



Analysis # 31187

06/12/2013 18:41 pm

Table of Contents

Analysis Summary	3
Analysis Summary	3
Digital Behavior Traits	3
File Activity	4
Deleted Files	4
Created Mutexes	5
Created Mutexes	5
Registry Activity	6
Created Keys	6
Set Values	7
Network Activity	8
Network Events	8
Network Traffic	9
DNS Requests	10
Virus Total Results	11

Analysis Summary	
Submitted File:	Scan_06122013_29911.exe
MD5:	8fcba93b00dba3d182b1228b529d3c9e
File Size:	115200
File Type:	PE32 executable for MS Windows (GUI) Intel 80386 3
Analysis Time:	2013-06-12 18:41:50
Start Reason:	AnalysisTarget
Termination Reason:	TerminatedBySelf
Start Time:	Wed, 12 Jun 2013 22:45:47 +0000
Termination Time:	Wed, 12 Jun 2013 22:46:00 +0000
Analysis Time:	2013-06-12 18:41:50
Sandbox:	XPSP3 - 00-0C-29-5E-B4-D8
Total Processes:	1
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 1] C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp\mmc1273C430.xml

Created Mutexes	
	mutex
[process 1]	Name: oleacc-msaa-loaded Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 1]	Name: Local\c:\docume~1\admini~1\locals~1\temp!temporary internet files!content.ie5! Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 1]	Name: Local\c:\docume~1\admini~1\locals~1\temp!cookies! Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 1]	Name: Local\c:\docume~1\admini~1\locals~1\temp!history!history.ie5! Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE

Created Keys	
	key
[process 1]	\REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\WinRAR
[process 1]	\REGISTRY\MACHINE\Software\Microsoft\Windows\CurrentVersion\Explorer\User Shell Folders
[process 1]	\REGISTRY\MACHINE\Software\Microsoft\Windows\CurrentVersion\Explorer\User Shell Folders
[process 1]	\REGISTRY\MACHINE\Software\Microsoft\Windows\CurrentVersion\Explorer\User Shell Folders
[process 1]	\REGISTRY\MACHINE\Software\Microsoft\Windows\CurrentVersion\Explorer\User Shell Folders
[process 1]	\REGISTRY\MACHINE\Software\Microsoft\Windows\CurrentVersion\Explorer\User Shell Folders
[process 1]	\REGISTRY\MACHINE\Software\Microsoft\Windows\CurrentVersion\Explorer\User Shell Folders
[process 1]	\REGISTRY\MACHINE\Software\Microsoft\Windows\CurrentVersion\Explorer\User Shell Folders
[process 1]	\REGISTRY\MACHINE\Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache

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-1-5-21-299502267-926492609-1801674531-500\Software\WinRAR Value: HWID
[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\Explorer\Shell Folders Value: Local AppData
[process 1]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders Value: Personal
[process 1]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\WinRAR Value: Client Hash
[process 1]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\{3259504d-e161-11e0-bf1d-806d6172696f} Value: BaseClass
[process 1]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\{3259504b-e161-11e0-bf1d-806d6172696f} Value: BaseClass
[process 1]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\{3259504a-e161-11e0-bf1d-806d6172696f} Value: BaseClass
[process 1]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders Value: Desktop

Network Events			
	Remote IP	Local IP	HTTP Command
[process 1]	71.19.227.135	10.20.25.247	POST /webstats/counter.php
[process 1]	205.178.152.164	10.20.25.247	GET /Aq70QrZ.exe
[process 1]	198.173.244.62	10.20.25.247	GET /dNYC.exe
[process 1]	204.8.121.24	10.20.25.247	GET /inZGwEH.exe
[process 1]	195.110.124.133	10.20.25.247	GET /UmQ.exe

Network Traffic		
	Remote IP	Local IP
Connection #1	10.20.25.255	10.20.25.247

DNS Requests	
Request	Result
forum.xcpus.com	71.19.227.135
apparellogisticsgroup.net	205.178.152.164
ftp.celebritynetworks.com	198.173.244.62
portal.wroctv.com	204.8.121.24
ftp.videotre.tv.it	195.110.124.133

Virus Total Results	
Last Scanned:	2013-06-12 22:44:26
MicroWorld-eScan:	Not Detected
nProtect:	Not Detected
CAT-QuickHeal:	Not Detected
McAfee:	Ransom-FCFH!8FCBA93B00DB
Malwarebytes:	Trojan.Agent.rf
K7AntiVirus:	Not Detected
K7GW:	Not Detected
TheHacker:	Not Detected
Agnitum:	Not Detected
F-Prot:	W32/Trojan3.FHL
Symantec:	Trojan.Zbot
Norman:	Hlux.ZY
TotalDefense:	Not Detected
TrendMicro-HouseCall:	TROJ_GEN.F47V0612
Avast:	Win32:Malware-gen
eSafe:	Not Detected
ClamAV:	Not Detected
Kaspersky:	Trojan-PSW.Win32.Tepfer.mfzj
BitDefender:	Gen:Variant.Kazy.186449
NANO-Antivirus:	Not Detected
SUPERAntiSpyware:	Not Detected
ByteHero:	Not Detected
Emsisoft:	Gen:Variant.Kazy.186449 (B)
Comodo:	Heur.Packed.Unknown
F-Secure:	Not Detected
DrWeb:	Not Detected
VIPRE:	Win32.Malware!Drop
AntiVir:	TR/Kryptik.TG.2
TrendMicro:	Not Detected
McAfee-GW-Edition:	Heuristic.LooksLike.Win32.Suspicious.B
Sophos:	Troj/Zbot-FLU
Jiangmin:	Not Detected
Antiy-AVL:	Not Detected
Kingsoft:	Win32.HeurC.KVMH004.a.(kcloud)
Microsoft:	Not Detected
ViRobot:	Not Detected
GData:	Gen:Variant.Kazy.186449
CommTouch:	W32/Trojan.ZZPQ-6037
AhnLab-V3:	Trojan/Win32.Tepfer
VBA32:	Malware-Cryptor.General.3
PCTools:	Not Detected
ESET-NOD32:	a variant of Win32/Kryptik.BDKC
Rising:	Backdoor.Agent!548E
Ikarus:	Not Detected
Fortinet:	W32/Kryptik.AGAJ!tr
AVG:	Not Detected
Panda:	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

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.