIJp cHzQcGTqLz

Filesystem Activity

Files Created: 13 Files Read: 22 Files Modified: 17 Files Deleted: 2

Path	PID	Action
C:\Documents and Settings\Administrator\Application Data\Microsoft\Windows\ZWcCUkGLY8aBx\ZWcCUkGLY8aBx.nfo	1996 (RegSvcs.exe)	Created
C:\Documents and Settings\Administrator\Application Data\pbt	1992 (sample.exe)	Created
C:\Documents and Settings\Administrator\Application Data\pbt\YXGRQ	904 (RegSvcs.exe)	Created
C:\Documents and Settings\Administrator\Application Data\pbt\spd	1304 (seq.exe)	Created
\AUTOEXEC.BAT	1028 (svchost.exe)	Read
\Documents and Settings\Administrator\Application Data\Microsoft\Windows\ZWcCUkGLY8aBx\ZWcCUkGLY8aBx.nfo	1996 (RegSvcs.exe)	Modified
\Documents and Settings\Administrator\Application Data\Microsoft\Windows\ZWcCUkGLY8aBx\ZWcCUkGLY8aBx.nfo	1228 (RegSvcs.exe)	Read
\Documents and Settings\Administrator\Application Data\Microsoft\Windows\ZWcCUkGLY8aBx\ZWcCUkGLY8aBx.svr	1996 (RegSvcs.exe)	Modified
\Documents and Settings\Administrator\Application Data\desktop.ini	904 (RegSvcs.exe)	Read
\Documents and Settings\Administrator\Application Data\desktop.ini	1996 (RegSvcs.exe)	Read
\Documents and Settings\Administrator\Application Data\desktop.ini	1228 (RegSvcs.exe)	Read
\Documents and Settings\Administrator\Application Data\desktop.ini	1304 (seq.exe)	Read
\Documents and Settings\Administrator\Application Data\pbt\YXGRQ	904 (RegSvcs.exe)	Modified
\Documents and Settings\Administrator\Application Data\pbt\YXGRQ	904 (RegSvcs.exe)	Read
\Documents and Settings\Administrator\Application Data\pbt\YXGRQ	1304 (seq.exe)	Read
\Documents and Settings\Administrator\Application Data\pbt__tmp_rar_sfx_access_check_3120356500	1992 (sample.exe)	Deleted
\Documents and Settings\Administrator\Application Data\pbt\apk.docx	1992 (sample.exe)	Modified
\Documents and Settings\Administrator\Application Data\pbt\dit.ktc	1992 (sample.exe)	Modified
\Documents and Settings\Administrator\Application Data\pbt\dit.ktc	904 (RegSvcs.exe)	Read
\Documents and Settings\Administrator\Application Data\pbt\jjw.ico	1992 (sample.exe)	Modified
\Documents and Settings\Administrator\Application Data\pbt\mke.dat	1992 (sample.exe)	Modified
\Documents and Settings\Administrator\Application Data\pbt\ndh.ico	1992 (sample.exe)	Modified
\Documents and Settings\Administrator\Application Data\pbt\seq.exe	1992 (sample.exe)	Modified
\Documents and Settings\Administrator\Application Data\pbt\seq.exe	1992 (sample.exe)	Read
\Documents and Settings\Administrator\Application Data\pbt\spd	1304 (seq.exe)	Modified
\Documents and Settings\Administrator\Application Data\pbt\spd	1304 (seq.exe)	Read
\Documents and Settings\Administrator\Application Data\pbt\spd	904 (RegSvcs.exe)	Deleted

\Documents and Settings\Administrator\Application Data\pbt\uhb.jpg	1992 (sample.exe)	Modified
\Documents and Settings\Administrator\Application Data\pbt\wsl.ppt	1992 (sample.exe)	Modified
\Documents and Settings\Administrator\Application Data\pbt\wsl.ppt	904 (RegSvcs.exe)	Read
\Documents and Settings\Administrator\Application Data\pbt\wsl.ppt	1304 (seq.exe)	Read
\Documents and Settings\Administrator\My Documents\desktop.ini	1992 (sample.exe)	Read
\Documents and Settings\All Users\Application Data\Microsoft\Network\Connections\Pbk\rasphone.pbk	1028 (svchost.exe)	Read
\Documents and Settings\All Users\Documents\desktop.ini	1992 (sample.exe)	Read
\TEMP\sample.exe	1992 (sample.exe)	Read
\WINDOWS\Registration\R00000000000b.clb	1992 (sample.exe)	Read
\WINDOWS\system32\CatRoot2\edb.log	1028 (svchost.exe)	Modified
\WINDOWS\system32\CatRoot2\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\catdb	1028 (svchost.exe)	Modified
\WINDOWS\system32\drivers\etc\hosts	1048 (svchost.exe)	Read
\WINDOWS\system32\rsaenh.dll	1048 (svchost.exe)	Read
\WINDOWS\system32\rsaenh.dll	1304 (seq.exe)	Read
\WINDOWS\system32\wbem\Repository\FS\INDEX.BTR	1028 (svchost.exe)	Read
\WINDOWS\system32\wbem\Repository\FS\OBJECTS.DATA	1028 (svchost.exe)	Read
\WINDOWS\system32\wbem\wbemdisp.tlb	1228 (RegSvcs.exe)	Read
\WINDOWS\win.ini	1992 (sample.exe)	Read
\lsarpc	1028 (svchost.exe)	Modified
\lsarpc	1992 (sample.exe)	Modified
\lsarpc	904 (RegSvcs.exe)	Modified
\lsarpc	1228 (RegSvcs.exe)	Modified
\lsarpc	1304 (seq.exe)	Modified
\lsarpc	1996 (RegSvcs.exe)	Modified
\lsarpc	1028 (svchost.exe)	Read
\lsarpc	1992 (sample.exe)	Read
\lsarpc	904 (RegSvcs.exe)	Read

\lsarpc	1228 (RegSvcs.exe)	Read
\lsarpc	1304 (seq.exe)	Read
\lsarpc	1996 (RegSvcs.exe)	Read
\lsass	672 (unknown)	Modified
\lsass	672 (unknown)	Read
\wkssvc	1992 (sample.exe)	Modified
\wkssvc	1028 (svchost.exe)	Modified
\wkssvc	1992 (sample.exe)	Read
\wkssvc	1028 (svchost.exe)	Read
__tmp_rar_sfx_access_check_3120356500	1992 (sample.exe)	Created
apk.docx	1992 (sample.exe)	Created
dit.ktc	1992 (sample.exe)	Created
jjw.ico	1992 (sample.exe)	Created
mke.dat	1992 (sample.exe)	Created
ndh.ico	1992 (sample.exe)	Created
seq.exe	1992 (sample.exe)	Created
uhb.jpg	1992 (sample.exe)	Created
wsl.ppt	1992 (sample.exe)	Created