VALKYRIE

CLEAN
Valkyrie Final Verdict

File Name: own.exe
File Type: PE32 executable (GUI) Intel 80386, for MS Windows
SHA1: 2f0b1b86e039e9e06315679b2d64b6dac0fcf913
MD5: e87d03f0ff7c9cfc2d6ab50a6508bf8e
First Seen Date: 2017-10-11 17:17:29 UTC
Number of Clients Seen: 2
Last Analysis Date: 2017-10-11 17:17:29 UTC
Human Expert Analysis Result: No human expert analysis verdict given to this sample yet.
Verdict Source: Trusted Vendor

Analysis Summary

ANALYSIS TYPE	DATE	VERDICT	
Signature Based Detection	2017-10-11 17:17:29 UTC	Clean	✓
Static Analysis Overall Verdict	2017-10-11 17:17:29 UTC	No Threat Found	?
Precise Detectors Overall Verdict	2017-10-11 17:17:29 UTC	No Match	?
File Certificate Validation		Certificate and Vendor name are Valid	✓

Static Analysis

STATIC ANALYSIS OVERALL VERDICT	RESULT
No Threat Found	?

DETECTOR	RESULT	
Optional Header LoaderFlags field is valued illegal	Clean	✓
Non-ascii or empty section names detected	Clean	✓
Illegal size of optional Header	Clean	✓
Packer detection on signature database	Unknown	?
Based on the sections entropy check! file is possibly packed	Clean	✓
Timestamp value suspicious	Clean	✓
Header Checksum is zero!	Clean	✓
Enrty point is outside the 1st(.code) section! Binary is possibly packed	Clean	✓
Optional Header NumberOfRvaAndSizes field is valued illegal	Clean	✓
Anti-vm present	Clean	✓
The Size Of Raw data is valued illegal! Binary might crash your disassembler/debugger	Clean	✓
TLS callback functions array detected	Clean	✓

Dynamic Analysis

DYNAMIC ANALYSIS OVERALL VERDICT	RESULT
No Threat Found	?

SUSPICIOUS BEHAVIORS	
Creates a child process	!
Writes to address space of another process	!
Uses a function clandestinely	!
Reads memory of another process	!
Opens a file in a system directory	!
Has no visible windows	!

Behavioral Information

CreateRegisteryKey

RegCreateKeyExA(80000002,Software\Microsoft\Fusion\GACChangeNotification\Default,0,<NULL>,0,20119,0,74835a00,0)
RegCreateKeyExW(,,,,,,,,) -> 0

RegCloseKey

RegCloseKey(b8)
RegCloseKey() -> 0
RegCloseKey(b4)
RegCloseKey(bc)
RegCloseKey(cc)
RegCloseKey(c8)
RegCloseKey(12c)
RegCloseKey(128)
RegCloseKey(18c)
RegCloseKey(180)
RegCloseKey(1b0)
RegCloseKey(2c8)
RegCloseKey(31c)
RegCloseKey(32c)
RegCloseKey(33c)
RegCloseKey(340)
RegCloseKey(1a4)

QueryFilePath

GetModuleFileNameA(0,748c32b8,104)
GetModuleFileNameA(,C:\own.exe,) -> a
GetModuleFileNameA(0,12f0898,104)
GetModuleFileNameA(12e0000,4edefdc,80)
GetModuleFileNameW(74880000,26f4c8,104)
GetModuleFileNameW(,C:\Windows\system32\mscoree.dll,) -> 1f
GetModuleFileNameW(0,5ad738,14d)
GetModuleFileNameW(,C:\own.exe,) -> a
GetModuleFileNameW(74230000,2673c4,1f40)
GetModuleFileNameW(,C:\Windows\WinSxS\x86_microsoft.vc80.crt_1fc8b3b9a1e18e3b_8.0.50727.4940_none_d08cc06a442b34fc\MSVCR80.dll,) -> 6a
GetModuleFileNameW(742d0000,26f5c0,104)
GetModuleFileNameW(,C:\Windows\Microsoft.NET\Framework\v2.0.50727\mscorwks.dll,) -> 3a
GetModuleFileNameW(0,26fa44,104)
GetModuleFileNameW(742d0000,7483a770,104)
GetModuleFileNameW(0,74837888,104)
GetModuleFileNameW(742d0000,160db0,104)
GetModuleFileNameW(0,26f9f0,104)
GetModuleFileNameW(742d0000,26ef38,104)
GetModuleFileNameW(742d0000,26ce78,104)
GetModuleFileNameW(71fe0000,4edda1c,104)
GetModuleFileNameW(,C:\Windows\SysWOW64\ieframe.dll,) -> 1f
GetModuleFileNameW(0,4eddcbc,104)
GetModuleFileNameW(0,620670,104)
GetModuleFileNameW(0,4edbefc,104)
GetModuleFileNameW(72dc0000,72e3a158,104)
GetModuleFileNameW(,C:\Windows\system32\PROPSYS.dll,) -> 1f

GetModuleFileNameW(0,4ede21c,104)

LowerChar

CharLowerW(file)
CharLowerW(file) -> file
CharLowerW(.exe)
CharLowerW(.exe) -> .exe
CharLowerW(program)
CharLowerW(program) -> program

ReadRegisteryKey

RegQueryValueExW(b8,InstallRoot,0,26f280,0,26f284)
RegQueryValueExW(,,,,,) -> 0
RegQueryValueExW(b8,InstallRoot,0,0,5ad768,26f284)
RegQueryValueExW(b4,InstallRoot,0,26f524,0,26f528)
RegQueryValueExW(b4,InstallRoot,0,0,5ad738,26f528)
RegQueryValueExW(b4,InstallRoot,0,26f4c0,0,26f4c4)
RegQueryValueExW(b4,InstallRoot,0,0,5ad738,26f4c4)
RegQueryValueExW(b4,CLRLoadLogDir,0,26eea4,0,26eea8)
RegQueryValueExW(,,,,,) -> 2
RegQueryValueExW(b4,OnlyUseLatestCLR,0,26f27c,26f284,26f280)
RegQueryValueExW(b4,InstallRoot,0,26ee70,0,26ee74)
RegQueryValueExW(b4,InstallRoot,0,0,5ad738,26ee74)
RegQueryValueExW(b4,InstallRoot,0,26e76c,0,26e770)
RegQueryValueExW(b4,InstallRoot,0,0,5ad738,26e770)
RegQueryValueExW(bc,GCStressStart,0,26f270,26f26c,26f25c)
RegQueryValueExW(bc,GCStressStartAtJit,0,26f270,26f26c,26f25c)
RegQueryValueExW(bc,DisableConfigCache,0,26fc98,26fc94,26fc84)
RegQueryValueExW(cc,CacheLocation,0,26f19c,26f1a4,26f198)
RegQueryValueExW(cc,DownloadCacheQuotaInKB,0,26f7d8,26f7e0,26f7ec)
RegQueryValueExW(c8,EnableLog,0,26f7ec,26f7f8,26f7e8)
RegQueryValueExW(c8,LoggingLevel,0,26f7ec,26f7f8,26f7e8)
RegQueryValueExW(c8,ForceLog,0,26f7ec,26f7f8,26f7e8)
RegQueryValueExW(c8,LogFailures,0,26f7ec,26f7f8,26f7e8)
RegQueryValueExW(c8,VersioningLog,0,26f7ec,26f7f8,26f7e8)
RegQueryValueExW(c8,LogResourceBinds,0,26f7ec,26f7f8,26f7e8)
RegQueryValueExW(c8,UseLegacyIdentityFormat,0,26f7ec,26f7f8,26f7e8)
RegQueryValueExW(c8,DisableMSIPeek,0,26f7ec,26f7f8,26f7e8)
RegQueryValueExW(c8,NoClientChecks,0,26f7ec,26f7f8,26f7e8)
RegQueryValueExW(c8,DevOverrideEnable,0,26f594,26f5a0,26f590)
RegQueryValueExW(180,LatestIndex,0,26f124,26f164,26f158)
RegQueryValueExW(184,LatestIndex,0,26ee7c,5d475c,26eea4)
RegQueryValueExW(18c,NIUsageMask,0,26ea68,26ea74,26ea70)
RegQueryValueExW(18c,ILUsageMask,0,26ea68,26ea74,26ea70)
RegQueryValueExW(180,DisplayName,0,26eac0,26eacc,26eac8)
RegQueryValueExW(180,ConfigMask,0,26eac0,26eacc,26eac8)
RegQueryValueExW(180,ConfigString,0,26eac0,26eacc,26eac8)
RegQueryValueExW(180,MVID,0,26eac0,26eacc,26eac8)
RegQueryValueExW(180,EvalationData,0,26eb58,26eb64,26eb60)
RegQueryValueExW(180,Status,0,26eb58,26eb64,26eb60)
RegQueryValueExW(180,ILDependencies,0,26eb58,26eb64,26eb60)
RegQueryValueExW(180,NIDependencies,0,26eb58,26eb64,26eb60)
RegQueryValueExW(180,MissingDependencies,0,26eb58,26eb64,26eb60)
RegQueryValueExW(180,DisplayName,0,26eb0c,26eb18,26eb14)
RegQueryValueExW(180,Status,0,26eb0c,26eb18,26eb14)
RegQueryValueExW(180,Modules,0,26eb0c,26eb18,26eb14)
RegQueryValueExW(180,SIG,0,26eb0c,26eb18,26eb14)
RegQueryValueExW(180,LastModTime,0,26eb0c,26eb18,26eb14)
RegQueryValueExW(180,mscorlib,2.0.0.0,,b77a5c561934e089,x86,0,26e924,26ef64,26e928)
RegQueryValueExW(1a4,Latest,0,26efd8,5bf9bc,26efdc)
RegQueryValueExW(1a4,index1,0,26eb8c,26eb98,26eb94)
RegQueryValueExW(1a4,LegacyPolicyTimeStamp,0,26efd8,5bf9dc,26efdc)
RegQueryValueExW(1b0,LatestIndex,0,26da4c,26da8c,26da80)
RegQueryValueExW(1b0,DisplayName,0,26d400,26d40c,26d408)
RegQueryValueExW(1b0,ConfigMask,0,26d400,26d40c,26d408)
RegQueryValueExW(1b0,ConfigString,0,26d400,26d40c,26d408)
RegQueryValueExW(1b0,MVID,0,26d400,26d40c,26d408)
RegQueryValueExW(1b0,EvalationData,0,26d498,26d4a4,26d4a0)
RegQueryValueExW(1b0,Status,0,26d498,26d4a4,26d4a0)
RegQueryValueExW(1b0,ILDependencies,0,26d498,26d4a4,26d4a0)
RegQueryValueExW(1b0,NIDependencies,0,26d498,26d4a4,26d4a0)

RegQueryValueExW(1b0,MissingDependencies,0,26d498,26d4a4,26d4a0)
RegQueryValueExW(1b0,DisplayName,0,26d44c,26d458,26d454)
RegQueryValueExW(1b0,Status,0,26d44c,26d458,26d454)
RegQueryValueExW(1b0,Modules,0,26d44c,26d458,26d454)
RegQueryValueExW(1b0,SIG,0,26d44c,26d458,26d454)
RegQueryValueExW(1b0,LastModTime,0,26d44c,26d458,26d454)
RegQueryValueExW(180,System,2.0.0.0,,b77a5c561934e089,MSIL,0,26ccd8,26d318,26ccdc)
RegQueryValueExW(180,System.Xml,2.0.0.0,,b77a5c561934e089,MSIL,0,26c7d0,26ce10,26c7d4)
RegQueryValueExW(180,System.Configuration,2.0.0.0,,b03f5f7f11d50a3a,MSIL,0,26c7d0,26ce10,26c7d4)
RegQueryValueExW(27c,CreateUriCacheSize,0,4edd9b0,766850a4,4edd9b4)
RegQueryValueExW(280,CreateUriCacheSize,0,4edd9b0,766850a4,4edd9b4)
RegQueryValueExW(284,CreateUriCacheSize,0,4edd9b0,766850a4,4edd9b4)
RegQueryValueExW(288,CreateUriCacheSize,0,4edd9b0,766850a4,4edd9b4)
RegQueryValueExW(27c,EnablePunycode,0,4edd778,76685048,4edd77c)
RegQueryValueExW(280,EnablePunycode,0,4edd778,76685048,4edd77c)
RegQueryValueExW(284,EnablePunycode,0,4edd778,76685048,4edd77c)
RegQueryValueExW(288,EnablePunycode,0,4edd778,76685048,4edd77c)
RegQueryValueExW(31c,FrameTabWindow,0,4eddb60,4eddb68,4eddb64)
RegQueryValueExW(320,FrameTabWindow,0,4eddb60,4eddb68,4eddb64)
RegQueryValueExW(31c,FrameMerging,0,4eddb60,4eddb68,4eddb64)
RegQueryValueExW(320,FrameMerging,0,4eddb60,4eddb68,4eddb64)
RegQueryValueExW(31c,SessionMerging,0,4eddb60,4eddb68,4eddb64)
RegQueryValueExW(320,SessionMerging,0,4eddb60,4eddb68,4eddb64)
RegQueryValueExW(31c,AdminTabProcs,0,4eddb60,4eddb68,4eddb64)
RegQueryValueExW(320,AdminTabProcs,0,4eddb60,4eddb68,4eddb64)
RegQueryValueExW(31c,TabProcGrowth,0,4eddb60,4ede458,4eddb64)
RegQueryValueExW(320,TabProcGrowth,0,4eddb60,4ede458,4eddb64)
RegQueryValueExW(31c,TabProcGrowth,0,4eddb68,4ede450,4eddb6c)
RegQueryValueExW(320,TabProcGrowth,0,4eddb68,4ede450,4eddb6c)
RegQueryValueExW(32c,DisableSecuritySettingsCheck,0,4edecb0,4edef10,4edecb4)
RegQueryValueExW(33c,SystemSetupInProgress,0,0,76e51030,4edec68)
RegQueryValueExW(27c,SpecialFoldersCacheSize,0,4eddb40,62d034,4eddb44)
RegQueryValueExW(280,SpecialFoldersCacheSize,0,4eddb40,62d034,4eddb44)
RegQueryValueExW(284,SpecialFoldersCacheSize,0,4eddb40,62d034,4eddb44)
RegQueryValueExW(288,SpecialFoldersCacheSize,0,4eddb40,62d034,4eddb44)

SetFilePointer

SetFilePointer(1f8,ffffffff8,26f3c4,2)
SetFilePointer(,,,) -> 1cec88
SetFilePointer(1f8,ffff6000,26f3c4,2)
SetFilePointer(,,,) -> 1c4c90
SetFilePointer(264,fffffc00,0,2)
SetFilePointer(,,,) -> c3b000
SetFilePointer(35c,fffffc00,0,2)
SetFilePointer(,,,) -> 11a00

CreateFile

CreateFileW(C:\own.exe.config,80000000,1,0,3,80,0)
CreateFileW(,,,,,,) -> ffffffff
CreateFileW(C:\own.exe,80000000,1,0,3,8000000,0)
CreateFileW(,,,,,,) -> b4
CreateFileMappingW(b4,0,2,0,0,<NULL>)
CreateFileMappingW(,,,,,) -> b8
CreateFileW(C:\Windows\Microsoft.NET\Framework\v2.0.50727\config\machine.config,80000000,1,0,3,80,0)
CreateFileW(,,,,,,) -> c8
CreateFileMappingW(ffffffff,5adf90,4,0,fb8,Global\Cor_Private_IPCBlock_2216)
CreateFileMappingW(,,,,,) -> cc
CreateFileMappingW(ffffffff,5ae008,4,0,134,Global\Cor_Public_IPCBlock_2216)
CreateFileMappingW(,,,,,) -> d0
CreateFileW(C:\Windows\Microsoft.NET\Framework\v2.0.50727\config\security.config,80000000,5,0,3,80,0)
CreateFileW(C:\Windows\Microsoft.NET\Framework\v2.0.50727\config\security.config.cch,80000000,5,0,3,80,0)
CreateFileW(C:\Windows\Microsoft.NET\Framework\v2.0.50727\config\enterprisesec.config,80000000,5,0,3,80,0)
CreateFileW(C:\Windows\Microsoft.NET\Framework\v2.0.50727\config\enterprisesec.config.cch,80000000,5,0,3,80,0)
CreateFileW(C:\Users\win7\AppData\Roaming\Microsoft\CLR Security Config\v2.0.50727.312\security.config,80000000,5,0,3,80,0)
CreateFileW(C:\Users\win7\AppData\Roaming\Microsoft\CLR Security Config\v2.0.50727.312\security.config.cch,80000000,5,0,3,80,0)
CreateFileW(C:\Windows\assembly\NativeImages_v2.0.50727_32\index1c2.dat,80000000,1,0,3,0,0)
CreateFileW(,,,,,,) -> 188
CreateFileMappingW(ffffffff,0,4,0,1600,<NULL>)
CreateFileMappingW(,,,,,) -> 1a0
CreateFileMappingW(ffffffff,0,4,0,100490,<NULL>)

CreateFileMappingW(,,,,,) -> 1a4
CreateFileW(C:\Windows\system32\rsaenh.dll,80000000,1,0,3,80,0)
CreateFileW(,,,,,,) -> 1a8
CreateFileW(C:\Windows\assembly\pubpol1.dat,80000000,1,0,3,0,0)
CreateFileW(,,,,,,) -> 1ac
CreateFileW(C:\Windows\Microsoft.NET\Framework\v2.0.50727\config\machine.config,80000000,5,0,3,80,0)
CreateFileW(C:\Windows\system32\l_intl.nls,80000000,1,26c98c,3,0,0)
CreateFileW(,,,,,,) -> 1b4
CreateFileMappingW(1b4,26c98c,2,0,0,<NULL>)
CreateFileMappingW(,,,,,) -> 1b0
CreateFileMappingW(ffffffff,0,4,0,3b400,<NULL>)
CreateFileMappingW(ffffffff,0,4,0,11200,<NULL>)
CreateFileW(C:\own.exe,80000000,1,0,3,100000,0)
CreateFileW(,,,,,,) -> 1f8
CreateFileW(C:\Users\win7\AppData\Local\Temp\setup.msi,c0000000,0,0,2,100000,0)
CreateFileW(,,,,,,) -> 1fc
CreateFileW(C:\Windows\assembly\GAC_32\mscorlib\2.0.0.0__b77a5c561934e089\sorttbls.nlp,80000000,5,0,3,80,0)
CreateFileW(,,,,,,) -> 200
CreateFileMappingW(200,0,2,0,0,<NULL>)
CreateFileMappingW(,,,,,) -> 204
CreateFileW(C:\Windows\assembly\GAC_32\mscorlib\2.0.0.0__b77a5c561934e089\sortkey.nlp,80000000,5,0,3,80,0)
CreateFileW(,,,,,,) -> 208
CreateFileMappingW(208,0,2,0,0,<NULL>)
CreateFileMappingW(,,,,,) -> 20c
CreateFileMappingW(ffffffff,0,4,0,63c00,<NULL>)
CreateFileMappingW(,,,,,) -> 214
CreateFileW(\??\C:\Windows\SysWOW64\ieframe.dll,80,7,0,3,80,0)
CreateFileW(,,,,,,) -> 25c
CreateFileW(C:\,100081,7,0,3,2000000,0)
CreateFileW(,,,,,,) -> 294
CreateFileW(C:\Windows,100081,7,0,3,2000000,0)
CreateFileW(,,,,,,) -> 290
CreateFileW(C:\Windows\System32,100081,7,0,3,2000000,0)
CreateFileW(C:\Users\win7\AppData\Local\Microsoft\Windows\Caches\cversions.1.db,80000000,3,0,3,0,0)
CreateFileW(,,,,,,) -> 2bc
CreateFileMappingW(2bc,4edc578,2,0,4000,Local\C:*Users*win7*AppData*Local*Microsoft*Windows*Caches*cversions.1.ro)
CreateFileMappingW(,,,,,) -> 2c8
CreateFileW(C:\Users\win7\AppData\Local\Microsoft\Windows\Caches\{AFBF9F1A-8EE8-4C77-AF34-C647E37CA0D9}.1.ver0x0000000000000008.db,80000000,1,0,3,0,0)
CreateFileMappingW(2bc,4edcbb4,2,0,0,Local\C:*Users*win7*AppData*Local*Microsoft*Windows*Caches*{AFBF9F1A-8EE8-4C77-AF34-C647E37CA0D9}.1.ver0x0000000000000008.db)
CreateFileMappingW(,,,,,) -> 2f0
CreateFileMappingW(ffffffff,0,4,0,1c,Local\UrlZonesSM_win7)
CreateFileMappingW(,,,,,) -> 338
CreateFileW(C:\Windows\System32\msiexec.exe,20000,3,0,3,0,0)
CreateFileW(,,,,,,) -> 33c

OpenRegisteryKey

RegOpenKeyExW(80000002,Software\Microsoft\.NETFramework\Policy\,0,20019,26fb90)
RegOpenKeyExW(,,,,) -> 0
RegOpenKeyExW(b4,v2.0,0,20019,26fb8c)
RegOpenKeyExW(80000002,Software\Microsoft\.NETFramework,0,20019,26f288)
RegOpenKeyExW(b4,Upgrades,0,20019,26fb8c)
RegOpenKeyExW(b4,Standards,0,20019,26fb8c)
RegOpenKeyExW(b4,AppPatch,0,20019,26fb8c)
RegOpenKeyExW(80000002,Software\Microsoft\.NETFramework,0,20019,26f52c)
RegOpenKeyExW(80000002,Software\Microsoft\.NETFramework,0,20019,26f4c8)
RegOpenKeyExW(80000002,Software\Microsoft\.NETFramework,0,20019,26eeac)
RegOpenKeyExW(80000002,Software\Microsoft\.NETFramework,0,20019,26f26c)
RegOpenKeyExW(80000002,Software\Microsoft\.NETFramework\Policy\AppPatch,0,20019,26f110)
RegOpenKeyExW(80000002,Software\Microsoft\.NETFramework,0,20019,26ee78)
RegOpenKeyExW(b8,v2.0.50727.00000,0,20019,26f214)
RegOpenKeyExW(b4,own.exe,0,20019,26f238)
RegOpenKeyExW(,,,,) -> 2
RegOpenKeyExW(80000002,Software\Microsoft\.NETFramework\Policy\,0,20019,26f260)
RegOpenKeyExW(b4,v2.0,0,20019,26f25c)
RegOpenKeyExW(80000002,Software\Microsoft\.NETFramework,0,20019,26e774)
RegOpenKeyExW(80000001,Software\Microsoft\.NETFramework,0,20019,26f268)
RegOpenKeyExW(80000002,Software\Microsoft\.NETFramework,0,20019,26f264)
RegOpenKeyExW(80000001,Software\Microsoft\.NETFramework,0,20019,26fc90)
RegOpenKeyExW(80000002,Software\Microsoft\.NETFramework,0,20019,26fc8c)
RegOpenKeyExW(80000001,Software\Microsoft\.NETFramework,0,20019,26fcc4)
RegOpenKeyExW(80000002,Software\Microsoft\.NETFramework,0,20019,26fcc4)
RegOpenKeyExW(80000002,Software\Microsoft\Fusion,0,20119,26f844)

RegOpenKeyExW(80000002,Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\own.exe,0,20119,26f840)
RegOpenKeyExW(80000002,Software\Microsoft\Fusion,0,20119,26f1a0)
RegOpenKeyExW(80000002,Software\Microsoft\Fusion,0,20119,26f7e8)
RegOpenKeyExW(80000001,Software\Microsoft\Fusion,0,20119,26f7e4)
RegOpenKeyExW(80000002,Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options,0,20119,26f5e0)
RegOpenKeyExW(80000002,Software\Microsoft\.NETFramework\Security\Policy\Extensions\NamedPermissionSets,0,20019,26f7e8)
RegOpenKeyExW(128,Internet,0,20019,26f7e4)
RegOpenKeyExW(128,LocalIntranet,0,20019,26f7e4)
RegOpenKeyExW(80000002,Software\Microsoft\Windows NT\CurrentVersion\ProfileList\S-1-5-21-3979321414-2393373014-2172761192-1000,0,20019,26f340)
RegOpenKeyExW(80000002,Software\Microsoft\.NETFramework\v2.0.50727\Security\Policy,0,20019,26fc4c)
RegOpenKeyExW(80000002,Software\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_32,0,20119,5d350c)
RegOpenKeyExW(80000002,Software\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_32,0,20119,5d3524)
RegOpenKeyExW(184,index1c2,0,20119,26eeb0)
RegOpenKeyExW(184,NI\181938c6\7950e2c5,0,20119,26ee90)
RegOpenKeyExW(184,NI\181938c6\7950e2c5\16,0,20119,26ef10)
RegOpenKeyExW(184,NI\181938c6\7950e2c5\16,0,20119,26efa8)
RegOpenKeyExW(184,IL\7950e2c5\4b5f28af\5f,0,20119,26ef88)
RegOpenKeyExA(80000002,Software\Microsoft\StrongName,0,20019,26f120)
RegOpenKeyExA(,,,,) -> 2
RegOpenKeyExW(80000002,Software\Microsoft\Fusion\PublisherPolicy\Default,0,20119,5bf9c4)
RegOpenKeyExW(1a4,policy.5.6.ScreenConnect.ClientInstallerRunner__4b14c015c87c1ad8,0,20119,26ea94)
RegOpenKeyExW(1a4,policy.2.0.System__b77a5c561934e089,0,20119,26d3a8)
RegOpenKeyExW(80000002,Software\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_32,0,20119,5e782c)
RegOpenKeyExW(184,NI\30bc7c4f\3f50fe4f,0,20119,26d7d0)
RegOpenKeyExW(184,NI\30bc7c4f\3f50fe4f\18,0,20119,26d850)
RegOpenKeyExW(184,NI\30bc7c4f\3f50fe4f\18,0,20119,26d8e8)
RegOpenKeyExW(184,IL\424bd4d8\324708cb\5c,0,20119,26d8c8)
RegOpenKeyExW(184,IL\19ab8d57\c91dbb2\5e,0,20119,26d8c8)
RegOpenKeyExW(184,IL\3f50fe4f\265c633d\60,0,20119,26d8c8)
RegOpenKeyExW(1a4,policy.2.0.System.Xml__b77a5c561934e089,0,20119,26c664)
RegOpenKeyExW(1a4,policy.2.0.System.Configuration__b03f5f7f11d50a3a,0,20119,26c664)
RegOpenKeyExW(80000002,SOFTWARE\Microsoft\.NETFramework\Policy\APTCA,0,20019,26e3d8)
RegOpenKeyExW(1a4,policy.5.6.ScreenConnect.Core__4b14c015c87c1ad8,0,20119,26d3a8)
RegOpenKeyExW(184,NI\51df596f\11793226,0,20119,26d7d0)
RegOpenKeyExW(80000002,SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\Managed\S-1-5-21-3979321414-2393373014-2172761192-1000\Installer\Assemblies\C:|own.exe,0,20119,26dc78)
RegOpenKeyExW(80000001,Software\Microsoft\Installer\Assemblies\C:|own.exe,0,20119,26dc78)
RegOpenKeyExW(80000002,SOFTWARE\Classes\Installer\Assemblies\C:|own.exe,0,20119,26dc78)
RegOpenKeyExW(80000002,SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\Managed\S-1-5-21-3979321414-2393373014-2172761192-1000\Installer\Assemblies\Global,0,20119,26de9c)
RegOpenKeyExW(80000001,Software\Microsoft\Installer\Assemblies\Global,0,20119,26de9c)
RegOpenKeyExW(80000002,SOFTWARE\Classes\Installer\Assemblies\Global,0,20119,26de9c)
RegOpenKeyExW(1a4,policy.5.6.ScreenConnect.Core__4b14c015c87c1ad8,0,20119,26c784)
RegOpenKeyExW(1a4,policy.5.6.ScreenConnect.WindowsInstaller__4b14c015c87c1ad8,0,20119,26c9e8)
RegOpenKeyExW(184,NI\3122e316\741323cd,0,20119,26ce10)
RegOpenKeyExW(1a4,policy.5.6.ScreenConnect.WindowsInstaller__4b14c015c87c1ad8,0,20119,26bdc4)
RegOpenKeyExW(1a4,policy.5.6.ScreenConnect.MonoServer__4b14c015c87c1ad8,0,20119,26d9a4)
RegOpenKeyExW(184,NI\506bc1f7\30a7feae,0,20119,26ddcc)
RegOpenKeyExW(1a4,policy.5.6.ScreenConnect.Windows__4b14c015c87c1ad8,0,20119,26d9a4)
RegOpenKeyExW(184,NI\7f9fce53\70d4170b,0,20119,26ddcc)
RegOpenKeyExW(1a4,policy.5.6.ScreenConnect.Windows__4b14c015c87c1ad8,0,20119,26cd84)
RegOpenKeyExW(80000002,Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings,0,20019,4edd944)
RegOpenKeyExW(80000001,Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings,0,20019,4edd944)
RegOpenKeyExW(80000001,Software\Microsoft\Windows\CurrentVersion\Internet Settings,0,20019,4edd944)
RegOpenKeyExW(80000002,Software\Microsoft\Windows\CurrentVersion\Internet Settings,0,20019,4edd944)
RegOpenKeyExW(80000002,Software\Policies\Microsoft\Internet Explorer\Main\FeatureControl,0,1,76681bec)
RegOpenKeyExW(80000001,Software\Policies\Microsoft\Internet Explorer\Main\FeatureControl,0,1,76681bf0)
RegOpenKeyExW(80000002,Software\Microsoft\Internet Explorer\Main\FeatureControl,0,1,76681bf4)
RegOpenKeyExW(80000001,Software\Microsoft\Internet Explorer\Main\FeatureControl,0,1,76681bf8)
RegOpenKeyExW(28c,FEATURE_ALLOW_REVERSE_SOLIDUS_IN_USERINFO_KB932562,0,1,4eddeb0)
RegOpenKeyExW(80000002,Software\Microsoft\Windows\CurrentVersion\Explorer\KindMap,0,20119,4ede404)
RegOpenKeyExW(28c,FEATURE_IGNORE_POLICIES_ZONEMAP_IF_ESC_ENABLED_KB918915,0,1,4ede500)
RegOpenKeyExW(28c,FEATURE_ZONES_CHECK_ZONEMAP_POLICY_KB941001,0,1,4ede524)
RegOpenKeyExW(80000002,Software\Policies,0,20019,4ede560)
RegOpenKeyExW(80000001,Software\Policies,0,20019,4ede560)
RegOpenKeyExW(80000001,Software,0,20019,4ede560)
RegOpenKeyExW(80000002,Software,0,20019,4ede560)
RegOpenKeyExW(80000002,Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings,0,1,4ede558)
RegOpenKeyExW(80000002,Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap,0,1,4ede558)
RegOpenKeyExW(80000001,Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings,0,1,4ede558)
RegOpenKeyExW(80000001,Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap,0,1,4ede558)
RegOpenKeyExW(80000001,Software\Microsoft\Internet Explorer\Main,0,20019,4eddaf4)
RegOpenKeyExW(80000002,Software\Microsoft\Internet Explorer\Main,0,20019,4eddaf4)
RegOpenKeyExW(80000002,Software\Policies\Microsoft\Internet Explorer\Main,0,20019,4eddaf4)
RegOpenKeyExW(80000001,Software\Policies\Microsoft\Internet Explorer\Main,0,20019,4eddaf4)
RegOpenKeyExW(28c,FEATURE_INITIALIZE_URLACTION_SHELLEXECUTE_TO_ALLOW_KB936610,0,1,4edf2d8)
RegOpenKeyExW(80000002,Software\Policies\Microsoft\Internet Explorer,0,1,4edec6c)

RegOpenKeyExW(80000001,Software\Policies\Microsoft\Internet Explorer,0,1,4edec6c)
RegOpenKeyExW(314,Microsoft\Internet Explorer\Security,0,20019,4edeca4)
RegOpenKeyExW(318,Microsoft\Internet Explorer\Security,0,20019,4edeca4)
RegOpenKeyExW(80000002,System\Setup,0,20019,4edec6c)
RegOpenKeyExW(80000001,Software\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\,0,20019,4edec94)
RegOpenKeyExW(33c,0,0,20019,4edec90)
RegOpenKeyExW(33c,1,0,20019,4edec90)
RegOpenKeyExW(33c,2,0,20019,4edec90)
RegOpenKeyExW(33c,3,0,20019,4edec90)
RegOpenKeyExW(33c,4,0,20019,4edec90)
RegOpenKeyExW(28c,FEATURE_LOCALMACHINE_LOCKDOWN,0,1,4edebdc)
RegOpenKeyExW(28c,FEATURE_ZONES_DEFAULT_DRIVE_INTRANET_KB941000,0,1,4ede818)
RegOpenKeyExW(28c,FEATURE_PROTOCOL_LOCKDOWN,0,1,4edeef0)

CreateMutex

CreateMutexW(0,0,<NULL>)
CreateMutexW(,,) -> b0
CreateMutexW(0,1,<NULL>)
CreateMutexW(,,) -> 110
CreateMutexW(,,) -> 2a0
CreateMutexW(,,) -> 2a8
CreateMutexA(0,0,Local\ZonesCacheCounterMutex)
CreateMutexA(,,) -> 340
CreateMutexA(0,0,Local\ZonesLockedCacheCounterMutex)
CreateMutexA(,,) -> 344

OpenMutex

OpenMutexW(120000,0,Global\CLR_CASOFF_MUTEX)
OpenMutexW(,,) -> 0

WriteFile

WriteFile(1fc,3c1c0c8,105000,26f2b8,0)
WriteFile(,,,,) -> 1

CreateProcess

CreateProcessW(C:\Windows\System32\msiexec.exe,"C:\Windows\System32\msiexec.exe" /i
"C:\Users\win7\AppData\Local\Temp\setup.msi",0,0,0,4080410,0,C:\Windows\system32,4edf3a4,6300c0)
CreateProcessW(,,,,,,,,,) -> 1 (proc:2712/350, thrd:1092/348

LoadLibrary

LoadLibraryW(mscoree.dll)
LoadLibraryW() -> 74880000
LoadLibraryA(ADVAPI32.dll)
LoadLibraryA() -> 76cd0000
LoadLibraryA(SHLWAPI.dll)
LoadLibraryA() -> 771c0000
LoadLibraryExW(C:\Windows\Microsoft.NET\Framework\v2.0.50727\mscorwks.dll,0,8)
LoadLibraryExW(,,) -> 742d0000
LoadLibraryExW(mscoree.dll,0,0)
LoadLibraryExW(,,) -> 74880000
LoadLibraryExW(ntdll,0,0)
LoadLibraryExW(,,) -> 77620000
LoadLibraryExW(advapi32.dll,0,0)
LoadLibraryExW(,,) -> 76cd0000
LoadLibraryExW(shell32.dll,0,0)
LoadLibraryExW(,,) -> 75400000
LoadLibraryExA(ADVAPI32.dll,0,0)
LoadLibraryExA(,,) -> 76cd0000
LoadLibraryExW(C:\Windows\assembly\NativeImages_v2.0.50727_32\mscorlib\38bf604432e1a30c954b2ee40d6a2d1c\mscorlib.ni.dll,0,8)
LoadLibraryExW(,,) -> 73730000

LoadLibraryExW(C:\Windows\Microsoft.NET\Framework\v2.0.50727\ole32.dll,0,8)
LoadLibraryExW(,,) -> 0
LoadLibraryA(ole32.dll)
LoadLibraryA() -> 76970000
LoadLibraryExW(C:\Windows\Microsoft.NET\Framework\v2.0.50727\OLEAUT32.dll,0,8)
LoadLibraryA(OLEAUT32.dll)
LoadLibraryA() -> 76ec0000
LoadLibraryExW(AdvApi32.dll,0,0)
LoadLibraryExW(C:\Windows\Microsoft.NET\Framework\v2.0.50727\mscorjit.dll,0,0)
LoadLibraryExW(,,) -> 736d0000
LoadLibraryExW(kernel32,0,0)
LoadLibraryExW(,,) -> 76b60000
LoadLibraryExA(CRYPTSP.dll,0,0)
LoadLibraryExA(,,) -> 74b40000
LoadLibraryExA(CRYPTBASE.dll,0,0)
LoadLibraryExA(,,) -> 74fa0000
LoadLibraryExW(C:\Windows\assembly\NativeImages_v2.0.50727_32\System\908ba9e296e92b4e14bdc2437edac603\System.ni.dll,0,8)
LoadLibraryExW(,,) -> 72ee0000
LoadLibraryExW(C:\Windows\Microsoft.NET\Framework\v2.0.50727\culture.dll,0,8)
LoadLibraryExW(,,) -> 72ed0000
LoadLibraryExW(C:\Windows\Microsoft.NET\Framework\v2.0.50727\en-US\mscorrc.dll,0,2)
LoadLibraryExW(C:\Windows\Microsoft.NET\Framework\v2.0.50727\en\mscorrc.dll,0,2)
LoadLibraryExW(C:\Windows\Microsoft.NET\Framework\v2.0.50727\mscorrc.dll,0,2)
LoadLibraryExW(,,) -> 4e0001
LoadLibraryExW(kernel32.dll,0,0)
LoadLibraryExW(C:\Windows\assembly\GAC_MSIL\System\2.0.0.0__b77a5c561934e089\psapi.dll,0,8)
LoadLibraryExW(psapi.dll,0,0)
LoadLibraryExW(,,) -> 76780000
LoadLibraryExW(C:\Windows\assembly\GAC_32\mscorlib\2.0.0.0__b77a5c561934e089\bcrypt.dll,0,8)
LoadLibraryExW(bcrypt.dll,0,0)
LoadLibraryExW(,,) -> 72ec0000
LoadLibraryExW(C:\Windows\assembly\GAC_MSIL\System\2.0.0.0__b77a5c561934e089\shell32.dll,0,8)
LoadLibraryExW(propsys.dll,0,22)
LoadLibraryExW(,,) -> 72dc0000
LoadLibraryExA(ole32.dll,0,0)
LoadLibraryExA(,,) -> 76970000
LoadLibraryW(comctl32.dll)
LoadLibraryW() -> 72c20000
LoadLibraryExW(C:\Windows\SysWOW64\ieframe.dll,0,22)
LoadLibraryExW(,,) -> 71fe0002
LoadLibraryExW(,,) -> 713a0002
LoadLibraryW(kernel32.dll)
LoadLibraryW() -> 76b60000
LoadLibraryExW(comctl32.dll,0,0)
LoadLibraryExW(,,) -> 72c20000
LoadLibraryExA(SHELL32.dll,0,0)
LoadLibraryExA(,,) -> 75400000
LoadLibraryExW(API-MS-Win-Core-LocalRegistry-L1-1-0.dll,0,8)
LoadLibraryW(ntmarta.dll)
LoadLibraryW() -> 71fa0000
LoadLibraryExA(Secur32.dll,0,0)
LoadLibraryExA(,,) -> 71f90000
LoadLibraryExW(API-MS-WIN-DOWNLEVEL-SHLWAPI-L1-1-0.DLL,0,0)
LoadLibraryExW(,,) -> 762e0000
LoadLibraryExA(OLEAUT32.dll,0,0)
LoadLibraryExA(,,) -> 76ec0000
LoadLibraryExW(ole32.dll,0,0)
LoadLibraryExW(,,) -> 76970000

Create Registry Key

{"h_key": "80000002", "samDesired": "20119", "Reserved": "0", "lpSecurityAttributes": "0", "lpdwDisposition": "0", "dwOptions": "0", "lpClass": "
<NULL>", "phkResult": "74835a00", "lpSubKey": "Software\\Microsoft\\Fusion\\GACChangeNotification\\Default"}

DeleteFile

DeleteFileW(C:\Windows\Microsoft.NET\Framework\v2.0.50727\config\security.config.cch.2216.176812)
DeleteFileW() -> 0
DeleteFileW(C:\Windows\Microsoft.NET\Framework\v2.0.50727\config\enterprisesec.config.cch.2216.176812)
DeleteFileW(C:\Users\win7\AppData\Roaming\Microsoft\CLR Security Config\v2.0.50727.312\security.config.cch.2216.176875)

QueryProcessAddress

GetProcAddress(76b60000,OpenProcess)
GetProcAddress(76b60000,OpenProcessW)
GetProcAddress(75400000,ShellExecuteEx)
GetProcAddress(75400000,ShellExecuteExW)

Precise Detectors Analysis Results

DETECTOR NAME	DATE	VERDICT		REASON
Static Precise PUA Detector 1	2017-10-11 17:17:24 UTC	No Match		NotDetected
Static Precise Virus Detector	2017-10-11 17:17:24 UTC	No Match		NotDetected
Static Precise Trojan Detector	2017-10-11 17:17:24 UTC	No Match		NotDetected
Static Precise Adware InstallCore Detector 1	2017-10-11 17:17:24 UTC	No Match		NotDetected
Static Precise Trojan Detector 2	2017-10-11 17:17:24 UTC	No Match		NotDetected
Static Precise Trojan Detector 3	2017-10-11 17:17:24 UTC	No Match		NotDetected
Static Precise Trojan Generic Cryptor Detector 1	2017-10-11 17:17:24 UTC	No Match		NotDetected
Static Precise Virus Detector 2	2017-10-11 17:17:24 UTC	No Match		NotDetected

Advance Heuristics

No Advanced Heuristic Analysis Result Received

Additional File Information

Vendor Validation - Verified ✔

[+] ScreenConnect Software

Status	Valid ✔

Certificate Validation - Success ✔

[+] ScreenConnect Software

Status	NoError ✔
Start Date	2016-02-02 00:00:00+00:00
End Date	2019-02-01 23:59:59+00:00
Sha256	289e7081453ca2255c9937a7c68220c823f9896b57f8baeab7027bb6eea2777d
Serial	04A03DBCE32C5A34420A419FB740AA1A
Subject Name	ScreenConnect Software
Subject Key Identifier	db ab 14 7e d0 14 c8 1e 0b 99 b5 0d ec 9a bf c4 69 11 e7 eb
Subject Organization	ScreenConnect Software
Subject Locality	Tampa
Subject State	Florida
Subject Country	US
Issuer Name	COMODO RSA Code Signing CA
Issuer Key Identifier	29 91 60 ff 8a 4d fa eb f9 a6 6a b8 cf f9 e6 4b bd 49 ce 12
Issuer Organization	COMODO CA Limited
Issuer Locality	Salford
Issuer State	Greater Manchester
Issuer Country	GB
Crl link	http://crl.comodoca.com/COMODORSACodeSigningCA.crl
Key Usage	Digital Signature (80)
Extended Usage	Code Signing (1.3.6.1.5.5.7.3.3)

[+] COMODO RSA Code Signing CA

Status	NoError ✔
Start Date	2013-05-09 00:00:00+00:00
End Date	2028-05-08 23:59:59+00:00
Sha256	be4b37864cefc39611d4b6a1de110074e5f282de90016aa5d36849ab452eab2c
Serial	2E7C87CC0E934A52FE94FD1CB7CD34AF
Subject Name	COMODO RSA Code Signing CA
Subject Key Identifier	29 91 60 ff 8a 4d fa eb f9 a6 6a b8 cf f9 e6 4b bd 49 ce 12
Subject Organization	COMODO CA Limited
Subject Locality	Salford
Subject State	Greater Manchester
Subject Country	GB
Issuer Name	COMODO RSA Certification Authority
Issuer Key Identifier	bb af 7e 02 3d fa a6 f1 3c 84 8e ad ee 38 98 ec d9 32 32 d4
Issuer Organization	COMODO CA Limited
Issuer Locality	Salford
Issuer State	Greater Manchester
Issuer Country	GB
Crl link	http://crl.comodoca.com/COMODORSACertificationAuthority.crl
Key Usage	Digital Signature,Certificate Signing,Off-line CRL Signing,CRL Signing (86)
Extended Usage	Code Signing (1.3.6.1.5.5.7.3.3)

[+] COMODO RSA Certification Authority

Status	NoError ✔
Start Date	2010-01-19 00:00:00+00:00
End Date	2038-01-18 23:59:59+00:00
Sha256	f1bc8293a80c7d1bb2fd1d6e9b714b06e6b66686ca9b26a76d91e06e2934fa83
Serial	4CAAF9CADB636FE01FF74ED85B03869D
Subject Name	COMODO RSA Certification Authority
Subject Key Identifier	bb af 7e 02 3d fa a6 f1 3c 84 8e ad ee 38 98 ec d9 32 32 d4
Subject Organization	COMODO CA Limited
Subject Locality	Salford
Subject State	Greater Manchester
Subject Country	GB
Issuer Name	COMODO RSA Certification Authority
Issuer Key Identifier	undefined
Issuer Organization	COMODO CA Limited
Issuer Locality	Salford
Issuer State	Greater Manchester
Issuer Country	GB
Crl link	undefined
Key Usage	Certificate Signing,Off-line CRL Signing,CRL Signing (06)
Extended Usage	undefined

[+] COMODO SHA-1 Time Stamping Signer

Status	NoError ✔
Start Date	2015-12-31 00:00:00+00:00
End Date	2019-07-09 18:40:36+00:00
Sha256	f49570a2c3e23ad1d7ef62a2c137f08af02d8a2855bd96053e2365e354572fe2
Serial	1688F039255E638E69143907E6330B
Subject Name	COMODO SHA-1 Time Stamping Signer
Subject Key Identifier	8e 6b 2d 33 6b f4 33 a7 93 b3 13 9a a5 e0 0a f7 12 35 6a 88
Subject Organization	COMODO CA Limited
Subject Locality	Salford
Subject State	Greater Manchester
Subject Country	GB
Issuer Name	UTN-USERFirst-Object
Issuer Key Identifier	da ed 64 74 14 9c 14 3c ab dd 99 a9 bd 5b 28 4d 8b 3c c9 d8
Issuer Organization	The USERTRUST Network
Issuer Locality	Salt Lake City
Issuer State	UT
Issuer Country	US
Issuer Organizational Unit	http://www.usertrust.com
Crl link	http://crl.usertrust.com/UTN-USERFirst-Object.crl
Key Usage	Digital Signature,Non-Repudiation (c0)
Extended Usage	Time Stamping (1.3.6.1.5.5.7.3.8)

[+] UTN-USERFirst-Object

Status	NoError ✔
Start Date	1999-07-09 18:31:20+00:00
End Date	2019-07-09 18:40:36+00:00
Sha256	2acd612cf8f03b495f01de23e4f5d695350d00ff6d27f0255362c79df0eca403
Serial	44BE0C8B500024B411D3362DE0B35F1B
Subject Name	UTN-USERFirst-Object
Subject Key Identifier	da ed 64 74 14 9c 14 3c ab dd 99 a9 bd 5b 28 4d 8b 3c c9 d8
Subject Organization	The USERTRUST Network
Subject Locality	Salt Lake City
Subject State	UT
Subject Country	US
Subject Organizational Unit	http://www.usertrust.com
Issuer Name	UTN-USERFirst-Object
Issuer Key Identifier	undefined
Issuer Organization	The USERTRUST Network
Issuer Locality	Salt Lake City
Issuer State	UT
Issuer Country	US
Issuer Organizational Unit	http://www.usertrust.com
Crl link	http://crl.usertrust.com/UTN-USERFirst-Object.crl
Key Usage	Digital Signature,Non-Repudiation,Certificate Signing,Off-line CRL Signing,CRL Signing (c6)
Extended Usage	Code Signing (1.3.6.1.5.5.7.3.3)

PE Headers

PROPERTY	VALUE
Compilation Time Stamp	0x54F8861E [Thu Mar 5 16:36:46 2015 UTC]
Entry Point	0x40124b (.text)
File Size	1895568
File Type Enum	6
Machine Type	Intel 386 or later - 32Bit
Mime Type	application/x-dosexec
Number Of Sections	5
Sha256	9a5d2b09cf52400455308eddec78cb713e2d6378d307756878c1dc272a1b8b3b

File Paths

FILE PATH ON CLIENT	SEEN COUNT
own.exe	1

PE Sections

NAME	VIRTUAL ADDRESS	VIRTUAL SIZE	RAW SIZE	ENTROPY	MD5
.text	0x1000	0x7ea6	0x8000	6.54460810086	3fc604f5f48402e5751f1bf725959b49
.rdata	0x9000	0x520a	0x5400	4.62206164364	23d3a2f1d3e872db6208c696590e2470
.data	0xf000	0x2c94	0xe00	2.38534962726	9f633594424ad7c63fc0b8399a0fb3f1
.rsrc	0x12000	0x1b21f4	0x1b2200	7.05387329202	1fb32a3bff2d39aaf0b470c090947bad
.reloc	0x1c5000	0x28d8	0x2a00	2.91870147301	49d9ac22d58aa78afba225e678f8e52b