Analysis # 2569

09/11/2014 17:32 pm

Table of Contents

Analysis Summary

Submitted File:	update.exe
MD5:	c01ab42fb00a340d8f00877acb8c9754
File Size:	200704
File Type:	PE32 executable for MS Windows (GUI) Intel 80386 3
Analysis Time:	2014-09-11 17:32:09
Start Reason:	AnalysisTarget
Termination Reason:	TerminatedBySelf
Start Time:	Thu, 11 Sep 2014 21:36:47 +0000
Termination Time:	Thu, 11 Sep 2014 21:37:51 +0000
Analysis Time:	2014-09-11 17:32:09
Sandbox:	XP-SP2 - 00-0C-29-B2-D2-62
Total Processes:	8
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**	✓

Stored Modified Files
[process 3] C:\DOCUME~1\Charlie\LOCALS~1\Temp\KB02344250.exe
[process 3] C:\DOCUME~1\Charlie\LOCALS~1\Temp\KB02348468.exe

Created Mutexes	
	mutex
[process 1]	Name: DDrawWindowListMutex
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 1]	Name: DDrawDriverObjectListMutex
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 1]	Name: __DDrawExclMode__
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 2]	Name: __DDrawCheckExclMode__
	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 3]	Name: CTF.TimListCache.FMPDefaultS-1-5-21-602162358-879983540-1177238915-1003MUTEX.DefaultS-1-5-21-6 02162358-879983540-1177238915-1003
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 3]	Name: SHIMLIB_LOG_MUTEX
	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-1-5-21-6 02162358-879983540-1177238915-1003
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 6]	Name: SHIMLIB_LOG_MUTEX
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 6]	Name: DDrawWindowListMutex
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 6]	Name: DDrawDriverObjectListMutex
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 6]	Name: __DDrawExclMode__
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 8]	Name: __DDrawCheckExclMode__
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 8]	Name: DDrawWindowListMutex
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 8]	Name: DDrawDriverObjectListMutex

	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 8]	Name: __DDrawExclMode__
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE

Created Keys	
	key
[process 3]	\REGISTRY\MACHINE\Software\Microsoft\Windows\CurrentVersion\policies\Explorer\Run
[process 3]	\REGISTRY\MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\policies\
[process 3]	\REGISTRY\MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\policies\Explorer\

Set Values	
	key
[process 1]	Key Name: \REGISTRY\MACHINE\SOFTWARE\Microsoft\Cryptography\RNG Value: Seed
[process 1]	Key Name: \REGISTRY\MACHINE\Software\Microsoft\DirectDraw\MostRecentApplication Value: Name
[process 1]	Key Name: \REGISTRY\MACHINE\Software\Microsoft\DirectDraw\MostRecentApplication Value: ID
[process 2]	Key Name: \REGISTRY\MACHINE\SOFTWARE\Microsoft\Cryptography\RNG Value: Seed
[process 2]	Key Name: \REGISTRY\MACHINE\SOFTWARE\Microsoft\Cryptography\RNG Value: Seed
[process 2]	Key Name: \REGISTRY\MACHINE\SOFTWARE\Microsoft\Cryptography\RNG Value: Seed
[process 2]	Key Name: \REGISTRY\MACHINE\SOFTWARE\Microsoft\Cryptography\RNG Value: Seed
[process 2]	Key Name: \REGISTRY\MACHINE\SOFTWARE\Microsoft\Cryptography\RNG Value: Seed
[process 2]	Key Name: \REGISTRY\MACHINE\SOFTWARE\Microsoft\Cryptography\RNG Value: Seed
[process 2]	Key Name: \REGISTRY\MACHINE\SOFTWARE\Microsoft\Cryptography\RNG Value: Seed
[process 2]	Key Name: \REGISTRY\MACHINE\SOFTWARE\Microsoft\Cryptography\RNG Value: Seed
[process 3]	Key Name: \REGISTRY\MACHINE\SOFTWARE\Microsoft\Cryptography\RNG Value: Seed
[process 3]	Key Name: \REGISTRY\MACHINE\SOFTWARE\Microsoft\Cryptography\RNG Value: Seed
[process 3]	Key Name: \REGISTRY\MACHINE\SOFTWARE\Microsoft\Cryptography\RNG Value: Seed
[process 3]	Key Name: \REGISTRY\MACHINE\SOFTWARE\Microsoft\Cryptography\RNG Value: Seed
[process 3]	Key Name: \REGISTRY\MACHINE\SOFTWARE\Microsoft\Cryptography\RNG Value: Seed
[process 3]	Key Name: \REGISTRY\MACHINE\SOFTWARE\Microsoft\Cryptography\RNG Value: Seed
[process 3]	Key Name: \REGISTRY\MACHINE\SOFTWARE\Microsoft\Cryptography\RNG Value: Seed
[process 3]	Key Name: \REGISTRY\MACHINE\SOFTWARE\Microsoft\Cryptography\RNG Value: Seed
[process 3]	Key Name: \REGISTRY\MACHINE\Software\Microsoft\Windows\CurrentVersion\policies\Explorer\Run Value: 3832326565
[process 3]	Key Name: \REGISTRY\MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer Value: TaskbarNoNotification
[process 3]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer Value: TaskbarNoNotification
[process 3]	Key Name: \REGISTRY\MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer Value: HideSCAHealth
[process 3]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer

	Value: HideSCAHealth
[process 3]	Key Name: \REGISTRY\MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\policies\system
	Value: EnableLUA
[process 3]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\software\Microsoft\Windows\CurrentVersion\Explorer\Advanced
	Value: ShowSuperHidden
[process 3]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\software\Microsoft\Windows\CurrentVersion\Explorer\Advanced
	Value: Hidden
[process 4]	Key Name: \REGISTRY\MACHINE\SOFTWARE\Microsoft\Cryptography\RNG
	Value: Seed
[process 6]	Key Name: \REGISTRY\MACHINE\SOFTWARE\Microsoft\Cryptography\RNG
	Value: Seed
[process 6]	Key Name: \REGISTRY\MACHINE\Software\Microsoft\DirectDraw\MostRecentApplication
	Value: Name
[process 6]	Key Name: \REGISTRY\MACHINE\Software\Microsoft\DirectDraw\MostRecentApplication
	Value: ID
[process 8]	Key Name: \REGISTRY\MACHINE\SOFTWARE\Microsoft\Cryptography\RNG
	Value: Seed
[process 8]	Key Name: \REGISTRY\MACHINE\Software\Microsoft\DirectDraw\MostRecentApplication
	Value: Name
[process 8]	Key Name: \REGISTRY\MACHINE\Software\Microsoft\DirectDraw\MostRecentApplication
	Value: ID

Network Events			
	Remote IP	**Local IP**	**HTTP Command**
[process 3]	8.8.4.4	10.20.25.250	none
[process 3]	157.56.77.156	10.20.25.250	none
[process 3]	8.8.4.4	10.20.25.250	none
[process 3]	109.120.177.164	10.20.25.250	POST /datastat/datacoll.php
[process 3]	8.8.4.4	10.20.25.250	none
[process 3]	90.182.221.59	10.20.25.250	GET /css/r.pack
[process 3]	8.8.4.4	10.20.25.250	none
[process 3]	90.182.221.59	10.20.25.250	GET /css/r.pack
[process 3]	8.8.4.4	10.20.25.250	none
[process 3]	109.120.177.164	10.20.25.250	POST /datastat/datacoll.php
[process 3]	8.8.4.4	10.20.25.250	none
[process 3]	90.182.221.59	10.20.25.250	GET /css/p.pack
[process 3]	8.8.4.4	10.20.25.250	none
[process 3]	90.182.221.59	10.20.25.250	GET /css/p.pack
[process 3]	8.8.4.4	10.20.25.250	none
[process 3]	109.120.177.164	10.20.25.250	POST /datastat/datacoll.php
[process 3]	8.8.4.4	10.20.25.250	none
[process 3]	90.182.221.59	10.20.25.250	GET /css/g.pack
[process 3]	8.8.4.4	10.20.25.250	none
[process 3]	90.182.221.59	10.20.25.250	GET /css/g.pack

Network Traffic		
	Remote IP	**Local IP**
Connection #1	10.20.25.255	10.20.25.250

DNS Requests	
Request	**Result**
update.microsoft.com	157.56.77.156
	65.55.138.126
cityhotlove.com	109.120.177.164
cyklopesek.cz	90.182.221.59
www.cyklopesek.cz	90.182.221.59

Virus Total Results	
Last Scanned:	**2014-09-11 15:20:12**
Bkav:	Not Detected
MicroWorld-eScan:	Not Detected
nProtect:	Not Detected
CMC:	Not Detected
CAT-QuickHeal:	Not Detected
McAfee:	Not Detected
Malwarebytes:	Trojan.Ransom.ED
Zillya:	Not Detected
TheHacker:	Not Detected
K7GW:	Not Detected
K7AntiVirus:	Not Detected
Agnitum:	Not Detected
F-Prot:	W32/Powessere.A.gen!Eldorado
Symantec:	Not Detected
Norman:	Not Detected
TotalDefense:	Not Detected
TrendMicro-HouseCall:	Not Detected
Avast:	Not Detected
ClamAV:	Not Detected
Kaspersky:	Not Detected
BitDefender:	Not Detected
NANO-Antivirus:	Not Detected
ViRobot:	Not Detected
AegisLab:	Not Detected
ByteHero:	Not Detected
Tencent:	Not Detected
Ad-Aware:	Not Detected
Sophos:	Not Detected
Comodo:	Not Detected
F-Secure:	Not Detected
DrWeb:	Not Detected
VIPRE:	Not Detected
TrendMicro:	Not Detected
McAfee-GW-Edition:	Not Detected
Emsisoft:	Trojan.Win32.Agent (A)
Cyren:	Not Detected
Jiangmin:	Not Detected
Avira:	Not Detected
Antiy-AVL:	Not Detected
Kingsoft:	Not Detected
Microsoft:	Not Detected
SUPERAntiSpyware:	Not Detected
GData:	Not Detected
AhnLab-V3:	Dropper/Win32.Necurs
VBA32:	Not Detected
AVware:	Not Detected
Panda:	Not Detected
Zoner:	Not Detected
ESET-NOD32:	Win32/TrojanDownloader.Wauchos.AF
Rising:	Not Detected
Ikarus:	Not Detected
Fortinet:	Not Detected
AVG:	Not Detected
Baidu-International:	Not Detected
Qihoo-360:	Not Detected

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