VALKYRIE COMODO

Summary

File Name: crypt_b.exe

File Type: PE32 executable (GUI) Intel 80386, for MS Windows

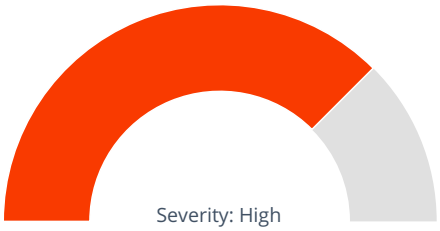
SHA1: 74339b2f522ed9b1b47ba4249b9a6234694c1ce4

MD5: 6f0640320d81a92aafb6835b4b8366fc

MALWARE

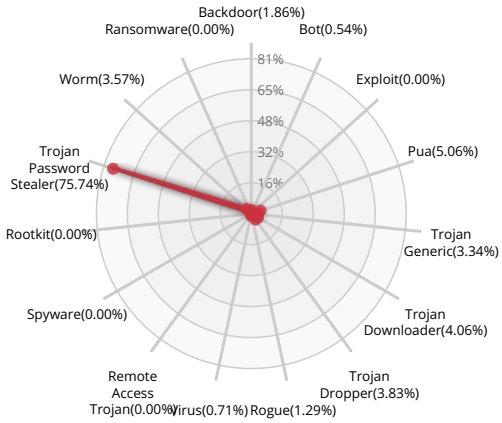
Valkyrie Final Verdict

DETECTION SECTION

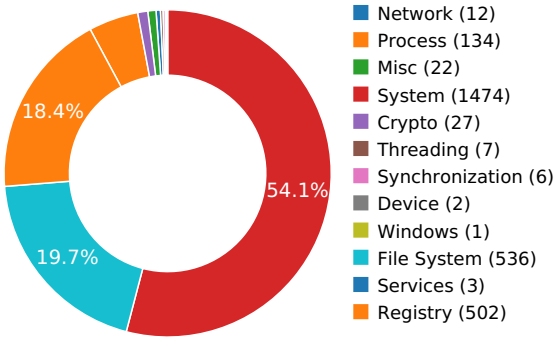


Verdict: Malware

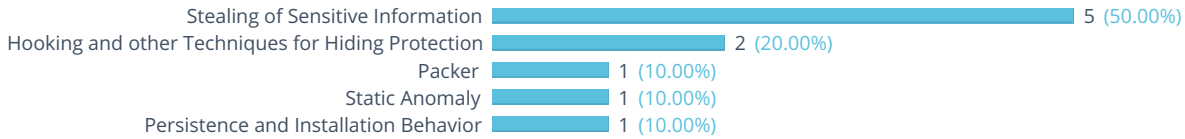
CLASSIFICATION



HIGH LEVEL BEHAVIOR DISTRIBUTION



ACTIVITY OVERVIEW



VALKYRIE COMODO

Activity Details

PACKER

The binary likely contains encrypted or compressed data. Show sources

STEALING OF SENSITIVE INFORMATION

Collects information to fingerprint the system Show sources

Steals private information from local Internet browsers Show sources

Harvests information related to installed instant messenger clients Show sources

Harvests credentials from local FTP client softwares Show sources

Harvests information related to installed mail clients Show sources

STATIC ANOMALY

Anomalous binary characteristics Show sources

PERSISTENCE AND INSTALLATION BEHAVIOR

Deletes its original binary from disk Show sources

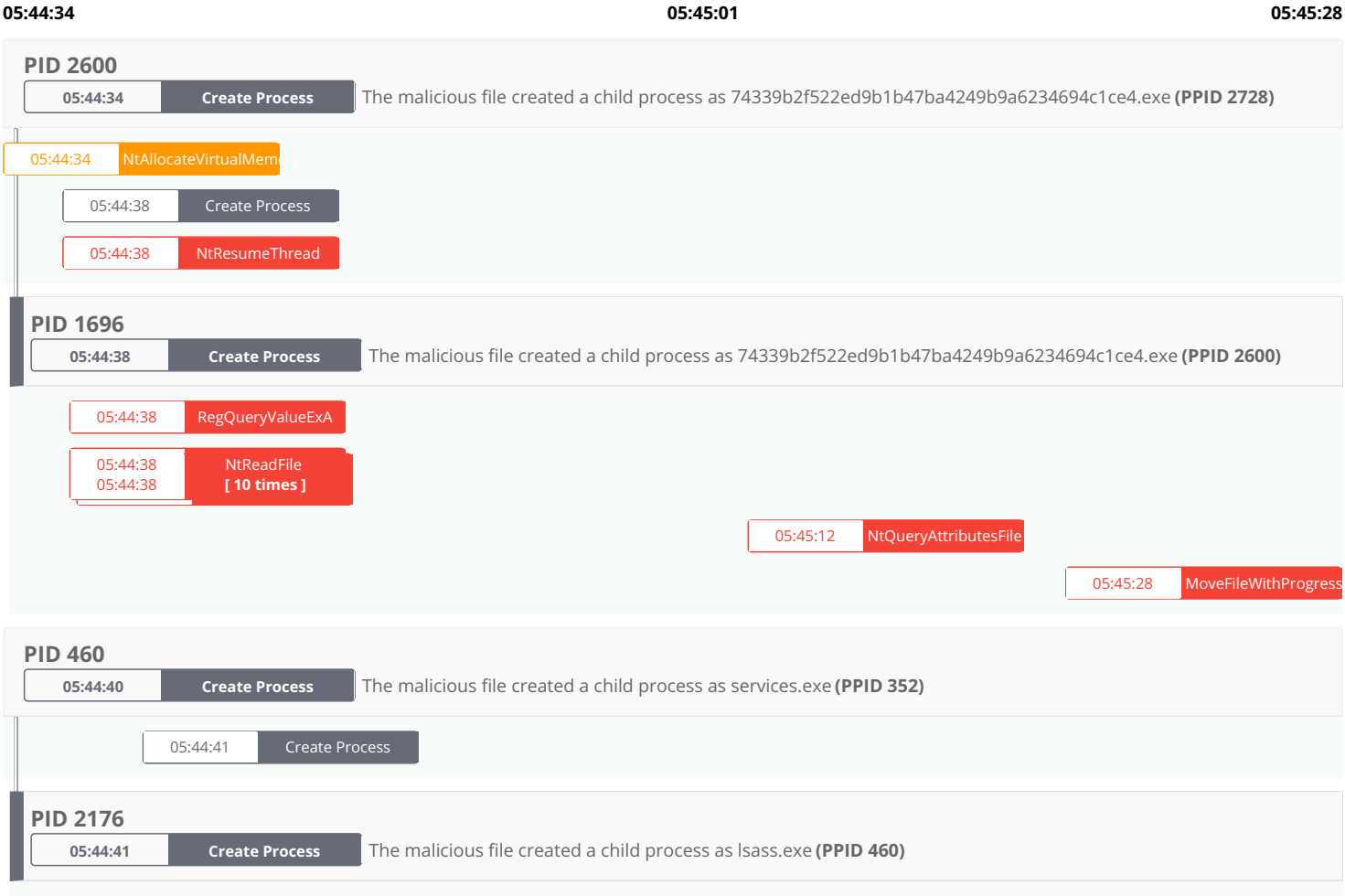
HOOKING AND OTHER TECHNIQUES FOR HIDING PROTECTION

Creates RWX memory Show sources

Executed a process and injected code into it, probably while unpacking Show sources

VALKYRIE COMODO

Behavior Graph



VALKYRIE COMODO

Behavior Summary

ACCESSED FILES

C:\Users\user\AppData\Local\Temp\74339b2f522ed9b1b47ba4249b9a6234694c1ce4.ENU
C:\Users\user\AppData\Local\Temp\74339b2f522ed9b1b47ba4249b9a6234694c1ce4.ENU.DLL
C:\Users\user\AppData\Local\Temp\74339b2f522ed9b1b47ba4249b9a6234694c1ce4.EN
C:\Users\user\AppData\Local\Temp\74339b2f522ed9b1b47ba4249b9a6234694c1ce4.EN.DLL
C:\Windows\Fonts\staticcache.dat
C:\Program Files (x86)\Mozilla Firefox\nss3.dll
C:\Users\user\AppData\Local\Temp\WINMM.dll
C:\Windows\System32\winmm.dll
C:\Users\user\AppData\Local\Temp\WSOCK32.dll
C:\Windows\System32\wsock32.dll
C:\Users\user\AppData\Local\Temp\MSVCR120.dll
C:\Windows\System32\MSVCR120.dll
C:\Windows\system\MSVCR120.dll
C:\Windows\MSVCR120.dll
C:\ProgramData\Oracle\Java\javapath\MSVCR120.dll
C:\Windows\System32\wbem\MSVCR120.dll
C:\Windows\System32\WindowsPowerShell\v1.0\MSVCR120.dll
C:\Program Files\Microsoft Network Monitor 3\MSVCR120.dll
C:\Program Files (x86)\Universal Extractor\MSVCR120.dll
C:\Program Files (x86)\Universal Extractor\bin\MSVCR120.dll
C:\Program Files (x86)\Windows Kits\8.1\Windows Performance Toolkit\MSVCR120.dll
C:\Python27\MSVCR120.dll
C:\Python27\Scripts\MSVCR120.dll
C:\tools\sysinternals\MSVCR120.dll
C:\tools\MSVCR120.dll
C:\tools\IDA_Pro_v6\python\MSVCR120.dll
C:\Program Files (x86)\Mozilla Firefox\msvcr120.dll
C:\Users\user\AppData\Local\Temp\mozglue.dll
C:\Windows\System32\mozglue.dll
C:\Windows\system\mozglue.dll
C:\Windows\mozglue.dll
C:\ProgramData\Oracle\Java\javapath\mozglue.dll

C:\Windows\System32\wbem\mozglue.dll
C:\Windows\System32\WindowsPowerShell\v1.0\mozglue.dll
C:\Program Files\Microsoft Network Monitor 3\mozglue.dll
C:\Program Files (x86)\Universal Extractor\mozglue.dll
C:\Program Files (x86)\Universal Extractor\bin\mozglue.dll
C:\Program Files (x86)\Windows Kits\8.1\Windows Performance Toolkit\mozglue.dll
C:\Python27\mozglue.dll
C:\Python27\Scripts\mozglue.dll
C:\tools\sysinternals\mozglue.dll
C:\tools\mozglue.dll
C:\tools\IDA_Pro_v6\python\mozglue.dll
C:\Program Files (x86)\Mozilla Firefox\mozglue.dll
C:\Users\user\AppData\Local\Temp\VERSION.dll
C:\Windows\System32\version.dll
C:\Users\user\AppData\Local\Temp\MSVCP120.dll
C:\Windows\System32\MSVCP120.dll
C:\Windows\system\MSVCP120.dll
C:\Windows\MSVCP120.dll
C:\ProgramData\Oracle\Java\javapath\MSVCP120.dll
C:\Windows\System32\wbem\MSVCP120.dll
C:\Windows\System32\WindowsPowerShell\v1.0\MSVCP120.dll
C:\Program Files\Microsoft Network Monitor 3\MSVCP120.dll
C:\Program Files (x86)\Universal Extractor\MSVCP120.dll
C:\Program Files (x86)\Universal Extractor\bin\MSVCP120.dll
C:\Program Files (x86)\Windows Kits\8.1\Windows Performance Toolkit\MSVCP120.dll
C:\Python27\MSVCP120.dll
C:\Python27\Scripts\MSVCP120.dll
C:\tools\sysinternals\MSVCP120.dll
C:\tools\MSVCP120.dll
C:\tools\IDA_Pro_v6\python\MSVCP120.dll
C:\Program Files (x86)\Mozilla Firefox\msvcp120.dll
C:\Users\user\AppData\Roaming\Mozilla\Firefox\profiles.ini
C:\Program Files (x86)\Mozilla Firefox\softokn3.dll
C:\Program Files (x86)\Mozilla Firefox\nssdbm3.dll
C:\Users\user\AppData\Roaming\Mozilla\Firefox\Profiles\jdm2a1on.default\secmod.db

C:\Windows\System32\tzres.dll
C:\Program Files (x86)\Mozilla Firefox\freebl3.dll
C:\
C:\Users\user\AppData\Roaming\Mozilla\Firefox\Profiles\jdm2a1on.default\cert8.db
C:\Users\user\AppData\Roaming\Mozilla\Firefox\Profiles\jdm2a1on.default\key3.db
C:\Users\user\AppData\Roaming\Mozilla\Firefox\Profiles\jdm2a1on.default\nssckbi.dll
C:\Users\user\AppData\Roaming\Mozilla\Firefox\Profiles\jdm2a1on.default\signons.sqlite
C:\Users\user\AppData\Roaming\Mozilla\Firefox\Profiles\jdm2a1on.default\logins.json
C:\Users\user\AppData\Roaming\Mozilla\Firefox\Profiles\jdm2a1on.default\signons.txt

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\Windows\Windows Error Reporting\WMR\Disable
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\Locale\00000409
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\Language Groups\1
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\DataStore_V1.0\Disable
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\DataStore_V1.0\DataFilePath
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane1
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane2
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane3
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane4
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane5
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane6
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane7
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane8
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane9
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane10
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane11
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane12
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane13
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane14
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane15
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane16
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\GRE_Initialize\DisableMetaFiles

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Cryptography\MachineGuid
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Mozilla\Mozilla Firefox\CurrentVersion
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Mozilla\Mozilla Firefox\46.0.1 (x86 en-US)\Main\Install Directory
HKEY_CURRENT_USER\Software\Ghisler\Total Commander\FtpIniName
HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\0a0d020000000000c000000000000046\Email
HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\13dbb0c8aa05101a9bb000aa002fc45a\Email
HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\27c571c20b901b4bae192bbd30c1921b\Email
HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\34b9531bce896442a8a090c8845e0b0c\Email
HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\3517490d76624c419a828607e2a54604\Email
HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\41bcc567153c3748a9b366420dae5a66\Email
HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\8503020000000000c000000000000046\Email
HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\9207f3e0a3b11019908b08002b2a56c2\Email
HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\Email
HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000001\Email
HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002\Email
HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002\SMTP Email Address
HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002\SMTP Server
HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002\SMTP User Name
HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002\SMTP User
HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002\POP3 Server
HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002\POP3 User Name
HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002\POP3 User
HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002\NNTP Email Address
HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002\NNTP User Name
HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002\NNTP Server

HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002\IMAP Server
HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002\IMAP User Name
HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002\IMAP User
HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002\HTTP User
HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002\HTTP Server URL
HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002\HTTPMail User Name
HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002\HTTPMail Server
HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002\POP3 Port
HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002\SMTP Port
HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002\IMAP Port
HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002\POP3 Password2
HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002\IMAP Password2
HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002\NNTP Password2
HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002\HTTPMail Password2
HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002\SMTP Password2
HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002\POP3 Password
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\services\crypt32\DebugHeapFlags
HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002\IMAP Password
HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002\NNTP Password
HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002\HTTP Password
HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002\SMTP Password
HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000003\Email
HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\c02ebc5353d9cd11975200aa004ae40e\Email
HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\f4102a07475a2f4bb2d7ccaf6665ac90\Email

HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\f86ed2903a4a11cfb57e524153480001\Email
HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\{D9734F19-8CFB-411D-BC59-833E334FCB5E}\Email
HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\{D9734F19-8CFB-411D-BC59-833E334FCB5E}\Calendar Summary\Email

MODIFIED FILES

C:\Users\user\AppData\Roaming\D5E2DE\E36C7A.lck
C:\Users\user\AppData\Roaming\D5E2DE\E36C7A.exe

RESOLVED APIS

kernel32.dll.GetDiskFreeSpaceExA
oleaut32.dll.VariantChangeTypeEx
oleaut32.dll.VarNeg
oleaut32.dll.VarNot
oleaut32.dll.VarAdd
oleaut32.dll.VarSub
oleaut32.dll.VarMul
oleaut32.dll.VarDiv
oleaut32.dll.VarIdiv
oleaut32.dll.VarMod
oleaut32.dll.VarAnd
oleaut32.dll.VarOr
oleaut32.dll.VarXor
oleaut32.dll.VarCmp
oleaut32.dll.VarI4FromStr
oleaut32.dll.VarR4FromStr
oleaut32.dll.VarR8FromStr
oleaut32.dll.VarDateFromStr
oleaut32.dll.VarCyFromStr
oleaut32.dll.VarBoolFromStr
oleaut32.dll.VarBstrFromCy
oleaut32.dll.VarBstrFromDate
oleaut32.dll.VarBstrFromBool
user32.dll.GetMonitorInfoA
user32.dll.GetSystemMetrics

user32.dll.EnumDisplayMonitors
dwmapi.dll.DwmIsCompositionEnabled
gdi32.dll.GetLayout
gdi32.dll.GdiRealizationInfo
gdi32.dll.FontIsLinked
advapi32.dll.RegOpenKeyExW
advapi32.dll.RegQueryInfoKeyW
gdi32.dll.GetTextFaceAliasW
advapi32.dll.RegEnumValueW
advapi32.dll.RegCloseKey
advapi32.dll.RegQueryValueExW
gdi32.dll.GetFontAssocStatus
advapi32.dll.RegQueryValueExA
advapi32.dll.RegEnumKeyExW
gdi32.dll.GdiIsMetaPrintDC
user32.dll.AnimateWindow
comctl32.dll.InitializeFlatSB
comctl32.dll.UninitializeFlatSB
comctl32.dll.FlatSB_GetScrollProp
comctl32.dll.FlatSB_SetScrollProp
comctl32.dll.FlatSB_EnableScrollBar
comctl32.dll.FlatSB_ShowScrollBar
comctl32.dll.FlatSB_GetScrollRange
comctl32.dll.FlatSB_GetScrollInfo
comctl32.dll.FlatSB_GetScrollPos
comctl32.dll.FlatSB_SetScrollPos
comctl32.dll.FlatSB_SetScrollInfo
comctl32.dll.FlatSB_SetScrollRange
user32.dll.SetLayeredWindowAttributes
user32.dll.GetLastInputInfo
kernel32.dll.VirtualProtect
cryptsp.dll.CryptAcquireContextW
cryptsp.dll.CryptCreateHash
cryptsp.dll.CryptHashData
cryptsp.dll.CryptGetHashParam

cryptsp.dll.CryptDestroyHash
cryptsp.dll.CryptReleaseContext
kernel32.dll.GetTickCount64
nss3.dll.NSS_Init
nss3.dll.NSS_Shutdown
nss3.dll.PK11_GetInternalKeySlot
nss3.dll.PK11_FreeSlot
nss3.dll.PK11_Authenticate
nss3.dll.PK11SDR_Decrypt
nss3.dll.PK11_CheckUserPassword
nss3.dll.SECITEM_FreeItem
kernel32.dll.InitializeCriticalSectionEx
softokn3.dll.NSC_GetFunctionList
softokn3.dll.NSC_ModuleDBFunc
nssdbm3.dll.legacy_Open
nssdbm3.dll.legacy_ReadSecmodDB

DELETED FILES

C:\Users\user\AppData\Roaming\D5E2DE\E36C7A.lck
C:\Users\user\AppData\Local\Temp\74339b2f522ed9b1b47ba4249b9a6234694c1ce4.exe

REGISTRY KEYS

HKEY_CURRENT_USER\Software\Borland\Locales
HKEY_LOCAL_MACHINE\Software\Borland\Locales
HKEY_CURRENT_USER\Software\Borland\Delphi\Locales
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\Windows\Windows Error Reporting\WMR
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\Windows Error Reporting\WMR\Disable
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Nls\Locale
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Nls\Locale\Alternate Sorts
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Nls\Language Groups
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\Locale\00000409

HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\Language Groups\1
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\FontLink\SystemLink
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\DataStore_V1.0
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\DataStore_V1.0\Disable
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\DataStore_V1.0\DataFilePath
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane1
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane2
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane3
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane4
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane5
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane6
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane7
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane8
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane9
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane10
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane11
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane12
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane13
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane14
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane15
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane16
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Segoe UI
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\GRE_Initialize
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\GRE_Initialize\DisableMetaFiles
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Cryptography
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Cryptography\MachineGuid
HKEY_LOCAL_MACHINE\SOFTWARE\Mozilla\Mozilla Firefox
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Mozilla\Mozilla Firefox\CurrentVersion
HKEY_LOCAL_MACHINE\SOFTWARE\Mozilla\Mozilla Firefox\46.0.1 (x86 en-US)\Main
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Mozilla\Mozilla Firefox\46.0.1 (x86 en-US)\Main\Install Directory
HKEY_LOCAL_MACHINE\SOFTWARE\ComodoGroup\IceDragon\Setup
HKEY_LOCAL_MACHINE\SOFTWARE\Apple Computer, Inc.\Safari
HKEY_LOCAL_MACHINE\SOFTWARE\K-Meleon
HKEY_LOCAL_MACHINE\SOFTWARE\mozilla.org\SeaMonkey

HKEY_LOCAL_MACHINE\SOFTWARE\Mozilla\SeaMonkey
HKEY_LOCAL_MACHINE\SOFTWARE\Mozilla\Flock
HKEY_CURRENT_USER\Software\QtWeb.NET\QtWeb Internet Browser\AutoComplete
HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\IntelliForms\Storage2
HKEY_LOCAL_MACHINE\SOFTWARE\8pecxstudios\Cyberfox86
HKEY_LOCAL_MACHINE\SOFTWARE\8pecxstudios\Cyberfox
HKEY_LOCAL_MACHINE\SOFTWARE\Mozilla\Pale Moon
HKEY_LOCAL_MACHINE\SOFTWARE\Mozilla\Waterfox
HKEY_CURRENT_USER\Software\LinasFTP\Site Manager
HKEY_CURRENT_USER\Software\FlashPeak\BlazeFtp\Settings
HKEY_CURRENT_USER\Software\Ghisler\Total Commander
HKEY_CURRENT_USER\Software\Ghisler\Total Commander\FtpIniName
HKEY_CURRENT_USER\Software
HKEY_CURRENT_USER\Software\7-Zip
HKEY_CURRENT_USER\Software\Adlice Software
HKEY_CURRENT_USER\Software\Adobe
HKEY_CURRENT_USER\Software\AppDataLow
HKEY_CURRENT_USER\Software\Clients
HKEY_CURRENT_USER\Software\Ghisler
HKEY_CURRENT_USER\Software\Google
HKEY_CURRENT_USER\Software\Hex-Rays
HKEY_CURRENT_USER\Software\JavaSoft
HKEY_CURRENT_USER\Software\JetBrains
HKEY_CURRENT_USER\Software\Macromedia
HKEY_CURRENT_USER\Software\Microsoft
HKEY_CURRENT_USER\Software\Mozilla
HKEY_CURRENT_USER\Software\MozillaPlugins
HKEY_CURRENT_USER\Software\MPC-HC

EXECUTED COMMANDS

"C:\Users\user\AppData\Local\Temp\74339b2f522ed9b1b47ba4249b9a6234694c1ce4.exe"
C:\Windows\system32\lsass.exe

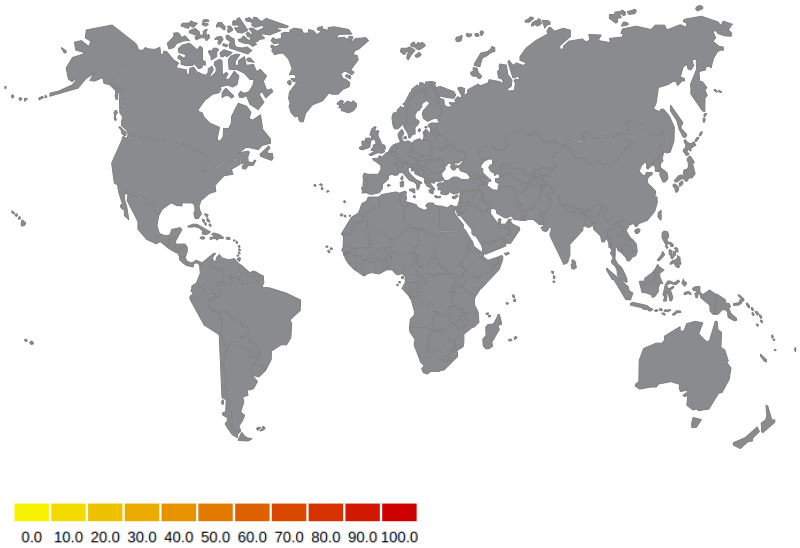
READ FILES

C:\Windows\Fonts\staticcache.dat

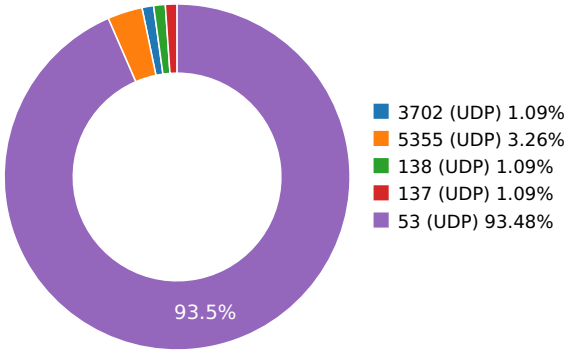
C:\Program Files (x86)\Mozilla Firefox\nss3.dll
C:\Windows\System32\winmm.dll
C:\Windows\System32\wsock32.dll
C:\Program Files (x86)\Mozilla Firefox\msvcr120.dll
C:\Program Files (x86)\Mozilla Firefox\mozglue.dll
C:\Windows\System32\version.dll
C:\Program Files (x86)\Mozilla Firefox\msvcp120.dll
C:\Users\user\AppData\Roaming\Mozilla\Firefox\profiles.ini
C:\Program Files (x86)\Mozilla Firefox\softokn3.dll
C:\Program Files (x86)\Mozilla Firefox\nssdbm3.dll
C:\Windows\System32\tzres.dll
C:\Users\user\AppData\Roaming\Mozilla\Firefox\Profiles\jdm2a1on.default\secmod.db
C:\Program Files (x86)\Mozilla Firefox\freebl3.dll
C:\Users\user\AppData\Roaming\Mozilla\Firefox\Profiles\jdm2a1on.default\cert8.db
C:\Users\user\AppData\Roaming\Mozilla\Firefox\Profiles\jdm2a1on.default\key3.db
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data
\Device\KsecDD
C:\Users\user\AppData\Roaming\D5E2DE\E36C7A.hdb
C:\Windows\System32\netapi32.dll
C:\Windows\System32\netutils.dll
C:\Windows\System32\srvcli.dll
C:\Users\user\AppData\Roaming\D5E2DE\E36C7A.lck

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
	8.8.8.8	United States	15169	Level 3 Parent, LLC	Malware Process

DNS QUERIES

Request	Type
creamzy.gq	A

UDP PACKETS

Call Time During Execution(sec)	Source IP	Dest IP	Dest Port
3.03494095802	Sandbox	224.0.0.252	5355
3.03604888916	Sandbox	224.0.0.252	5355
3.04610991478	Sandbox	239.255.255.250	3702
3.07908701897	Sandbox	192.168.56.255	137
5.59445595741	Sandbox	224.0.0.252	5355
9.07910084724	Sandbox	192.168.56.255	138
46.954007864	Sandbox	8.8.4.4	53
47.3801100254	Sandbox	8.8.8.8	53
50.2540159225	Sandbox	8.8.8.8	53
50.8020129204	Sandbox	8.8.4.4	53
53.6878459454	Sandbox	8.8.8.8	53
54.2314929962	Sandbox	8.8.4.4	53

Call Time During Execution(sec)	Source IP	Dest IP	Dest Port
57.0164768696	Sandbox	8.8.8.8	53
57.5065050125	Sandbox	8.8.4.4	53
60.4117069244	Sandbox	8.8.8.8	53
60.8987619877	Sandbox	8.8.4.4	53
63.5944769382	Sandbox	8.8.8.8	53
64.151362896	Sandbox	8.8.4.4	53
76.890848875	Sandbox	8.8.8.8	53
77.4356939793	Sandbox	8.8.4.4	53
80.2034180164	Sandbox	8.8.8.8	53
80.7464108467	Sandbox	8.8.4.4	53
93.4850120544	Sandbox	8.8.8.8	53
93.9875049591	Sandbox	8.8.4.4	53
96.7037570477	Sandbox	8.8.8.8	53
97.2006659508	Sandbox	8.8.4.4	53
109.969917059	Sandbox	8.8.8.8	53
110.444665909	Sandbox	8.8.4.4	53
113.206683874	Sandbox	8.8.8.8	53
113.691478014	Sandbox	8.8.4.4	53
126.473723888	Sandbox	8.8.8.8	53
126.949292898	Sandbox	8.8.4.4	53
129.68758893	Sandbox	8.8.8.8	53
130.174315929	Sandbox	8.8.4.4	53
142.891636848	Sandbox	8.8.8.8	53
143.366482019	Sandbox	8.8.4.4	53
146.171941042	Sandbox	8.8.8.8	53
146.716034889	Sandbox	8.8.4.4	53
159.484662056	Sandbox	8.8.8.8	53
159.961410046	Sandbox	8.8.4.4	53
162.750356913	Sandbox	8.8.8.8	53
163.225013018	Sandbox	8.8.4.4	53
180.735445976	Sandbox	8.8.8.8	53
181.221055031	Sandbox	8.8.4.4	53
185.738069057	Sandbox	8.8.8.8	53
186.212139845	Sandbox	8.8.4.4	53
198.890202045	Sandbox	8.8.8.8	53
199.365238905	Sandbox	8.8.4.4	53
202.037662029	Sandbox	8.8.8.8	53

Call Time During Execution(sec)	Source IP	Dest IP	Dest Port
202.512654066	Sandbox	8.8.4.4	53
215.184767008	Sandbox	8.8.8.8	53
215.659653902	Sandbox	8.8.4.4	53
220.73731184	Sandbox	8.8.8.8	53
221.21340704	Sandbox	8.8.4.4	53
233.882957935	Sandbox	8.8.8.8	53
234.369468927	Sandbox	8.8.4.4	53
237.037565947	Sandbox	8.8.8.8	53
237.527005911	Sandbox	8.8.4.4	53
250.193943024	Sandbox	8.8.8.8	53
250.726418018	Sandbox	8.8.4.4	53
253.415086031	Sandbox	8.8.8.8	53
253.906024933	Sandbox	8.8.4.4	53
266.592010975	Sandbox	8.8.8.8	53
267.066572905	Sandbox	8.8.4.4	53
269.743592024	Sandbox	8.8.8.8	53
270.230988026	Sandbox	8.8.4.4	53
282.897356033	Sandbox	8.8.8.8	53
283.386567831	Sandbox	8.8.4.4	53
286.053683996	Sandbox	8.8.8.8	53
286.539876938	Sandbox	8.8.4.4	53
299.20955801	Sandbox	8.8.8.8	53
299.699651957	Sandbox	8.8.4.4	53
302.369091988	Sandbox	8.8.8.8	53
302.84679985	Sandbox	8.8.4.4	53
315.521800041	Sandbox	8.8.8.8	53
316.000136852	Sandbox	8.8.4.4	53
318.663025856	Sandbox	8.8.8.8	53
319.149257898	Sandbox	8.8.4.4	53
331.819562912	Sandbox	8.8.8.8	53
332.296900034	Sandbox	8.8.4.4	53
334.974709988	Sandbox	8.8.8.8	53
335.464555025	Sandbox	8.8.4.4	53
348.131612062	Sandbox	8.8.8.8	53
348.689806938	Sandbox	8.8.4.4	53
351.36907196	Sandbox	8.8.8.8	53
351.845367908	Sandbox	8.8.4.4	53

Call Time During Execution(sec)	Source IP	Dest IP	Dest Port
364.529258013	Sandbox	8.8.8.8	53
365.00628686	Sandbox	8.8.4.4	53
367.679095984	Sandbox	8.8.8.8	53
368.168207884	Sandbox	8.8.4.4	53
380.850144863	Sandbox	8.8.8.8	53
381.324838877	Sandbox	8.8.4.4	53

VALKYRIE COMODO

DETAILED FILE INFO

CREATED / DROPPED FILES

FILE PATH	TYPE AND HASHES
C:\Users\User\AppData\Roaming\D5E2DE\E36C7A.Lck	**Type :** very short file (no magic) **MD5 :** c4ca4238a0b923820dcc509a6f75849b **SHA-1 :** 356a192b7913b04c54574d18c28d46e6395428ab **SHA-256 :** 6b86b273ff34fce19d6b804eff5a3f5747ada4eaa2 **SHA-512 :** 4dff4ea340f0a823f15d3f4f01ab62eae0e5da579(**Size :** 0.001 Kilobytes.

STATIC FILE INFO

File Name:	crypt_b.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
SHA1:	74339b2f522ed9b1b47ba4249b9a6234694c1ce4
MD5:	6f0640320d81a92aafb6835b4b8366fc
First Seen Date:	2018-05-08 13:48:47.072345 (about 20 hours ago)
Number Of Clients Seen:	2
Last Analysis Date:	2018-05-08 13:48:47.072345 (about 20 hours ago)
Human Expert Analysis Result:	No human expert analysis verdict given to this sample yet.

VALKYRIE COMODO

DETAILED FILE INFO

ADDITIONAL FILE INFORMATION

PE Headers

PROPERTY	VALUE
Magic Literal Enum	3
File Type Enum	6
Debug Artifacts	[]
Number Of Sections	8
Trid	[]
Compilation Time Stamp	0x297B4218 [Mon Jan 20 21:41:44 1992 UTC] [SUSPICIOUS]
Entry Point	0x465378 (CODE)
Machine Type	Intel 386 or later - 32Bit
File Size	614912
Ssdeep	
Sha256	35a76eaf06b8b734159c02c2446dc9d8669cdefe99533b51b6251ed86d55b9fd
Exifinfo	[]
Mime Type	application/x-dosexec
Imphash	

PE Sections

NAME	VIRTUAL ADDRESS	VIRTUAL SIZE	RAW SIZE	ENTROPY	MD5
CODE	0x1000	0x643c0	0x64400	6.58720480411	b5a7e97fbb8bdc097619507c43ba13be
DATA	0x66000	0x1264	0x1400	3.86340707666	fef08dd4a0f21098221630a78638228e
BSS	0x68000	0xc0d	0x0	0.0	d41d8cd98f00b204e9800998ecf8427e
.idata	0x69000	0x21e0	0x2200	5.03710654782	34fe1493467a2474b12286dfe3f71cdc
.tls	0x6c000	0x10	0x0	0.0	d41d8cd98f00b204e9800998ecf8427e
.rdata	0x6d000	0x18	0x200	0.20058190744	8b32af3e8d3851e5964e7328753a5f50
.reloc	0x6e000	0x7304	0x7400	6.63292347594	987b8244cc23e0715725ab49f8078d62
.rsrc	0x76000	0x26c40	0x26e00	6.90159016577	6a679d140e745776226de9bff0e171f2

PE Resources

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_CURSOR', u'offset': 487480, u'sha256': u'b8e6fc93d423931acbddae3c27dd3c4eb2a394005d746951a971cb700e0ee510', u'type': u'data', u'size': 308}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_CURSOR', u'offset': 487788, u'sha256': u'ce19ace18e87b572e6912306776226af5b8e63959c61cde70a8ff05b3bbdcc41', u'type': u'data', u'size': 308}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_CURSOR', u'offset': 488096, u'sha256': u'ee1c9c194199c320c893b367602ccc7ee7270bd4395d029f727e097634f47f8c', u'type': u'data', u'size': 308}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_CURSOR', u'offset': 488404, u'sha256': u'9d9edf87ca203ecc60b246cc783d54218dd0ce77d3a025d0bafc580995a4abd8', u'type': u'data', u'size': 308}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_CURSOR', u'offset': 488712, u'sha256': u'99676c52310db365580965ea646ece86c62951bfd97ec0aae9f738a202a90593', u'type': u'data', u'size': 308}
{u'lang': u'LANG_NEUTRAL', u'name': u'RT_CURSOR', u'offset': 489020, u'sha256': u'11726dcf1eebe23a1df5eb0ee2af39196b702eddd69083d646e4475335130b28', u'type': u'data', u'size': 308}
{u'lang': u'LANG_NEUTRAL', u'name': u'RT_CURSOR', u'offset': 489328, u'sha256': u'6f938aab0a03120de4ef8b27aff6ba5146226c92a056a6f04e5ec8d513ce5f9d', u'type': u'data', u'size': 308}
{u'lang': u'LANG_NEUTRAL', u'name': u'RT_BITMAP', u'offset': 489636, u'sha256': u'c0ede68a98bd2bc58c78564dfb42f1640dc29766d3ab2782ab8b5ed28c6fd414', u'type': u'data', u'size': 464}
{u'lang': u'LANG_NEUTRAL', u'name': u'RT_BITMAP', u'offset': 490100, u'sha256': u'46cfc44afa8ab31ae3da35fa8346e4c085c441659d9992b09fc8ad517f2b289a', u'type': u'data', u'size': 484}
{u'lang': u'LANG_NEUTRAL', u'name': u'RT_BITMAP', u'offset': 490584, u'sha256': u'c0ede68a98bd2bc58c78564dfb42f1640dc29766d3ab2782ab8b5ed28c6fd414', u'type': u'data', u'size': 464}
{u'lang': u'LANG_NEUTRAL', u'name': u'RT_BITMAP', u'offset': 491048, u'sha256': u'f8e1696801fe89b88936ac4226cea03bfa5aa345aa33ca982822ae7fbc6557e2', u'type': u'data', u'size': 464}
{u'lang': u'LANG_NEUTRAL', u'name': u'RT_BITMAP', u'offset': 491512, u'sha256': u'cb7421b5c6af74c3159c361f3bb78bba8a488d8979d1250e106fa96cbf928789', u'type': u'data', u'size': 464}
{u'lang': u'LANG_NEUTRAL', u'name': u'RT_BITMAP', u'offset': 491976, u'sha256': u'41f05a4df5f42d92b879493d51941de342d36460fe15c0f3b63b2b706b928fef', u'type': u'data', u'size': 464}
{u'lang': u'LANG_NEUTRAL', u'name': u'RT_BITMAP', u'offset': 492440, u'sha256': u'81265e63c89ee5c2e5126452e22f84e9be9452449f3e5959ab6d346cb58b2bde', u'type': u'data', u'size': 464}
{u'lang': u'LANG_NEUTRAL', u'name': u'RT_BITMAP', u'offset': 492904, u'sha256': u'6b97877cdd547e6ba6467f86055f1fc7b06660b034439f0da4c137538ef14a83', u'type': u'data', u'size': 464}
{u'lang': u'LANG_NEUTRAL', u'name': u'RT_BITMAP', u'offset': 493368, u'sha256': u'c925e4a8cbf6d42dbb1220a510614df725558f8d843338982bab8c4e020f6429', u'type': u'data', u'size': 464}
{u'lang': u'LANG_NEUTRAL', u'name': u'RT_BITMAP', u'offset': 493832, u'sha256': u'6b97877cdd547e6ba6467f86055f1fc7b06660b034439f0da4c137538ef14a83', u'type': u'data', u'size': 464}
{u'lang': u'LANG_NEUTRAL', u'name': u'RT_BITMAP', u'offset': 494296, u'sha256': u'78507a772de646626b196a743cee75b298a68c33a0fd482842071519d59037b2', u'type': u'GLS_BINARY_LSB_FIRST', u'size': 232}
{u'lang': u'LANG_NEUTRAL', u'name': u'RT_BITMAP', u'offset': 494528, u'sha256': u'1d66fd6a469d10a5674582dd5b438f5e1a0cf0082e524caa2bfcd29dd3f0ea4e', u'type': u'data', u'size': 152}
{u'lang': u'LANG_NEUTRAL', u'name': u'RT_BITMAP', u'offset': 494680, u'sha256': u'd2829ee569905c1b546c1323f3ff585ecb613f6dbdb5ce10c0dd2cb4b10bfcbb', u'type': u'data', u'size': 152}
{u'lang': u'LANG_ENGLISH', u'name': u'RT_BITMAP', u'offset': 494832, u'sha256': u'75a7dba04ebe559c14d8e0eab66cd6eaa3b3867c66d71425e6f023d2464b2e25', u'type': u'data', u'size': 4809}
{u'lang': u'LANG_ENGLISH', u'name': u'RT_BITMAP', u'offset': 499644, u'sha256': u'20afa97775e114abc3220fea89428ff7bfe740add73fcbdf77632fe99f4383ee', u'type': u'data', u'size': 4809}
{u'lang': u'LANG_ENGLISH', u'name': u'RT_BITMAP', u'offset': 504456, u'sha256': u'bca59913e4b959b1fec863f7d42402e095d6900aca4e7ac88bdd249c015e95ec', u'type': u'data', u'size': 4809}
{u'lang': u'LANG_ENGLISH', u'name': u'RT_BITMAP', u'offset': 509268, u'sha256': u'3e13ea0d425ce152d5e1c14879b77a548edb37691b4861cc2a1a807c225fcfa0', u'type': u'data', u'size': 4809}
{u'lang': u'LANG_ENGLISH', u'name': u'RT_BITMAP', u'offset': 514080, u'sha256': u'23a6b525291d51504bcd4e0a888d87b0663a42250f4809d14069ffbe2dc9284b', u'type': u'data', u'size': 4809}
{u'lang': u'LANG_ENGLISH', u'name': u'RT_BITMAP', u'offset': 518892, u'sha256': u'80027f5b863d5f5d23c835f270df81a568ae8838eb0ad00bd6c059e420c629df', u'type': u'data', u'size': 4809}
{u'lang': u'LANG_ENGLISH', u'name': u'RT_BITMAP', u'offset': 523704, u'sha256': u'7f378ada8c68bfce4ddab43b16ac3ece545f39c846c162762f56e5ebc46143da', u'type': u'data', u'size': 4809}
{u'lang': u'LANG_ENGLISH', u'name': u'RT_BITMAP', u'offset': 528516, u'sha256': u'3a7d8cf9132c4a060e422e7d747c38f36afbcc70dae39e634d0dd5f16ee76520', u'type': u'data', u'size': 4809}
{u'lang': u'LANG_ENGLISH', u'name': u'RT_BITMAP', u'offset': 533328, u'sha256': u'c5ead8aa913ac26deebff65b58f1d3a4cb9ba88f6e5a7661a67447685298641a', u'type': u'data', u'size': 4809}
{u'lang': u'LANG_ENGLISH', u'name': u'RT_BITMAP', u'offset': 538140, u'sha256': u'c97376749e194b85f439f0dbc28928e9d5d9f54ac55ac403b0b6fe8cfeebc001', u'type': u'data', u'size': 4809}
{u'lang': u'LANG_ENGLISH', u'name': u'RT_BITMAP', u'offset': 542952, u'sha256': u'1372cf1215221be4bfe5b2672305e58ba57772ea3412b331fe982ff2bcffaa86', u'type': u'data', u'size': 4809}
{u'lang': u'LANG_ENGLISH', u'name': u'RT_BITMAP', u'offset': 547764, u'sha256': u'f5000e3c37b807cd0ba42d833b48f111e43cdd5c4496d37e6391d6ae1bbf51bb', u'type': u'data', u'size': 4809}
{u'lang': u'LANG_ENGLISH', u'name': u'RT_BITMAP', u'offset': 552576, u'sha256': u'271ef0364703a5029cf2e4d61d3affc379e25ef9ea325ea435ee82465842b30b', u'type': u'data', u'size': 4809}
{u'lang': u'LANG_ENGLISH', u'name': u'RT_BITMAP', u'offset': 557388, u'sha256': u'350c19251b7984e7d3c506755387caf079201d32c1e979efc58ed6f0b853abc6', u'type': u'data', u'size': 4809}
{u'lang': u'LANG_ENGLISH', u'name': u'RT_BITMAP', u'offset': 562200, u'sha256': u'95a43777be5d2fa1a242c18054a130d25ae9706a3a17a7e17c781b36827e9a5e', u'type': u'data', u'size': 4809}
{u'lang': u'LANG_ENGLISH', u'name': u'RT_BITMAP', u'offset': 567012, u'sha256': u'72d859cc1f749ac7dd2cbad359b79063bb43c164f12ca5d679b005d5447e44d5', u'type': u'data', u'size': 4809}
{u'lang': u'LANG_ENGLISH', u'name': u'RT_BITMAP', u'offset': 571824, u'sha256': u'08c31ec2d19d10c7a043ad998aa35a0ad9b46c8bf219c18df2e6e3fef376ba9e', u'type': u'data', u'size': 4809}
{u'lang': u'LANG_ENGLISH', u'name': u'RT_BITMAP', u'offset': 576636, u'sha256': u'1993c42af5a4c1ff497247d87184876381e9794c2f1fd01569fd570c3acec5b6', u'type': u'data', u'size': 4809}
{u'lang': u'LANG_ENGLISH', u'name': u'RT_BITMAP', u'offset': 581448, u'sha256':

u'0bbb12e605147f9b193e50813761f319f95c512894b04388a9939823260e48d0', u'type': u'data', u'size': 4809}

{u'lang': u'LANG_ENGLISH', u'name': u'RT_BITMAP', u'offset': 586260, u'sha256': u'0f8e29cdae2b0def0a8eb9f6255a4d18447a7c42cbc608de9d92495f8b1caa22', u'type': u'data', u'size': 4809}

{u'lang': u'LANG_ENGLISH', u'name': u'RT_BITMAP', u'offset': 591072, u'sha256': u'6d8ed4cf670fca02838facf49c117f99230db67bbbc381b5fc21f2fa45071111', u'type': u'data', u'size': 4809}

{u'lang': u'LANG_ENGLISH', u'name': u'RT_BITMAP', u'offset': 595884, u'sha256': u'83edcf9494f380a3ed3c8c98cd2b91cd04caa801e34ad6b7f2857680fe7e84c2', u'type': u'data', u'size': 4809}

{u'lang': u'LANG_ENGLISH', u'name': u'RT_BITMAP', u'offset': 600696, u'sha256': u'da98df9b19a38a59fe51b82813d9bc55323940a54ab03c64ff7e1517a14dac1d', u'type': u'data', u'size': 4809}

{u'lang': u'LANG_ENGLISH', u'name': u'RT_BITMAP', u'offset': 605508, u'sha256': u'6f281226139932f89fecd05a757905bea1ad7cfa9b7e5c4079dab548730541e4', u'type': u'data', u'size': 4809}

{u'lang': u'LANG_ENGLISH', u'name': u'RT_BITMAP', u'offset': 610320, u'sha256': u'7d7a5ddb17c0c73c7f2de8b6518ca559d07df43aa492b19068b8a0ce024de23c', u'type': u'data', u'size': 4809}

{u'lang': u'LANG_ENGLISH', u'name': u'RT_BITMAP', u'offset': 615132, u'sha256': u'd79aa380dc8b237fcf100e20f971ccd2dbc48ecf2d24c00dcdafc2f30aef6fc3', u'type': u'ASCII text, with very long lines, with no line terminators', u'size': 4809}

{u'lang': u'LANG_ENGLISH', u'name': u'RT_ICON', u'offset': 619944, u'sha256': u'1c8e3f9dc4e869aba339ae5659d9acae941e4832ca8d121c661c87971df26202', u'type': u'data', u'size': 9640}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_DIALOG', u'offset': 629584, u'sha256': u'771f64afb45a9edc8c4f6c5b2039f9b32623cea53bf0cab5bf1f371cc5d1abe4', u'type': u'data', u'size': 82}

{u'lang': u'LANG_ENGLISH', u'name': u'RT_STRING', u'offset': 629668, u'sha256': u'620eebe09cef8e23fc266103271aba62e285b6e24fe18f75d4f178b9fc29a41e', u'type': u'data', u'size': 162}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_STRING', u'offset': 629832, u'sha256': u'2f5ef294c0be01993445cf1704f10e5c02b5777894f8f67d667fe59bee29fe4a', u'type': u'data', u'size': 400}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_STRING', u'offset': 630232, u'sha256': u'696286cc8f56db772be8618da6e3dbe6b70f64a694983c23dda36921a18054da', u'type': u'data', u'size': 492}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_STRING', u'offset': 630724, u'sha256': u'a439ccc4d688076392c4c3eb6dbc602694213c2a5dc318da04c4a63a93a22b2a', u'type': u'Hitachi SH big-endian COFF object, not stripped', u'size': 236}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_STRING', u'offset': 630960, u'sha256': u'4c8f897c5713ac0b26906391e8d5bd26e7e75243cd4f461c1f694ee4692cc1dd', u'type': u'Hitachi SH big-endian COFF object, not stripped', u'size': 804}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_STRING', u'offset': 631764, u'sha256': u'49af5aa2b95c25004d5f8aeacc2b502bca1caa6da00971408d259a1a01aa137a', u'type': u'data', u'size': 188}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_STRING', u'offset': 631952, u'sha256': u'bc20932ea873b6fb92bb8ffac75f417626cf55ff402f74eb5094ca12736f8a22', u'type': u'data', u'size': 320}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_STRING', u'offset': 632272, u'sha256': u'd2223e83f974e00dd26a748b1a9a77213f42b9994524919176a5fc46c007a29c', u'type': u'data', u'size': 644}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_STRING', u'offset': 632916, u'sha256': u'4fae408f74f7ac4548620c2683e788ed38d1d5526f1a0ac3a2880212f9ea0e19', u'type': u'data', u'size': 1116}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_STRING', u'offset': 634032, u'sha256': u'd9a0df5de02dd847b1955ae174120eef9436e7735a7d02947ff87c35060aadf1', u'type': u'data', u'size': 852}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_STRING', u'offset': 634884, u'sha256': u'e3545d8fe699de2fb1537d4fcff27e44889764416796b8bbf2f71fe5dc0b4d99', u'type': u'data', u'size': 1000}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_STRING', u'offset': 635884, u'sha256': u'8087b6f485dbc8b45ceed7b1120d0ca0567e5633c8dfe94041f3cac6e209b8ac', u'type': u'data', u'size': 564}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_STRING', u'offset': 636448, u'sha256': u'26afa355a3a2ddfa48dc66f4b1a36a6427d76fc7c4879a257331e0a1549ea3b9', u'type': u'data', u'size': 236}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_STRING', u'offset': 636684, u'sha256': u'490f9355796a96874ad9d123678a906478fd8ba86c0ceee9482acf059f5c9ddc', u'type': u'data', u'size': 436}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_STRING', u'offset': 637120, u'sha256': u'1842ebf764d5843e9f737302e07352e000131e0d2da2e199030ec644dd96de86', u'type': u'data', u'size': 996}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_STRING', u'offset': 638116, u'sha256': u'7b186924e5438e52e53f29035df7a4f31dd67f35fd1eb5473cba5405048df6e1', u'type': u'data', u'size': 856}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_STRING', u'offset': 638972, u'sha256': u'ce28bb03eda08a374750ce5be8f32f5739cfed85bf3b6d667be80938fd92615b', u'type': u'data', u'size': 692}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_RCDATA', u'offset': 639664, u'sha256': u'88d14cc6638af8a0836f6d868dfab60df92907a2d7becaefbbd7e007acb75610', u'type': u'Sendmail frozen configuration ', u'size': 16}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_RCDATA', u'offset': 639680, u'sha256': u'c5ab24d84e3ad30b37eb7d324c760c12d40a465349e6ed3ca244958be7cafad5', u'type': u'data', u'size': 636}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_RCDATA', u'offset': 640316, u'sha256': u'903f46ea9ce5a1367f286e33d2550a1e9081689e41136ab914dbd359173a9674', u'type': u"Delphi compiled form 'TForm1'", u'size': 1635}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_GROUP_CURSOR', u'offset': 641952, u'sha256': u'c53efa8085835ba129c1909beaff8a67b45f50837707f22dfff0f24d8cd26710', u'type': u'MS Windows cursor resource - 1 icon, 32x256, hotspot @1x1', u'size': 20}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_GROUP_CURSOR', u'offset': 641972, u'sha256': u'b07e022f8ef0a8e5fd3f56986b2e5bf06df07054e9ea9177996b0a6c27d74d7c', u'type': u'MS Windows cursor resource - 1 icon, 32x256, hotspot @1x1', u'size': 20}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_GROUP_CURSOR', u'offset': 641992, u'sha256': u'43f40dd5140804309a4c901ec3c85b54481316e67a6fe18beb9d5c0ce3a42c3a', u'type': u'MS Windows cursor resource - 1 icon, 32x256, hotspot

@1x1', u'size': 20}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_GROUP_CURSOR', u'offset': 642012, u'sha256': u'ff47a48c11c234903a7d625cb8b62101909f735ad84266c98dd4834549452c39', u'type': u'MS Windows cursor resource - 1 icon, 32x256, hotspot @1x1', u'size': 20}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_GROUP_CURSOR', u'offset': 642032, u'sha256': u'a0adcedb82b57089f64e2857f97cefd6cf25f4d27eefc6648bda83fd5fef66bb', u'type': u'MS Windows cursor resource - 1 icon, 32x256, hotspot @1x1', u'size': 20}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_GROUP_CURSOR', u'offset': 642052, u'sha256': u'6e1e7738a1b6373d8829f817915822ef415a1727bb5bb7cfe809e31b3c143ac5', u'type': u'MS Windows cursor resource - 1 icon, 32x256, hotspot @1x1', u'size': 20}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_GROUP_CURSOR', u'offset': 642072, u'sha256': u'326c048595bbc72e3f989cb3b95fbf09dc83739ced3cb13eb6f03336f95d74f1', u'type': u'MS Windows cursor resource - 1 icon, 32x256, hotspot @1x1', u'size': 20}

{u'lang': u'LANG_ENGLISH', u'name': u'RT_GROUP_ICON', u'offset': 642092, u'sha256': u'8ba3a2e4e72ee5f60718eb9ad3f29fa859b38e7b5e52a9b03ebd6547d54019d3', u'type': u'MS Windows icon resource - 1 icon, 48x96', u'size': 20}

CERTIFICATE VALIDATION

- Certificate Validation is not Applicable ?

SCREENSHOTS