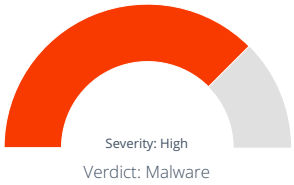
VALKYRIE COMODO

Summary

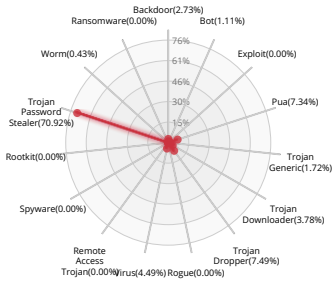
File Name: A74C1985D541E302ACF7EB49887E7137C35E3237
File Type: PE32 executable (GUI) Intel 80386, for MS Windows
SHA1: 0c13ace5116c5fc0ba3be8d06caa4f68463ec1ee
MD5: f1d8a2a0e4c25e7db06e4f975d9ce8ce

MALWARE
Valkyrie Final Verdict

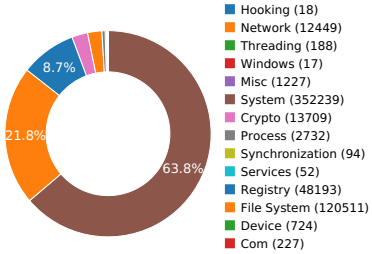
DETECTION SECTION



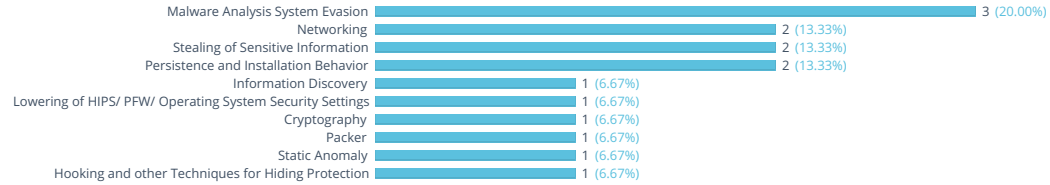
CLASSIFICATION



HIGH LEVEL BEHAVIOR DISTRIBUTION



ACTIVITY OVERVIEW



VALKYRIE COMODO

Activity Details

INFORMATION DISCOVERY

Reads data out of its own binary image	Show sources

NETWORKING

Attempts to connect to a dead IP:Port (6 unique times)	Show sources
Performs some HTTP requests	Show sources

LOWERING OF HIPS/ PFW/ OPERATING SYSTEM SECURITY SETTINGS

Attempts to block SafeBoot use by removing registry keys	Show sources

CRYPTOGRAPHY

At least one IP Address, Domain, or File Name was found in a crypto call	Show sources

PACKER

The binary likely contains encrypted or compressed data.	Show sources

STEALING OF SENSITIVE INFORMATION

Attempts to create or modify system certificates	Show sources
Steals private information from local Internet browsers	Show sources

STATIC ANOMALY

Anomalous binary characteristics	Show sources

HOOKING AND OTHER TECHNIQUES FOR HIDING PROTECTION

Creates RWX memory	Show sources

PERSISTENCE AND INSTALLATION BEHAVIOR

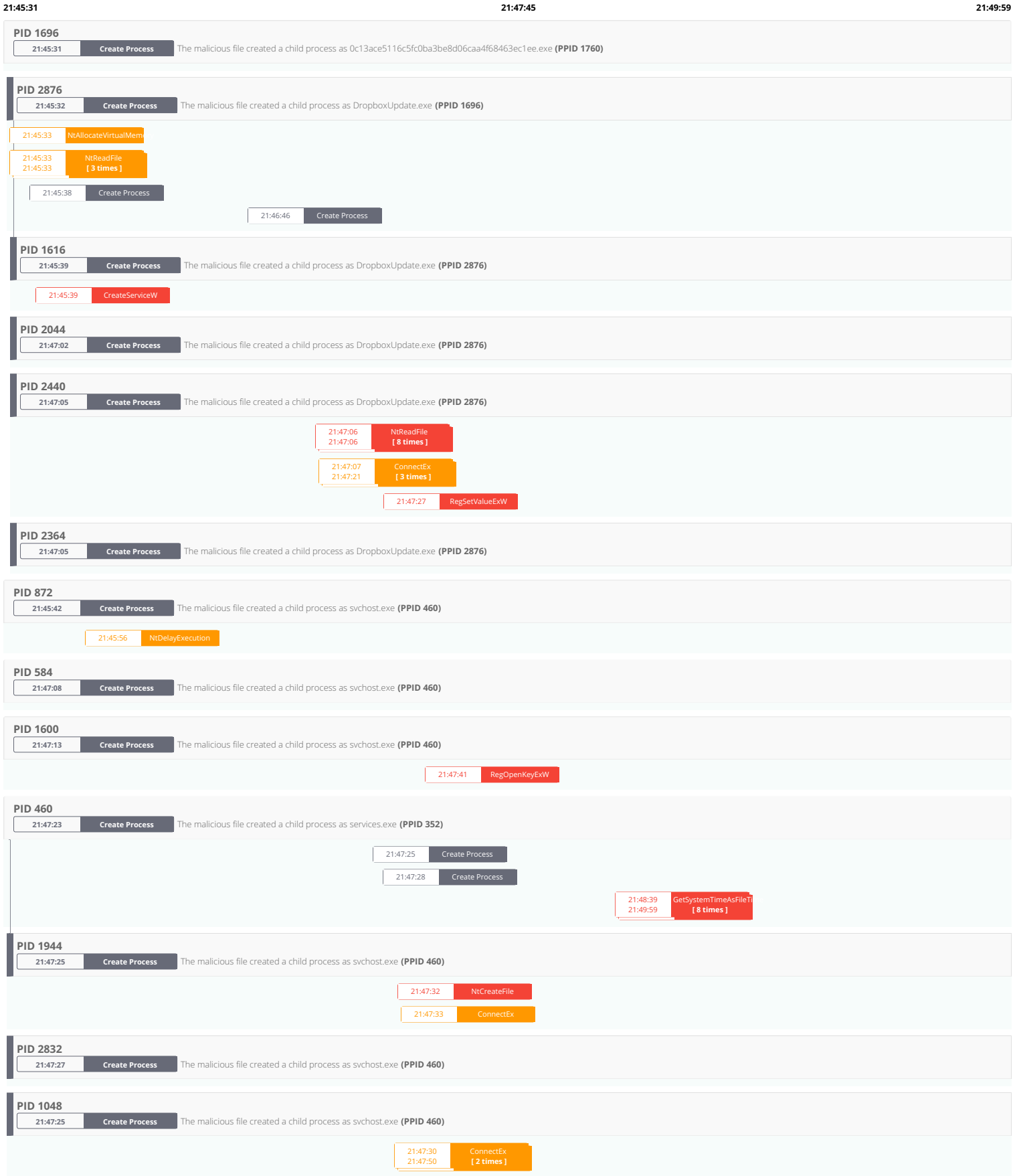
Installs itself for autorun at Windows startup	Show sources
Created a service that was not started	Show sources

MALWARE ANALYSIS SYSTEM EVASION

A process attempted to delay the analysis task.	Show sources
Attempts to repeatedly call a single API many times in order to delay analysis time	Show sources
Creates a hidden or system file	Show sources

VALKYRIE COMODO

Behavior Graph



Behavior Summary

CREATED SERVICES

dbupdate
dbupdatem

ACCESSED FILES

\Device\KsecDD
C:\Users\user\AppData\Local\Temp\
C:\Users\user\AppData\Local\Temp
C:\Users\user\AppData\Local\Temp\GUM469E.tmp
C:\Users\user\AppData\Local\Temp\GUT469F.tmp
C:\Users\user\AppData\Local\Temp\GUM469E.tmp\DropboxUpdate.exe
C:\Users\user\AppData\Local\Temp\GUM469E.tmp\DropboxCrashHandler.exe
C:\Users\user\AppData\Local\Temp\GUM469E.tmp\goopdate.dll
C:\Users\user\AppData\Local\Temp\GUM469E.tmp\npDropboxUpdate3.dll
C:\Users\user\AppData\Local\Temp\GUM469E.tmp\DropboxUpdateHelper.msi
C:\Users\user\AppData\Local\Temp\GUM469E.tmp\DropboxUpdateBroker.exe
C:\Users\user\AppData\Local\Temp\GUM469E.tmp\DropboxUpdateOnDemand.exe
C:\Users\user\AppData\Local\Temp\GUM469E.tmp\psmachine.dll
C:\Users\user\AppData\Local\Temp\GUM469E.tmp\psuser.dll
C:\Users\user\AppData\Local\Temp\GUM469E.tmp\goopdateres_da.dll
C:\Users\user\AppData\Local\Temp\GUM469E.tmp\goopdateres_de.dll
C:\Users\user\AppData\Local\Temp\GUM469E.tmp\goopdateres_en.dll
C:\Users\user\AppData\Local\Temp\GUM469E.tmp\goopdateres_es.dll
C:\Users\user\AppData\Local\Temp\GUM469E.tmp\goopdateres_es-419.dll
C:\Users\user\AppData\Local\Temp\GUM469E.tmp\goopdateres_fr.dll
C:\Users\user\AppData\Local\Temp\GUM469E.tmp\goopdateres_id.dll
C:\Users\user\AppData\Local\Temp\GUM469E.tmp\goopdateres_it.dll
C:\Users\user\AppData\Local\Temp\GUM469E.tmp\goopdateres_ja.dll
C:\Users\user\AppData\Local\Temp\GUM469E.tmp\goopdateres_ko.dll
C:\Users\user\AppData\Local\Temp\GUM469E.tmp\goopdateres_ms.dll
C:\Users\user\AppData\Local\Temp\GUM469E.tmp\goopdateres_nl.dll
C:\Users\user\AppData\Local\Temp\GUM469E.tmp\goopdateres_no.dll
C:\Users\user\AppData\Local\Temp\GUM469E.tmp\goopdateres_pl.dll
C:\Users\user\AppData\Local\Temp\GUM469E.tmp\goopdateres_pt-BR.dll
C:\Users\user\AppData\Local\Temp\GUM469E.tmp\goopdateres_ru.dll
C:\Users\user\AppData\Local\Temp\GUM469E.tmp\goopdateres_sv.dll
C:\Users\user\AppData\Local\Temp\GUM469E.tmp\goopdateres_th.dll
C:\Users\user\AppData\Local\Temp\GUM469E.tmp\goopdateres_uk.dll
C:\Users\user\AppData\Local\Temp\GUM469E.tmp\goopdateres_zh-CN.dll
C:\Users\user\AppData\Local\Temp\GUM469E.tmp\goopdateres_zh-TW.dll
C:\Users\user\AppData\Local\Temp\0c13ace5116c5fc0ba3be8d06caa4f68463ec1ee.exe
C:\Windows\Globalization\Sorting\sortdefault.nls
C:\Windows\System32\p2pcollab.dll
C:\Windows\System32\qagentrt.dll
C:\Windows\System32\dnsapi.dll
C:\Windows\System32\en-US\dnsapi.dll.mui
C:\Users\user\AppData\Roaming\Microsoft\SystemCertificates\My\Certificates*
C:\Users\user\AppData\Roaming\Microsoft\SystemCertificates\My\Certificates\1233B8D21D2ECB0483D16253D1FF3964BD09EF0C
C:\Users\user\AppData\Roaming\Microsoft\SystemCertificates\My\Certificates\16B1DD478BCE71A0FB1822E8F4F30AB467BBEFD4
C:\Users\user\AppData\Roaming\Microsoft\SystemCertificates\My\Certificates\2064A97B987412930E2994D60AE7EB72D89BC4F7
C:\Users\user\AppData\Roaming\Microsoft\SystemCertificates\My\Certificates\37998502C2CC1852F8774DAF543DD76D10D6FD93
C:\Users\user\AppData\Roaming\Microsoft\SystemCertificates\My\Certificates\418C30DD41197CBAABF21675F8559794F5551115

C:\Users\user\AppData\Roaming\Microsoft\SystemCertificates\My\Certificates\44E5AE16D06F9FBB92D6D9444B5C65C0F331D0EC
C:\Users\user\AppData\Roaming\Microsoft\SystemCertificates\My\Certificates\4FDDCB932603534677ECAE8C7D0FD914FD443E83
C:\Users\user\AppData\Roaming\Microsoft\SystemCertificates\My\Certificates\5D247FE955609769879FB1DD016537EEF650B8EC
C:\Users\user\AppData\Roaming\Microsoft\SystemCertificates\My\Certificates\6A8C669D7D1D5759CE7C1E0C5BE286257C31F366
C:\Users\user\AppData\Roaming\Microsoft\SystemCertificates\My\Certificates\744CDF45BF43EF285758286CAC89AF786F938342
C:\Users\user\AppData\Roaming\Microsoft\SystemCertificates\My\Certificates\761F091EA5F80A98B0D89734231D300CF9C027E8
C:\Users\user\AppData\Roaming\Microsoft\SystemCertificates\My\Certificates\7A5F1A5DE6AA551C795CC508128C6D894FA2C502
C:\Users\user\AppData\Roaming\Microsoft\SystemCertificates\My\Certificates\8291DA84F9266F6D0ED367AF8BE3FA722529EB91
C:\Users\user\AppData\Roaming\Microsoft\SystemCertificates\My\Certificates\871E3CD70B6F8EE3C1E7BE4C7BEF4FFCCE673E32
C:\Users\user\AppData\Roaming\Microsoft\SystemCertificates\My\Certificates\8A82FE0617F4170E0BF052CF6BABFC628DA51919
C:\Users\user\AppData\Roaming\Microsoft\SystemCertificates\My\Certificates\8B943CF0CAEF7F6F04E98C9405960323B23C516D
C:\Users\user\AppData\Roaming\Microsoft\SystemCertificates\My\Certificates\9317D002FC43BDA932B8397B6E729B83D48EEB8D
C:\Users\user\AppData\Roaming\Microsoft\SystemCertificates\My\Certificates\95EEF9A37407C5B87BCF95D69B01DCFDAFD07635
C:\Users\user\AppData\Roaming\Microsoft\SystemCertificates\My\Certificates\A092A81885DDD5AAD1EC1A803D7183779D81B6F9
C:\Users\user\AppData\Roaming\Microsoft\SystemCertificates\My\Certificates\BAED8A8C5A147CFA78E686BB4A8E5829C2F934F5
C:\Users\user\AppData\Roaming\Microsoft\SystemCertificates\My\Certificates\C8A51E044BF5AF39158BB24E414E8FDCD2891C3A
C:\Users\user\AppData\Roaming\Microsoft\SystemCertificates\My\Certificates\FB45378AB288E369B22C860D123A809F530D5CC1
C:\Users\user\AppData\Roaming\Microsoft\SystemCertificates\My\CRLs*
C:\Users\user\AppData\Roaming\Microsoft\SystemCertificates\My\CTLs*
C:\Users\user\AppData\LocalLow
C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\EE44ECA143B76F2B9F2A5AA75B5D1EC6_*
C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\CA4458E7366E94A3C3A9C1FE548B6D21_*
C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\BAEBE581FCB73249406FC21094EA252E_*
C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\D84E548583BE1EE7DB5A935821009D26_*
C:\Users\user\AppData\Local\Temp\GUM469E.tmp\IPHLPAPI.DLL
C:\Windows\System32\IPHLPAPI.DLL
C:\Users\user\AppData\Local\Temp\GUM469E.tmp\WINNSI.DLL
C:\Windows\System32\winnsi.dll
C:\Users\user\AppData\Local\Temp\GUM469E.tmp\NETAPI32.dll

READ REGISTRY KEYS

HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\CustomLocale\en-US
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\ExtendedLocale\en-US
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Cryptography\Providers\Trust\Certificate\{00AAC56B-CD44-11D0-8CC2-00C04FC295EE}\$DLL
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Cryptography\Providers\Trust\Certificate\{00AAC56B-CD44-11D0-8CC2-00C04FC295EE}\$Function
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Cryptography\Providers\Trust\FinalPolicy\{00AAC56B-CD44-11D0-8CC2-00C04FC295EE}\$DLL
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Cryptography\Providers\Trust\FinalPolicy\{00AAC56B-CD44-11D0-8CC2-00C04FC295EE}\$Function
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Cryptography\Providers\Trust\Initialization\{00AAC56B-CD44-11D0-8CC2-00C04FC295EE}\$DLL
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Cryptography\Providers\Trust\Initialization\{00AAC56B-CD44-11D0-8CC2-00C04FC295EE}\$Function
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Cryptography\Providers\Trust\Message\{00AAC56B-CD44-11D0-8CC2-00C04FC295EE}\$DLL
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Cryptography\Providers\Trust\Message\{00AAC56B-CD44-11D0-8CC2-00C04FC295EE}\$Function
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Cryptography\Providers\Trust\Signature\{00AAC56B-CD44-11D0-8CC2-00C04FC295EE}\$DLL
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Cryptography\Providers\Trust\Signature\{00AAC56B-CD44-11D0-8CC2-00C04FC295EE}\$Function
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Cryptography\Providers\Trust\CertCheck\{00AAC56B-CD44-11D0-8CC2-00C04FC295EE}\$DLL
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Cryptography\Providers\Trust\CertCheck\{00AAC56B-CD44-11D0-8CC2-00C04FC295EE}\$Function
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Cryptography\Providers\Trust\Cleanup\{00AAC56B-CD44-11D0-8CC2-00C04FC295EE}\$DLL
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Cryptography\Providers\Trust\Cleanup\{00AAC56B-CD44-11D0-8CC2-00C04FC295EE}\$Function
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\WinTrust\Trust Providers\Software Publishing\State
HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Security\Safety Warning Level
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\services\crypt32\DiagLevel
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\services\crypt32\DiagMatchAnyMask
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Cryptography\OID\EncodingType 0\CryptDllFindOIDInfo\1.3.6.1.4.1.311.44.3.4!7\Name
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\MUI\StringCacheSettings\StringCacheGeneration

HKEY_CURRENT_USER\Software\Classes\Local Settings\MuiCache\6D\52C64B7E\@%SystemRoot%\system32\p2pcollab.dll,-8042
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Cryptography\OID\EncodingType 0\CryptDllFindOIDInfo\1.3.6.1.4.1.311.47.1.1!7\Name
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Cryptography\OID\EncodingType 0\CryptDllFindOIDInfo\1.3.6.1.4.1.311.64.1.1!7\Name
HKEY_CURRENT_USER\Software\Classes\Local Settings\MuiCache\6D\52C64B7E\@%SystemRoot%\system32\dnsapi.dll,-103
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\Windows Error Reporting\WMR\Disable
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\SystemCertificates\AuthRoot\DisableRootAutoUpdate
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\AuthRoot\AutoUpdate\DisallowedCertSyncDeltaTime
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Cryptography\OID\EncodingType 0\CertDllCreateCertificateChainEngine\Config\DisableMandatoryBasicConstraints
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Cryptography\OID\EncodingType 0\CertDllCreateCertificateChainEngine\Config\DisableCANameConstraints
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Cryptography\OID\EncodingType 0\CertDllCreateCertificateChainEngine\Config\DisableUnsupportedCriticalExtensions
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Cryptography\OID\EncodingType 0\CertDllCreateCertificateChainEngine\Config\MaxAIAUrlCountInCert
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Cryptography\OID\EncodingType 0\CertDllCreateCertificateChainEngine\Config\MaxAIAUrlRetrievalCountPerChain
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Cryptography\OID\EncodingType 0\CertDllCreateCertificateChainEngine\Config\MaxUrlRetrievalByteCount
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Cryptography\OID\EncodingType 0\CertDllCreateCertificateChainEngine\Config\MaxAIAUrlRetrievalByteCount
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Cryptography\OID\EncodingType 0\CertDllCreateCertificateChainEngine\Config\MaxAIAUrlRetrievalCertCount
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Cryptography\OID\EncodingType 0\CertDllCreateCertificateChainEngine\Config\CryptnetPreFetchTriggerPeriodSeconds
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Cryptography\OID\EncodingType 0\CertDllCreateCertificateChainEngine\Config\EnableWeakSignatureFlags
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Cryptography\OID\EncodingType 0\CertDllCreateCertificateChainEngine\Config\MinRsaPubKeyBitLength
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Cryptography\OID\EncodingType 0\CertDllCreateCertificateChainEngine\Config\WeakRsaPubKeyTime
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Cryptography\OID\EncodingType 0\CertDllCreateCertificateChainEngine\Config\ChainCacheResyncFiletime
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Cryptography\OID\EncodingType 0\CertDllCreateCertificateChainEngine\Config\WeakMD5ThirdPartyFlags
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Cryptography\OID\EncodingType 0\CertDllCreateCertificateChainEngine\Config\WeakMD5AllFlags
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Cryptography\OID\EncodingType 0\CertDllCreateCertificateChainEngine\Config\WeakSHA1ThirdPartyFlags
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Cryptography\OID\EncodingType 0\CertDllCreateCertificateChainEngine\Config\WeakSHA1AllFlags
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Cryptography\OID\EncodingType 0\CertDllCreateCertificateChainEngine\Config\WeakRSAThirdPartyFlags
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Cryptography\OID\EncodingType 0\CertDllCreateCertificateChainEngine\Config\WeakRSAAllFlags
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Cryptography\OID\EncodingType 0\CertDllCreateCertificateChainEngine\Config\WeakDSAThirdPartyFlags
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Cryptography\OID\EncodingType 0\CertDllCreateCertificateChainEngine\Config\WeakDSAAllFlags
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Cryptography\OID\EncodingType 0\CertDllCreateCertificateChainEngine\Config\WeakECDSAThirdPartyFlags
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Cryptography\OID\EncodingType 0\CertDllCreateCertificateChainEngine\Config\WeakECDSAAllFlags
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\ProfileList\S-1-5-21-2298303332-66077612-2598613238-1000\ProfileImagePath
HKEY_CURRENT_USER\Software\Microsoft\SystemCertificates\CA\Certificates\9317D002FC43BDA932B8397B6E729B83D48EEB8D\Blob
HKEY_CURRENT_USER\Software\Microsoft\SystemCertificates\CA\Certificates\E6A3B45B062D509B3382282D196EFE97D5956CCB\Blob
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\CA\Certificates\109F1CAED645BB78B3EA2B94C0697C740733031C\Blob
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\CA\Certificates\D559A586669B08F46A30A133F8A9ED3D038E2EA8\Blob
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\CA\Certificates\FEE449EE0E3965A5246F000E87FDE2A065FD89D4\Blob
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\CA\CRLs\A377D1B1C0538833035211F4083D00FECC414DAB\Blob
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\Disallowed\Certificates\1916A2AF346D399F50313C393200F14140456616\Blob
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\Disallowed\Certificates\2A83E9020591A55FC6DDAD3FB102794C52B24E70\Blob
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\Disallowed\Certificates\2B84BFBB34EE2EF949FE1CBE30AA026416EB2216\Blob
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\Disallowed\Certificates\305F8BD17AA2CBC483A4C41B19A39A0C75DA39D6\Blob
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\Disallowed\Certificates\367D4B3B4FCBBC0B767B2EC0CDB2A36EAB71A4EB\Blob
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\Disallowed\Certificates\3A850044D8A195CD401A680C012CB0A3B5F8DC08\Blob
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\Disallowed\Certificates\40AA38731BD189F9CDB5B9DC35E2136F38777AF4\Blob
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\Disallowed\Certificates\43D9BCB568E039D073A74A71D8511F7476089CC3\Blob
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\Disallowed\Certificates\471C949A8143DB5AD5CDF1C972864A2504FA23C9\Blob
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\Disallowed\Certificates\51C3247D60F356C7CA3BAF4C3F429DAC93EE7B74\Blob
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\Disallowed\Certificates\5DE83EE82AC5090AEA9D6AC4E7A6E213F946E179\Blob
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\Disallowed\Certificates\61793FCBFA4F9008309BBA5FF12D2CB29CD4151A\Blob
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\Disallowed\Certificates\637162CC59A3A1E25956FA5FA8F60D2E1C52EAC6\Blob
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\Disallowed\Certificates\63FEAE960BAA91E343CE2BD8B71798C76BDB77D0\Blob
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\Disallowed\Certificates\6431723036FD26DEA502792FA5959224930 30F97\Blob

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\Disallowed\Certificates\7D7F4414CCEF168ADF6BF40753B5BECD78375931\Blob
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\Disallowed\Certificates\80962AE4D6C5B442894E95A13E4A699E07D694CF\Blob

MODIFIED FILES

C:\Users\user\AppData\Local\Temp\GUT469F.tmp
C:\Users\user\AppData\Local\Temp\GUM469E.tmp\DropboxUpdate.exe
C:\Users\user\AppData\Local\Temp\GUM469E.tmp\DropboxCrashHandler.exe
C:\Users\user\AppData\Local\Temp\GUM469E.tmp\goopdate.dll
C:\Users\user\AppData\Local\Temp\GUM469E.tmp\npDropboxUpdate3.dll
C:\Users\user\AppData\Local\Temp\GUM469E.tmp\DropboxUpdateHelper.msi
C:\Users\user\AppData\Local\Temp\GUM469E.tmp\DropboxUpdateBroker.exe
C:\Users\user\AppData\Local\Temp\GUM469E.tmp\DropboxUpdateOnDemand.exe
C:\Users\user\AppData\Local\Temp\GUM469E.tmp\psmachine.dll
C:\Users\user\AppData\Local\Temp\GUM469E.tmp\psuser.dll
C:\Users\user\AppData\Local\Temp\GUM469E.tmp\goopdateres_da.dll
C:\Users\user\AppData\Local\Temp\GUM469E.tmp\goopdateres_de.dll
C:\Users\user\AppData\Local\Temp\GUM469E.tmp\goopdateres_en.dll
C:\Users\user\AppData\Local\Temp\GUM469E.tmp\goopdateres_es.dll
C:\Users\user\AppData\Local\Temp\GUM469E.tmp\goopdateres_es-419.dll
C:\Users\user\AppData\Local\Temp\GUM469E.tmp\goopdateres_fr.dll
C:\Users\user\AppData\Local\Temp\GUM469E.tmp\goopdateres_id.dll
C:\Users\user\AppData\Local\Temp\GUM469E.tmp\goopdateres_it.dll
C:\Users\user\AppData\Local\Temp\GUM469E.tmp\goopdateres_ja.dll
C:\Users\user\AppData\Local\Temp\GUM469E.tmp\goopdateres_ko.dll
C:\Users\user\AppData\Local\Temp\GUM469E.tmp\goopdateres_ms.dll
C:\Users\user\AppData\Local\Temp\GUM469E.tmp\goopdateres_nl.dll
C:\Users\user\AppData\Local\Temp\GUM469E.tmp\goopdateres_no.dll
C:\Users\user\AppData\Local\Temp\GUM469E.tmp\goopdateres_pl.dll
C:\Users\user\AppData\Local\Temp\GUM469E.tmp\goopdateres_pt-BR.dll
C:\Users\user\AppData\Local\Temp\GUM469E.tmp\goopdateres_ru.dll
C:\Users\user\AppData\Local\Temp\GUM469E.tmp\goopdateres_sv.dll
C:\Users\user\AppData\Local\Temp\GUM469E.tmp\goopdateres_th.dll
C:\Users\user\AppData\Local\Temp\GUM469E.tmp\goopdateres_uk.dll
C:\Users\user\AppData\Local\Temp\GUM469E.tmp\goopdateres_zh-CN.dll
C:\Users\user\AppData\Local\Temp\GUM469E.tmp\goopdateres_zh-TW.dll
C:\ProgramData\Dropbox\Update\Log\DropboxUpdate.log-2018-04-24-00-45-58-918-2876
\??\PIPE\wkssvc
C:\Program Files (x86)\Dropbox\Update\1.3.65.1\DropboxUpdate.exe
C:\Program Files (x86)\Dropbox\Update\1.3.65.1\goopdate.dll
C:\Program Files (x86)\Dropbox\Update\1.3.65.1\DropboxCrashHandler.exe
C:\Program Files (x86)\Dropbox\Update\1.3.65.1\goopdateres_da.dll
C:\Program Files (x86)\Dropbox\Update\1.3.65.1\goopdateres_de.dll
C:\Program Files (x86)\Dropbox\Update\1.3.65.1\goopdateres_en.dll
C:\Program Files (x86)\Dropbox\Update\1.3.65.1\goopdateres_es.dll
C:\Program Files (x86)\Dropbox\Update\1.3.65.1\goopdateres_es-419.dll
C:\Program Files (x86)\Dropbox\Update\1.3.65.1\goopdateres_fr.dll
C:\Program Files (x86)\Dropbox\Update\1.3.65.1\goopdateres_id.dll
C:\Program Files (x86)\Dropbox\Update\1.3.65.1\goopdateres_it.dll
C:\Program Files (x86)\Dropbox\Update\1.3.65.1\goopdateres_ja.dll
C:\Program Files (x86)\Dropbox\Update\1.3.65.1\goopdateres_ko.dll
C:\Program Files (x86)\Dropbox\Update\1.3.65.1\goopdateres_ms.dll
C:\Program Files (x86)\Dropbox\Update\1.3.65.1\goopdateres_nl.dll
C:\Program Files (x86)\Dropbox\Update\1.3.65.1\goopdateres_no.dll

C:\Program Files (x86)\Dropbox\Update\1.3.65.1\goopdateres_pl.dll
C:\Program Files (x86)\Dropbox\Update\1.3.65.1\goopdateres_pt-BR.dll
C:\Program Files (x86)\Dropbox\Update\1.3.65.1\goopdateres_ru.dll
C:\Program Files (x86)\Dropbox\Update\1.3.65.1\goopdateres_sv.dll
C:\Program Files (x86)\Dropbox\Update\1.3.65.1\goopdateres_th.dll
C:\Program Files (x86)\Dropbox\Update\1.3.65.1\goopdateres_uk.dll
C:\Program Files (x86)\Dropbox\Update\1.3.65.1\goopdateres_zh-CN.dll
C:\Program Files (x86)\Dropbox\Update\1.3.65.1\goopdateres_zh-TW.dll
C:\Program Files (x86)\Dropbox\Update\1.3.65.1\DropboxUpdateHelper.msi
C:\Program Files (x86)\Dropbox\Update\1.3.65.1\psuser.dll
C:\Program Files (x86)\Dropbox\Update\1.3.65.1\psmachine.dll
C:\Program Files (x86)\Dropbox\Update\DropboxUpdate.exe
C:\Program Files (x86)\Dropbox\Update\1.3.65.1\npDropboxUpdate3.dll
C:\Program Files (x86)\Dropbox\Update\1.3.65.1\DropboxUpdateBroker.exe
C:\Program Files (x86)\Dropbox\Update\1.3.65.1\DropboxUpdateOnDemand.exe
C:\Windows\Tasks\DropboxUpdateTaskMachineCore.job
C:\Windows\Tasks\DropboxUpdateTaskMachineUA.job
C:\Users\user\AppData\Local\Temp\MSIa69d6.LOG
C:\ProgramData\Dropbox\Update\Log\DropboxUpdate.log-2018-04-24-00-53-52-254-2876
C:\ProgramData\Dropbox\Update\Log\DropboxUpdate.log-2018-04-24-00-53-52-254-2876-finished
C:\ProgramData\Dropbox\Update\Log\DropboxUpdate.log-2018-04-24-00-45-39-723-1616
C:\ProgramData\Dropbox\Update\Log\DropboxUpdate.log-2018-04-24-00-45-39-723-1616-finished
C:\Windows\sysnative\Tasks\DropboxUpdateTaskMachineCore
C:\Windows\sysnative\Tasks\DropboxUpdateTaskMachineUA
\??\PIPE\srvsvc
\Device\LanmanDatagramReceiver
C:\Windows\Temp\fwtsqmfile00.sqm

RESOLVED APIS

kernel32.dll.FlsAlloc
kernel32.dll.FlsGetValue
kernel32.dll.FlsSetValue
kernel32.dll.FlsFree
cryptbase.dll.SystemFunction036
uxtheme.dll.ThemeInitApiHook
user32.dll.IsProcessDPIAware
shlwapi.dll.PathRemoveFileSpecW
shell32.dll.SHGetFolderPathW
shlwapi.dll.PathAppendW
user32.dll.CharLowerBuffW
shell32.dll.#680
wintrust.dll.WinVerifyTrust
wintrust.dll.WintrustCertificateTrust
wintrust.dll.SoftpubAuthenticode
wintrust.dll.SoftpubInitialize
wintrust.dll.SoftpubLoadMessage
wintrust.dll.SoftpubLoadSignature
wintrust.dll.SoftpubCheckCert
wintrust.dll.SoftpubCleanup
cryptsp.dll.CryptAcquireContextA
kernel32.dll.SortGetHandle
kernel32.dll.SortCloseHandle
wintrust.dll.CryptSIPPutSignedDataMsg

wintrust.dll.CryptSIPGetSignedDataMsg
imagehlp.dll.ImageGetCertificateData
user32.dll.LoadStringW
ncrypt.dll.BCryptOpenAlgorithmProvider
bcryptprimitives.dll.GetHashInterface
ncrypt.dll.BCryptGetProperty
ncrypt.dll.BCryptCreateHash
ncrypt.dll.BCryptHashData
wintrust.dll.CryptSIPVerifyIndirectData
bcrypt.dll.BCryptOpenAlgorithmProvider
bcrypt.dll.BCryptGetProperty
bcrypt.dll.BCryptCreateHash
bcrypt.dll.BCryptHashData
bcrypt.dll.BCryptFinishHash
bcrypt.dll.BCryptDestroyHash
bcrypt.dll.BCryptCloseAlgorithmProvider
ncrypt.dll.BCryptFinishHash
cryptsp.dll.CryptCreateHash
cryptsp.dll.CryptSetHashParam
cryptsp.dll.CryptVerifySignatureA
cryptsp.dll.CryptDestroyKey
cryptsp.dll.CryptDestroyHash
ncrypt.dll.BCryptDestroyHash
userenv.dll.GetUserProfileDirectoryW
sechost.dll.ConvertSidToStringSidW
sechost.dll.ConvertStringSidToSidW
userenv.dll.RegisterGPNotification
gpapi.dll.RegisterGPNotificationInternal
sechost.dll.OpenSCManagerW
sechost.dll.OpenServiceW
sechost.dll.CloseServiceHandle
sechost.dll.QueryServiceConfigW
cryptsp.dll.CryptGetKeyParam
cryptsp.dll.CryptHashData
cryptnet.dll.CertDllVerifyRevocation
profapi.dll.#104
advapi32.dll.SaferiSearchMatchingHashRules
cryptsp.dll.CryptReleaseContext
crypt32.dll.CryptQueryObject
crypt32.dll.CertEnumCertificatesInStore
crypt32.dll.CertDuplicateCertificateContext
crypt32.dll.CertGetNameStringW
crypt32.dll.CertCloseStore
crypt32.dll.CertFreeCertificateContext
kernel32.dll.IsProcessorFeaturePresent
shlwapi.dll.PathStripPathW
shlwapi.dll.PathRemoveExtensionW
version.dll.GetFileVersionInfoSizeW
version.dll.GetFileVersionInfoW
version.dll.VerQueryValueW
goopdate.dll.DllEntry
shlwapi.dll.PathIsRelativeW

DELETED FILES

C:\Users\user\AppData\Local\Temp\GUM469E.tmp
C:\Windows\Tasks\DropboxUpdateTask.job
C:\Windows\Tasks\DropboxUpdateTaskMachine.job
C:\ProgramData\Dropbox\Update\Log\DropboxUpdate.log-2018-04-24-00-53-52-254-2876
C:\ProgramData\Dropbox\Update\Log\DropboxUpdate.log-2018-04-24-00-45-39-723-1616
C:\ProgramData\Dropbox\Update\Log\DropboxUpdate.log-2018-04-24-00-47-23-135-2044
C:\ProgramData\Dropbox\Update\Log\DropboxUpdate.log-2018-04-24-00-47-23-330-2044
C:\ProgramData\Dropbox\Update\Log\DropboxUpdate.log-2018-04-24-00-47-23-495-2044
C:\ProgramData\Dropbox\Update\Log\DropboxUpdate.log-2018-04-24-00-47-02-880-2044
C:\ProgramData\Dropbox\Update\Log\DropboxUpdate.log-2018-04-24-00-47-05-566-2440
C:\Users\user\AppData\Local\Temp\BITF1CE.tmp
C:\Windows\sysnative\config\systemprofile\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\26969811E3D01AC44AB62601783F7AE6
C:\Windows\sysnative\config\systemprofile\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\26969811E3D01AC44AB62601783F7AE6
C:\Windows\sysnative\config\systemprofile\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\37C951188967C8EB88D99893D9D191FE
C:\Windows\sysnative\config\systemprofile\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\37C951188967C8EB88D99893D9D191FE
C:\Windows\sysnative\config\systemprofile\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\43507F87C1453B2187C030286C2D44AB
C:\Windows\sysnative\config\systemprofile\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\43507F87C1453B2187C030286C2D44AB
C:\Windows\sysnative\config\systemprofile\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\4C7F163ED126D5C3CB9457F68EC64E9E
C:\Windows\sysnative\config\systemprofile\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\4C7F163ED126D5C3CB9457F68EC64E9E
C:\Windows\sysnative\config\systemprofile\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\A583E2A51BFBDC1E492A57B7C8325850
C:\Windows\sysnative\config\systemprofile\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\A583E2A51BFBDC1E492A57B7C8325850
C:\Windows\sysnative\config\systemprofile\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\BE7FFD2FD84D3B32FD43DC8F575A9F28
C:\Windows\sysnative\config\systemprofile\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\BE7FFD2FD84D3B32FD43DC8F575A9F28

DELETED REGISTRY KEYS

HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\DropboxUpdate\Update\eulaaccepted
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\DropboxUpdate\Update\mi
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\DropboxUpdate\Update\ui
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\DropboxUpdate\Update\LastChecked
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\DropboxUpdate\Update\ClientState\{D8968FF2-E0B1-4A13-A3E2-C9F2995F3BC6}\UpdateAvailableCount
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\DropboxUpdate\Update\ClientState\{D8968FF2-E0B1-4A13-A3E2-C9F2995F3BC6}\UpdateAvailableSince
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WBEM\CIMOM\LastServiceStart
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\DropboxUpdate\Update\network\secure\sk
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\DropboxUpdate\Update\network\secure\c
HKEY_CURRENT_USER\Software\Microsoft\SystemCertificates\CA\Certificates\A031C46782E6E6C662C2C87C76DA9AA62CCABD8E

REGISTRY KEYS

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Nls\CustomLocale
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\CustomLocale\en-US
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Nls\ExtendedLocale
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\ExtendedLocale\en-US
HKEY_LOCAL_MACHINE\Software\Microsoft\Cryptography\Providers\Trust\Certificate\{00AAC56B-CD44-11D0-8CC2-00C04FC295EE}
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Cryptography\Providers\Trust\Certificate\{00AAC56B-CD44-11D0-8CC2-00C04FC295EE}\$DLL
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Cryptography\Providers\Trust\Certificate\{00AAC56B-CD44-11D0-8CC2-00C04FC295EE}\$Function
HKEY_LOCAL_MACHINE\Software\Microsoft\Cryptography\Providers\Trust\FinalPolicy\{00AAC56B-CD44-11D0-8CC2-00C04FC295EE}
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Cryptography\Providers\Trust\FinalPolicy\{00AAC56B-CD44-11D0-8CC2-00C04FC295EE}\$DLL
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Cryptography\Providers\Trust\FinalPolicy\{00AAC56B-CD44-11D0-8CC2-00C04FC295EE}\$Function
HKEY_LOCAL_MACHINE\Software\Microsoft\Cryptography\Providers\Trust\Initialization\{00AAC56B-CD44-11D0-8CC2-00C04FC295EE}
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Cryptography\Providers\Trust\Initialization\{00AAC56B-CD44-11D0-8CC2-00C04FC295EE}\$DLL
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Cryptography\Providers\Trust\Initialization\{00AAC56B-CD44-11D0-8CC2-00C04FC295EE}\$Function
HKEY_LOCAL_MACHINE\Software\Microsoft\Cryptography\Providers\Trust\Message\{00AAC56B-CD44-11D0-8CC2-00C04FC295EE}
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Cryptography\Providers\Trust\Message\{00AAC56B-CD44-11D0-8CC2-00C04FC295EE}\$DLL
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Cryptography\Providers\Trust\Message\{00AAC56B-CD44-11D0-8CC2-00C04FC295EE}\$Function

HKEY_LOCAL_MACHINE\Software\Microsoft\Cryptography\Providers\Trust\Signature\{00AAC56B-CD44-11D0-8CC2-00C04FC295EE}
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Cryptography\Providers\Trust\Signature\{00AAC56B-CD44-11D0-8CC2-00C04FC295EE}\$DLL
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Cryptography\Providers\Trust\Signature\{00AAC56B-CD44-11D0-8CC2-00C04FC295EE}\$Function
HKEY_LOCAL_MACHINE\Software\Microsoft\Cryptography\Providers\Trust\CertCheck\{00AAC56B-CD44-11D0-8CC2-00C04FC295EE}
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Cryptography\Providers\Trust\CertCheck\{00AAC56B-CD44-11D0-8CC2-00C04FC295EE}\$DLL
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Cryptography\Providers\Trust\CertCheck\{00AAC56B-CD44-11D0-8CC2-00C04FC295EE}\$Function
HKEY_LOCAL_MACHINE\Software\Microsoft\Cryptography\Providers\Trust\DiagnosticPolicy\{00AAC56B-CD44-11D0-8CC2-00C04FC295EE}
HKEY_LOCAL_MACHINE\Software\Microsoft\Cryptography\Providers\Trust\Cleanup\{00AAC56B-CD44-11D0-8CC2-00C04FC295EE}
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Cryptography\Providers\Trust\Cleanup\{00AAC56B-CD44-11D0-8CC2-00C04FC295EE}\$DLL
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Cryptography\Providers\Trust\Cleanup\{00AAC56B-CD44-11D0-8CC2-00C04FC295EE}\$Function
HKEY_USERS\S-1-5-21-2298303332-66077612-2598613238-1000
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\WinTrust\Trust Providers\Software Publishing
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\WinTrust\Trust Providers\Software Publishing\State
HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Security
HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Security\Safety Warning Level
HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\SystemCertificates\TrustedPublisher\Safer
HKEY_CURRENT_USER\Software\Policies\Microsoft\SystemCertificates\TrustedPublisher\Safer
HKEY_LOCAL_MACHINE\Software\Microsoft\SystemCertificates\TrustedPublisher\Safer
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\crypt32
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\services\crypt32\DiagLevel
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\services\crypt32\DiagMatchAnyMask
HKEY_LOCAL_MACHINE\Software\Microsoft\Cryptography\Wintrust\Config
HKEY_LOCAL_MACHINE\Software\Microsoft\Cryptography\OID
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Cryptography\OID\EncodingType 0
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Cryptography\OID\EncodingType 0\CryptSIPDllPutSignedDataMsg
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Cryptography\OID\EncodingType 0\CryptSIPDllPutSignedDataMsg\{000C10F1-0000-0000-C000-000000000046}
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Cryptography\OID\EncodingType 0\CryptSIPDllPutSignedDataMsg\{06C9E010-38CE-11D4-A2A3-00104BD35090}
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Cryptography\OID\EncodingType 0\CryptSIPDllPutSignedDataMsg\{1629F04E-2799-4DB5-8FE5-ACE10F17EBAB}
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Cryptography\OID\EncodingType 0\CryptSIPDllPutSignedDataMsg\{1A610570-38CE-11D4-A2A3-00104BD35090}
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Cryptography\OID\EncodingType 0\CryptSIPDllPutSignedDataMsg\{603BCC1F-4B59-4E08-B724-D2C6297EF351}
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Cryptography\OID\EncodingType 0\CryptSIPDllPutSignedDataMsg\{9BA61D3F-E73A-11D0-8CD2-00C04FC295EE}
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Cryptography\OID\EncodingType 0\CryptSIPDllPutSignedDataMsg\{AB13F5B1-F718-11D0-82AA-00AA00C065E1}
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Cryptography\OID\EncodingType 0\CryptSIPDllPutSignedDataMsg\{C689AAB8-8E78-11D0-8C47-00C04FC295EE}
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Cryptography\OID\EncodingType 0\CryptSIPDllPutSignedDataMsg\{C689AAB9-8E78-11D0-8C47-00C04FC295EE}
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Cryptography\OID\EncodingType 0\CryptSIPDllPutSignedDataMsg\{C689AABA-8E78-11D0-8C47-00C04FC295EE}
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Cryptography\OID\EncodingType 0\CryptSIPDllPutSignedDataMsg\{DE351A42-8E59-11D0-8C47-00C04FC295EE}
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Cryptography\OID\EncodingType 0\CryptSIPDllPutSignedDataMsg\{DE351A43-8E59-11D0-8C47-00C04FC295EE}
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Cryptography\OID\EncodingType 1
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Cryptography\OID\EncodingType 1\CryptSIPDllPutSignedDataMsg
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Cryptography\OID\EncodingType 0\CryptSIPDllGetSignedDataMsg
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Cryptography\OID\EncodingType 0\CryptSIPDllGetSignedDataMsg\{000C10F1-0000-0000-C000-000000000046}
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Cryptography\OID\EncodingType 0\CryptSIPDllGetSignedDataMsg\{06C9E010-38CE-11D4-A2A3-00104BD35090}
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Cryptography\OID\EncodingType 0\CryptSIPDllGetSignedDataMsg\{1629F04E-2799-4DB5-8FE5-ACE10F17EBAB}
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Cryptography\OID\EncodingType 0\CryptSIPDllGetSignedDataMsg\{1A610570-38CE-11D4-A2A3-00104BD35090}
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Cryptography\OID\EncodingType 0\CryptSIPDllGetSignedDataMsg\{603BCC1F-4B59-4E08-B724-D2C6297EF351}
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Cryptography\OID\EncodingType 0\CryptSIPDllGetSignedDataMsg\{9BA61D3F-E73A-11D0-8CD2-00C04FC295EE}
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Cryptography\OID\EncodingType 0\CryptSIPDllGetSignedDataMsg\{AB13F5B1-F718-11D0-82AA-00AA00C065E1}
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Cryptography\OID\EncodingType 0\CryptSIPDllGetSignedDataMsg\{C689AAB8-8E78-11D0-8C47-00C04FC295EE}
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Cryptography\OID\EncodingType 0\CryptSIPDllGetSignedDataMsg\{C689AAB9-8E78-11D0-8C47-00C04FC295EE}
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Cryptography\OID\EncodingType 0\CryptSIPDllGetSignedDataMsg\{C689AABA-8E78-11D0-8C47-00C04FC295EE}
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Cryptography\OID\EncodingType 0\CryptSIPDllGetSignedDataMsg\{DE351A42-8E59-11D0-8C47-00C04FC295EE}
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Cryptography\OID\EncodingType 0\CryptSIPDllGetSignedDataMsg\{DE351A43-8E59-11D0-8C47-00C04FC295EE}

HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Cryptography\OID\EncodingType 1\CryptSIPDllGetSignedDataMsg
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Cryptography\OID\EncodingType 0\CryptDllFindOIDInfo
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Cryptography\OID\EncodingType 0\CryptDllFindOIDInfo\1.3.6.1.4.1.311.44.3.4!7
HKEY_LOCAL_MACHINE\Software\Microsoft\Cryptography\OID\EncodingType 0\CryptDllFindOIDInfo\1.3.6.1.4.1.311.44.3.4!7
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Cryptography\OID\EncodingType 0\CryptDllFindOIDInfo\1.3.6.1.4.1.311.44.3.4!7\Name
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\MUI\StringCacheSettings
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\MUI\StringCacheSettings\StringCacheGeneration
HKEY_CURRENT_USER

EXECUTED COMMANDS

"C:\Program Files (x86)\Dropbox\Update\DropboxUpdate.exe" /regsvc
"C:\Program Files (x86)\Dropbox\Update\DropboxUpdate.exe" /regserver
C:\Program Files (x86)\Dropbox\Update\DropboxUpdate.exe /ping PD94bWwgdmVyc2lvbj0iMS4wIiBlbmNvZGluZz0iVVRGLTgiPz48cmVxdWVzdCBkcm9wYm94X2RhdGE9ImV5SlVRVWRUSWpvaVpVcDVjbFpwY0U5TVV6ZFBlazB0VEhvd2VGSnpiRWwzVFdwVk1rMXFRVE5PUkVWM1RsUlZlazU2VlhoTlZFVXlUV3BaTVhScVFURk9lb PG9zIHBsYXRmb3JtPSJ3aW4iIHZlcnNpb249IjYuMSIgc3A9IlNlcnZpY2UgUGFjayAxIiBhcmNoPSJ4NjQiLz48YXBwIGFwcGlkPSJ7RDg5NjhGRjItRTBCMS00QTEzLUEzRTItQzlGMjk5NUYzQkM2fSIgdmVyc2lvbj0iIiBuZXh0dmVyc2lvbj0iMS4zLjY1LjEiIGxhbmc9IiIgYnJhb
C:\Windows\System32\svchost.exe -k netsvcs
C:\Windows\system32\svchost.exe -k LocalServiceAndNoImpersonation

READ FILES

\Device\KsecDD
C:\Users\user\AppData\Local\Temp\GUM469E.tmp
C:\Users\user\AppData\Local\Temp\GUT469F.tmp
C:\Users\user\AppData\Local\Temp\0c13ace5116c5fc0ba3be8d06caa4f68463ec1ee.exe
C:\Users\user\AppData\Local\Temp\GUM469E.tmp\goopdate.dll
C:\Windows\Globalization\Sorting\sortdefault.nls
C:\Windows\System32\p2pcollab.dll
C:\Windows\System32\dnsapi.dll
C:\Windows\System32\en-US\dnsapi.dll.mui
C:\Users\user\AppData\Roaming\Microsoft\SystemCertificates\My\Certificates\1233B8D21D2ECB0483D16253D1FF3964BD09EF0C
C:\Users\user\AppData\Roaming\Microsoft\SystemCertificates\My\Certificates\16B1DD478BCE71A0FB1822E8F4F30AB467BBEFD4
C:\Users\user\AppData\Roaming\Microsoft\SystemCertificates\My\Certificates\2064A97B987412930E2994D60AE7EB72D89BC4F7
C:\Users\user\AppData\Roaming\Microsoft\SystemCertificates\My\Certificates\37998502C2CC1852F8774DAF543DD76D10D6FD93
C:\Users\user\AppData\Roaming\Microsoft\SystemCertificates\My\Certificates\418C30DD41197CBAABF21675F8559794F5551115
C:\Users\user\AppData\Roaming\Microsoft\SystemCertificates\My\Certificates\44E5AE16D06F9FBB92D6D9444B5C65C0F331D0EC
C:\Users\user\AppData\Roaming\Microsoft\SystemCertificates\My\Certificates\4FDDCB932603534677ECAE8C7D0FD914FD443E83
C:\Users\user\AppData\Roaming\Microsoft\SystemCertificates\My\Certificates\5D247FE955609769879FB1DD016537EEF650B8EC
C:\Users\user\AppData\Roaming\Microsoft\SystemCertificates\My\Certificates\6A8C669D7D1D5759CE7C1E0C5BE286257C31F366
C:\Users\user\AppData\Roaming\Microsoft\SystemCertificates\My\Certificates\744CDF45BF43EF285758286CAC89AF786F938342
C:\Users\user\AppData\Roaming\Microsoft\SystemCertificates\My\Certificates\761F091EA5F80A98B0D89734231D300CF9C027E8
C:\Users\user\AppData\Roaming\Microsoft\SystemCertificates\My\Certificates\7A5F1A5DE6AA551C795CC508128C6D894FA2C502
C:\Users\user\AppData\Roaming\Microsoft\SystemCertificates\My\Certificates\8291DA84F9266F6D0ED367AF8BE3FA722529EB91
C:\Users\user\AppData\Roaming\Microsoft\SystemCertificates\My\Certificates\871E3CD70B6F8EE3C1E7BE4C7BEF4FFCCE673E32
C:\Users\user\AppData\Roaming\Microsoft\SystemCertificates\My\Certificates\8A82FE0617F4170E0BF052CF6BABFC628DA51919
C:\Users\user\AppData\Roaming\Microsoft\SystemCertificates\My\Certificates\8B943CF0CAEF7F6F04E98C9405960323B23C516D
C:\Users\user\AppData\Roaming\Microsoft\SystemCertificates\My\Certificates\9317D002FC43BDA932B8397B6E729B83D48EEB8D
C:\Users\user\AppData\Roaming\Microsoft\SystemCertificates\My\Certificates\95EEF9A37407C5B87BCF95D69B01DCFDAFD07635
C:\Users\user\AppData\Roaming\Microsoft\SystemCertificates\My\Certificates\A092A81885DDD5AAD1EC1A803D7183779D81B6F9
C:\Users\user\AppData\Roaming\Microsoft\SystemCertificates\My\Certificates\BAED8A8C5A147CFA78E686BB4A8E5829C2F934F5
C:\Users\user\AppData\Roaming\Microsoft\SystemCertificates\My\Certificates\C8A51E044BF5AF39158BB24E414E8FDCD2891C3A
C:\Users\user\AppData\Roaming\Microsoft\SystemCertificates\My\Certificates\FB45378AB288E369B22C860D123A809F530D5CC1
C:\Windows\System32\IPHLPAPI.DLL
C:\Windows\System32\winnsi.dll
C:\Windows\System32\netapi32.dll
C:\Windows\System32\netutils.dll

C:\Windows\System32\srvcli.dll
C:\Windows\winsxs\x86_microsoft.windows.common-controls_6595b64144ccf1df_6.0.7601.17514_none_41e6975e2bd6f2b2\comctl32.dll
C:\Windows\System32\msi.dll
\??\PIPE\wkssvc
C:\Program Files (x86)\Dropbox\CrashReports
C:\Users\user\AppData\Local\Temp\GUM469E.tmp\goopdateres_en.dll
C:\Users\user\AppData\Local\Temp\GUM469E.tmp\DropboxUpdate.exe
C:\Program Files (x86)\Dropbox\Update\1.3.65.1\DropboxUpdate.exe
C:\Program Files (x86)\Dropbox\Update\1.3.65.1\goopdate.dll
C:\Users\user\AppData\Local\Temp\GUM469E.tmp\DropboxCrashHandler.exe
C:\Program Files (x86)\Dropbox\Update\1.3.65.1\DropboxCrashHandler.exe
C:\Users\user\AppData\Local\Temp\GUM469E.tmp\goopdateres_da.dll
C:\Program Files (x86)\Dropbox\Update\1.3.65.1\goopdateres_da.dll
C:\Users\user\AppData\Local\Temp\GUM469E.tmp\goopdateres_de.dll
C:\Program Files (x86)\Dropbox\Update\1.3.65.1\goopdateres_de.dll
C:\Program Files (x86)\Dropbox\Update\1.3.65.1\goopdateres_en.dll
C:\Users\user\AppData\Local\Temp\GUM469E.tmp\goopdateres_es.dll
C:\Program Files (x86)\Dropbox\Update\1.3.65.1\goopdateres_es.dll
C:\Users\user\AppData\Local\Temp\GUM469E.tmp\goopdateres_es-419.dll
C:\Program Files (x86)\Dropbox\Update\1.3.65.1\goopdateres_es-419.dll
C:\Users\user\AppData\Local\Temp\GUM469E.tmp\goopdateres_fr.dll
C:\Program Files (x86)\Dropbox\Update\1.3.65.1\goopdateres_fr.dll
C:\Users\user\AppData\Local\Temp\GUM469E.tmp\goopdateres_id.dll
C:\Program Files (x86)\Dropbox\Update\1.3.65.1\goopdateres_id.dll
C:\Users\user\AppData\Local\Temp\GUM469E.tmp\goopdateres_it.dll
C:\Program Files (x86)\Dropbox\Update\1.3.65.1\goopdateres_it.dll
C:\Users\user\AppData\Local\Temp\GUM469E.tmp\goopdateres_ja.dll
C:\Program Files (x86)\Dropbox\Update\1.3.65.1\goopdateres_ja.dll
C:\Users\user\AppData\Local\Temp\GUM469E.tmp\goopdateres_ko.dll
C:\Program Files (x86)\Dropbox\Update\1.3.65.1\goopdateres_ko.dll
C:\Users\user\AppData\Local\Temp\GUM469E.tmp\goopdateres_ms.dll
C:\Program Files (x86)\Dropbox\Update\1.3.65.1\goopdateres_ms.dll
C:\Users\user\AppData\Local\Temp\GUM469E.tmp\goopdateres_nl.dll
C:\Program Files (x86)\Dropbox\Update\1.3.65.1\goopdateres_nl.dll
C:\Users\user\AppData\Local\Temp\GUM469E.tmp\goopdateres_no.dll
C:\Program Files (x86)\Dropbox\Update\1.3.65.1\goopdateres_no.dll
C:\Users\user\AppData\Local\Temp\GUM469E.tmp\goopdateres_pl.dll
C:\Program Files (x86)\Dropbox\Update\1.3.65.1\goopdateres_pl.dll
C:\Users\user\AppData\Local\Temp\GUM469E.tmp\goopdateres_pt-BR.dll
C:\Program Files (x86)\Dropbox\Update\1.3.65.1\goopdateres_pt-BR.dll
C:\Users\user\AppData\Local\Temp\GUM469E.tmp\goopdateres_ru.dll

MUTEXES

_Dropbox_Update_logging_mutex_C:ProgramDataDropboxUpdateLogDropboxUpdate.log-2018-04-24-00-45-58-918-2876
Global\Dropbox{567EDB56-FF4F-4850-B1F4-992864DC7948}
CicLoadWinStaWinSta0
Local\MSCTF.CtfMonitorInstMutexDefault1
Global\Dropbox{6E8D9200-0F55-4328-A477-50D38A739277}
Global\MSILOG_4bfcd7ae1d3db33GOL.6d96aISM_pmeT_lacoL_ataDppA_resu_sresU_:C
Global_MSIExecute
_Dropbox_Update_logging_mutex_C:ProgramDataDropboxUpdateLogDropboxUpdate.log-2018-04-24-00-53-52-254-2876
Global\Dropbox{AB1D842F-65E4-4EAB-8006-D37976AC2300}
_Dropbox_Update_logging_mutex_C:ProgramDataDropboxUpdateLogDropboxUpdate.log-2018-04-24-00-45-39-723-1616

_Dropbox_Update_logging_mutex_C:ProgramDataDropboxUpdateLogDropboxUpdate.log-2018-04-24-00-47-02-880-2044
_Dropbox_Update_logging_mutex_C:ProgramDataDropboxUpdateLogDropboxUpdate.log-2018-04-24-00-47-23-135-2044
_Dropbox_Update_logging_mutex_C:ProgramDataDropboxUpdateLogDropboxUpdate.log-2018-04-24-00-47-23-330-2044
_Dropbox_Update_logging_mutex_C:ProgramDataDropboxUpdateLogDropboxUpdate.log-2018-04-24-00-47-23-495-2044
_Dropbox_Update_logging_mutex_C:ProgramDataDropboxUpdateLogDropboxUpdate.log-2018-04-24-00-47-05-566-2440
_Dropbox_Update_logging_mutex_C:ProgramDataDropboxUpdateLogDropboxUpdate.log-2018-04-24-00-47-05-810-2364
_Dropbox_Update_logging_mutex_C:ProgramDataDropboxUpdateLogDropboxUpdate.log-2018-04-24-00-48-16-836-2364

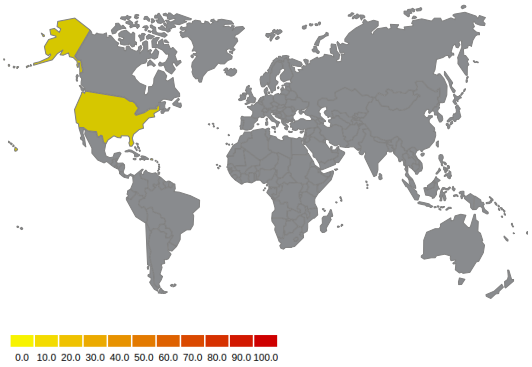
MODIFIED REGISTRY KEYS

HKEY_CURRENT_USER\Software\Classes\Local Settings\MuiCache\6D\52C64B7E\LanguageList
HKEY_CURRENT_USER\Software\Classes\Local Settings\MuiCache\6D\52C64B7E\@%SystemRoot%\system32\p2pcollab.dll,-8042
HKEY_CURRENT_USER\Software\Classes\Local Settings\MuiCache\6D\52C64B7E\@%SystemRoot%\system32\dnsapi.dll,-103
HKEY_LOCAL_MACHINE\Software\DropboxUpdate\Update\network
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\DropboxUpdate\Update\network\secure
HKEY_LOCAL_MACHINE\Software\DropboxUpdate\Update\ClientState\
HKEY_LOCAL_MACHINE\Software\DropboxUpdate\Update\Clients\
HKEY_LOCAL_MACHINE\Software\DropboxUpdate\Update\Clients\{D8968FF2-E0B1-4A13-A3E2-C9F2995F3BC6}
HKEY_LOCAL_MACHINE\Software\DropboxUpdate\Update\ClientState\{D8968FF2-E0B1-4A13-A3E2-C9F2995F3BC6}
HKEY_LOCAL_MACHINE\Software\DropboxUpdate\Update\ClientStateMedium\
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\DropboxUpdate\Update\path
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\DropboxUpdate\Update\Clients\{D8968FF2-E0B1-4A13-A3E2-C9F2995F3BC6}\pv
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\DropboxUpdate\Update\Clients\{D8968FF2-E0B1-4A13-A3E2-C9F2995F3BC6}\name
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\DropboxUpdate\Update\ClientState\{D8968FF2-E0B1-4A13-A3E2-C9F2995F3BC6}\pv
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\DropboxUpdate.exe
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\DropboxUpdate.exe\DisableExceptionChainValidation
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\DropboxUpdate\Update\version
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\DropboxUpdate\Update\ClientState\{D8968FF2-E0B1-4A13-A3E2-C9F2995F3BC6}\brand
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\DropboxUpdate\Update\ClientState\{D8968FF2-E0B1-4A13-A3E2-C9F2995F3BC6}\InstallTime
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\DropboxUpdate\Update\uid
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\AppID\{96D1EED3-701E-4FE5-B996-A543A8465897}
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\AppID\{96D1EED3-701E-4FE5-B996-A543A8465897}\(Default)
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\AppID\DropboxUpdate.exe
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\AppID\DropboxUpdate.exe\AppID
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\AppID\{96D1EED3-701E-4FE5-B996-A543A8465897}\LocalService
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\AppID\{96D1EED3-701E-4FE5-B996-A543A8465897}\ServiceParameters
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\DropboxUpdate.Update3COMClassService.1.0
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\DropboxUpdate.Update3COMClassService.1.0\(Default)
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\DropboxUpdate.Update3COMClassService.1.0\CLSID
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\DropboxUpdate.Update3COMClassService.1.0\CLSID\(Default)
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\DropboxUpdate.Update3COMClassService
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\DropboxUpdate.Update3COMClassService\(Default)
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\DropboxUpdate.Update3COMClassService\CLSID
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\DropboxUpdate.Update3COMClassService\CLSID\(Default)
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\DropboxUpdate.Update3COMClassService\CurVer
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\DropboxUpdate.Update3COMClassService\CurVer\(Default)
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{96D1EED3-701E-4FE5-B996-A543A8465897}
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{96D1EED3-701E-4FE5-B996-A543A8465897}\(Default)
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{96D1EED3-701E-4FE5-B996-A543A8465897}\ProgID
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{96D1EED3-701E-4FE5-B996-A543A8465897}\ProgID\(Default)
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{96D1EED3-701E-4FE5-B996-A543A8465897}\VersionIndependentProgID
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{96D1EED3-701E-4FE5-B996-A543A8465897}\VersionIndependentProgID\(Default)
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{96D1EED3-701E-4FE5-B996-A543A8465897}\AppID
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\AppID\{76E258F0-DE86-4CEC-9D30-3F728A898741}

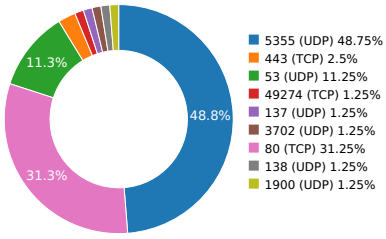
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\AppID\{76E258F0-DE86-4CEC-9D30-3F728A898741}\(Default)
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\AppID\{76E258F0-DE86-4CEC-9D30-3F728A898741}\LocalService
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\AppID\{76E258F0-DE86-4CEC-9D30-3F728A898741}\ServiceParameters
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\DropboxUpdate.OnDemandCOMClassSvc.1.0
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\DropboxUpdate.OnDemandCOMClassSvc.1.0\(Default)
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\DropboxUpdate.OnDemandCOMClassSvc.1.0\CLSID
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\DropboxUpdate.OnDemandCOMClassSvc.1.0\CLSID\(Default)
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\DropboxUpdate.OnDemandCOMClassSvc
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\DropboxUpdate.OnDemandCOMClassSvc\(Default)
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\DropboxUpdate.OnDemandCOMClassSvc\CLSID
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\DropboxUpdate.OnDemandCOMClassSvc\CLSID\(Default)
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\DropboxUpdate.OnDemandCOMClassSvc\CurVer
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\DropboxUpdate.OnDemandCOMClassSvc\CurVer\(Default)
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{76E258F0-DE86-4CEC-9D30-3F728A898741}
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{76E258F0-DE86-4CEC-9D30-3F728A898741}\(Default)
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{76E258F0-DE86-4CEC-9D30-3F728A898741}\ProgID
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{76E258F0-DE86-4CEC-9D30-3F728A898741}\ProgID\(Default)
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{76E258F0-DE86-4CEC-9D30-3F728A898741}\VersionIndependentProgID
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{76E258F0-DE86-4CEC-9D30-3F728A898741}\VersionIndependentProgID\(Default)
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{76E258F0-DE86-4CEC-9D30-3F728A898741}\AppID
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\DropboxUpdate.Update3WebSvc.1.0
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\DropboxUpdate.Update3WebSvc.1.0\(Default)
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\DropboxUpdate.Update3WebSvc.1.0\CLSID
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\DropboxUpdate.Update3WebSvc.1.0\CLSID\(Default)
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\DropboxUpdate.Update3WebSvc
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\DropboxUpdate.Update3WebSvc\(Default)
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\DropboxUpdate.Update3WebSvc\CLSID
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\DropboxUpdate.Update3WebSvc\CLSID\(Default)
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\DropboxUpdate.Update3WebSvc\CurVer
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\DropboxUpdate.Update3WebSvc\CurVer\(Default)
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{E58F67C2-BC84-4C7C-AC35-4FFBB25A47E6}
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{E58F67C2-BC84-4C7C-AC35-4FFBB25A47E6}\(Default)

Network Behavior

CONTACTED IPS



NETWORK PORT DISTRIBUTION



Name	IP	Country	ASN	ASN Name	Trigger Process Type
	8.8.4.4	United States	15169	Level 3 Parent, LLC	Malware Process
	104.16.241.184	United States	13335	Cloudflare, Inc.	Malware Process
	162.125.6.3	United States	19679	Dropbox, Inc.	Malware Process
	184.26.44.105	United States	20940	Akamai Technologies, Inc.	OS Process
	23.67.250.123	United States	20940	Akamai Technologies, Inc.	OS Process
	54.192.39.119	United States	16509	Amazon Technologies Inc.	Malware Process
	162.125.7.3		19679	Dropbox, Inc.	Malware Process
	66.225.197.197		30081	Server Central Network	Malware Process
	54.192.39.240		16509	Amazon Technologies Inc.	Malware Process
	72.21.91.29		15133	MCI Communications Services, Inc. d/b/a Verizon Busines...	Malware Process
	184.26.44.97		20940	Akamai Technologies, Inc.	OS Process
	72.21.91.29		15133	MCI Communications Services, Inc. d/b/a Verizon Busines...	Malware Process
	72.21.91.29		15133	MCI Communications Services, Inc. d/b/a Verizon Busines...	Malware Process
	23.194.112.8		20940	Akamai Technologies, Inc.	OS Process
	104.31.75.124		13335	Cloudflare, Inc.	Malware Process

VALKYRIE COMODO

HTTP PACKETS

Host	Port	Method	Version	User Agent	Count	Call Time During Execution(Sec)
ctldl.windowsupdate.com	80	GET	1.1	Microsoft-CryptoAPI/6.1	1	41.762748003
Path: /msdownload/update/v3/static/trustedr/en/disallowedcertstl.cab?d3c5adb2a4c4b8fa **URI:** http://ctldl.windowsupdate.com/msdownload/update/v3/static/trustedr/en/disallowedcertstl.cab?d3c5adb2a4c4b8fa						
ocsp.digicert.com	80	GET	1.1	Microsoft-CryptoAPI/6.1	1	74.6563780308
Path: /MFEwTzBNMEswSTAJBgUrDgMCGgUABBT3xL4LQLXDRDM9P665TW442vrsUQQUReuir%2FSSy4IxLVGLp6chnfNtyA8CEA%2BoSQYV1wCgviF2%2FcXsbb0%3D **URI:** http://ocsp.digicert.com/MFEwTzBNMEswSTAJBgUrDgMCGgUABBT3xL4LQLXDRDM9P665TW442vrsUQQUReuir%2FSSy4IxLVGLp6chnfNtyA8CEA%2BoSQYV1wCgviF2%2FcXsbb0%3D						
crl3.digicert.com	80	GET	1.1	Microsoft-CryptoAPI/6.1	1	78.06782794
Path: /DigiCertAssuredIDRootCA.crl **URI:** http://crl3.digicert.com/DigiCertAssuredIDRootCA.crl						
crl4.digicert.com	80	GET	1.1	Microsoft-CryptoAPI/6.1	1	82.6069250107
Path: /DigiCertAssuredIDRootCA.crl **URI:** http://crl4.digicert.com/DigiCertAssuredIDRootCA.crl						
ocsp.digicert.com	80	GET	1.1	Microsoft-CryptoAPI/6.1	1	84.2369959354
Path: /MFEwTzBNMEswSTAJBgUrDgMCGgUABBSYagvY3tfizDNoybzVSPFZmSEm0wQUe2jOKarAF75JeuHIP9an90WPNTICEAjFm8I8U0vytRT358KGA6Y%3D **URI:** http://ocsp.digicert.com/MFEwTzBNMEswSTAJBgUrDgMCGgUABBSYagvY3tfizDNoybzVSPFZmSEm0wQUe2jOKarAF75JeuHIP9an90WPNTICEAjFm8I8U0vytRT358KGA6Y%3D						
crl3.digicert.com	80	GET	1.1	Microsoft-CryptoAPI/6.1	1	85.205024004
Path: /assured-cs-g1.crl **URI:** http://crl3.digicert.com/assured-cs-g1.crl						
crl4.digicert.com	80	GET	1.1	Microsoft-CryptoAPI/6.1	1	85.6748631001
Path: /assured-cs-g1.crl **URI:** http://crl4.digicert.com/assured-cs-g1.crl						
ocsp.digicert.com	80	GET	1.1	Microsoft-CryptoAPI/6.1	1	86.8451731205
Path: /MFEwTzBNMEswSTAJBgUrDgMCGgUABBSnR4FoxLLkI7vkvsUIFlZt%2BlGH3gQUWsS5eyoKo6XqcQPAYPkt9mV1DlgCEAXibxWoiKXlI0cyDYA8j6k%3D **URI:** http://ocsp.digicert.com/MFEwTzBNMEswSTAJBgUrDgMCGgUABBSnR4FoxLLkI7vkvsUIFlZt%2BlGH3gQUWsS5eyoKo6XqcQPAYPkt9mV1DlgCEAXibxWoiKXlI0cyDYA8j6k%3D						
cacerts.digicert.com	80	GET	1.1	Microsoft-CryptoAPI/6.1	2	101.688365936
Path: /DigiCertSHA2HighAssuranceServerCA.crt **URI:** http://cacerts.digicert.com/DigiCertSHA2HighAssuranceServerCA.crt						
ocsp.digicert.com	80	GET	1.1	Microsoft-CryptoAPI/6.1	2	107.716504097
Path: /MFEwTzBNMEswSTAJBgUrDgMCGgUABBTfqhLjKLEJQZPin0KCzkdAQpVYowQUsT7DaQP4v0cB1JgmGggC72NkK8MCEATh56TcXPLzbcArQrhdFZ8%3D **URI:** http://ocsp.digicert.com/MFEwTzBNMEswSTAJBgUrDgMCGgUABBTfqhLjKLEJQZPin0KCzkdAQpVYowQUsT7DaQP4v0cB1JgmGggC72NkK8MCEATh56TcXPLzbcArQrhdFZ8%3D						
ocsp.digicert.com	80	GET	1.1	Microsoft-CryptoAPI/6.1	2	113.720342159
Path: /MFEwTzBNMEswSTAJBgUrDgMCGgUABBTPJvUY%2Bsl%2Bj4yzQuAcL2oQno5fCgQUUWj%2FkK8CB3U8zNIlZGKiErhZcjsCEAP4cVEQS8cwnZzLED4tzxA%3D **URI:** http://ocsp.digicert.com/MFEwTzBNMEswSTAJBgUrDgMCGgUABBTPJvUY%2Bsl%2Bj4yzQuAcL2oQno5fCgQUUWj%2FkK8CB3U8zNIlZGKiErhZcjsCEAP4cVEQS8cwnZzLED4tzxA%3D						
crl.microsoft.com	80	GET	1.1	Microsoft-CryptoAPI/6.1	1	122.975301981
Path: /pki/crl/products/tspca.crl **URI:** http://crl.microsoft.com/pki/crl/products/tspca.crl						
crl.microsoft.com	80	GET	1.1	Microsoft-CryptoAPI/6.1	1	129.09206605
Path: /pki/crl/products/CodeSignPCA2.crl **URI:** http://crl.microsoft.com/pki/crl/products/CodeSignPCA2.crl						
crl.microsoft.com	80	GET	1.1	Microsoft-CryptoAPI/6.1	1	135.626918077
Path: /pki/crl/products/WinPCA.crl **URI:** http://crl.microsoft.com/pki/crl/products/WinPCA.crl						
crl.globalsign.net	80	GET	1.1	Microsoft-CryptoAPI/6.1	1	142.423764944
Path: /primobject.crl **URI:** http://crl.globalsign.net/primobject.crl						

DNS QUERIES

Request	Type
ctldl.windowsupdate.com	A
Answers - ctldl.windowsupdate.nsatc.net (CNAME) - 184.26.44.105 (A) - a1621.g.akamai.net (CNAME) - 184.26.44.97 (A) - ctldl.windowsupdate.com.edgesuite.net (CNAME)	
ocsp.digicert.com	A
Answers - cs9.wac.phicdn.net (CNAME) - 72.21.91.29 (A)	
crl3.digicert.com	A
crl4.digicert.com	A
Answers - digicert.cachefly.net (CNAME) - 66.225.197.197 (A) - rvip1.ue.cachefly.net (CNAME)	
client.dropbox.com	A
Answers - client.dropbox-dns.com (CNAME) - 162.125.6.3 (A)	
cacerts.digicert.com	A
Answers - 104.16.239.184 (A) - 104.16.238.184 (A) - cdn.digicertcdn.com (CNAME) - 104.16.240.184 (A) - 104.16.241.184 (A) - 104.16.237.184 (A)	
crl.microsoft.com	A
Answers - 23.67.250.115 (A) - 23.67.250.123 (A) - crl.www.ms.akadns.net (CNAME) - a1363.dscg.akamai.net (CNAME)	
clientupdates.dropboxstatic.com	A
Answers - 54.192.39.66 (A) - 54.192.39.158 (A) - 54.192.39.119 (A) - 54.192.39.240 (A)	
crl.globalsign.net	A
Answers - 104.31.75.124 (A) - global.prd.cdn.globalsign.com (CNAME) - cdn.globalsigncdn.com.cdn.cloudflare.net (CNAME) - 104.31.74.124 (A)	

TCP PACKETS

Call Time During Execution(sec)	Source IP	Dest IP	Dest Port
41.762748003	Sandbox	184.26.44.105	80
74.6563780308	Sandbox	72.21.91.29	80
78.06782794	Sandbox	72.21.91.29	80
82.6069250107	Sandbox	66.225.197.197	80
94.5191731453	Sandbox	162.125.6.3	443
101.688365936	Sandbox	104.16.241.184	80
101.688562155	Sandbox	104.16.241.184	80
107.716504097	Sandbox	72.21.91.29	80
108.139616966	Sandbox	72.21.91.29	80
122.975301981	Sandbox	23.67.250.123	80
125.117679119	Sandbox	54.192.39.119	443
142.423764944	Sandbox	104.31.75.124	80
174.253252029	Sandbox	192.168.56.10	49274

VALKYRIE COMODO

UDP PACKETS

Call Time During Execution(sec)	Source IP	Dest IP	Dest Port
3.14694404602	Sandbox	192.168.56.255	137
3.16498112679	Sandbox	224.0.0.252	5355
3.36075806618	Sandbox	224.0.0.252	5355
3.36702513695	Sandbox	239.255.255.250	3702
5.92541408539	Sandbox	224.0.0.252	5355
9.15791106224	Sandbox	192.168.56.255	138
35.0646409988	Sandbox	224.0.0.252	5355
37.9707119465	Sandbox	224.0.0.252	5355
41.1397681236	Sandbox	8.8.4.4	53
64.0275850296	Sandbox	224.0.0.252	5355
71.9734799862	Sandbox	224.0.0.252	5355
72.6627340317	Sandbox	224.0.0.252	5355
74.6115341187	Sandbox	8.8.4.4	53
75.4395000935	Sandbox	224.0.0.252	5355
76.970279932	Sandbox	224.0.0.252	5355
78.0220370293	Sandbox	8.8.4.4	53
78.9398090839	Sandbox	224.0.0.252	5355
79.6029729843	Sandbox	224.0.0.252	5355
79.8615880013	Sandbox	224.0.0.252	5355
80.1912341118	Sandbox	224.0.0.252	5355
81.5334579945	Sandbox	224.0.0.252	5355
81.6752309799	Sandbox	224.0.0.252	5355
82.5042541027	Sandbox	8.8.4.4	53
82.6420490742	Sandbox	224.0.0.252	5355
83.1112411022	Sandbox	224.0.0.252	5355
84.2374329567	Sandbox	224.0.0.252	5355
94.0336699486	Sandbox	8.8.4.4	53
95.9334599972	Sandbox	224.0.0.252	5355
96.0491211414	Sandbox	224.0.0.252	5355
98.8921499252	Sandbox	224.0.0.252	5355
99.0327050686	Sandbox	224.0.0.252	5355
101.597106934	Sandbox	8.8.4.4	53
102.110793114	Sandbox	224.0.0.252	5355
102.361258984	Sandbox	224.0.0.252	5355
105.00247097	Sandbox	224.0.0.252	5355
105.362071991	Sandbox	224.0.0.252	5355
108.127552032	Sandbox	224.0.0.252	5355
108.803391933	Sandbox	224.0.0.252	5355
111.064608097	Sandbox	224.0.0.252	5355
111.569060087	Sandbox	224.0.0.252	5355
117.520828009	Sandbox	224.0.0.252	5355
120.337741137	Sandbox	224.0.0.252	5355
122.366734028	Sandbox	239.255.255.250	1900
122.919919968	Sandbox	8.8.4.4	53
123.599740982	Sandbox	224.0.0.252	5355
125.034250975	Sandbox	8.8.4.4	53
126.356652975	Sandbox	224.0.0.252	5355
130.221776962	Sandbox	224.0.0.252	5355
132.952850103	Sandbox	224.0.0.252	5355
135.940725088	Sandbox	224.0.0.252	5355
139.646866083	Sandbox	224.0.0.252	5355
142.37749505	Sandbox	8.8.4.4	53

VALKYRIE COMODO

DETAILED FILE INFO

CREATED / DROPPED FILES

FILE PATH	TYPE AND HASHES

MATCH YARA RULES

MATCH RULES

STATIC FILE INFO

File Name:	A74C1985D541E302ACF7EB49887E7137C35E3237
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
SHA1:	0c13ace5116c5fc0ba3be8d06caa4f68463ec1ee
MD5:	f1d8a2a0e4c25e7db06e4f975d9ce8ce
First Seen Date:	2018-04-23 16:35:18.298250 (about a year ago)
Number Of Clients Seen:	3
Last Analysis Date:	2018-04-23 16:35:18.298250 (about a year ago)
Human Expert Analysis Date:	2018-04-23 18:35:23.950760 (about a year ago)
Human Expert Analysis Result:	Malware

VALKYRIE COMODO

DETAILED FILE INFO

ADDITIONAL FILE INFORMATION

PE Headers

PROPERTY	VALUE
Magic Literal Enum	3
File Type Enum	6
Debug Artifacts	[{u'Path': u'mi_exe_stub.pdb\x00', u'GUID': u'{da9b22c7-8e67-4f49-9c4e-7d27a2360109}', u'timestamp': u'2017-01-13 19:55:44'}]
Number Of Sections	5
Trid	[[67.4, u'Win32 Executable MS Visual C++ (generic)'], [14.2, u'Win32 Dynamic Link Library (generic)'], [9.7, u'Win32 Executable (generic)'], [4.3, u'Generic Win/DOS Executable'], [4.3, u'DOS Executable Generic']]
Compilation Time Stamp	0x587930C0 [Fri Jan 13 19:55:44 2017 UTC]
LegalCopyright	Copyright: Dropbox, Inc. 2015 (Omaha Copyright Google Inc.)
InternalName	Dropbox Update Setup
FileVersion	1.3.65.1
CompanyName	Dropbox, Inc.
LanguageId	en
ProductName	Dropbox Update
ProductVersion	1.3.65.1
FileDescription	Dropbox Update Setup
OriginalFilename	DropboxUpdateSetup.exe
Translation	0x0409 0x04b0
Entry Point	0x404aac (.text)
Machine Type	Intel 386 or later - 32Bit
File Size	699362
Ssdeep	12288:z/iSuVAsiFPybsPTRy0uYBKGpXh9ng6m/YDfO/ayupX4ecZvmH03AE:z/iRLiF6Y7RwYBXh9ngfAD2/0poLV+Gh
Sha256	677ad16e8f80b7a9022b312b74aa2cf1057341a05e8c4952ef818bc073ce739f
Exifinfo	[{u'EXE:FileSubtype': 0, u'File:FilePermissions': u'rw-r--r--', u'SourceFile': u'/nfs/fvs/valkyrie_shared/core/valkyrie_files/0/c/1/3/0c13ace5116c5fc0ba3be8d06caa4f68463ec1ee', u'EXE:OriginalFileName': u'DropboxUpdateSetup.exe', u'EXE:ProductName': u'Dropbox Update', u'EXE:InternalName': u'Dropbox Update Setup', u'File:MIMEType': u'application/octet-stream', u'File:FileAccessDate': u'2018:04:23 16:34:38+00:00', u'EXE:InitializedDataSize': 626176, u'File:FileModifyDate': u'2018:04:23 16:34:38+00:00', u'EXE:FileVersionNumber': u'1.3.65.1', u'EXE:FileVersion': u'1.3.65.1', u'File:FileSize': u'683 kB', u'EXE:CharacterSet': u'Unicode', u'EXE:MachineType': u'Intel 386 or later, and compatibles', u'EXE:FileOS': u'Windows NT 32-bit', u'EXE:ProductVersion': u'1.3.65.1', u'EXE:ObjectFileType': u'Executable application', u'File:FileType': u'Win32 EXE', u'EXE:CompanyName': u'Dropbox, Inc.', u'File:FileName': u'0c13ace5116c5fc0ba3be8d06caa4f68463ec1ee', u'EXE:ImageVersion': 0.0, u'EXE:LanguageId': u'en', u'File:FileTypeExtension': u'exe', u'EXE:OSVersion': 5.0, u'EXE:PEType': u'PE32', u'EXE:TimeStamp': u'2017:01:13 19:55:44+00:00', u'EXE:FileFlagsMask': u'0x003f', u'EXE:LegalCopyright': u'Copyright: Dropbox, Inc. 2015 (Omaha Copyright Google Inc.)', u'EXE:LinkerVersion': 9.0, u'EXE:FileFlags': u'(none)', u'EXE:Subsystem': u'Windows GUI', u'File:Directory': u'/nfs/fvs/valkyrie_shared/core/valkyrie_files/0/c/1/3', u'EXE:FileDescription': u'Dropbox Update Setup', u'EXE:EntryPoint': u'0x4aac', u'EXE:SubsystemVersion': 5.0, u'EXE:CodeSize': 48128, u'File:FileInodeChangeDate': u'2018:04:23 16:34:38+00:00', u'EXE:UninitializedDataSize': 0, u'EXE:LanguageCode': u'English (U.S.)', u'ExifTool:ExifToolVersion': 10.1, u'EXE:ProductVersionNumber': u'1.3.65.1'}]
Mime Type	application/x-dosexec
Imphash	959c9df12e2ee961f3fcecfec5f9b8d1

PE Sections

NAME	VIRTUAL ADDRESS	VIRTUAL SIZE	RAW SIZE	ENTROPY	MD5
.text	0x1000	0xbac2	0xbc00	6.67150253549	21c3add426a813db165efd2aba2e0b1a
.rdata	0xd000	0x2a62	0x2c00	5.40445554324	c0fd823401c140af007dbce2a6d4a243
.data	0x10000	0x191c	0xe00	2.47997444427	e6e7837972cb681f94abd93319824caa
.rsrc	0x12000	0x93c9c	0x93e00	7.94258401945	48b5820f630239be05c51f89f01b154f
.reloc	0xa6000	0x150c	0x1600	3.82527315923	bb2ddca32513472b20628c4e21629288

PE Imports

- KERNEL32.dll
  - GetProcAddress
  - ExitProcess
  - WriteFile
  - GetStdHandle
  - GetModuleFileNameA
  - FreeEnvironmentStringsA
  - GetEnvironmentStrings
  - FreeEnvironmentStringsW
  - WideCharToMultiByte
  - GetLastError
  - GetEnvironmentStringsW
  - SetHandleCount
  - GetFileType
  - DeleteCriticalSection
  - TlsGetValue
  - TlsAlloc
  - TlsSetValue
  - TlsFree
  - InterlockedIncrement
  - SetLastError
  - GetCurrentThreadId
  - InterlockedDecrement

- HeapCreate
- HeapDestroy
- VirtualFree
- HeapFree
- QueryPerformanceCounter
- GetTickCount
- GetCurrentProcessId
- GetSystemTimeAsFileTime
- LeaveCriticalSection
- EnterCriticalSection
- TerminateProcess
- Sleep
- UnhandledExceptionFilter
- IsDebuggerPresent
- LoadLibraryA
- InitializeCriticalSectionAndSpinCount
- GetCPInfo
- GetACP
- GetOEMCP
- IsValidCodePage
- HeapAlloc
- VirtualAlloc
- HeapReAlloc
- RtlUnwind
- HeapSize
- GetLocaleInfoA
- LCMapStringA
- MultiByteToWideChar
- LCMapStringW
- GetStringTypeA
- GetStringTypeW
- GetProcessHeap
- InitializeCriticalSection
- GetModuleHandleW
- SetUnhandledExceptionFilter
- GetStartupInfoA
- GetCurrentProcess
- GetCommandLineA
- GetTempFileNameW
- FindResourceExW
- FindResourceW
- LoadResource
- VerSetConditionMask
- SetFilePointerEx
- CreateDirectoryW
- SizeofResource
- FormatMessageW
- GetVersionExW
- GetModuleFileNameW
- CreateFileW
- lstrlenW
- GetTempPathW
- RaiseException
- VerifyVersionInfoW
- Process32FirstW
- LockResource
- RemoveDirectoryW
- Process32NextW
- CreateToolhelp32Snapshot
- CloseHandle
- DeleteFileW
- LocalFree
- CreateProcessW
- WaitForSingleObject
- GetExitCodeProcess
- GetStartupInfoW
- MapViewOfFile
- UnmapViewOfFile
- VirtualQuery
- CreateFileMappingW
- SetFilePointer
- ReadFile

- SHLWAPI.dll
  - PathQuoteSpacesW
- ADVAPI32.dll
  - OpenServiceW
  - OpenSCManagerW
  - CloseServiceHandle
  - QueryServiceStatusEx
- ole32.dll
  - CoUninitialize
  - CoInitializeEx
- USER32.dll
  - wvsprintfW
  - CharLowerBuffW
  - MessageBoxW

PE Resources

{u'lang': u'LANG_NEUTRAL', u'name': u'B', u'offset': 74904, u'sha256': u'4129d9a4f96c86e29bcd83f45599129ce693b4464a03ca0ac8e30a8b084bc7a6', u'type': u'LZMA compressed data, non-streamed, size 3135478', u'size': 561753}
{u'lang': u'LANG_NEUTRAL', u'name': u'GOOGLEUPDATE', u'offset': 636660, u'sha256': u'67abdd721024f0ff4e0b3f4c2fc13bc5bad42d0b7851d456d88d203d15aaa450', u'type': u'data', u'size': 4}
{u'lang': u'LANG_ENGLISH', u'name': u'RT_ICON', u'offset': 636664, u'sha256': u'aa15cbe0c34485cc3bf56f8ff9e660cda329e621859a8d63286d2ccfb93a8d08', u'type': u'GLS_BINARY_LSB_FIRST', u'size': 1320}
{u'lang': u'LANG_ENGLISH', u'name': u'RT_ICON', u'offset': 637984, u'sha256': u'698dea7755175a4111cfe5e2e5bee6ded2b1544fb22bcbd4137872007a92e85d', u'type': u'dBase IV DBT of @.DBF, block length 5120, next free block index 40, next free block 0, next used block 0', u'size': 5160}
{u'lang': u'LANG_ENGLISH', u'name': u'RT_ICON', u'offset': 643144, u'sha256': u'f62b037921c27db308990ec27ba9a9287c0b8b1562478ac3da3e7652e9fed30a', u'type': u'data', u'size': 11560}
{u'lang': u'LANG_ENGLISH', u'name': u'RT_ICON', u'offset': 654704, u'sha256': u'8b8d91d20611febc78b432c7d72908ca381171ddaf05bcf3197c4d790e0a067c', u'type': u'PNG image data, 256 x 256, 8-bit/color RGBA, non-interlaced', u'size': 12186}
{u'lang': u'LANG_CHINESE', u'name': u'RT_STRING', u'offset': 666892, u'sha256': u'547f6dda905f5d42fd834295879213990ca0a1986ea504b1271878a81f40a9bf', u'type': u'data', u'size': 274}
{u'lang': u'LANG_DANISH', u'name': u'RT_STRING', u'offset': 667168, u'sha256': u'1b7e5393f5368099a9f0caa0845468608b83070e397b4d6cf1ee68c619d3f69c', u'type': u'data', u'size': 538}
{u'lang': u'LANG_GERMAN', u'name': u'RT_STRING', u'offset': 667708, u'sha256': u'6adefb1585ef13026e71f3fbded4f9e620a46f0936c66fa5e1035f30b7ae5a73', u'type': u'data', u'size': 596}
{u'lang': u'LANG_ENGLISH', u'name': u'RT_STRING', u'offset': 668304, u'sha256': u'1ff4babc697229f5e2eac814228e9f5af3381e7626ab2bd7f3328d92b34191e1', u'type': u'data', u'size': 422}
{u'lang': u'LANG_FRENCH', u'name': u'RT_STRING', u'offset': 668728, u'sha256': u'04b11f06c5cd333974df4d1780e2da9f75f4bd7950e5b048a787f6cd2187cda1', u'type': u'data', u'size': 714}
{u'lang': u'LANG_ITALIAN', u'name': u'RT_STRING', u'offset': 669444, u'sha256': u'03d7da87c37f069dfcb7cff48b0c1acb68d3d4fa3a59835923505c667878e4e5', u'type': u'data', u'size': 538}
{u'lang': u'LANG_JAPANESE', u'name': u'RT_STRING', u'offset': 669984, u'sha256': u'457eebbe606749eadf0ab1bbf05de975c024d7622ebcf116e0f010944c624017', u'type': u'data', u'size': 348}
{u'lang': u'LANG_KOREAN', u'name': u'RT_STRING', u'offset': 670332, u'sha256': u'808abda0443a9e446623dd3ae09ceb8c8c8ca9d6334c2f58d5ae7fe8fb66d097', u'type': u'data', u'size': 344}
{u'lang': u'LANG_DUTCH', u'name': u'RT_STRING', u'offset': 670676, u'sha256': u'333fc974a4edb251c74c15968091de2bb26b6ff23723369bcf35d5b1f24285f9', u'type': u'data', u'size': 560}
{u'lang': u'LANG_NORWEGIAN', u'name': u'RT_STRING', u'offset': 671236, u'sha256': u'63a6a706486c4672a50eee6f5fe8e301d65f90a011a4c44eb72b4c19b536d4cd', u'type': u'data', u'size': 526}
{u'lang': u'LANG_POLISH', u'name': u'RT_STRING', u'offset': 671764, u'sha256': u'32d56168e0e8c803719368ca2e2c6cd8955a2dc152bc67630e0c16dd17b0b884', u'type': u'data', u'size': 558}
{u'lang': u'LANG_PORTUGUESE', u'name': u'RT_STRING', u'offset': 672324, u'sha256': u'a237ecc0ccf6561825d64009741b5a8d9a98119072149f923cfdf271f90588c2', u'type': u'data', u'size': 510}
{u'lang': u'LANG_RUSSIAN', u'name': u'RT_STRING', u'offset': 672836, u'sha256': u'badfad8dd14c1b74dbf1afbe3b884c490b4b9d3e512ef1929aa3d988a5471f1b', u'type': u'data', u'size': 596}

{u'lang': u'LANG_SWEDISH', u'name': u'RT_STRING', u'offset': 673432, u'sha256': u'0463adf8e4c4e918a3638b23b30376a754b47badc002db1ef74f90e9fad22017', u'type': u'data', u'size': 538}
{u'lang': u'LANG_THAI', u'name': u'RT_STRING', u'offset': 673972, u'sha256': u'e7aa199b16360ca9de0e4e7a9a1c1adb4d78c2532fab41f42c27616354268e78', u'type': u'data', u'size': 472}
{u'lang': u'LANG_INDONESIAN', u'name': u'RT_STRING', u'offset': 674444, u'sha256': u'bba01278b25392a894f0e3c60dd79b4b5d85d8f6aaf11d55a3eaa13c7e4a2c4a', u'type': u'data', u'size': 516}
{u'lang': u'LANG_UKRAINIAN', u'name': u'RT_STRING', u'offset': 674960, u'sha256': u'429bc067868eb1f6a72cb313eb038a902a45eb791f6af2db1faebb902c3a26b3', u'type': u'data', u'size': 522}
{u'lang': u'LANG_MALAY', u'name': u'RT_STRING', u'offset': 675484, u'sha256': u'00049702ad9b88c8c2ec3af1a581d07426eb7907e0482011f478c5cb49bccecb', u'type': u'data', u'size': 464}
{u'lang': u'LANG_CHINESE', u'name': u'RT_STRING', u'offset': 675948, u'sha256': u'8ea270bc53f5da3a294cb6b6f96ebd4d9e25a295040252199a32917caabb8379', u'type': u'data', u'size': 278}
{u'lang': u'LANG_SPANISH', u'name': u'RT_STRING', u'offset': 676228, u'sha256': u'f5620e9ec531d9dc17ca4bda7ae7ffa38394bc94d73bc78754f3d6361ec0b611', u'type': u'data', u'size': 602}
{u'lang': u'LANG_SPANISH', u'name': u'RT_STRING', u'offset': 676832, u'sha256': u'deaeda8830e40fcf7e3da9799c9cc056dda5498eb100333f6b2609bf4ebbc66d', u'type': u'data', u'size': 540}
{u'lang': u'LANG_ENGLISH', u'name': u'RT_GROUP_ICON', u'offset': 677372, u'sha256': u'8817eafd6b4cc5ccc9c3e0a663793537047cc70f1107cabefa6cf036fd033a20', u'type': u'MS Windows icon resource - 4 icons, 16x16', u'size': 62}
{u'lang': u'LANG_ENGLISH', u'name': u'RT_VERSION', u'offset': 677436, u'sha256': u'f7dbd758050b3833550c80360a361e6232e35a7991b5736bcc1d2c3b51509ae7', u'type': u'data', u'size': 892}
{u'lang': u'LANG_NEUTRAL', u'name': u'RT_MANIFEST', u'offset': 678328, u'sha256': u'89578403db056c3e309c1e6615864e5947209b60ffe08a7b05cbed9b8f309d85', u'type': u'XML 1.0 document, ASCII text', u'size': 738}

CERTIFICATE VALIDATION

- SignatureOrFileCorrupt ✖

[+] Dropbox, Inc	
Status	NoError ✔
Start Date	2016-12-28 02:00:00
End Date	2019-01-02 02:00:00
Sha256	67507f3b25ec814ff7cebaa85f5c1a647f30c79aec09c1ce79380a1b7233dc13
Serial	08C59BC23C534BF2B514F7E7C28603A6
Subject Key Identifier	0d 75 52 10 1d f1 e3 78 16 96 8e 19 95 d7 6b 38 b4 43 cc f5
Issuer Name	DigiCert Assured ID Code Signing CA-1
Issuer Key Identifier	7b 68 ce 29 aa c0 17 be 49 7a e1 e5 3f d6 a7 f7 45 8f 35 32
Crl link	http://crl3.digicert.com/assured-cs-g1.crl,http://crl4.digicert.com/assured-cs-g1.crl
Key Usage	Digital Signature (80)
Extended Usage	Code Signing (1.3.6.1.5.5.7.3.3)

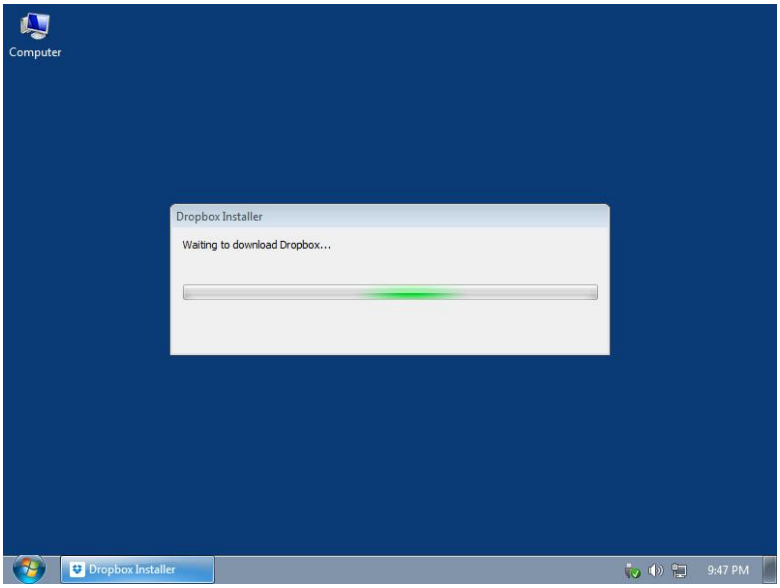
[+] DigiCert Assured ID Code Signing CA-1	
Status	NoError ✔
Start Date	2011-02-11 02:00:00
End Date	2026-02-10 02:00:00
Sha256	81b521a169883864d27d613d122312aff4bb9283c4225e32defeb7889173962a
Serial	0FA8490615D700A0BE2176FDC5EC6DBD
Subject Key Identifier	7b 68 ce 29 aa c0 17 be 49 7a e1 e5 3f d6 a7 f7 45 8f 35 32
Issuer Name	DigiCert Assured ID Root CA
Issuer Key Identifier	45 eb a2 af f4 92 cb 82 31 2d 51 8b a7 a7 21 9d f3 6d c8 0f
Crl link	http://crl3.digicert.com/DigiCertAssuredIDRootCA.crl,http://crl4.digicert.com/DigiCertAssuredIDRootCA.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)

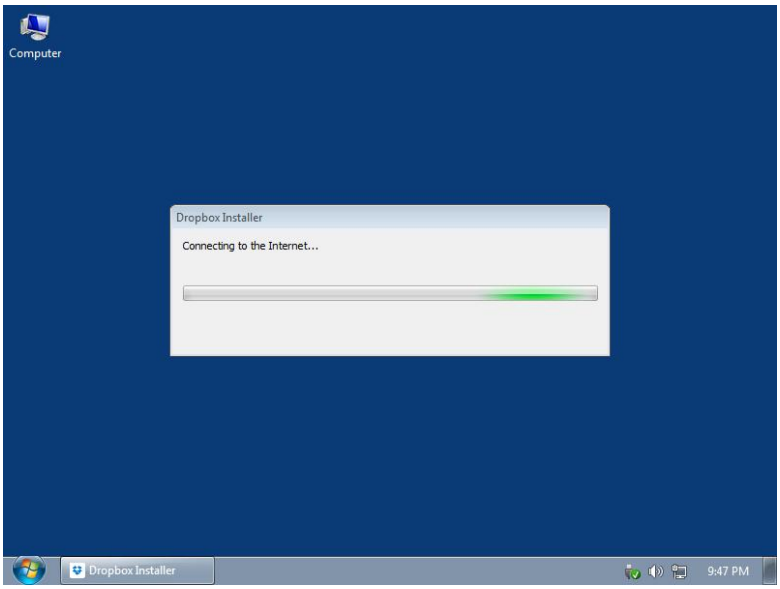
[+] DigiCert Assured ID Root CA	
Status	NoError ✔
Start Date	2006-11-10 02:00:00
End Date	2031-11-10 02:00:00
Sha256	69656a6548d46f112fad68a56675b12667e863fe923f84fb47014c2cc5352b40
Serial	0CE7E0E517D846FE8FE560FC1BF03039
Subject Key Identifier	45 eb a2 af f4 92 cb 82 31 2d 51 8b a7 a7 21 9d f3 6d c8 0f
Issuer Name	DigiCert Assured ID Root CA
Issuer Key Identifier	45 eb a2 af f4 92 cb 82 31 2d 51 8b a7 a7 21 9d f3 6d c8 0f
Crl link	undefined
Key Usage	Digital Signature,Certificate Signing,Off-line CRL Signing,CRL Signing (86)
Extended Usage	undefined

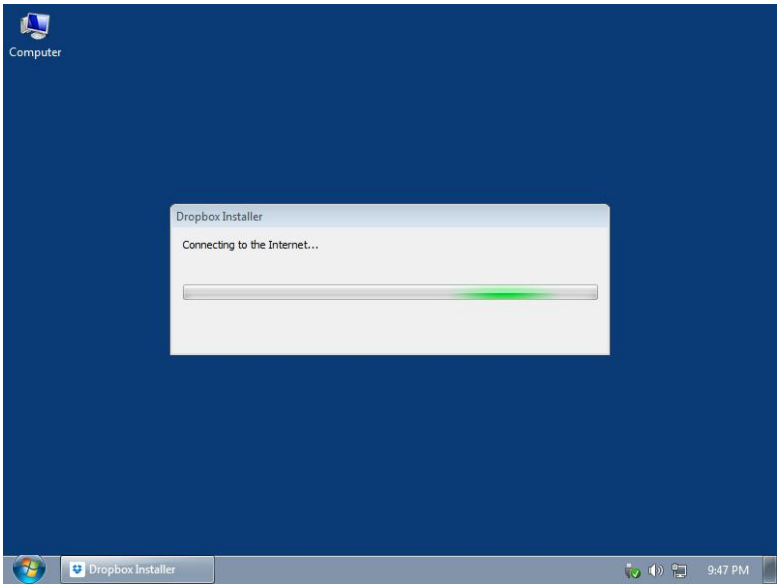
[+] Symantec Time Stamping Services CA - G2	
Status	NoError ✔
Start Date	2012-12-21 02:00:00
End Date	2020-12-31 01:59:59
Sha256	0b44526ab89f4778858bf831045ec218d0d57734caa10208ea3d8c90c1043266
Serial	7E93EBFB7CC64E59EA4B9A77D406FC3B
Subject Key Identifier	5f 9a f5 6e 5c cc cc 74 9a d4 dd 7d ef 3f db ec 4c 80 2e dd
Issuer Name	Thawte Timestamping CA
Issuer Key Identifier	undefined
Crl link	http://crl.thawte.com/ThawteTimestampingCA.crl
Key Usage	Certificate Signing,Off-line CRL Signing,CRL Signing (06)
Extended Usage	Time Stamping (1.3.6.1.5.5.7.3.8)

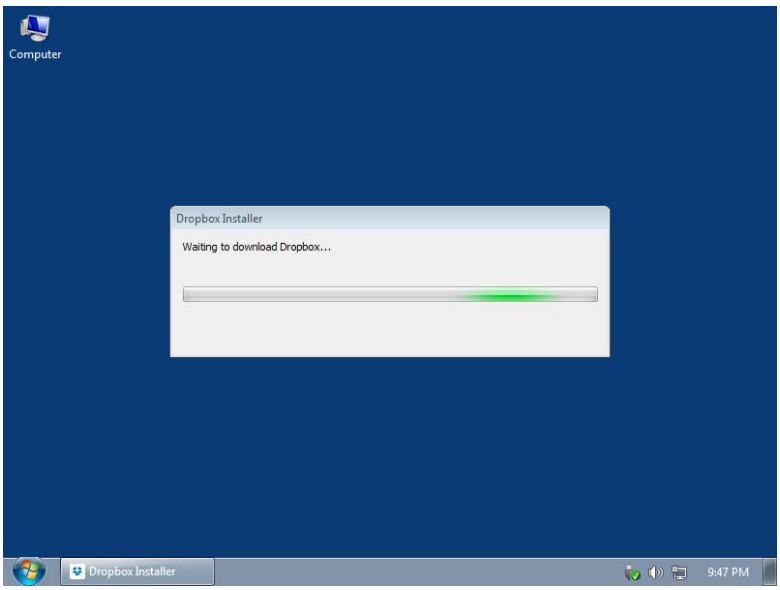
[+] Thawte Timestamping CA	
Status	NoError ✔
Start Date	1997-01-01 02:00:00
End Date	2021-01-01 01:59:59
Sha256	f429a67538b1053ebe3ad5587247d3a6845a82b3e687e079263181f53dbe26d7
Serial	00
Subject Key Identifier	undefined
Issuer Name	Thawte Timestamping CA
Issuer Key Identifier	undefined
Crl link	undefined
Key Usage	undefined
Extended Usage	undefined

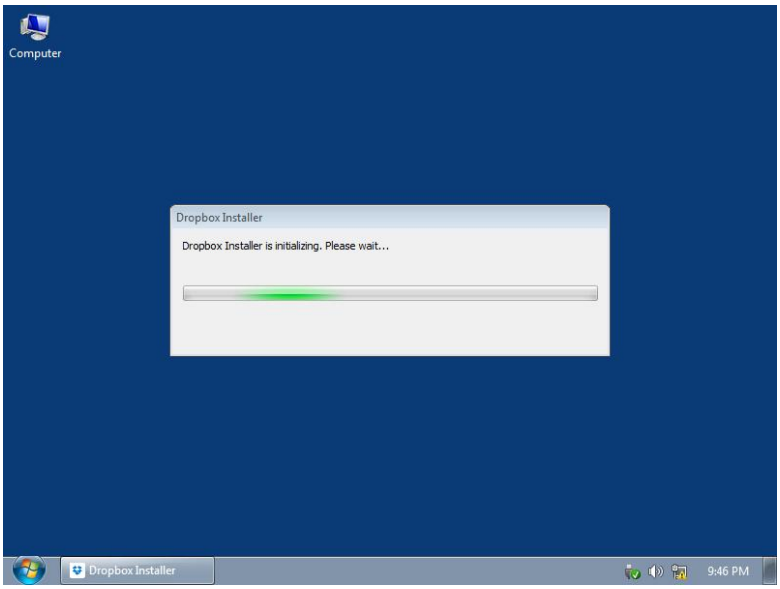
SCREENSHOTS

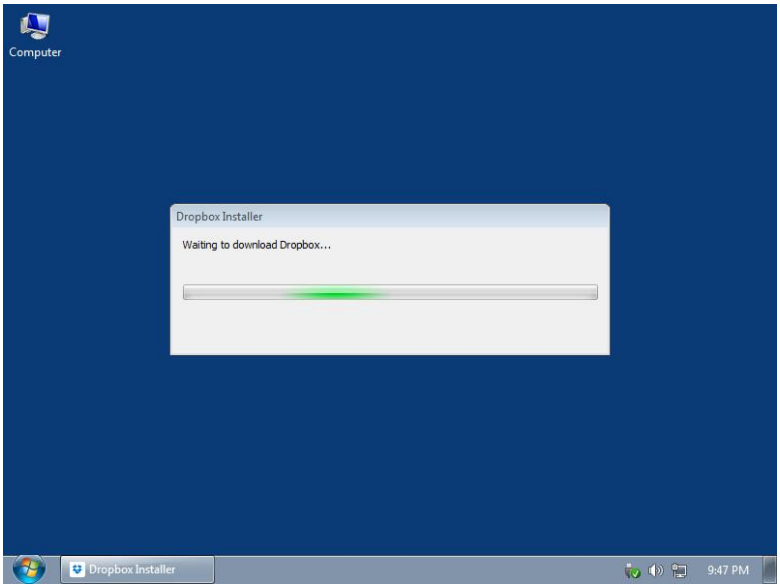


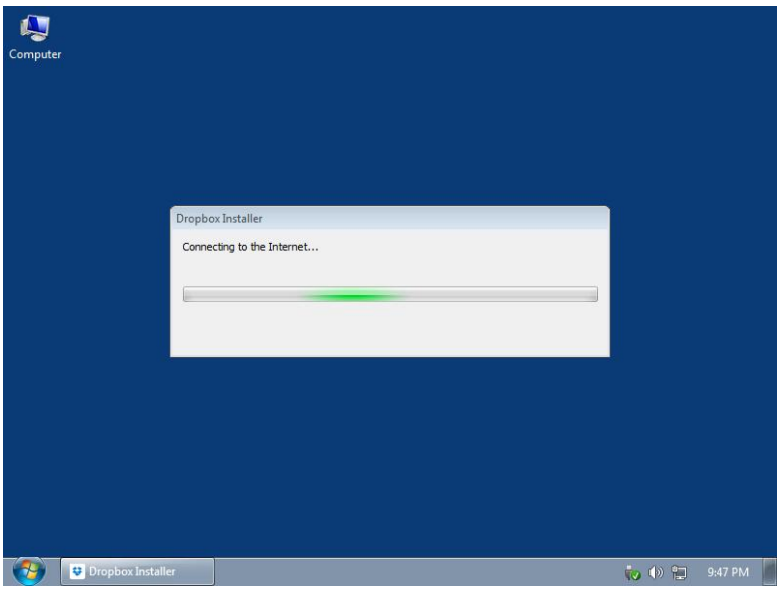

Computer
Dropbox Installer
Connecting to the Internet...
Dropbox Installer
9:47 PM

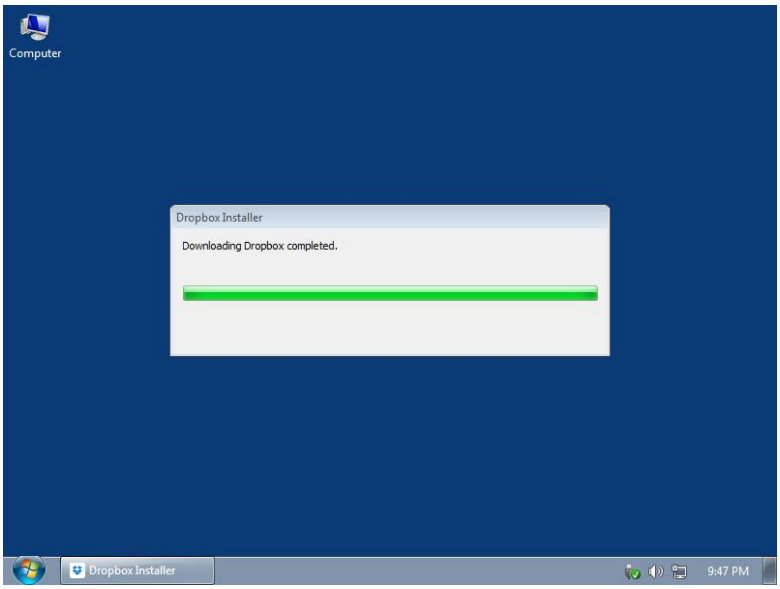

Computer
Dropbox Installer
Connecting to the Internet...
Dropbox Installer
9:47 PM

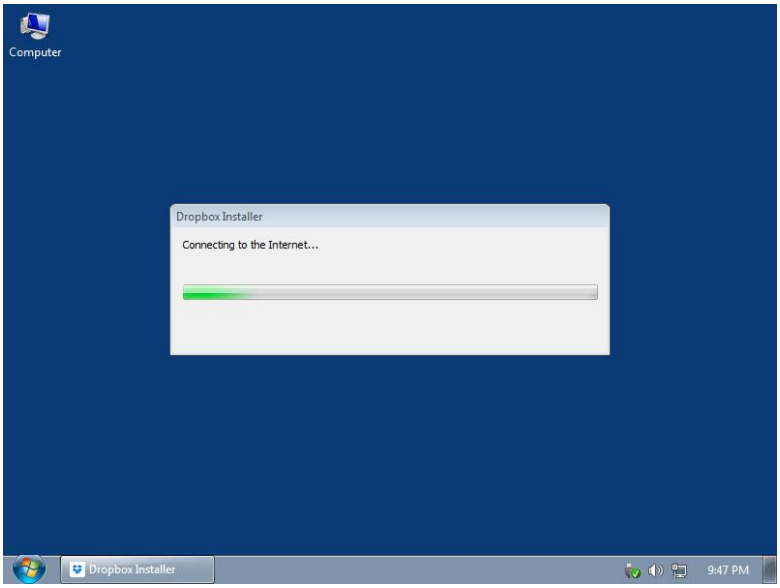

Computer
Dropbox Installer
Waiting to download Dropbox...
Dropbox Installer
9:47 PM

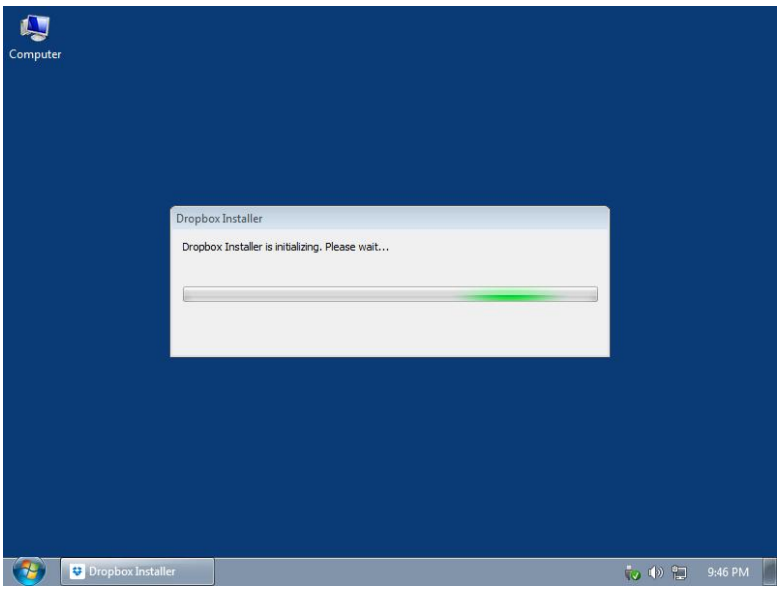

Computer
Dropbox Installer
Dropbox Installer is initializing. Please wait...
Dropbox Installer
9:46 PM

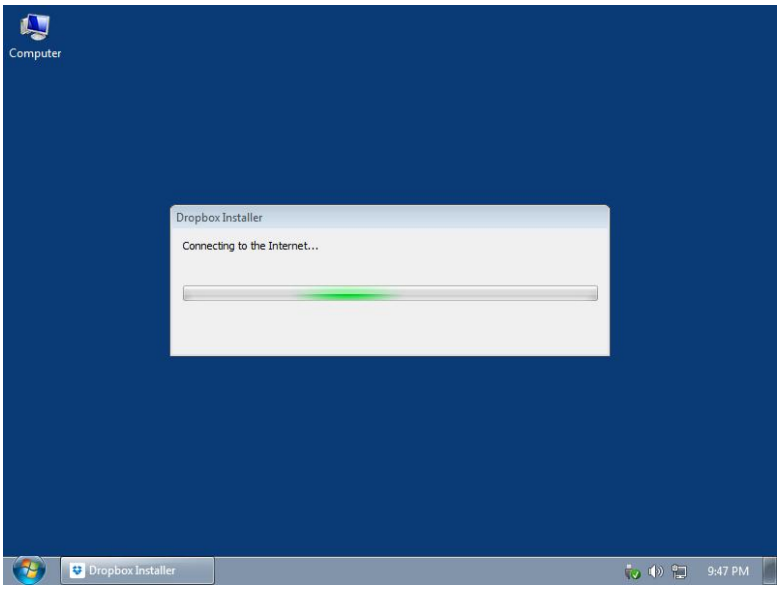

Computer
Dropbox Installer
Waiting to download Dropbox...
Dropbox Installer
9:47 PM

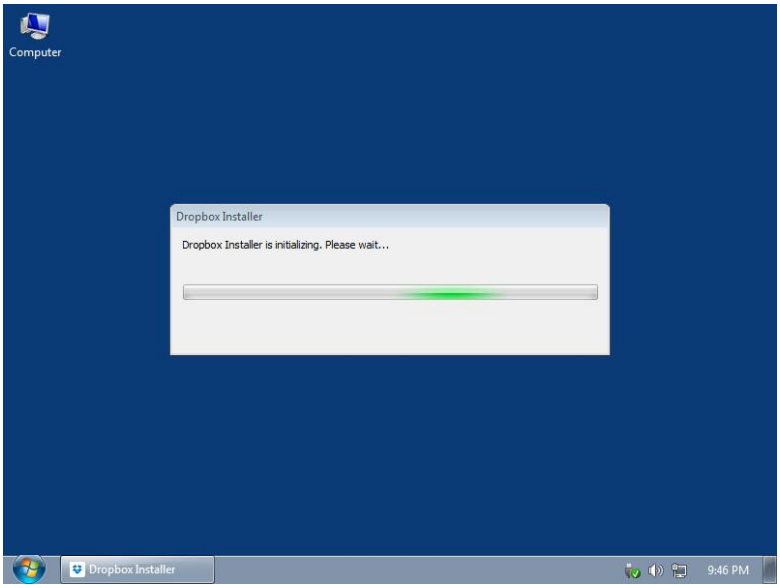

Computer
Dropbox Installer
Connecting to the Internet...
Dropbox Installer
9:47 PM

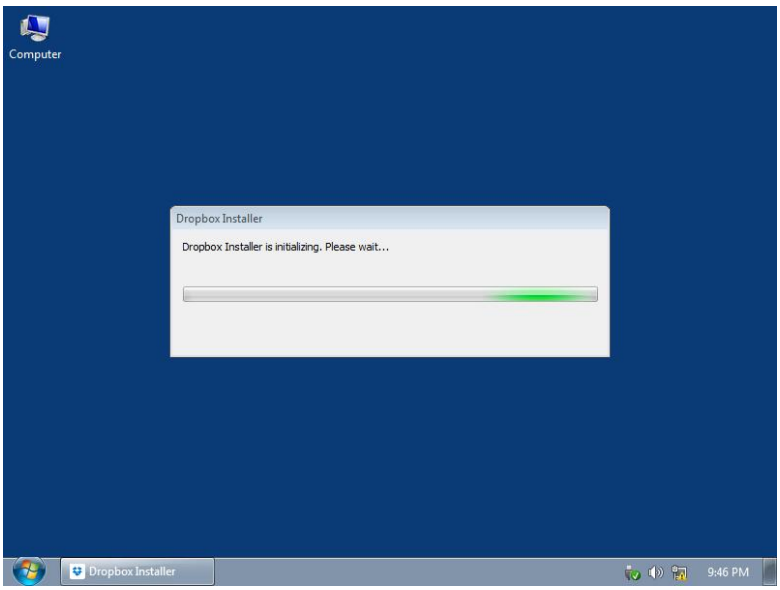

Computer
Dropbox Installer
Downloading Dropbox completed.
Dropbox Installer
9:47 PM

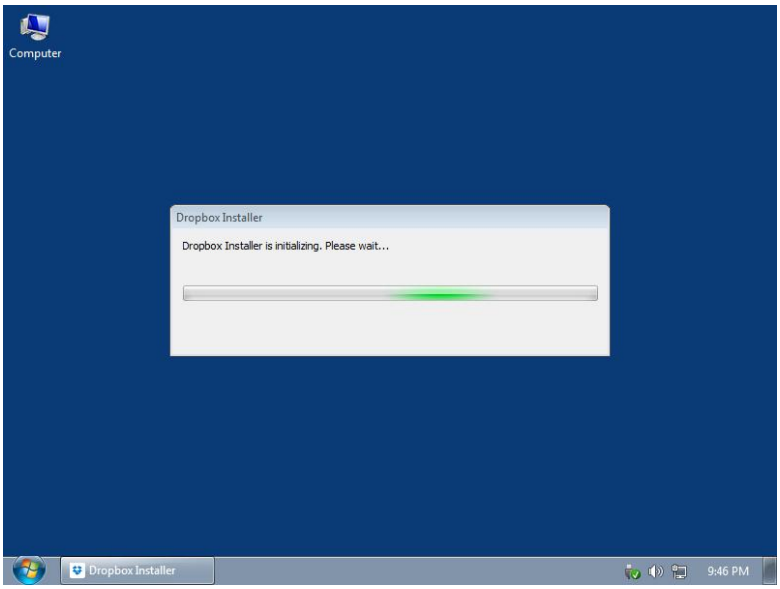

Computer
Dropbox Installer
Connecting to the Internet...
Dropbox Installer
9:47 PM

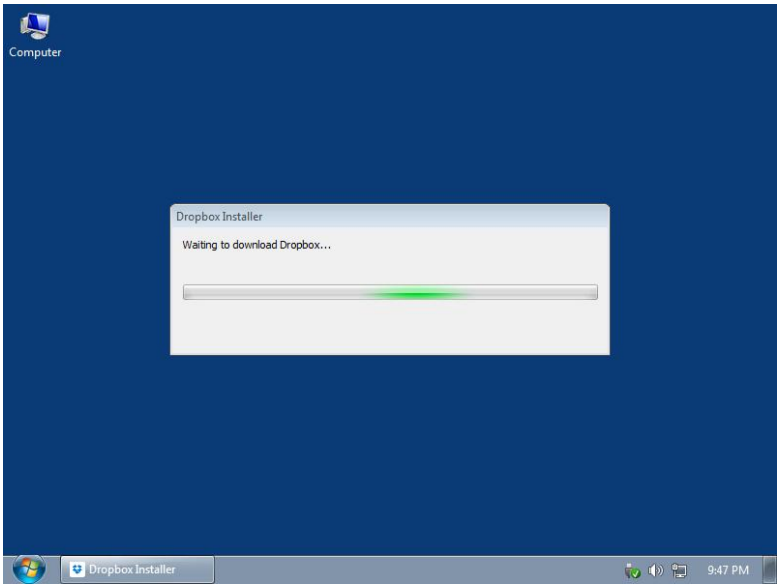

Computer
Dropbox Installer
Dropbox Installer is initializing. Please wait...
Dropbox Installer
9:46 PM

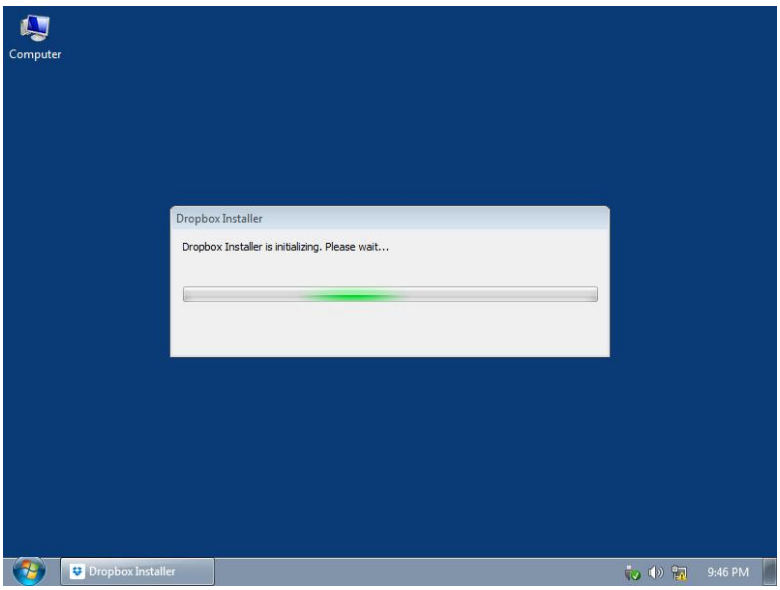

Computer
Dropbox Installer
Connecting to the Internet...
Dropbox Installer
9:47 PM

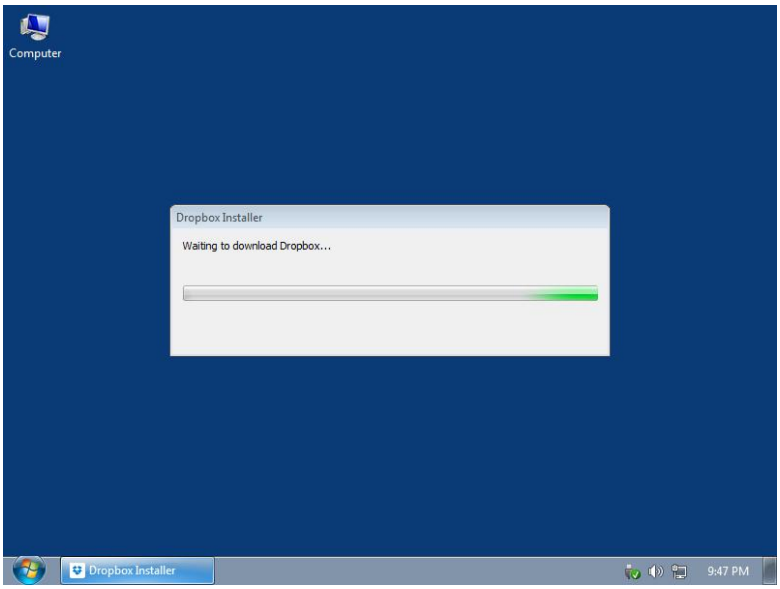

Computer
Dropbox Installer
Dropbox Installer is initializing. Please wait...
Dropbox Installer
9:46 PM

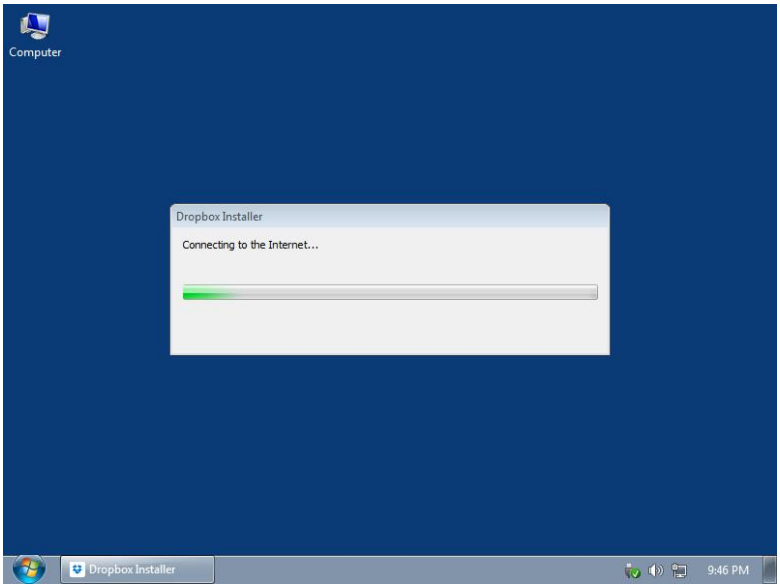

Computer
Dropbox Installer
Dropbox Installer is initializing. Please wait...
Dropbox Installer
9:46 PM

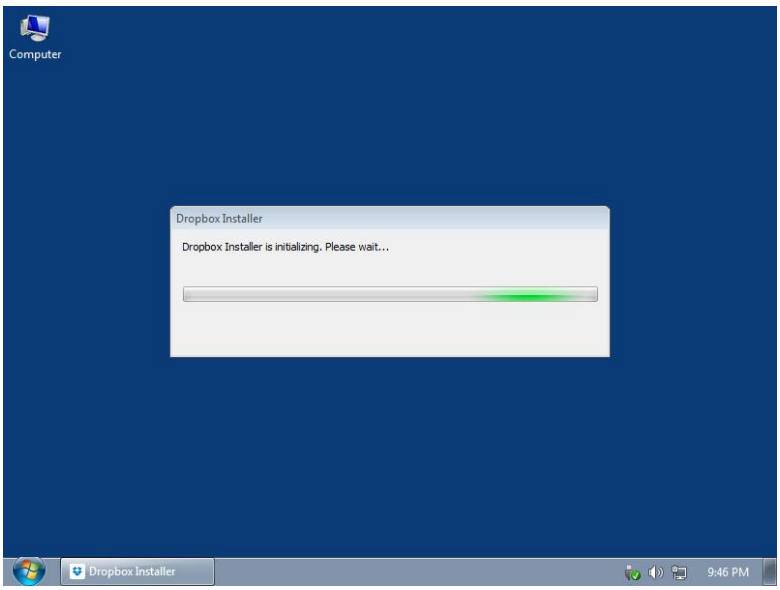

Computer
Dropbox Installer
Dropbox Installer is initializing. Please wait...
Dropbox Installer
9:46 PM

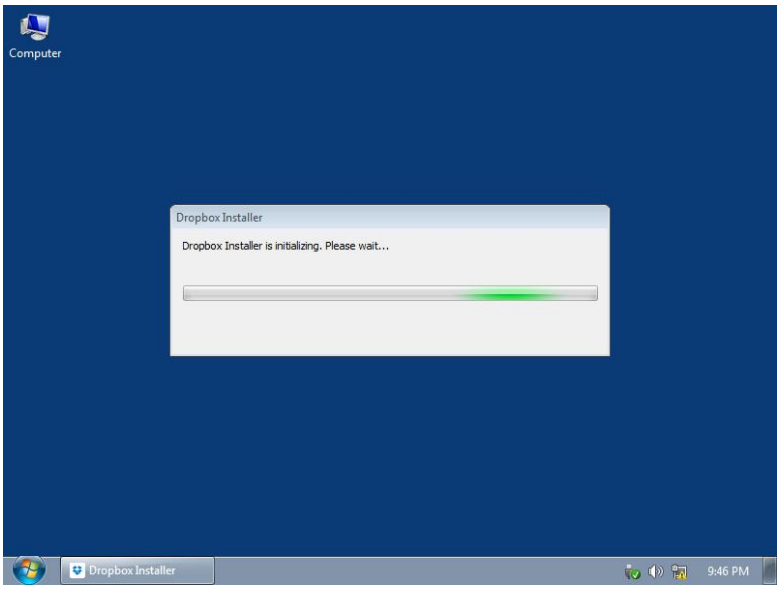

Computer
Dropbox Installer
Waiting to download Dropbox...
Dropbox Installer
9:47 PM

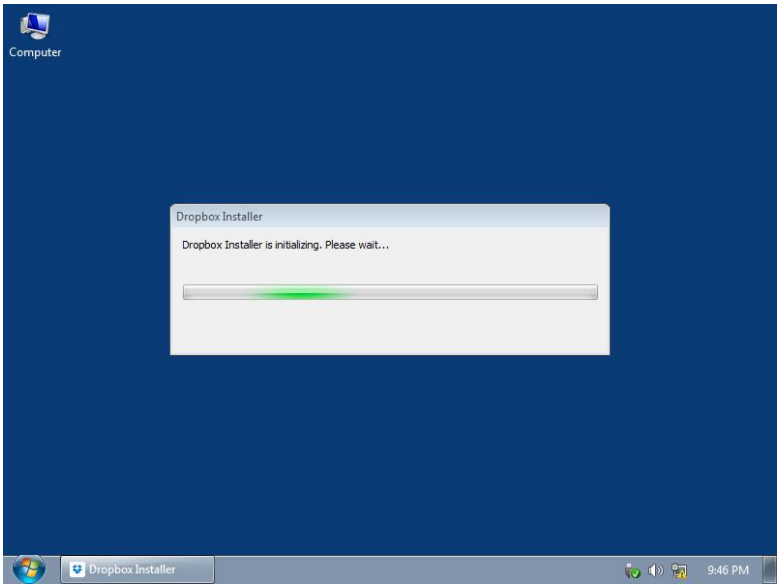

Computer
Dropbox Installer
Dropbox Installer is initializing. Please wait...
Dropbox Installer
9:46 PM

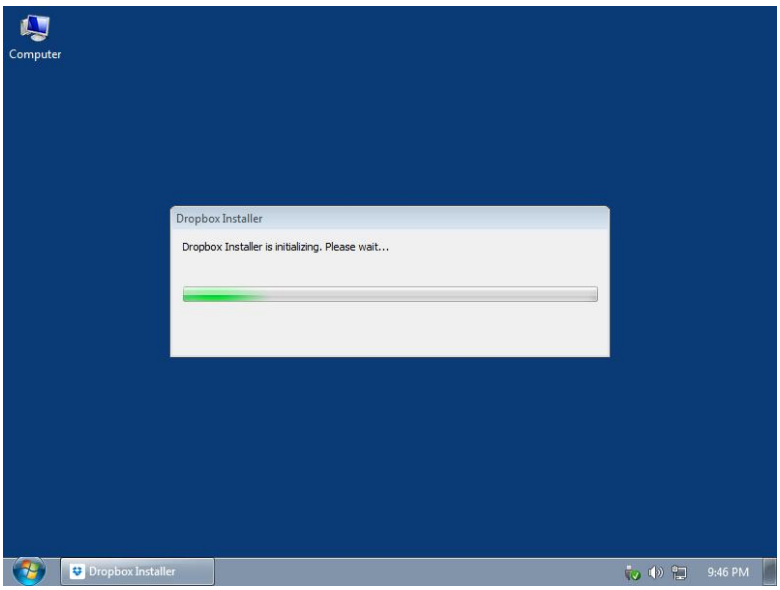

Computer
Dropbox Installer
Waiting to download Dropbox...
Dropbox Installer
9:47 PM

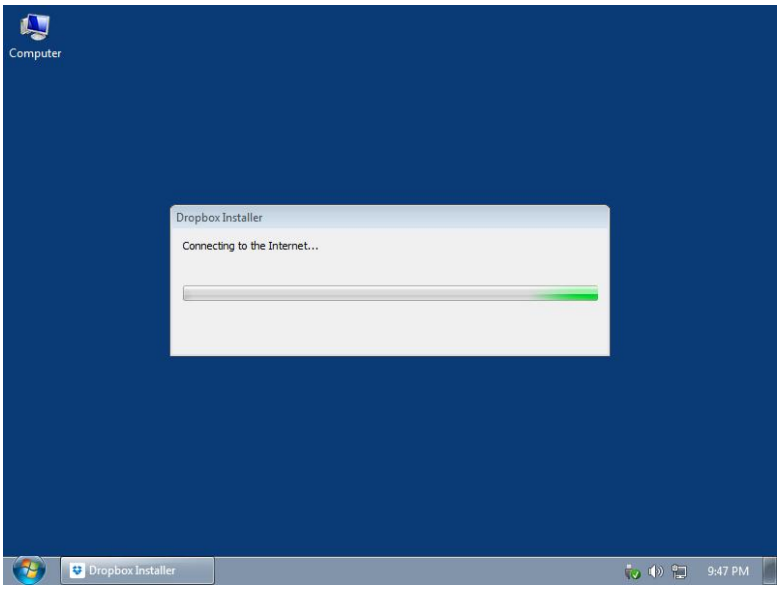

Computer
Dropbox Installer
Connecting to the Internet...
Dropbox Installer
9:46 PM

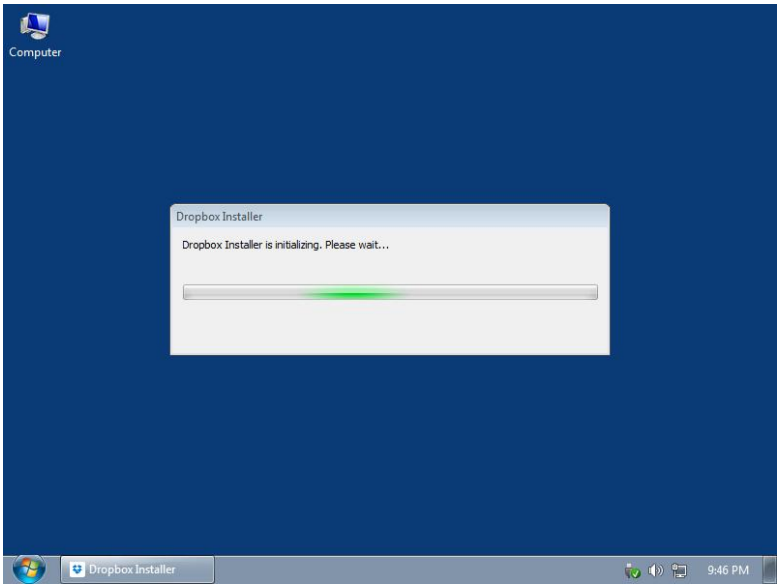

Computer
Dropbox Installer
Dropbox Installer is initializing. Please wait...
Dropbox Installer
9:46 PM

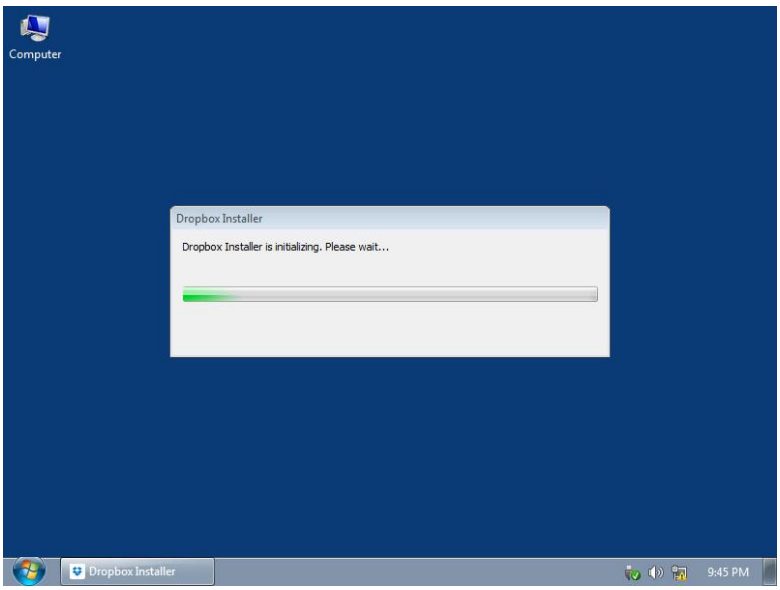

Computer
Dropbox Installer
Dropbox Installer is initializing. Please wait...
Dropbox Installer
9:46 PM

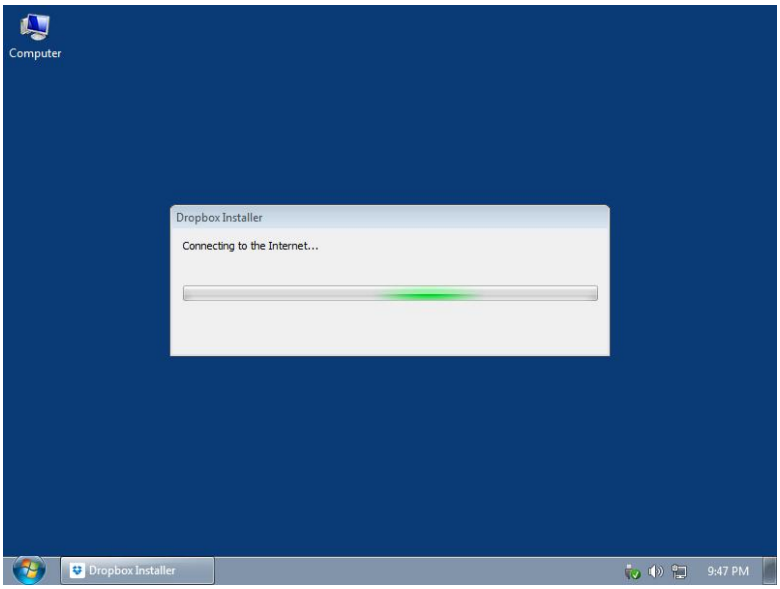

Computer
Dropbox Installer
Dropbox Installer is initializing. Please wait...
Dropbox Installer
9:46 PM


Computer
Dropbox Installer
Dropbox Installer is initializing. Please wait...
Dropbox Installer
9:46 PM

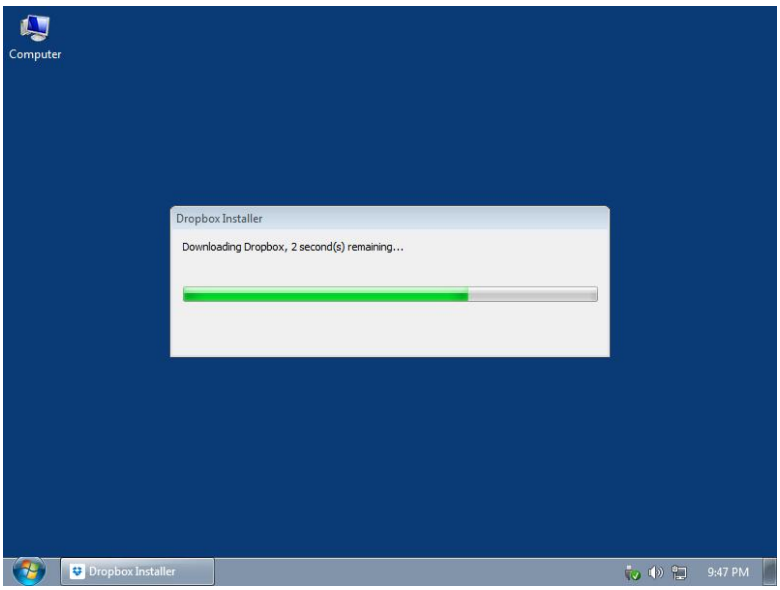

Computer
Dropbox Installer
Connecting to the Internet...
Dropbox Installer
9:47 PM

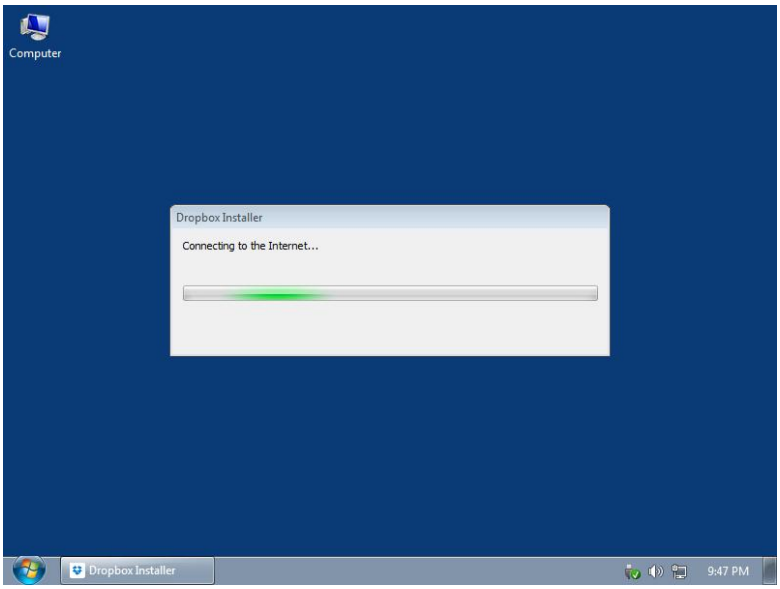

Computer
Dropbox Installer
Dropbox Installer is initializing. Please wait...
Dropbox Installer
9:46 PM

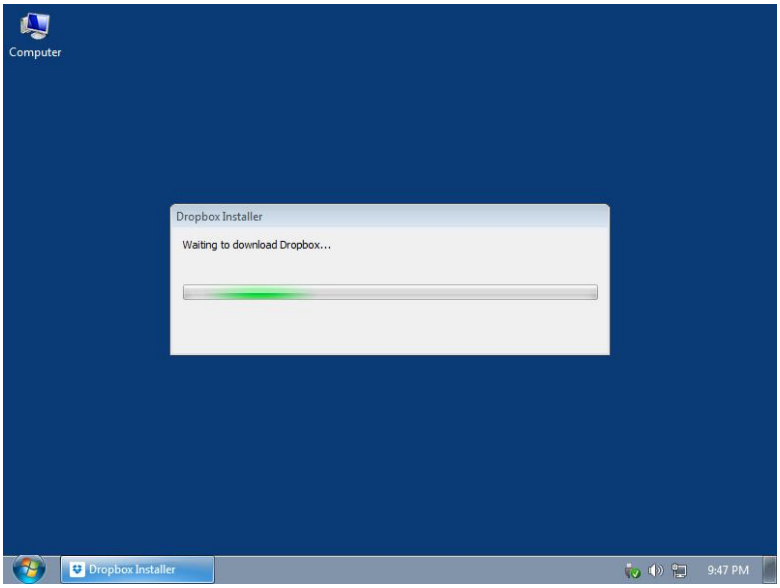

Computer
Dropbox Installer
Dropbox Installer is initializing. Please wait...
Dropbox Installer
9:45 PM

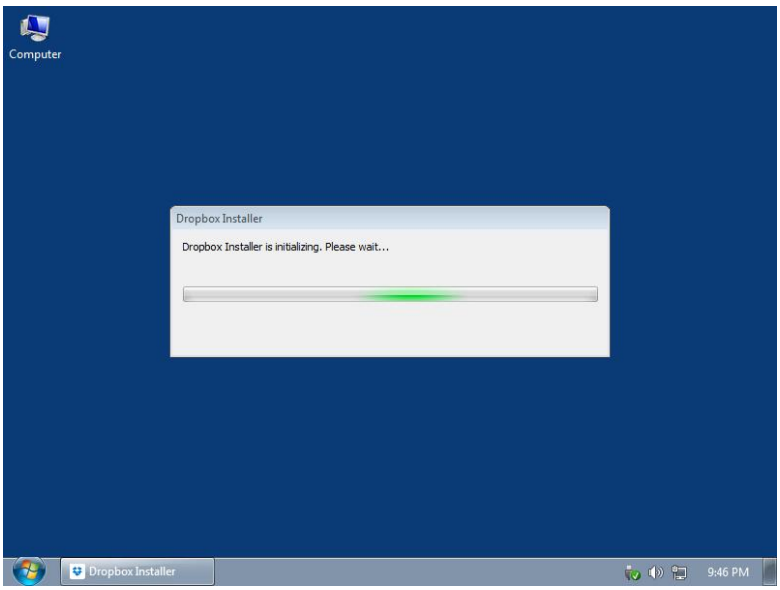

Computer
Dropbox Installer
Connecting to the Internet...
Dropbox Installer
9:47 PM

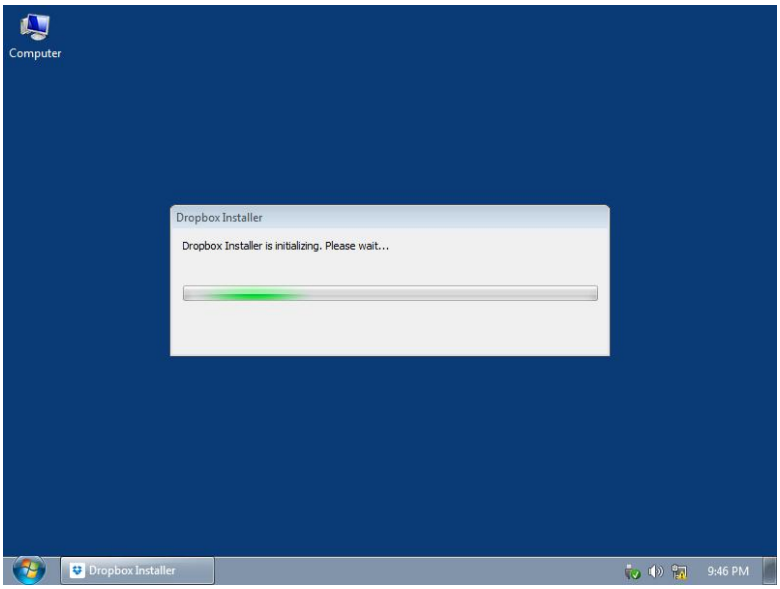

Computer
9:45 PM

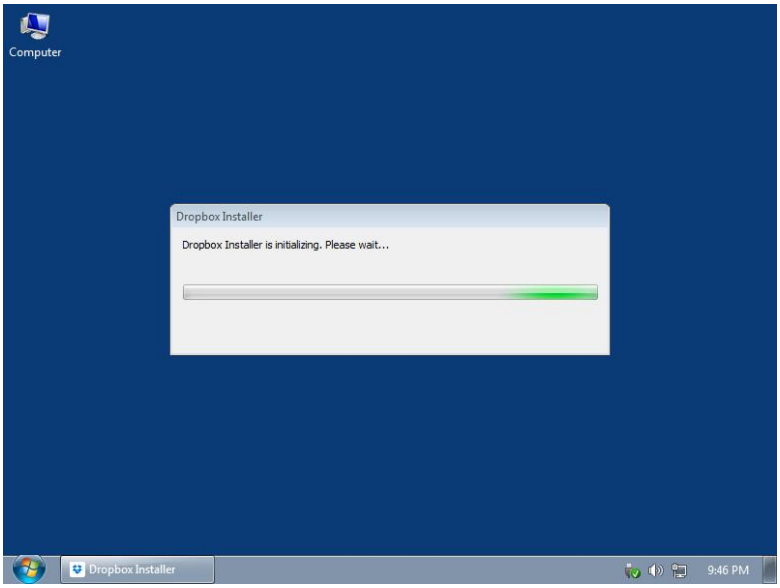

Computer
Dropbox Installer
Downloading Dropbox, 2 second(s) remaining...
Dropbox Installer
9:47 PM

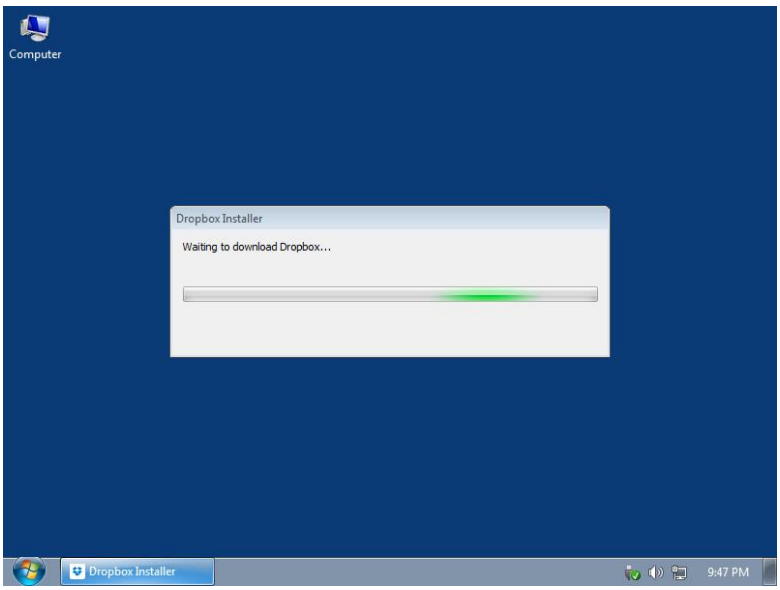

Computer
Dropbox Installer
Connecting to the Internet...
Dropbox Installer
9:47 PM

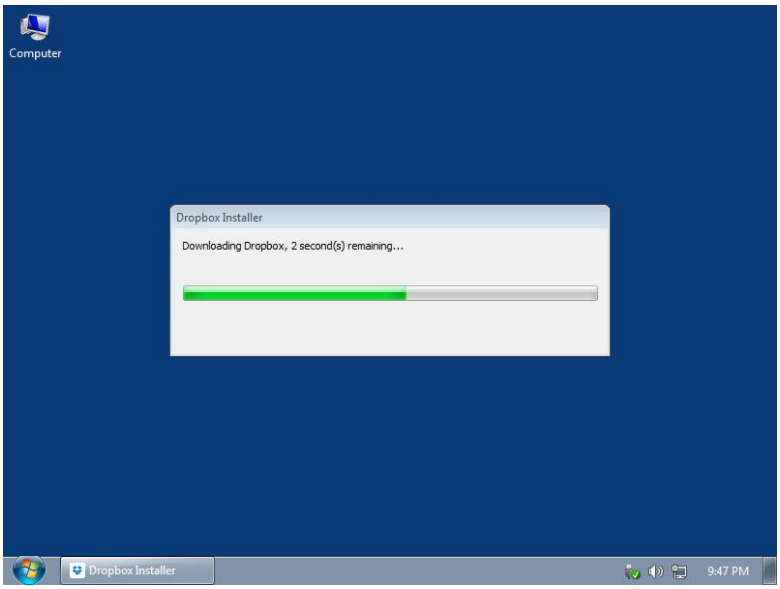

Computer
Dropbox Installer
Waiting to download Dropbox...
Dropbox Installer
9:47 PM

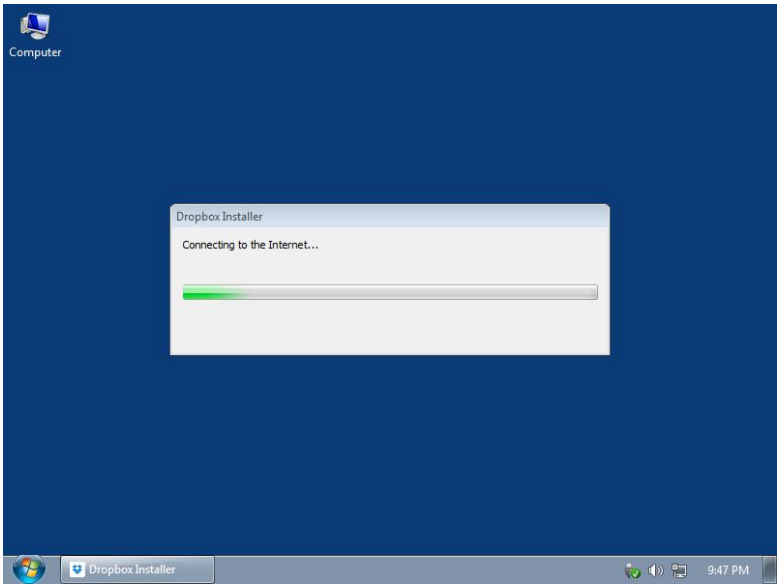

Computer
Dropbox Installer
Dropbox Installer is initializing. Please wait...
Dropbox Installer
9:46 PM

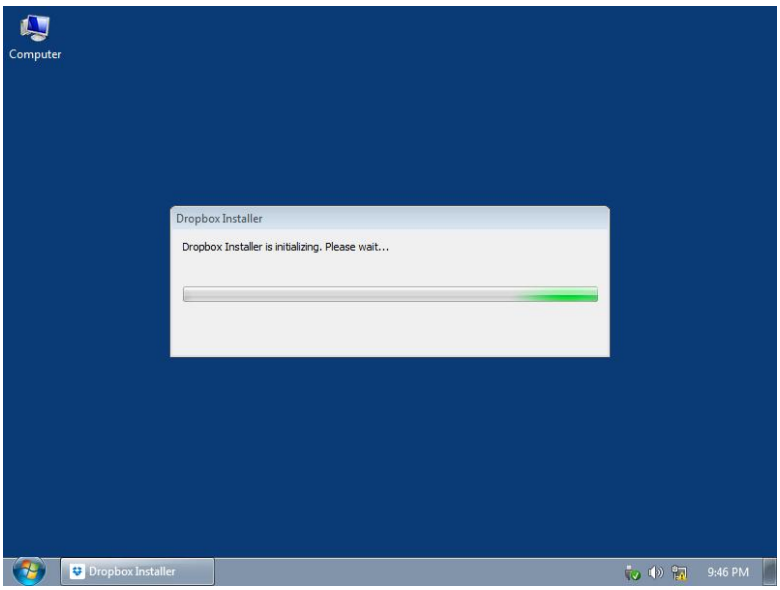

Computer
Dropbox Installer
Dropbox Installer is initializing. Please wait...
Dropbox Installer
9:46 PM

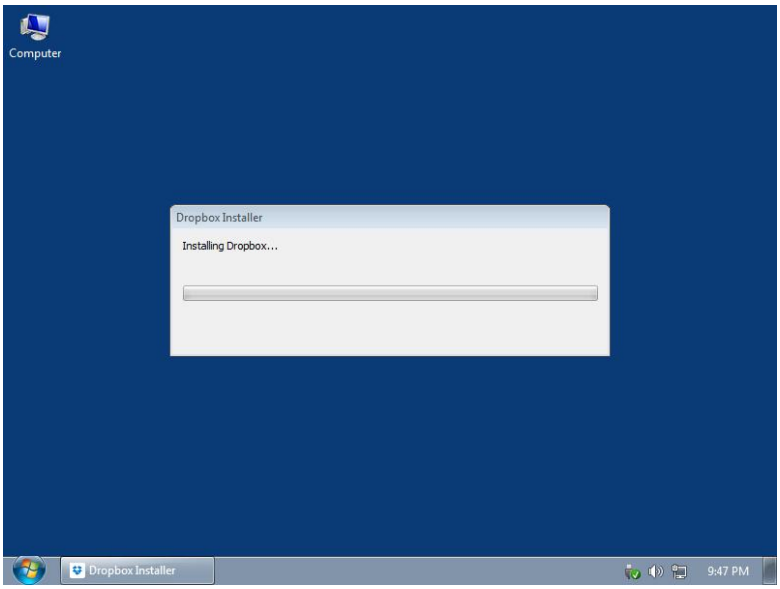

Computer
Dropbox Installer
Dropbox Installer is initializing. Please wait...
Dropbox Installer
9:46 PM

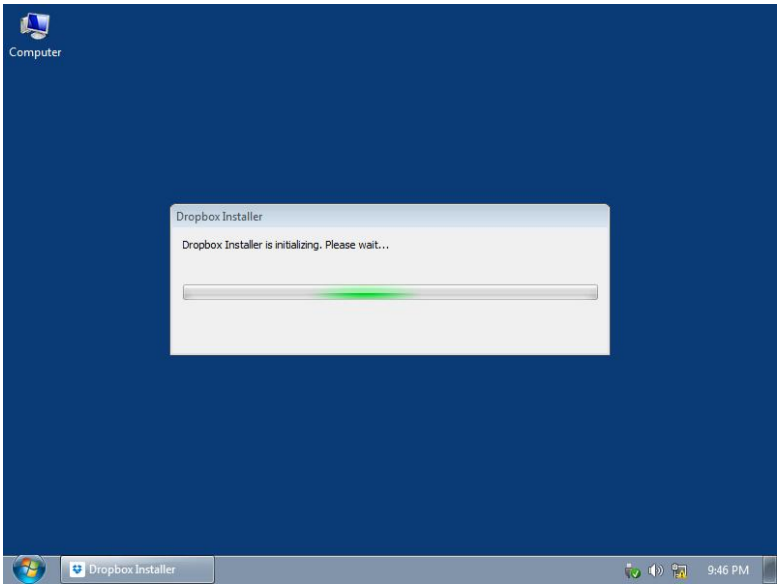

Computer
Dropbox Installer
Waiting to download Dropbox...
Dropbox Installer
9:47 PM

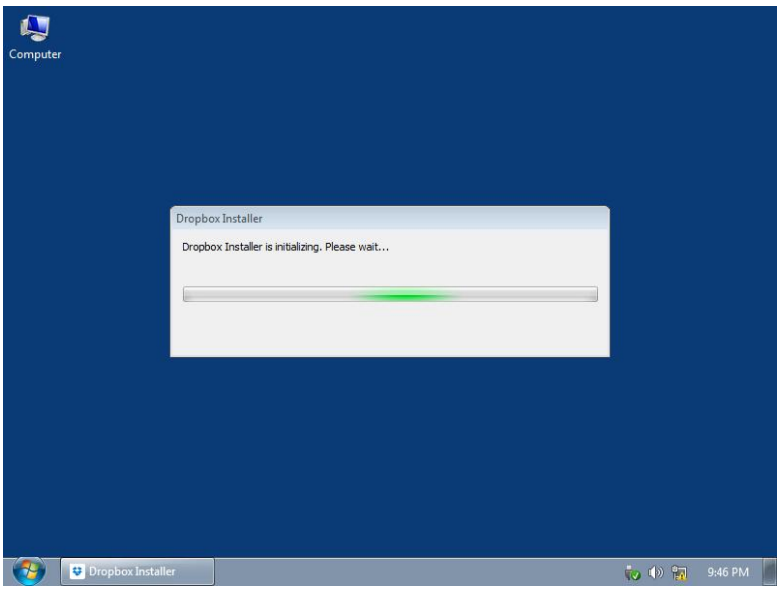

Computer
Dropbox Installer
Downloading Dropbox, 2 second(s) remaining...
Dropbox Installer
9:47 PM

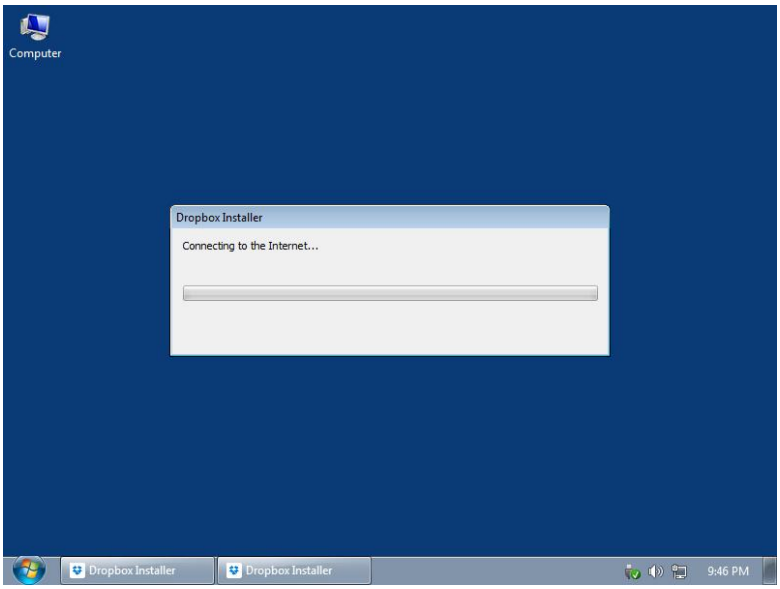

Computer
Dropbox Installer
Connecting to the Internet...
Dropbox Installer
9:47 PM

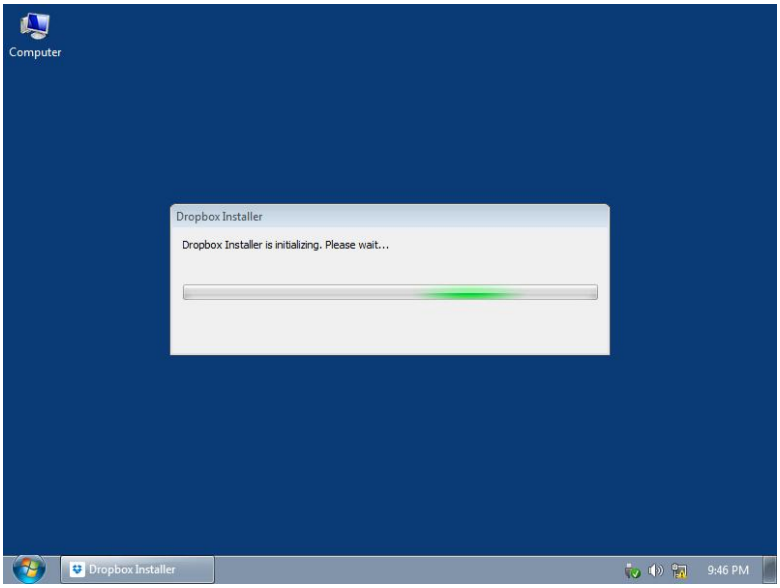

Computer
Dropbox Installer
Dropbox Installer is initializing. Please wait...
Dropbox Installer
9:46 PM

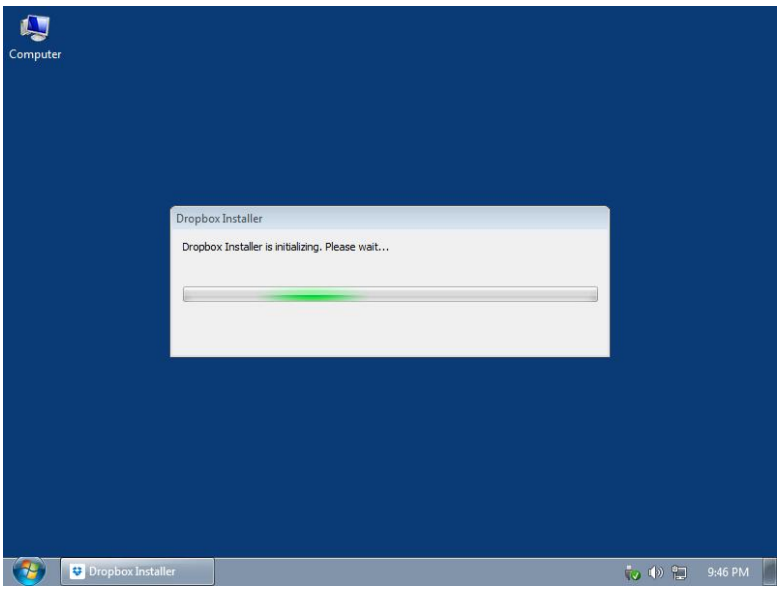

Computer
Dropbox Installer
Installing Dropbox...
Dropbox Installer
9:47 PM

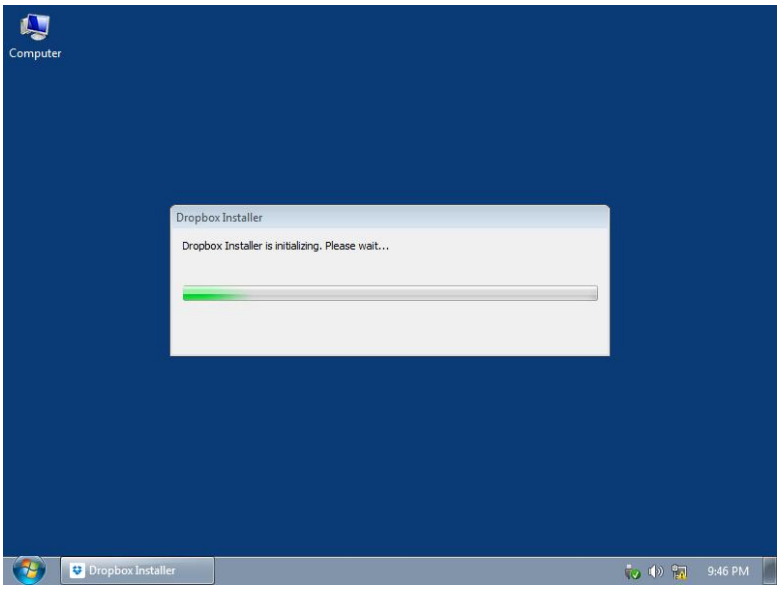

Computer
Dropbox Installer
Dropbox Installer is initializing. Please wait...
Dropbox Installer
9:46 PM

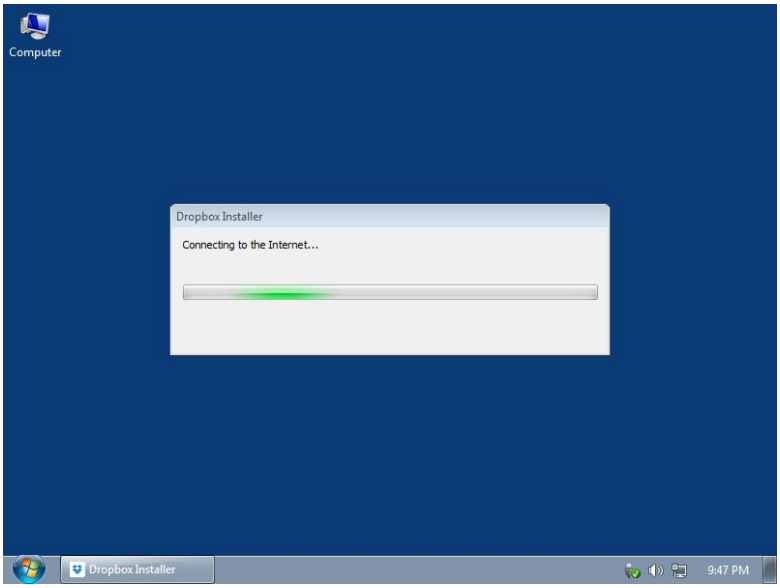

Computer
Dropbox Installer
Dropbox Installer is initializing. Please wait...
Dropbox Installer
9:46 PM

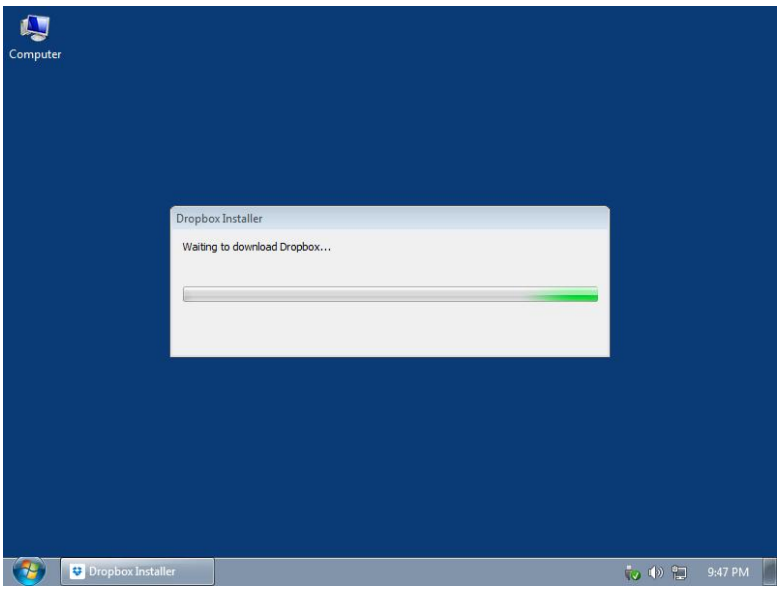

Computer
Dropbox Installer
Connecting to the Internet...
Dropbox Installer
Dropbox Installer
9:46 PM

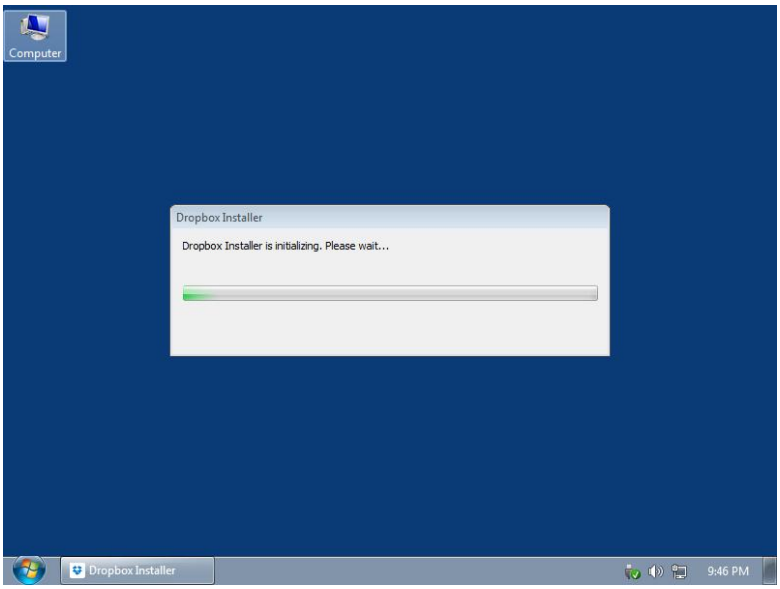

Computer
Dropbox Installer
Dropbox Installer is initializing. Please wait...
Dropbox Installer
9:46 PM


Computer
Dropbox Installer
Dropbox Installer is initializing. Please wait...
Dropbox Installer
9:46 PM


Computer
Dropbox Installer
Dropbox Installer is initializing. Please wait...
Dropbox Installer
9:46 PM


Computer
Dropbox Installer
Connecting to the Internet...
Dropbox Installer
9:47 PM


Computer
Dropbox Installer
Waiting to download Dropbox...
Dropbox Installer
9:47 PM


Computer
Dropbox Installer
Dropbox Installer is initializing. Please wait...
Dropbox Installer
9:46 PM