



Analysis # 3614

12/05/2014 05:54 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	10
Network Activity	11
Network Events	11
Network Traffic	12
DNS Requests	13
Virus Total Results	14

Analysis Summary	
Submitted File:	bin.exe
MD5:	d37256439d5ab7f25561cc390d8aa1ea
File Size:	73728
File Type:	PE32 executable for MS Windows (GUI) Intel 80386 3
Analysis Time:	2014-12-05 05:54:00
Start Reason:	AnalysisTarget
Termination Reason:	TerminatedBySelf
Start Time:	Fri, 05 Dec 2014 10:54:09 +0000
Termination Time:	Fri, 05 Dec 2014 10:55:08 +0000
Analysis Time:	2014-12-05 05:54:00
Sandbox:	XP-SP2 - 00-0C-29-B2-D2-62
Total Processes:	3
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:\2.tmp

Stored Modified Files

[process 1] C:\2.tmp

[process 1] C:\2.tmp

Created Mutexes	
	mutex
[process 2]	Name: __PDH_PLA_MUTEX__ Desired Access: DELETE_READ_CONTROL SYNCHRONIZE_WRITE_DAC WRITE_OWNER_MUTEX_MODIFY_STATE
[process 2]	Name: SHIMLIB_LOG_MUTEX Desired Access: DELETE_READ_CONTROL SYNCHRONIZE_WRITE_DAC WRITE_OWNER_MUTEX_MODIFY_STATE
[process 2]	Name: __PDH_PLA_MUTEX__ 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-1-5-21-602162358-879983540-1177238915-1003\Mutex.DefaultS-1-5-21-602162358-879983540-1177238915-1003 Desired Access: DELETE_READ_CONTROL SYNCHRONIZE_WRITE_DAC WRITE_OWNER_MUTEX_MODIFY_STATE
[process 3]	Name: Global\{25552fbed462e2903e088d6161beede} Desired Access: DELETE_READ_CONTROL SYNCHRONIZE_WRITE_DAC WRITE_OWNER_MUTEX_MODIFY_STATE
[process 3]	Name: __PDH_PLA_MUTEX__ Desired Access: DELETE_READ_CONTROL SYNCHRONIZE_WRITE_DAC WRITE_OWNER_MUTEX_MODIFY_STATE
[process 3]	Name: Global\63d71d75bef41fa7b50175fa09e620f4 Desired Access: DELETE_READ_CONTROL SYNCHRONIZE_WRITE_DAC WRITE_OWNER_MUTEX_MODIFY_STATE
[process 3]	Name: Global\4d6503e9458d4b4989dfa7569bdac720 Desired Access: DELETE_READ_CONTROL SYNCHRONIZE_WRITE_DAC WRITE_OWNER_MUTEX_MODIFY_STATE
[process 3]	Name: Global\{25552fbed462e2903e088d6161beede} Desired Access: DELETE_READ_CONTROL SYNCHRONIZE_WRITE_DAC WRITE_OWNER_MUTEX_MODIFY_STATE
[process 3]	Name: Global\59ef73befc3e39c96a3592accb51fdd0 Desired Access: DELETE_READ_CONTROL SYNCHRONIZE_WRITE_DAC WRITE_OWNER_MUTEX_MODIFY_STATE
[process 3]	Name: Global\ec3c032da22259ce1e8599ed4fb060d4 Desired Access: DELETE_READ_CONTROL SYNCHRONIZE_WRITE_DAC WRITE_OWNER_MUTEX_MODIFY_STATE
[process 3]	Name: Global\{3058f6f42f7eed7201f952d7392a629} Desired Access: DELETE_READ_CONTROL SYNCHRONIZE_WRITE_DAC WRITE_OWNER_MUTEX_MODIFY_STATE
[process 3]	Name: Global\1a3272bc19f831f1afc6ad0da1430c32 Desired Access: DELETE_READ_CONTROL SYNCHRONIZE_WRITE_DAC WRITE_OWNER_MUTEX_MODIFY_STATE
[process 3]	Name: Global\0f098b281562f5e76b32695c615befdd Desired Access: DELETE_READ_CONTROL SYNCHRONIZE_WRITE_DAC WRITE_OWNER_MUTEX_MODIFY_STATE
[process 3]	Name: Global\aeff2c2ed47042919a52b72bbb215e64 Desired Access: DELETE_READ_CONTROL SYNCHRONIZE_WRITE_DAC WRITE_OWNER_MUTEX_MODIFY_STATE
[process 3]	Name: Global\4368b89957cbaf8c0664b3466606e45 Desired Access: DELETE_READ_CONTROL SYNCHRONIZE_WRITE_DAC WRITE_OWNER_MUTEX_MODIFY_STATE
[process 3]	Name: Global\342c2b7dc8f6b677270009423d94d822 Desired Access: DELETE_READ_CONTROL SYNCHRONIZE_WRITE_DAC WRITE_OWNER_MUTEX_MODIFY_STATE
[process 3]	Name: Global\3bffb610c5ce9a1b674b27cd0ff0da82 Desired Access: DELETE_READ_CONTROL SYNCHRONIZE_WRITE_DAC WRITE_OWNER_MUTEX_MODIFY_STATE
[process 3]	Name: Global\{81f48c8e5835f2e08e6e45bbac94971} Desired Access: DELETE_READ_CONTROL SYNCHRONIZE_WRITE_DAC WRITE_OWNER_MUTEX_MODIFY_STATE

[process 3]	Name: Global\8b489383e154beca85b0c0e99b8a5ebb Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 3]	Name: Global\9fe75a646856ee20197ac905b36c164 Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 3]	Name: Global\084188c65f1f6246475919472bad801 Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 3]	Name: Global\42802bb79083d5b8546d24585b97f5fe Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 3]	Name: Global\2e256d1a5732754c710de552c7953a08 Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 3]	Name: Global\dea5fba21dcfadb6c08284a694115f7a Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 3]	Name: Global\24bee683f9a06734c14d16c521f7ebe4 Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 3]	Name: Global\b10eb361d81ca9f1b7bd41fdd5f97acb Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE

Created Keys	
	key
[process 1]	\REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{687C2530-10CD-8BEE-E069-B763913F3084}\ShellFolder
[process 1]	\REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\
[process 1]	\REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{687C2530-10CD-8BEE-E069-B763913F3084}\ShellFolder
[process 3]	\REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{4670BCCB-A0D3-6E45-81E1-4A346FCBD0AE}\ShellFolder
[process 3]	\REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\
[process 3]	\REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{4670BCCB-A0D3-6E45-81E1-4A346FCBD0AE}\
[process 3]	\REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{BE75A49C-CA11-D141-E7B2-41E95054153B}\ShellFolder
[process 3]	\REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{BE75A49C-CA11-D141-E7B2-41E95054153B}\
[process 3]	\REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{E86BD4FA-944B-2D7A-73D3-0862BA615172}\ShellFolder
[process 3]	\REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{E86BD4FA-944B-2D7A-73D3-0862BA615172}\
[process 3]	\REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{693C5F7C-78B4-5363-6BDD-77B4A11E89B9}\ShellFolder
[process 3]	\REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{693C5F7C-78B4-5363-6BDD-77B4A11E89B9}\
[process 3]	\REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{5F8FA48D-0C76-69BA-6F6C-51E969996E81}\ShellFolder
[process 3]	\REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{5F8FA48D-0C76-69BA-6F6C-51E969996E81}\
[process 3]	\REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{64949C86-B2AB-02A6-5132-C4A2A6BB8B05}\ShellFolder
[process 3]	\REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{64949C86-B2AB-02A6-5132-C4A2A6BB8B05}\

Set Values	
	key
[process 1]	Key Name: \REGISTRY\MACHINE\SOFTWARE\Microsoft\Cryptography\ RNG Value: Seed
[process 1]	Key Name: \REGISTRY\MACHINE\SOFTWARE\Microsoft\Cryptography\ RNG Value: Seed
[process 1]	Key Name: \REGISTRY\MACHINE\SOFTWARE\Microsoft\Cryptography\ RNG Value: Seed
[process 1]	Key Name: \REGISTRY\MACHINE\SOFTWARE\Microsoft\Cryptography\ RNG Value: Seed
[process 1]	Key Name: \REGISTRY\MACHINE\SOFTWARE\Microsoft\Cryptography\ RNG Value: Seed
[process 1]	Key Name: \REGISTRY\MACHINE\SOFTWARE\Microsoft\Cryptography\ RNG Value: Seed
[process 1]	Key Name: \REGISTRY\MACHINE\SOFTWARE\Microsoft\Cryptography\ RNG Value: Seed
[process 1]	Key Name: \REGISTRY\MACHINE\SOFTWARE\Microsoft\Cryptography\ RNG Value: Seed
[process 1]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{687C2530-10CD-8BEE-E069-B763913F3084}\ShellFolder Value: 0
[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 2]	Key Name: \REGISTRY\MACHINE\SOFTWARE\Microsoft\Cryptography\ RNG Value: Seed
[process 3]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{687C2530-10CD-8BEE-E069-B763913F3084}\ShellFolder Value: 01D01079DA4ED882

Deleted Values	
	key
[process 3]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{687C2530-10CD-8BEE-E069-B763913F3084}\ShellFolder Value: 0
[process 3]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\Windows\CurrentVersion\Run Value: wwnotify

Network Events			
	Remote IP	Local IP	HTTP Command
[process 1]	203.172.141.250	10.20.25.250	POST /

Network Traffic		
	Remote IP	Local IP
Connection #1	10.20.25.255	10.20.25.250

DNS Requests	
Request	Result
No activity	--

Virus Total Results	
Last Scanned:	2014-12-05 10:39:33
Bkav:	Not Detected
MicroWorld-eScan:	Not Detected
nProtect:	Not Detected
CMC:	Not Detected
CAT-QuickHeal:	Not Detected
ALYac:	Not Detected
Malwarebytes:	Not Detected
VIPRE:	Not Detected
SUPERAntiSpyware:	Not Detected
TheHacker:	Not Detected
K7GW:	Not Detected
K7AntiVirus:	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
ClamAV:	Not Detected
Kaspersky:	Not Detected
BitDefender:	Not Detected
NANO-Antivirus:	Not Detected
ViRobot:	Not Detected
ByteHero:	Not Detected
Tencent:	Not Detected
Ad-Aware:	Not Detected
Comodo:	Not Detected
F-Secure:	Not Detected
DrWeb:	Not Detected
Zillya:	Not Detected
TrendMicro:	Not Detected
McAfee-GW-Edition:	Not Detected
Sophos:	Not Detected
Cyren:	Not Detected
Jiangmin:	Not Detected
Avira:	Not Detected
Antiy-AVL:	Not Detected
Kingsoft:	Not Detected
Microsoft:	Not Detected
AegisLab:	Not Detected
GData:	Not Detected
AhnLab-V3:	Not Detected
McAfee:	Not Detected
AVware:	Not Detected
VBA32:	Not Detected
Panda:	Not Detected
Zoner:	Not Detected
ESET-NOD32:	Not Detected
Rising:	Not Detected
Ikarus:	Not Detected
Fortinet:	Not Detected
AVG:	Not Detected
Baidu-International:	Not Detected
Qihoo-360:	HEUR/QVM20.1.Malware.Gen

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.