



Analysis # 2568

09/11/2014 16:52 pm

Table of Contents

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

Analysis Summary	
Submitted File:	111.exe
MD5:	d54b7bd12cb516945972242ea9ac84e2
File Size:	173056
File Type:	PE32 executable for MS Windows (GUI) Intel 80386 3
Analysis Time:	2014-09-11 16:52:12
Start Reason:	AnalysisTarget
Termination Reason:	TerminatedBySelf
Start Time:	Fri, 12 Sep 2014 01:56:48 +0000
Termination Time:	Fri, 12 Sep 2014 01:57:48 +0000
Analysis Time:	2014-09-11 16:52:12
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	

Stored Modified Files

[process 2] C:\WINDOWS\system32\stubyoyn.exe

[process 2] C:\Documents and Settings\Charlie\stubyoyn.exe

Created Mutexes	
	mutex
[process 3]	Name: SHIMLIB_LOG_MUTEX Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE

Set Values	
	key
[process 1]	Key Name: \REGISTRY\MACHINE\SOFTWARE\Microsoft\Cryptography\ RNG Value: Seed
[process 2]	Key Name: \REGISTRY\MACHINE\Software\Microsoft\Windows\CurrentVersion\Run Value: stubyoyn
[process 2]	Key Name: \REGISTRY\USER\S-1-5-21-602162358-879983540-1177238915-1003\Software\Microsoft\Windows\CurrentVersion\Run Value: stubyoyn
[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

Network Events			
	Remote IP	Local IP	HTTP Command
[process 3]	193.169.86.151	10.20.25.250	none
[process 3]	193.19.184.20	10.20.25.250	none

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:	2014-09-11 20:55:01
Bkav:	HW32.Laneul.sswu
MicroWorld-eScan:	Gen:Variant.Graftor.155018
nProtect:	Not Detected
CMC:	Not Detected
CAT-QuickHeal:	Not Detected
McAfee:	RDN/Generic.dxldfh
Malwarebytes:	Trojan.Ransom.ED
VIPRE:	Not Detected
AegisLab:	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
Avast:	Win32:Malware-gen
ClamAV:	Not Detected
Kaspersky:	Trojan.Win32.Cutwail.eet
BitDefender:	Gen:Variant.Graftor.155018
NANO-Antivirus:	Not Detected
SUPERAntiSpyware:	Not Detected
Tencent:	Win32.Trojan.Bp-generic.Jaiu
Ad-Aware:	Gen:Variant.Graftor.155018
Sophos:	Mal/Generic-S
Comodo:	Not Detected
F-Secure:	Gen:Variant.Graftor.155018
DrWeb:	Not Detected
Zillya:	Not Detected
McAfee-GW-Edition:	BehavesLike.Win32.PWSZbot.ch
Emsisoft:	Gen:Variant.Graftor.155018 (B)
Cyren:	Not Detected
Jiangmin:	Not Detected
Avira:	TR/Cutwail.eet
Antiy-AVL:	Not Detected
Kingsoft:	Not Detected
Microsoft:	Not Detected
ViRobot:	Not Detected
AhnLab-V3:	Dropper/Win32.Necurs
GData:	Gen:Variant.Graftor.155018
ByteHero:	Not Detected
VBA32:	Not Detected
AVware:	Not Detected
Baidu-International:	Trojan.Win32.Wigon.BKQ
Zoner:	Not Detected
ESET-NOD32:	Win32/Wigon.KQ
Rising:	Not Detected
Ikarus:	Trojan.Win32.Wigon
Fortinet:	Not Detected
AVG:	Inject2.AVGR
Panda:	Not Detected
Qihoo-360:	Win32/Trojan.Multi.daf

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.