



Analysis # 2956

10/10/2014 06:34 am

Table of Contents

Analysis Summary	3
Analysis Summary	3
Digital Behavior Traits	3
File Activity	4
Deleted Files	4
Stored Modified Files	5
Created Mutexes	6
Created Mutexes	6
Registry Activity	8
Created Keys	8
Set Values	9
Deleted Values	13
Network Activity	14
Network Events	14
Network Traffic	15
DNS Requests	16
Virus Total Results	17

Analysis Summary	
Submitted File:	document_73128_91898_pdf.exe
MD5:	5b94fb32ed60cb839ca4284f80ae3b16
File Size:	23040
File Type:	PE32 executable for MS Windows (GUI) Intel 80386 3
Analysis Time:	2014-10-10 06:34:02
Start Reason:	AnalysisTarget
Termination Reason:	TerminatedBySelf
Start Time:	Fri, 10 Oct 2014 10:39:29 +0000
Termination Time:	Fri, 10 Oct 2014 10:40:29 +0000
Analysis Time:	2014-10-10 06:34:02
Sandbox:	XP-SP2 - 00-0C-29-B2-D2-62
Total Processes:	5
Sample Notes:	

Digital Behavior Traits			
Alters Windows Firewall		Hooks Keyboard	
Checks For Debugger		Injected Code	
Copies to Windows		Makes Network Connection	
Could Not Load		Modifies File in System	
Creates DLL in System		Modifies Local DNS	
Creates EXE in System		More than 5 Processes	
Creates Hidden File		Opens Physical Memory	
Creates Mutex		Starts EXE in Documents	
Creates Service		Starts EXE in Recycle	
Deletes File in System		Starts EXE in System	
Deletes Original Sample		Windows/Run Registry Key Set	

Deleted Files

[process 2] C:\document_73128_91898_pdf.exe

[process 4] C:\DOCUME~1\Charlie\LOCALS~1\Temp\onicm.exe

Created Mutexes	
	mutex
[process 1]	Name: CTF.LBES.MutexDefaultS-1-5-21-602162358-879983540-1177238915-1003 Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 1]	Name: CTF.Compart.MutexDefaultS-1-5-21-602162358-879983540-1177238915-1003 Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 1]	Name: CTF.Asm.MutexDefaultS-1-5-21-602162358-879983540-1177238915-1003 Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 1]	Name: CTF.Layouts.MutexDefaultS-1-5-21-602162358-879983540-1177238915-1003 Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 1]	Name: CTF.TMD.MutexDefaultS-1-5-21-602162358-879983540-1177238915-1003 Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 2]	Name: CTF.TimListCache.FMPDefaultS-1-5-21-602162358-879983540-1177238915-1003MUTEX.DefaultS-1-5-21-602162358-879983540-1177238915-1003 Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 2]	Name: CTF.LBES.MutexDefaultS-1-5-21-602162358-879983540-1177238915-1003 Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 2]	Name: CTF.Compart.MutexDefaultS-1-5-21-602162358-879983540-1177238915-1003 Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 2]	Name: CTF.Asm.MutexDefaultS-1-5-21-602162358-879983540-1177238915-1003 Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 2]	Name: CTF.Layouts.MutexDefaultS-1-5-21-602162358-879983540-1177238915-1003 Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 2]	Name: CTF.TMD.MutexDefaultS-1-5-21-602162358-879983540-1177238915-1003 Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 2]	Name: CTF.TimListCache.FMPDefaultS-1-5-21-602162358-879983540-1177238915-1003MUTEX.DefaultS-1-5-21-602162358-879983540-1177238915-1003 Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 2]	Name: Local\c:\documents and settings\charlie\local settings\temporary internet files\content.ie5! Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 2]	Name: Local\c:\documents and settings\charlie\cookies! Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 2]	Name: Local\c:\documents and settings\charlie\local settings\history\history.ie5! Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 2]	Name: Local\WininetConnectionMutex Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 2]	Name: RasPbFile Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 2]	Name: Local\ZonesCounterMutex Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 2]	Name: Local\ZoneAttributeCacheCounterMutex Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 2]	Name: Local\ZonesCacheCounterMutex Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 3]	Name: Local\ZonesLockedCacheCounterMutex Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 3]	Name: CTF.LBES.MutexDefaultS-1-5-21-602162358-879983540-1177238915-1003 Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 3]	Name: CTF.Compart.MutexDefaultS-1-5-21-602162358-879983540-1177238915-1003 Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 3]	Name: CTF.Asm.MutexDefaultS-1-5-21-602162358-879983540-1177238915-1003 Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE

[process 3]	Name: CTF.Layouts.MutexDefaultS-1-5-21-602162358-879983540-1177238915-1003 Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 3]	Name: CTF.TMD.MutexDefaultS-1-5-21-602162358-879983540-1177238915-1003 Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 4]	Name: CTF.TimListCache.FMPDefaultS-1-5-21-602162358-879983540-1177238915-1003MUTEX.DefaultS-1-5-21-602162358-879983540-1177238915-1003 Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 4]	Name: CTF.LBES.MutexDefaultS-1-5-21-602162358-879983540-1177238915-1003 Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 4]	Name: CTF.Compart.MutexDefaultS-1-5-21-602162358-879983540-1177238915-1003 Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 4]	Name: CTF.Asm.MutexDefaultS-1-5-21-602162358-879983540-1177238915-1003 Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 4]	Name: CTF.Layouts.MutexDefaultS-1-5-21-602162358-879983540-1177238915-1003 Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 4]	Name: CTF.TMD.MutexDefaultS-1-5-21-602162358-879983540-1177238915-1003 Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 5]	Name: CTF.TimListCache.FMPDefaultS-1-5-21-602162358-879983540-1177238915-1003MUTEX.DefaultS-1-5-21-602162358-879983540-1177238915-1003 Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 5]	Name: Global\1g2hk1hyj Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 5]	Name: Local\c:\windows\system32\config\systemprofile\local settings\temporary internet files\content.ie5! Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 5]	Name: Local\c:\windows\system32\config\systemprofile\cookies! Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 5]	Name: Local\c:\windows\system32\config\systemprofile\local settings\history\history.ie5! Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 5]	Name: RasPbFile Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 5]	Name: Local\ZonesCounterMutex Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 5]	Name: Local\c:\windows\system32\config\systemprofile\ietldcache! Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 5]	Name: Local\ZoneAttributeCacheCounterMutex Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 5]	Name: Local\ZonesCacheCounterMutex Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE

Created Keys	
	key
[process 5]	\REGISTRY\USER\DEFAULT\Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\Extensible Cache\ietId
[process 5]	\REGISTRY\USER\DEFAULT\Software\Microsoft\Internet Explorer\IETId
[process 5]	\REGISTRY\USER\DEFAULT\Software\Microsoft\Internet Explorer\BrowserEmulation

	Value: AutoDetect
[process 2]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap Value: ProxyBypass
[process 2]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap Value: IntranetName
[process 2]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap Value: UNCAsIntranet
[process 2]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap Value: AutoDetect
[process 2]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\Windows\CurrentVersion\Internet Settings Value: ProxyEnable
[process 2]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\windows\CurrentVersion\Internet Settings\Connections Value: SavedLegacySettings
[process 2]	Key Name: \REGISTRY\MACHINE\Software\Microsoft\Rpc Value: UuidSequenceNumber
[process 3]	Key Name: \REGISTRY\MACHINE\SOFTWARE\Microsoft\Cryptography\ RNG Value: Seed
[process 4]	Key Name: \REGISTRY\MACHINE\SOFTWARE\Microsoft\Cryptography\ RNG Value: Seed
[process 4]	Key Name: \REGISTRY\MACHINE\SOFTWARE\Microsoft\Cryptography\ RNG Value: Seed
[process 4]	Key Name: \REGISTRY\MACHINE\SOFTWARE\Microsoft\Cryptography\ RNG Value: Seed
[process 4]	Key Name: \REGISTRY\MACHINE\SOFTWARE\Microsoft\Cryptography\ RNG Value: Seed
[process 4]	Key Name: \REGISTRY\MACHINE\SOFTWARE\Microsoft\Cryptography\ RNG Value: Seed
[process 4]	Key Name: \REGISTRY\MACHINE\SOFTWARE\Microsoft\Cryptography\ RNG Value: Seed
[process 4]	Key Name: \REGISTRY\MACHINE\SOFTWARE\Microsoft\Cryptography\ RNG Value: Seed
[process 4]	Key Name: \REGISTRY\MACHINE\SOFTWARE\Microsoft\Cryptography\ RNG Value: Seed
[process 4]	Key Name: \REGISTRY\MACHINE\SOFTWARE\Microsoft\Cryptography\ RNG Value: Seed
[process 5]	Key Name: \REGISTRY\USER\DEFAULT\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders Value: AppData
[process 5]	Key Name: \REGISTRY\USER\DEFAULT\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders Value: Cache
[process 5]	Key Name: \REGISTRY\USER\DEFAULT\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders Value: Cookies
[process 5]	Key Name: \REGISTRY\USER\DEFAULT\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders Value: History
[process 5]	Key Name: \REGISTRY\USER\DEFAULT\Software\Microsoft\Windows NT\CurrentVersion\Winlogon Value: ParseAutoexec
[process 5]	Key Name: \REGISTRY\USER\DEFAULT\Software\Microsoft\Windows NT\CurrentVersion\Winlogon Value: ParseAutoexec

[process 5]	Key Name: \REGISTRY\MACHINE\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders Value: Common AppData
[process 5]	Key Name: \REGISTRY\USER\DEFAULT\Software\Microsoft\Windows NT\CurrentVersion\Winlogon Value: ParseAutoexec
[process 5]	Key Name: \REGISTRY\USER\DEFAULT\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders Value: AppData
[process 5]	Key Name: \REGISTRY\USER\DEFAULT\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings Value: ProxyEnable
[process 5]	Key Name: \REGISTRY\USER\DEFAULT\Software\Microsoft\windows\CurrentVersion\Internet Settings\Connections Value: SavedLegacySettings
[process 5]	Key Name: \REGISTRY\USER\DEFAULT\Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\Extensible Cache\ietld Value: CachePath
[process 5]	Key Name: \REGISTRY\USER\DEFAULT\Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\Extensible Cache\ietld Value: CachePrefix
[process 5]	Key Name: \REGISTRY\USER\DEFAULT\Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\Extensible Cache\ietld Value: CacheLimit
[process 5]	Key Name: \REGISTRY\USER\DEFAULT\Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\Extensible Cache\ietld Value: CacheOptions
[process 5]	Key Name: \REGISTRY\USER\DEFAULT\Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\Extensible Cache\ietld Value: CachePath
[process 5]	Key Name: \REGISTRY\USER\DEFAULT\Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\Extensible Cache\ietld Value: CacheRepair
[process 5]	Key Name: \REGISTRY\USER\DEFAULT\Software\Microsoft\Internet Explorer\IETId Value: IETIdDIIVersionHigh
[process 5]	Key Name: \REGISTRY\USER\DEFAULT\Software\Microsoft\Internet Explorer\IETId Value: IETIdDIIVersionLow
[process 5]	Key Name: \REGISTRY\USER\DEFAULT\Software\Microsoft\Internet Explorer\IETId Value: IETIdVersionHigh
[process 5]	Key Name: \REGISTRY\USER\DEFAULT\Software\Microsoft\Internet Explorer\IETId Value: IETIdVersionLow
[process 5]	Key Name: \REGISTRY\USER\DEFAULT\Software\Microsoft\Internet Explorer\IETId Value: StaleIETIdCache
[process 5]	Key Name: \REGISTRY\USER\DEFAULT\Software\Microsoft\Internet Explorer\BrowserEmulation Value: TLDUpdates
[process 5]	Key Name: \REGISTRY\USER\DEFAULT\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap Value: ProxyBypass
[process 5]	Key Name: \REGISTRY\USER\DEFAULT\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap Value: IntranetName
[process 5]	Key Name: \REGISTRY\USER\DEFAULT\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap Value: UNCAsintranet
[process 5]	Key Name: \REGISTRY\USER\DEFAULT\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap

	p Value: AutoDetect
[process 5]	Key Name: \REGISTRY\USER\DEFAULT\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMa p Value: ProxyBypass
[process 5]	Key Name: \REGISTRY\USER\DEFAULT\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMa p Value: IntranetName
[process 5]	Key Name: \REGISTRY\USER\DEFAULT\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMa p Value: UNCAsIntranet
[process 5]	Key Name: \REGISTRY\USER\DEFAULT\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMa p Value: AutoDetect
[process 5]	Key Name: \REGISTRY\USER\DEFAULT\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings Value: ProxyEnable
[process 5]	Key Name: \REGISTRY\USER\DEFAULT\Software\Microsoft\windows\CurrentVersion\Internet Settings\Connec tions Value: SavedLegacySettings
[process 5]	Key Name: \REGISTRY\USER\DEFAULT\Software\Microsoft\Windows NT\CurrentVersion\Winlogon Value: ParseAutoexec
[process 5]	Key Name: \REGISTRY\MACHINE\SOFTWARE\Microsoft\SystemCertificates\AuthRoot\Certificates\02FAF3E29143 5468607857694DF5E45B68851868 Value: Blob
[process 5]	Key Name: \REGISTRY\USER\DEFAULT\Software\Microsoft\Windows NT\CurrentVersion\Winlogon Value: ParseAutoexec
[process 5]	Key Name: \REGISTRY\USER\DEFAULT\Software\Microsoft\Windows NT\CurrentVersion\Winlogon Value: ParseAutoexec
[process 5]	Key Name: \REGISTRY\USER\DEFAULT\Software\Microsoft\Windows NT\CurrentVersion\Winlogon Value: ParseAutoexec

Deleted Values	
	key
[process 2]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\Windows\CurrentVersion\Internet Settings Value: ProxyServer
[process 2]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\Windows\CurrentVersion\Internet Settings Value: ProxyOverride
[process 2]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\Windows\CurrentVersion\Internet Settings Value: AutoConfigURL
[process 2]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\Windows\CurrentVersion\Internet Settings Value: ProxyServer
[process 2]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\Windows\CurrentVersion\Internet Settings Value: ProxyOverride
[process 2]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\Windows\CurrentVersion\Internet Settings Value: AutoConfigURL
[process 5]	Key Name: \REGISTRY\USER\DEFAULT\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings Value: ProxyServer
[process 5]	Key Name: \REGISTRY\USER\DEFAULT\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings Value: ProxyOverride
[process 5]	Key Name: \REGISTRY\USER\DEFAULT\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings Value: AutoConfigURL
[process 5]	Key Name: \REGISTRY\USER\DEFAULT\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings Value: ProxyServer
[process 5]	Key Name: \REGISTRY\USER\DEFAULT\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings Value: ProxyOverride
[process 5]	Key Name: \REGISTRY\USER\DEFAULT\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings Value: AutoConfigURL
[process 5]	Key Name: \REGISTRY\MACHINE\SOFTWARE\Microsoft\SystemCertificates\AuthRoot\Certificates Value: 02FAF3E291435468607857694DF5E45B68851868

Network Events			
	Remote IP	Local IP	HTTP Command
[process 2]	94.75.233.13	10.20.25.250	GET /1010uk1/NODE01/0/51-SP3/0/
[process 2]	94.75.233.13	10.20.25.250	GET /1010uk1/NODE01/1/0/0/
[process 2]	98.158.189.196	10.20.25.250	GET /beanz/1010uk1.rtf
[process 2]	94.75.233.13	10.20.25.250	GET /1010uk1/NODE01/41/5/1/ POST /private/sandbox_status.php
[process 5]	74.125.229.168	10.20.25.250	none
[process 5]	66.228.45.110	10.20.25.250	none
[process 5]	74.125.229.168	10.20.25.250	none
[process 5]	37.59.48.138	10.20.25.250	none
[process 5]	23.201.103.147	10.20.25.250	GET /msdownload/update/v3/static/trustedr/en/authroots eq.txt GET /msdownload/update/v3/static/trustedr/en/authroots tl.cab

Network Traffic		
	Remote IP	Local IP
Connection #1	10.20.25.255	10.20.25.250
Connection #2	239.255.255.250	10.20.25.250
Connection #3	66.228.45.110	10.20.25.250

DNS Requests	
Request	Result
beanztech.com	98.158.189.196
google.com	74.125.229.168
	74.125.229.165
	74.125.229.162
	74.125.229.174
	74.125.229.166
	74.125.229.164
	74.125.229.160
	74.125.229.169
	74.125.229.167
	74.125.229.161
74.125.229.163	
numb.viagenie.ca	66.228.45.110

Virus Total Results

No Results

ThreatTrack Security, Inc.

33 North Garden Avenue, Suite 1200, Clearwater, Florida, USA 33755

Telephone: (855) 443-4284 Intl: +1(813)367-9907

Email: Sales@ThreatTrack.com

Disclaimer © 2013. ThreatTrack Security, Inc. All rights reserved. All product and company names herein may be trademarks of their respective owners. The information and content in this document is provided for informational purposes only and is provided "as is" with no warranty of any kind, either express or implied, including but not limited to the implied warranties of merchantability, fitness for a particular purpose, and non-infringement. ThreatTrack Security, Inc. is not liable for any damages, including any consequential damages, of any kind that may result from the use of this document. The information is obtained from publicly available sources. Though reasonable effort has been made to ensure the accuracy of the data provided, ThreatTrack Security makes no claim, promise or guarantee about the completeness, accuracy, recency or adequacy of information and is not responsible for misprints, out-of-date information, or errors. ThreatTrack Security makes no warranty, express or implied, and assumes no legal liability or responsibility for the accuracy or completeness of any information contained in this document. If you believe there are any factual errors in this document, please contact us and we will review your concerns as soon as practical.