Analysis # 7662

03/08/2016 02:33 am

Table of Contents

Analysis Summary

Submitted File:	keygen.exe
MD5:	966326af9d55cae505a52bca19b049d4
File Size:	3747840
File Type:	PE32 executable for MS Windows (GUI) Intel 80386 3
Analysis Time:	2016-03-08 02:33:59
Start Reason:	AnalysisTarget
Termination Reason:	Timeout
Start Time:	Tue, 08 Mar 2016 07:34:44 +0000
Termination Time:	Tue, 08 Mar 2016 07:35:44 +0000
Analysis Time:	2016-03-08 02:33:59
Sandbox:	XPPubClient1 - 00-50-56-2F-96-25
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**	—

Created Mutexes	
	mutex
[process 1]	Name: DirectSound DllMain mutex (0x000006D0)
	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 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

Network Events			
	Remote IP	**Local IP**	**HTTP Command**
[process]			none

Network Traffic		
	Remote IP	**Local IP**
	No activity	--

DNS Requests	
Request	**Result**
No activity	--

Virus Total Results	
Last Scanned:	**2016-03-05 20:28:47**
Bkav:	Not Detected
MicroWorld-eScan:	Not Detected
nProtect:	Not Detected
CMC:	Not Detected
CAT-QuickHeal:	HackTool.Keygen.g2 (Not a Virus)
McAfee:	Artemis!966326AF9D55
Malwarebytes:	Not Detected
VIPRE:	Trojan.Win32.Generic.pak!cobra
SUPERAntiSpyware:	Not Detected
TheHacker:	Not Detected
Alibaba:	Not Detected
K7GW:	Trojan (0048d3881)
K7AntiVirus:	Trojan (0048d3881)
NANO-Antivirus:	Not Detected
Cyren:	W32/Trojan.SHGI-7119
Symantec:	Backdoor.Sdbot
ByteHero:	Not Detected
TrendMicro-HouseCall:	Not Detected
Avast:	Not Detected
ClamAV:	Not Detected
GData:	Win32.Trojan.Agent.N49T22
Kaspersky:	Not Detected
BitDefender:	Not Detected
Agnitum:	PUP.Agent!
ViRobot:	Trojan.Win32.S.Agent.3747840.B[h]
Tencent:	Not Detected
Ad-Aware:	Not Detected
Sophos:	DI Keygen (PUA)
Comodo:	UnclassifiedMalware
F-Secure:	Not Detected
DrWeb:	Not Detected
Zillya:	Tool.Keygen.Win32.2
TrendMicro:	TROJ_GEN.R0CBC0EBJ16
McAfee-GW-Edition:	BehavesLike.Win32.CrackSuspicious.wc
Emsisoft:	Not Detected
F-Prot:	Not Detected
Jiangmin:	Trojan/Genome.ctgr
Avira:	TR/Agent.3747840.7
Arcabit:	Not Detected
AegisLab:	Troj.Agent.Gen!c
Microsoft:	HackTool:Win32/Keygen
AhnLab-V3:	Unwanted/Win32.HackTool
ALYac:	Not Detected
AVware:	Trojan.Win32.Generic.pak!cobra
VBA32:	Not Detected
Baidu-International:	Not Detected
Zoner:	Not Detected
ESET-NOD32:	a variant of Win32/Keygen.HU potentially unsafe
Rising:	PE:Malware.Generic/QRS!1.9E2D [F]
Ikarus:	not-a-virus:Keygen.SuspectCRC
Fortinet:	Not Detected
AVG:	Crack.AAQ
Panda:	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