VALKYRIE COMODO

Summary

File Name: coolboy_topst.exe

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

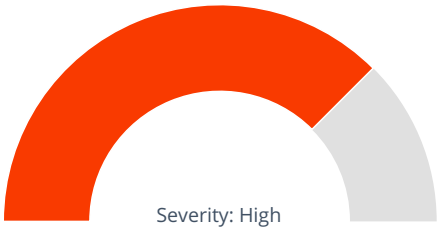
SHA1: 7d159ee6b8c2c214c32d0c1e1cec8bfb2679e7e8

MD5: ea70905af5ddffacb3ad0fd39060e589

MALWARE

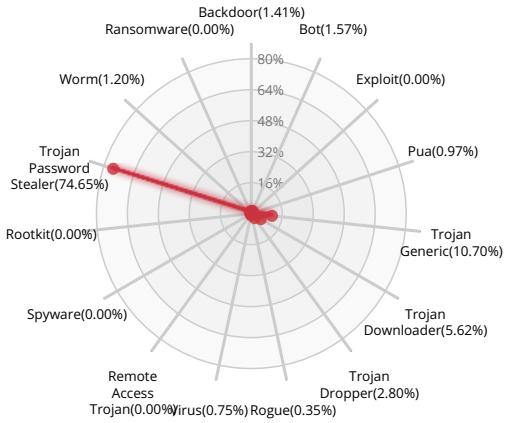
Valkyrie Final Verdict

DETECTION SECTION

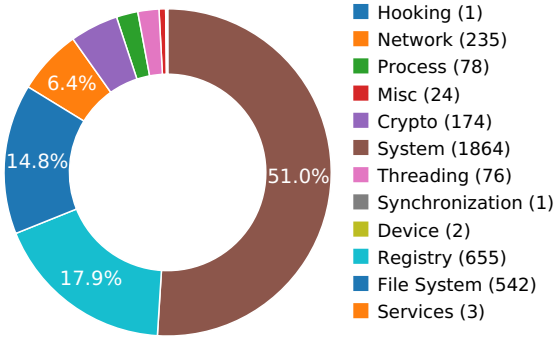


Verdict: Malware

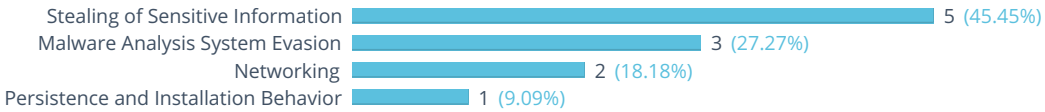
CLASSIFICATION



HIGH LEVEL BEHAVIOR DISTRIBUTION



ACTIVITY OVERVIEW



VALKYRIE COMODO

Activity Details

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

NETWORKING

HTTP traffic contains suspicious features which may be indicative of malware related traffic	Show sources
Performs some HTTP requests	Show sources

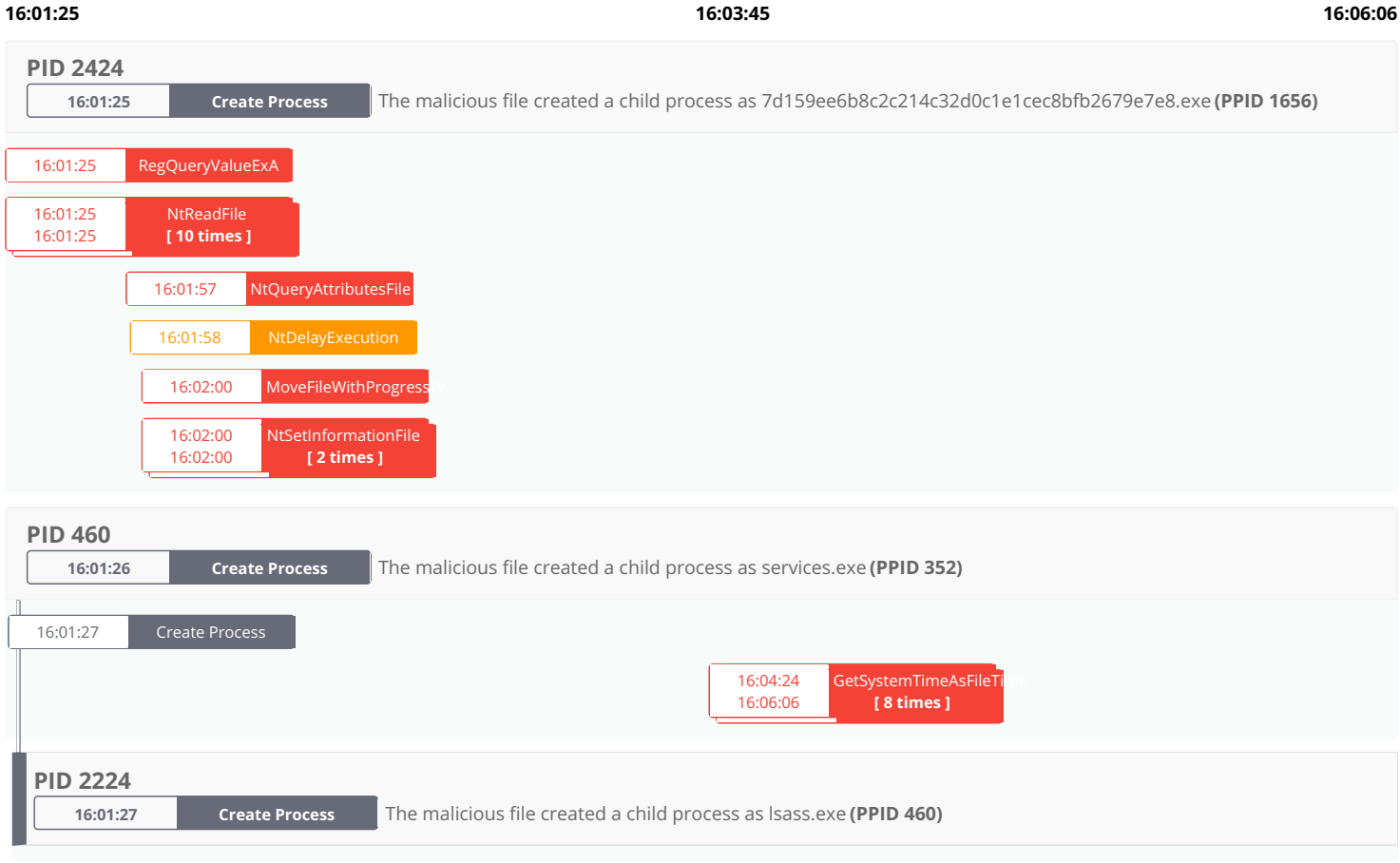
PERSISTENCE AND INSTALLATION BEHAVIOR

Deletes its original binary from disk	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

Behavior Graph



VALKYRIE COMODO

Behavior Summary

ACCESSED FILES

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
C:\Users\user\AppData\Roaming\Mozilla\Firefox\Profiles\jdm2a1on.default\signons2.txt
C:\Users\user\AppData\Roaming\Mozilla\Firefox\Profiles\jdm2a1on.default\signons3.txt
C:\Program Files\NETGATE\Black Hawk
C:\Program Files (x86)\Lunascape\Lunascape6\plugins\{9BDD5314-20A6-4d98-AB30-8325A95771EE}
C:\Users\user\AppData\Local\Comodo\Dragon\User Data\Default\Login Data

READ REGISTRY KEYS

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_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\Windows Error Reporting\WMR\Disable
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
HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\{D9734F19-8CFB-411D-BC59-833E334FCB5E}\Reminders\Email
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\services\LanmanWorkstation\Parameters\RpcCacheTimeout
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\services\DcomLaunch\ObjectName
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\services\RpcEptMapper\ObjectName
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\services\RpcSs\ObjectName
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\services\VaultSvc\ObjectName
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\services\VaultSvc\ImagePath
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\services\VaultSvc\WOW64
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\ProfileList\ProgramData
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\ProfileList\Public
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\ProfileList\Default
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\ProgramFilesDir
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\CommonFilesDir
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\ProgramFilesDir (x86)
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\CommonFilesDir (x86)
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\ProgramW6432Dir
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\CommonW6432Dir
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\ProfileList\S-1-5-18\ProfileImagePath

HKEY_USERS\.DEFAULT\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\User Shell Folders\AppData
HKEY_USERS\.DEFAULT\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\User Shell Folders\Local AppData
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\services\VaultSvc\Environment
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\services\VaultSvc\RequiredPrivileges
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\services\AeLookupSvc\ImagePath

MODIFIED FILES

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

RESOLVED APIS

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
nssdbm3.dll.legacy_ReleaseSecmodDBData
nssdbm3.dll.legacy_DeleteSecmodDB
nssdbm3.dll.legacy_AddSecmodDB
nssdbm3.dll.legacy_Shutdown

nssdbm3.dll.legacy_SetCryptFunctions
freebl3.dll.FREEBL_GetVector
cryptbase.dll.SystemFunction001
cryptbase.dll.SystemFunction002
cryptbase.dll.SystemFunction003
cryptbase.dll.SystemFunction004
cryptbase.dll.SystemFunction005
cryptbase.dll.SystemFunction028
cryptbase.dll.SystemFunction029
cryptbase.dll.SystemFunction034
cryptbase.dll.SystemFunction036
cryptbase.dll.SystemFunction040
cryptbase.dll.SystemFunction041
vaultcli.dll.VaultEnumerateItems
vaultcli.dll.VaultEnumerateVaults
vaultcli.dll.VaultFree
vaultcli.dll.VaultGetItem
vaultcli.dll.VaultOpenVault
vaultcli.dll.VaultCloseVault
rpcrt4.dll.RpcStringBindingComposeW
rpcrt4.dll.RpcBindingFromStringBindingW
rpcrt4.dll.NdrClientCall2
rpcrt4.dll.RpcStringFreeW
rpcrt4.dll.RpcBindingFree
sechost.dll.LookupAccountSidLocalW
netapi32.dll.NetUserGetInfo
cryptsp.dll.CryptImportKey
cryptsp.dll.CryptSetKeyParam
cryptsp.dll.CryptDecrypt
cryptsp.dll.CryptDestroyKey

DELETED FILES

C:\Users\user\AppData\Roaming\D5E2DE\E36C7A.hdb
C:\Users\user\AppData\Roaming\D5E2DE\E36C7A.lck
C:\Users\user\AppData\Local\Temp\7d159ee6b8c2c214c32d0c1e1cec8bfb2679e7e8.exe

REGISTRY KEYS

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\Microsoft\Windows\Windows Error Reporting\WMR
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\Windows Error Reporting\WMR\Disable
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
HKEY_CURRENT_USER\Software\Netscape
HKEY_CURRENT_USER\Software\NTCore
HKEY_CURRENT_USER\Software\ODBC
HKEY_CURRENT_USER\Software\PEiD
HKEY_CURRENT_USER\Software\Policies
HKEY_CURRENT_USER\Software\Sysinternals
HKEY_CURRENT_USER\Software\Telerik
HKEY_CURRENT_USER\Software\VB and VBA Program Settings
HKEY_CURRENT_USER\Software\Wow6432Node
HKEY_CURRENT_USER\Software\Classes
HKEY_CURRENT_USER\Software\Far\Plugins\FTP\Hosts
HKEY_CURRENT_USER\Software\Far2\Plugins\FTP\Hosts
HKEY_CURRENT_USER\Software\Bitvise\BvSshClient
HKEY_CURRENT_USER\Software\VanDyke\SecureFX
HKEY_LOCAL_MACHINE\Software\NCH Software\Fling\Accounts
HKEY_CURRENT_USER\Software\NCH Software\Fling\Accounts
HKEY_LOCAL_MACHINE\Software\NCH Software\ClassicFTP\FTPAccounts
HKEY_CURRENT_USER\Software\NCH Software\ClassicFTP\FTPAccounts
HKEY_CURRENT_USER\Software\9bis.com\KiTTY\Sessions
HKEY_CURRENT_USER\Software\SimonTatham\PuTTY\Sessions
HKEY_LOCAL_MACHINE\Software\SimonTatham\PuTTY\Sessions
HKEY_LOCAL_MACHINE\Software\9bis.com\KiTTY\Sessions
HKEY_LOCAL_MACHINE\SOFTWARE\Mozilla\Mozilla Thunderbird
HKEY_CURRENT_USER\Software\IncrediMail\Identities
HKEY_LOCAL_MACHINE\Software\IncrediMail\Identities
HKEY_CURRENT_USER\Software\Martin Prikryl
HKEY_LOCAL_MACHINE\Software\Martin Prikryl
HKEY_LOCAL_MACHINE\SOFTWARE\Postbox\Postbox

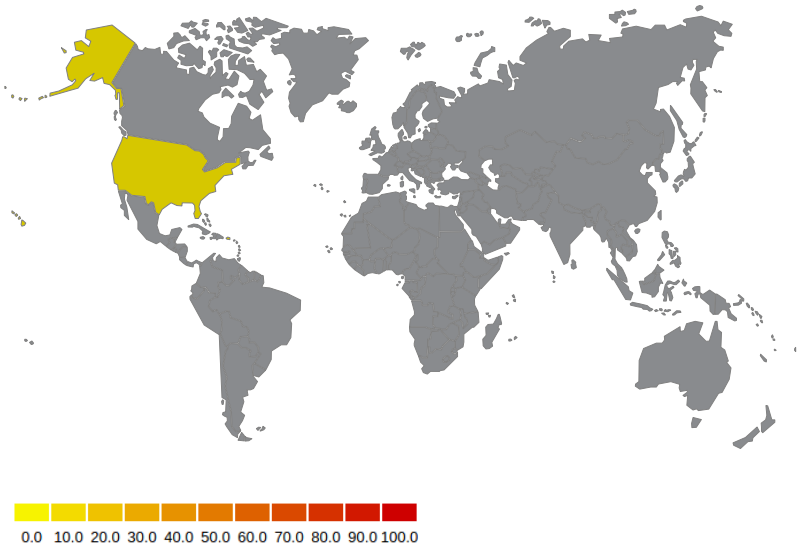
HKEY_LOCAL_MACHINE\SOFTWARE\Mozilla\FossaMail
HKEY_CURRENT_USER\Software\WinChips\UserAccounts
HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook
HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\0a0d020000000000c000000000000046
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
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

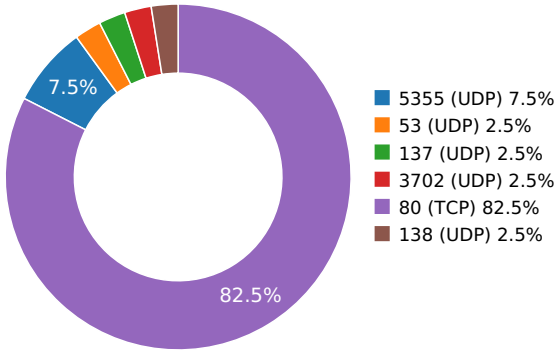
READ FILES

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
topstar-it.com	37.72.171.98	Netherlands	35017		Malware Process

HTTP PACKETS

Host	Port	Method	Version	User Agent	Count	Call Time During Execution(Sec)
topstar-it.com	80	POST	1.0	Mozilla/4.08 (Charon; Inferno)	1	40.068780899
Path: /coolboy/fre.php **URI:** http://topstar-it.com/coolboy/fre.php						
topstar-it.com	80	POST	1.0	Mozilla/4.08 (Charon; Inferno)	1	40.5450270176
Path: /coolboy/fre.php **URI:** http://topstar-it.com/coolboy/fre.php						
topstar-it.com	80	POST	1.0	Mozilla/4.08 (Charon; Inferno)	28	40.8571400642
Path: /coolboy/fre.php **URI:** http://topstar-it.com/coolboy/fre.php						

DNS QUERIES

Request	Type
topstar-it.com	A
Answers - 37.72.171.98 (A)	

VALKYRIE COMODO

TCP PACKETS

Call Time During Execution(sec)	Source IP	Dest IP	Dest Port
40.068780899	Sandbox	37.72.171.98	80
40.5450270176	Sandbox	37.72.171.98	80
40.8571400642	Sandbox	37.72.171.98	80
51.0914120674	Sandbox	37.72.171.98	80
61.3325819969	Sandbox	37.72.171.98	80
71.5493888855	Sandbox	37.72.171.98	80
81.7640318871	Sandbox	37.72.171.98	80
92.0023860931	Sandbox	37.72.171.98	80
102.218780994	Sandbox	37.72.171.98	80
114.109827042	Sandbox	37.72.171.98	80
124.314164877	Sandbox	37.72.171.98	80
134.53154397	Sandbox	37.72.171.98	80
146.15891099	Sandbox	37.72.171.98	80
156.391697884	Sandbox	37.72.171.98	80
166.624887943	Sandbox	37.72.171.98	80
176.859675884	Sandbox	37.72.171.98	80
192.393403053	Sandbox	37.72.171.98	80
202.581721067	Sandbox	37.72.171.98	80
212.770063877	Sandbox	37.72.171.98	80
223.20696187	Sandbox	37.72.171.98	80
233.397875071	Sandbox	37.72.171.98	80
243.58477807	Sandbox	37.72.171.98	80
253.789629936	Sandbox	37.72.171.98	80
263.993164062	Sandbox	37.72.171.98	80
274.196209908	Sandbox	37.72.171.98	80
284.397345066	Sandbox	37.72.171.98	80
294.604971886	Sandbox	37.72.171.98	80
304.812082052	Sandbox	37.72.171.98	80
315.009656906	Sandbox	37.72.171.98	80
325.209466934	Sandbox	37.72.171.98	80

UDP PACKETS

Call Time During Execution(sec)	Source IP	Dest IP	Dest Port
3.07768893242	Sandbox	224.0.0.252	5355
3.10544705391	Sandbox	224.0.0.252	5355
3.10619688034	Sandbox	239.255.255.250	3702
3.14642596245	Sandbox	192.168.56.255	137
5.6633579731	Sandbox	224.0.0.252	5355
9.1455988884	Sandbox	192.168.56.255	138
39.739661932	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.Hdb	**Type :** Non-ISO extended-ASCII text, with no line terminators **MD5 :** 2dbe489818384a5d5bd0ab2d67e9802c **SHA-1 :** 86a63fc1aaeeedb9bfec837c396a005d6e6cdfa9 **SHA-256 :** 2be993ceb49bd489a40eb761574b5861330ce17 **SHA-512 :** b98c9af0b6f4fdc18c5f0eb4991639cc4ed2e5a44 **Size :** 0.004 Kilobytes.
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.

MATCH YARA RULES

MATCH RULES

STATIC FILE INFO

File Name:	coolboy_topst.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
SHA1:	7d159ee6b8c2c214c32d0c1e1cec8bfb2679e7e8
MD5:	ea70905af5ddffacb3ad0fd39060e589
First Seen Date:	2018-05-22 11:09:35.097293 (9 months ago)
Number Of Clients Seen:	6
Last Analysis Date:	2018-05-22 11:09:35.097293 (9 months 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	4
Trid	[]
Compilation Time Stamp	0x576C0885 [Thu Jun 23 16:04:21 2016 UTC]
Entry Point	0x4139de (.text)
Machine Type	Intel 386 or later - 32Bit
File Size	106496
Ssdeep	
Sha256	5597c6844b64ca2c64b0da111842bb49ac361837e5ffe45d07a37d7f6df589f1
Exifinfo	[]
Mime Type	application/x-dosexec
Imphash	

PE Sections

NAME	VIRTUAL ADDRESS	VIRTUAL SIZE	RAW SIZE	ENTROPY	MD5
.text	0x1000	0x136f5	0x13800	6.49204829439	94fa411af1cc6bb168a3ea0e66e80f78
.rdata	0x15000	0x4060	0x4200	4.25599948305	15686b489e8ad18c33f8b12a6e57b4ee
.data	0x1a000	0x85e24	0x200	0.321716074313	955b3a57edf41d6c47c7225e8d847f91
.x	0xa0000	0x2000	0x2000	0.198125552412	d41ca8bec3ea08c65834c8d115dd089a

CERTIFICATE VALIDATION

- Certificate Validation is not Applicable ?

SCREENSHOTS